

C-Series and FTOS Release Notes

FTOS Version 7.8.1.0

December 4, 2008



Table of Contents

Table of Contents	2
How To Use This Document	3
New Hardware Features	3
Supported Hardware	3
Default CLI Syntax or Behavior Changes	5
FTOS 7.8.1.0 Software Features	5
C-Series Software Upgrade Procedures	8
Software Upgrade Command Changes	8
Software Upgrade for a Single RPM on a C-Series	9
Software Upgrade for Dual RPM on a C-Series	10
Documentation Errata	11
Caveats	11
Caveat Definitions	12
Resolved C-Series Hardware Caveats	12
Open C-Series Hardware Caveats	12
Rejected C-Series Software Caveats	12
Resolved C-Series Software Caveats	13
Open C- Series Software Caveats	20
Technical Support	45
Accessing iSupport Services	45
Contacting the Technical Assistance Center	46
Requesting a Hardware Replacement	46
MIBS	47

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 7.8.1.0 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.

New Hardware Features

The new C-Series components available with FTOS version 7.8.1.0 are:

- **Enhanced Fan Tray:** The enhanced fan tray for the C-Series switch/router provides more efficient cooling and automatically adjusts the fan speed based on the system temperature, which may also reduce fan noise. Catalog numbers CC-C150-FAN2 for the C150 chassis and CC-C300-FAN2 for the C300 chassis are now supported in FTOS 7.8.1.0.

Supported Hardware

Hardware	Catalog Number	Minimum Software Version Required
C150 Chassis	CH-C150	7.6.1.0
Route Processor Module	LC-CB-RPM	2.2.1.1
AC Power Supply 1200W	CC-C1200W-AC	2.2.1.1
DC Power Entry Module	CC-C-PWR-DC	7.7.1.0
C300 Chassis	CH-C300	2.2.1.1
Route Processor Module	LC-CB-RPM	2.2.1.1
AC Power Supply 1200W	CC-C1200W-AC	2.2.1.1
DC Power Entry Module	CC-C-PWR-DC	7.7.1.0

* Applies on newer version RPMs.

** Do not mix AC and DC power supplies.

Supported Hardware

Line Cards	Catalog Number	Card Type Indicator	C150 Minimum Software Version Required	C300 Minimum Software Version Required
C150 and C300 Line Cards (all cards are series CB)				
4 port 10Gigabit Ethernet, XFP optics required	LC-CB-10GE-4P	EX4PB	7.6.1.0	2.2.1.1
8 port 10Gigabit Ethernet, XFP optics required	LC-CB-10GE-8P	EX8PB	7.6.1.0	7.6.1.0
FlexMedia (PoE version): 36-port 10/100/1000 Base-T RJ45 interface, inline power (PoE) ; 8-port 1Gigabit Ethernet; SFP optics required; 2-port 10Gigabit Ethernet, SFP+ optics required	LC-CB-10G-1G-36V	E36VB	7.7.1.0	7.7.1.0
FlexMedia (non-PoE): 36-port 10/100/1000 Base-T RJ45 interface (non-PoE); 8-port 1Gigabit Ethernet, SFP optics required; 2-port 10Gigabit Ethernet, SFP+ optics required	LC-CB-10G-1G-36T	E36TB	7.7.1.0	7.7.1.0
48 port 1Gigabit Ethernet, SFP optics required	LC-CB-GE-48P	E48PB	7.6.1.0	7.6.1.0
48 port 10/100/1000Base-T RJ45 interface	LC-CB-GE-48T	E48TB	7.6.1.0	2.2.1.1
48 port 10/100/1000Base-T RJ45 interface, inline power (PoE)	LC-CB-GE-48V	E48VB	7.6.1.0	2.2.1.1

Default CLI Syntax or Behavior Changes

CAM

CAM ACL configuration — A C-Series line card could go to card-problem state if inserted in a chassis that is configured with a different CAM profile. The line card can be recovered by configuring it to have the same CAM ACL profile as that of the chassis and then resetting it. Use the **cam acl linecard** command in EXEC privilege mode to configure the line card CAM ACL profile.

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

Before FTOS 7.8.1.0, the timeout was 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 major new software features introduced in FTOS version 7.8.1.0 for the C-Series are summarized here:

Table 3: New Features in FTOS 7.8.1.0 for the C-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.
BGP for IPv6: The FTOS IPv6 feature set is extended to the C-Series with support for BGP multiprotocol extensions for IPv6 routing, as defined in RFC 2545.
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 Fan Tray: The enhanced fan tray for the C-Series switch/router provides more efficient cooling and automatically adjusts the fan speed based on the system temperature, which also reduces fan noise. Catalog numbers CC-C150-FAN2 for the C150 chassis and CC-C300-FAN2 for the C300 chassis are now supported in FTOS 7.8.1.0.
Ethernet Flow Control: IEEE 802.3x pause frames are a control frame type 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.

Table 3: New Features in FTOS 7.8.1.0 for the C-Series (continued)

<p>FTSA/Call Home Proactive Monitoring Tests: The Force10 Service Agent (FTSA), part of the FTOS serviceability feature set, manages the automated "call home" monitoring and reporting system. FTOS 7.8.1.0 introduces a suite of proactive tests that can be customized to monitor and report abnormal software, hardware and network conditions. FTOS release 7.8.1.0 introduces new options to the policy-test-list and policy-action-list commands for refining your Call Home policies.</p>
<p>IGMPv2 to PIM-SSM Mapping for Transition to IGMPv3: The FTOS multicast feature set on the C-Series switch/router is extended to support IGMPv2 to PIM-SSM mappings, as a solution for transitioning to IGMPv3 and PIM-SSM while maintaining compatibility for IGMPv2. It is required if the receivers only support IGMPv2.</p>
<p>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.</p>
<p>IPv6 Routing: The FTOS IPv6 routing feature set is extended to the C-Series switch/routers with IPv6 addressing, static routing, ACLs, and management features.</p>
<p>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.</p>
<p>MAC Learning Limit Violation Logging and Shutdown Options: The FTOS MAC Learning Limit feature introduced in version 7.7.1.0 on the C-Series is enhanced with support for logging and/or shutting down the interface when a violation is detected. This feature was also introduced in FTOS 7.7.1.1.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>OSPFv3 Optimizations: The FTOS OSPFv3 implementation is optimized for higher scalability and lower convergence.</p>
<p>OSPFv3: OSPFv3, as defined in RFC 2740, is now supported on the C-Series switch/router as part of the IPv6 routing feature set.</p>
<p>PIM-SM Support on Port-channel Interfaces: FTOS 7.7.1.0 introduced PIM-SM on the C-Series for physical and VLAN interfaces. FTOS 7.8.1.0 adds support for PIM-SM for port-channel interfaces.</p>
<p>PIM-SSM Custom Filtering Ranges: The IP multicast feature set is extended to support the ip pim ssm-range command, which enables you to change the SSM range using an ACL. This feature was also introduced in FTOS 7.7.1.1.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>

Table 3: New Features in FTOS 7.8.1.0 for the C-Series (continued)

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.
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 (source address validation) 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.
sFlow SNMP Set Configuration: The FTOS implementation of the sFlow MIB is enhanced to support sFlow configuration via SNMP sets.
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.
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-configuration file to the "running-config".
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.
User-configurable CAM Allocations: Content Addressable Memory (CAM) stores lookup information in hardware to provide line-rate packet lookups and forwarding. Specifically, it consists of several subregions where entries for Layer 2, IPv4/IPv6, QoS, and ACLs are stored. This feature enables you to optimize CAM usage by allocating CAM space based on specific network requirements.
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.

C-Series Software Upgrade Procedures

C-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.



Warning: When upgrading from an FTOS version prior to 7.5.1.0, you must *first* upgrade the RPM bootcode to version 2.4.1.1.

- [Software Upgrade for a Single RPM on a C-Series](#) — upgrade procedure for C-Series systems with only one RPM (Route Processor Module)
- [Software Upgrade for Dual RPM on a C-Series on page 10](#) — upgrade procedure for C-Series systems with two RPMs



Note: For clarity, these procedures assume RPM 0 is the primary RPM and RPM 1 is the secondary RPM.

Software Upgrade Command Changes

Field Upgradeable FPGA changes — FTOS 7.7.1.0 and later upgrades have been enhanced to support downloads to the FPGA. The following new commands were introduced in FTOS 7.7.1.0:

- The **upgrade** command has been enhanced to include new download options:

```
Force10# upgrade {bootflash-image | bootselector-image | fpga-image | system-image} {all | linecard {slot#} | rpm {slot#} | sfm {slot#}} [all-fpga | link-fpga | system-fpga] [file-url | booted]
```

Enter one of the following for the *file-url* variable:

 - flash:** System image file URL ([flash://]filename)
 - ftp:** System image file URL (ftp://userid:password@hostip/filepath)
 - slot0:** System image file URL ([slot0://]filename)
 - tftp:** System image file URL (tftp://hostip/filepath)

The **booted** keyword denotes the image booted.
- The **restore** command was simplified:

```
Force10# restore fpga [rpm | linecard] number
```
- The following upgrade commands have been deprecated with the introduction of the commands above.
 - **download alt-boot-image flash://<new_image>**
 - **upgrade alt-** commands such as

```
Force10# upgrade alt-bootflash-image rpm
```

```
Force10# upgrade alt-system-image
```


```
Force10# upgrade alt-bootselector-image
```

```
Force10# upgrade alt-bootflash-image
```

Software Upgrade for a Single RPM on a C-Series

To copy a new FTOS image and change boot parameters in a chassis with only one RPM, follow the procedure below. The FTOS image is labeled FTOS-CB-w.x.y.z.bin (where w, x, y, and z are replaced by the current release numbers), for example FTOS-CB-7.8.1.0.bin.

To copy a new FTOS image and change boot parameters in a chassis with only one RPM, follow the procedure below. The FTOS image is labeled FTOS-EF-w.x.y.z.bin (where w, x, y, and z are replaced by the current release numbers), for example FTOS-EF-7.8.1.0.bin. The Software Upgrade Procedure is modified to include the upgrade of partition A and B of the RPM bootcode.

Step	Command Syntax	Command Mode	Purpose
1.	show rpm	EXEC Privilege	View the current RPM status.
2.	copy file-url flash://filepath boot-image Where <i>file-url</i> is the location of the source file. For example: ftp://userid:password@hostlocation/filepath tftp://hostlocation/filepath scp://userid:password@location/filepath	EXEC Privilege	Copy the FTOS image onto the RPM (internal flash) and update the boot variables with the new image.
3.	write memory	EXEC Privilege	Commit the changes made to the bootvar configuration to the startup-configuration file.
4.	show bootvar	EXEC Privilege	View configuration of system images and their configuration. This command only displays information found on the NVRAM.
5.	reload	EXEC Privilege	Reboot the system.
 After you complete Step 4, upgrade the FPGA as described in the section “Upgrading FPGAs on the C-Series” in the “Upgrade Procedures” chapter of the FTOS Configuration Guide. Version 5.0 of the RPM FPGA fixes a critical issue which can manifest as a boot failure or as both RPMs appearing as the master.			

If you enter the filename incorrectly...

If you enter an incorrect file name or location, FTOS will continue to try to locate the boot image. To change or correct the boot image file name or location while the system is booting, enter the BOOT_USER mode and change the boot file name or location.

Step	Command Syntax	Command Mode	Purpose
1.	CTRL+^ or CTRL+~		Enter the break control sequence to enter the BOOT_USER mode.
2.	show bootvar	BOOT_USER	View the saved boot configuration. Double check that the files listed are valid.

Step	Command Syntax	Command Mode	Purpose
3.	boot change {primary secondary default} Enter one of the following parameters: The primary boot parameters is used in the first attempt to boot the system. The secondary boot parameters is used if the primary file is not available. The default boot parameters is used if the secondary boot file is not available.	BOOT_USER	After you enter the keywords, you are prompted for a response. Enter a new file name or press ENTER to accept the current parameter. Enter . (period) to clear a field. Enter - (dash) to edit a field above the current cursor position. Note: If you enter a new file name that extends beyond 80 characters, do not use the BACKSPACE key to correct typos. If you make a mistake, you must re-enter the file name.
4.	reload	BOOT_USER	Reload the software and boot the system.


Software Upgrade for Dual RPM on a C-Series

To copy a new FTOS image and change boot parameters in a chassis with both a Primary RPM and Secondary RPM, follow the procedure below. The FTOS image is labeled FTOS-CB-w.x.y.z.bin (where w, x, y, and z are replaced by the current release numbers), for example FTOS-CB-7.8.1.0.bin.



Warning: Both RPMs must contain the same software version.

Step	Command Syntax	Command Mode	Purpose
1.	show rpm	EXEC Privilege	View the current RPM status.
2.	copy file-url flash://filepath boot-image synchronize-rpm Where <i>file-url</i> is the location of the source file. For example: ftp://userid:password@hostlocation/filepath tftp://hostlocation/filepath scp://userid:password@location/filepath	EXEC Privilege	Copy the FTOS image onto both RPMs (internal flash), update the boot variable with the new image by including the keyword boot-image , and copy the image to secondary RPM and change the boot variable by including the keyword synchronize-rpm .
3.	write memory	EXEC Privilege	Commit the changes made to the bootvar configuration to the startup-configuration file.
4.	show bootvar	EXEC Privilege	Verify that the boot variable is set for the image you specified in Step 1.
5.	reload	EXEC Privilege	Reboot the system; both RPMs will have the new image loaded.

Step	Command Syntax	Command Mode	Purpose
	After you complete Step 4, upgrade the FPGA as described in the section “Upgrading FPGAs on the C-Series” in the “Upgrade Procedures” chapter of the FTOS Configuration Guide. Version 5.0 of the RPM FPGA fixes a critical issue which can manifest as a boot failure or as both RPMs appearing as the master.		



Note: For clarity, these procedures assume RPM 0 is the primary RPM and RPM 1 is the secondary RPM.

Documentation Errata

The following updates are corrections or additions to the documentation:

- **Jumbo Frames** — C-Series are, by default, capable of handling jumbo frames, so references in Force10 user documentation to a non-jumbo mode do not pertain to C-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 12](#)
- [Resolved C-Series Hardware Caveats on page 12](#)
- [Open C-Series Hardware Caveats on page 12](#)
- [Rejected C-Series Software Caveats on page 12](#)
- [Resolved C-Series Software Caveats on page 13](#)
- [Open C-Series Software Caveats on page 20](#)



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 C-Series Hardware Caveats

None

Open C-Series Hardware Caveats

None

Rejected C-Series Software Caveats

Caveats that appear in this section were reported in FTOS 7.8.1.0 as open, but have since been rejected. Rejected caveats are those that are found to be invalid, not reproducible, or not scheduled for resolution.

None

Resolved C-Series Software Caveats

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

BGP (Resolved)

PR# 80652

Severity: S3

Synopsis: Updates containing Martian prefix should be processed after ignoring these prefixes

Release Notes: When an update with Martian prefixes is received, the update should not be dropped. The rest of the prefixes in the update should be processed.

Workaround: None.

Control Plane (Resolved)

PR# 78067

Severity: S2

Synopsis: Receiving a large, consistent number of packets with TTL set to 0/1 may lead to high CPU utilization.

Release Notes: Receiving a large, consistent number of packets with TTL set to 0/1 may lead to high CPU utilization. Use the "show cpu-traffic-stats" command to determine the source interface and type of received traffic leading to the CPU utilization.

Workaround: Increase the TTL value.

FIB (Resolved)

PR# 74605

Severity: S3

Resolved C-Series Software Caveats

Synopsis: The "hash-algorithm" command will no longer take effect after a line card reset.

Release Notes: The "hash-algorithm" command will no longer take effect after a line card reset.

Workaround: Remove and re-configure the command after a reset.

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.

Multicast (Resolved)

PR# 78241

Severity: S2

Synopsis: In IGMP snooping configuration, data forwarding may not work if data is to be switched across line cards and a port-channel interface is the only OIF.

Release Notes: In an IGMP snooping configuration, data forwarding may not work if data is to be switched across line cards and a port-channel interface is the only outgoing interface.

Workaround: Add another port from the same line card, which has the port-channel members, to the outgoing interface list if possible.

PR# 78458

Severity: S1

Synopsis: Egress forwarding index exhaustion will result in an RPM reload.

Release Notes: Stale egress forwarding indexes are not cleared in some scenarios, resulting in exhaustion of these indexes and a subsequent RPM reload.

Workaround: None.

PR# 79449

Severity: S2

Synopsis: Without multicast/IGMP enabled, packets to multicast addresses are flooded.

Release Notes: Without multicast/IGMP enabled, packets to multicast addresses with time-to-live (TTL) of 1 or 2 are sent to the linecard processor and flooded back to all members of the VLAN. This may result in loop-like symptoms if there are two or more C-Series systems with Layer 3 VLANs trunked together.

Workaround: Enable IGMP snooping globally so the packets will be consumed, instead of flooding them back to all VLAN members.

OS / OS Infrastructure (Resolved)

PR# 77288

Severity: S1

Synopsis: A software exception on CP processor may be seen when simultaneous traceroutes on console and Telnet sessions are done with unreachable domain server.

Release Notes: A software exception on the RPM's CP processor may be seen when simultaneous traceroutes on console and Telnet sessions are done with an unreachable domain server.

Workaround: None.

PR# 77735

Severity: S2

Synopsis: The "show interfaces tengigabitethernet {slot}" command will be rejected with "% Error: Slot type mis-match" message for FlexMedia line card.

Release Notes: The "show interfaces tengigabitethernet {slot}" command will be rejected with "% Error: Slot type mis-match" message for FlexMedia line card.

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

PR# 78059

Severity: S3

Synopsis: CtrlC will not work if it is not the first character pressed in all scenarios that support CtrlC.

Release Notes: CtrlC will not work for the ping and traceroute commands if it is not the first character pressed.

Workaround: Do not press any other character except CtrlC.

PR# 78279

Severity: S2

Resolved C-Series Software Caveats

Synopsis: Startup config will not be applied on a newly transioned RPM when doing a warm failover from 7.6.1.0 to 7.7.1.0. or 7.6.1.0 to 7.6.1.2 or 7.7.1.1

Release Notes: Startup config will not be applied on a newly transioned RPM when doing a warm failover from 7.6.1.0 to 7.7.1.0. or from 7.6.1.0 to 7.6.1.2 or from 7.7.1.0 to 7.7.1.1

Workaround: Manually apply the startup-config on the new primary RPM using the "copy startup-config running-config" command after the warm failover completes.

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# 79375

Severity: S2

Synopsis: Unconfiguring the "flowcontrol" command does not revert the threshold values back to the default.

Release Notes: Unconfiguring the "flowcontrol" command does not revert the threshold values back to the default.

Workaround: Use the "flowcontrol" command to specifically configure the default values.

PR# 79443

Severity: S2

Synopsis: The flow control threshold settings specified in a startup-config file will not actually be applied.

Release Notes: The flow control threshold settings specified in a startup-config file will not actually be programmed in hardware upon bootup. Instead, default initialization values will be programmed.

Workaround: Reconfigure the threshold settings using the "flowcontrol" command.

PR# 79447

Severity: S2

Synopsis: Flow control threshold values in hardware will be reset to max values after a line card is reset.

Release Notes: Flow control threshold values in hardware will be reset to max values after a line card is reset.

Workaround: Unconfigure and then re-configure the "flowcontrol" with threshold settings commands.

PR# 79448

Severity: S2

Synopsis: Removing flow-control configuration with threshold options may not work after a linecard reset

Release Notes: Unconfiguring flow-control with threshold options may not work after a linecard reset. Executing the "no flowcontrol rx on tx on" command will fail, and an error message of "% Error: Configured values do not match." will be printed.

Workaround: Use the "flowcontrol rx <> tx <>" command without any threshold options.

PR# 79460

Severity: S3

Synopsis: The uptime displayed in the output of the "show rpm" command remains stuck at "0 sec" after an reload.

Release Notes: The uptime displayed in the output of the "show rpm" command remains stuck at "0 sec" after an reload.

Workaround: None.

PR# 79509

Severity: S2

Synopsis: Flowcontrol configuration with default threshold values may not get applied if the ports are flowcontrol enabled with non-default threshold values.

Release Notes: If the "flowcontrol" with default threshold values command is applied to ports which already have been configured with non-default values, the threshold values may not get set to default threshold values.

Workaround: Unconfigure the "flowcontrol" command to remove the non-default values and then re-configure it with default threshold values.

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.

OSPF (Resolved)

PR# 75968

Severity: S2
Synopsis: Bad LSA request bounces the adjacencies from FULL state when ospf process is cleared or restarted.
Release Notes: Bad LSA request bounces the adjacencies from FULL state when ospf process is cleared or restarted.
Workaround: shut/no shut the port.

PIM (Resolved)

PR# 78189

Severity: S2
Synopsis: PIM-SM and IGMP are not supported on LAG interfaces in FTOS 7.7.1
Release Notes: PIM-SM and IGMP are not supported on LAG interfaces in this release.
Workaround: None.

PR# 78577

Severity: S1
Synopsis: Under certain conditions, the FTOS PIM task will leak memory, leading to a task crash.
Release Notes: Under certain conditions, the FTOS PIM task will leak memory, leading to a task crash.
Workaround: None.

QoS (Resolved)

PR# 72353

Severity: S2
Synopsis: Ingress port-based rate policing with the "rate police" command might not work on an interface configuration mode of a layer 3 port.
Release Notes: Inbound port-based rate policing configured with the "rate police" command in interface configuration mode will not take effect on a Layer 3 port.
Workaround: Use policy-based QoS.

PR# 75009

Severity: S3

Synopsis: The "dot1p-priority" command in interface configuration mode is not supported with configuration rollback.

Release Notes: The "dot1p-priority" command in interface configuration mode is not supported with configuration rollback. If the command is added after an archive file is written and a "config replace" command is executed to roll back to the archived file, the "dot1p-priority" command will continue to be in the running configuration.

Workaround: None. Remove the command manually.

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.

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.

SSH (Resolved)

PR# 70989

Severity: S3

Synopsis: Banner MOTD message is not displayed for users logging in via SSH.

Release Notes: Banner MOTD message is not displayed for users logging in via SSH. This issue is not seen for Telnet users.

Workaround: None.

TACACS (Resolved)

PR# 71838

Severity: S3

Synopsis: TACACS authentication will fail when an invalid host is configured before a valid host.

Release Notes: TACACS authentication will fail when an invalid host is configured before a valid host.

Workaround: Ensure that only valid host information is entered with the "tacacs-server host" command.

Open C- Series Software Caveats

ARP (Open)

PR# 78115

Severity: S2

Synopsis: ARP may not be resolved for a VLAN interface when a member interface previously was part of a port-channel interface.

Release Notes: ARP may not be resolved for a VLAN interface when a member interface previously was part of a port-channel interface.

Workaround: None.

BFD (Open)

PR# 80357

Severity: S2

Synopsis: In rare cases, BFD cannot be enabled on the system if multicast routing is enabled.

Release Notes: In rare case, BFD cannot be enabled on the system if multicast routing also is enabled.

Workaround: None.

CLI (Open)

PR# 63119

Severity: S3

Synopsis: The "show command-history" command will not display the portion of the executed CLI after the "| grep" option.

Release Notes: The "show command-history" command will not display the portion of the executed CLI after the "| grep" option. EG : Force10#show version | grep Version Force10 Operating System Version: 1.0 Force10 Application Software Version: 7.4.1.0 [7/12 6:22:23]:
CMD-(TEL46):[show version]by admin from vty0 (10.16.127.51) [7/12 6:23:11]:
CMD-(TEL46):[show command-history]by admin from vty0 (10.16.127.51)

Workaround: None.

PR# 70730

Severity: S3

Synopsis: After bootup, primary config might fail to load if the file is at remote location.

Release Notes: If the boot config is set to remote host using "boot network URL" or "boot host URL" command, such as "boot host primary ftp://...", the configuration may fail to load and instead report %RPM0-P:CP %CFG-5-NETWORK_CONFIG: Failed to load primary boot network config file.

Workaround: Apply the configuration manually using the "copy" command. Example: "copy ftp://myname:passwd123@hostname1//myconfig.cfg running-config".

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.

Control Plane (Open)

PR# 80929

Severity: S2

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

Open C- Series Software Caveats

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# 80861

Severity:	S1
Synopsis:	Software exception may happen when system receives continuous DHCP request packets from many clients with DHCP snooping enabled.
Release Notes:	A software exception may happen when the system receives continuous DHCP request packets from a significant number of hosts (more than 2000) with DHCP snooping enabled.
Workaround:	None.

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.

Diagnostic (Open)

PR# 78127

Severity:	S2
Synopsis:	An incorrect "Number of Diagnostics performed" value will be displayed on completion of offline diagnostics

Release Notes:	The "Number of Diagnostics performed" value displayed after the execution of offline diagnostics might be incorrect. This is a cosmetic error and does not affect the diagnostics.
Workaround:	None. Use the output of the "show diagnostic linecard {slot#}" to confirm that all of the tests were run.

FIB (Open)

PR# 64376

Severity:	S3
Synopsis:	The "show ip fib linecard" may display incorrect next-hop information for ECMP recursive next-hop when the ARP becomes unresolved for the next-hop.
Release Notes:	The "show ip fib linecard" command may display incorrect next-hop information for ECMP recursive next-hop when the ARP becomes unresolved for the next-hop.
Workaround:	None. This is a display issue only. Functionality is not affected.

PR# 71819

Severity:	S2
Synopsis:	Up to 14 ECMP paths are supported on the C-Series.
Release Notes:	Up to 14 ECMP paths are supported on the C-Series. An error message similar to "%FIB6-2-FIB6_HW_WRITE_ERROR:" may appear when routes with 16 ECMP are present in the FIB table.
Workaround:	None.

PR# 72808

Severity:	S1
Synopsis:	With large number of routes/ARPs in CAM, executing "show ip fib linecard {#}" simultaneously on console and Telnet session may lead to system reset.
Release Notes:	With large number of routes/ARPs in CAM, executing "show ip fib linecard {#}" simultaneously on console and Telnet session may lead to system reset.
Workaround:	Do not execute the "show ip fib linecard {slot#}" command simultaneously from console and Telnet sessions when a large number of ARPs or routes are learned and written to CAM.

PR# 73273

Severity:	S2
Synopsis:	The "show ip fib" command may return an error and CPU utilization on linecard may be high when routes are withdrawn/learning.
Release Notes:	The "show ip fib" command may return an error and CPU utilization on a line card may be high when routes are being withdrawn or learning.
Workaround:	Re-issue the "show ip fib" command after the routes have been learned or withdrawn.

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# 79531

Severity: S3

Synopsis: "Fib6_PF_TreeAdd error" messages may be printed to the console upon an RPM failover

Release Notes: "Fib6_PF_TreeAdd error" messages may be printed to the console upon an RPM failover on a system with a few thousand prefixes in the FIB. This error is seen when the entry that gets added into the database is already present.

Workaround: Ignore these messages, which do not impact functionality.

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.

FTP (Open)

PR# 63388

Severity: S3

Synopsis: If access to a system is made via FTP, all directories in flash will be accessible even though "ftp topdir" is not configured.

Release Notes: If access to a system is made via FTP, all directories in flash will be accessible even though "ftp topdir" is not configured.

Workaround: None.

PR# 65311

Severity: S3

Synopsis: "ip ftp source-interface" functionality is not correct when a loopback interface is configured as source interface.

Release Notes: If interface specified in "ip ftp source-interface" is a loopback interface and if it is shut down the system continues to use the loopback interface as the source interface rather than the system's management IP.

Workaround: None.

IPv4 (Open)

PR# 71121

Severity: S3

Synopsis: During an RPM failover, a syslog message similar to ""%VXW-1-INT_ERR: rtinit: wrong ifa" may be reported for a particular line card.

Release Notes: During an RPM failover, a syslog message similar to ""%VXW-1-INT_ERR: rtinit: wrong ifa (eb16d38) was (eb15bb0)" may be reported for a particular line card.

Workaround: None. The system should initialize successfully.

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# 80343

Severity: S2

Synopsis: In C Series, "show IPv6 FIB linecard summary" output shows incorrect CAM count for IPv6 prefixes.

Open C- Series Software Caveats

Release Notes: In C Series, "show IPv6 FIB linecard summary" output shows incorrect CAM count for IPv6 prefixes.

Workaround: Use "sh ipv6 route summary" 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.

PR# 81182

Severity: S2

Synopsis: ipv6 address-family BGP commands are not getting applied via config-rollback.

Release Notes: IPV6 address-family BGP commands may to be applied to running-config via config-rollback.

Workaround: None.

LACP (Open)

PR# 69442

Severity: S3

Synopsis: Changing speed on LAG member while interface is shutdown and then adding interfaces to LAG results in "port property does not match" error.

Release Notes: Changing speed on LAG member interfaces while an interface is shutdown and then adding interfaces to a LAG will result in "port property does not match" error.

Workaround: None. Change the speed only when interfaces are operationally up.

Layer 2 (Open)

PR# 70063

Severity: S3

Synopsis: Improper MAC learning may happen when a fully loaded chassis is reloaded with POE-enabled ports.

Release Notes: Improper MAC learning may happen when a fully loaded chassis is reloaded with POE-enabled ports. As a result, incoming frames will not be forwarded.

Workaround: Execute the "clear mac-address-table dynamic all" command or reduce the MAC table aging time to recover. In addition, execute the "clear mac" command before the "show mac-address-table count" command to ascertain the exact count of learned addresses.

PR# 72771

Severity: S2

Synopsis: The "show cam mac" command will return "% Error: Linecard 1 is not available." if the command is issued immediately after a line card is reset.

Release Notes: The "show cam mac" command will return "% Error: Linecard 1 is not available." if the command is issued immediately after a line card is reset. In addition, the "show mac-address-table interface" command will display an empty forwarding table, even when continuous Layer 2 traffic is being sent across the interface. These conditions result from the time required to complete internal processing of changes to a large MAC database by the line card agent software process.

Workaround: Do not issue the "show cam mac" command when any of the line cards are being reset.

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# 66345

Severity: S2

Synopsis: ACL hit counters in "show ip accounting access-list" may increment for unexpected ACL entries depending upon lookup engine match and sequence number.

Release Notes: Hardware table values may correspond to similar information from the lookup engine perspective. As a result, ACL hit counters will inappropriately count identical entries for the same data-set as individual "counts", when they should be treated as a single "count". This results in inappropriate counters incrementation.

Workaround: None.

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.

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 disruption to the hosts

Release Notes: When Source and receivers are on the same VLAN, disabling IGMP snooping globally may show a traffic disruption 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.

NTP (Open)

PR# 64251

Severity: S2

Synopsis: NTP packets retain the original IP address when the IP address of a loopback or Gigabit Ethernet interface set to ntp source is changed.

Release Notes: NTP packets will retain the original IP address when the IP address of a loopback or Gigabit Ethernet interface set to "ntp source" is changed. As a result, the system will not synchronize to the NTP server.

Workaround: Avoid changing the IP address.

OS / OS Infrastructure (Open)

PR# 64467

Severity: S2

Synopsis: Intermittently, the "show proc cpu" may indicate non-zero CPU utilization for a process which is not configured.

Release Notes: Intermittently, the "show proc cpu" may indicate non-zero CPU utilization for a process, such as OSPF, which is not configured.

Workaround: None.

PR# 64517

Severity: S2

Synopsis: Sum of CPU utilization of individual tasks may not equal the CPU utilization value shown in "show process cpu".

Release Notes: Sum of CPU utilization of individual tasks may not equal the CPU utilization value shown in "show process cpu".

Workaround: None.

PR# 65075

Severity: S3

Synopsis: The "show inventory" command will display the "Required Type" line card instead of the "Current Type" when in a mismatch card type condition.

Release Notes: The "show inventory" command displays the "Required Type" line card instead of the "Current Type" in the event of mismatch card type condition.

Workaround: Use the show linecard command to view the Current Type.

PR# 65539

Severity: S3

Synopsis: When auto-negotiation is disabled and different speeds configured at two ends, the line protocol will be shown incorrectly as up.

Release Notes: If auto-negotiation is disabled and mismatched, hard-coded speeds are configured on two ends of a GE link, the line protocol will remain incorrectly in an up state.

Workaround: Ensure you configure matching speeds on the two ends if auto-negotiation is disabled.

PR# 69618

Severity: S2

Synopsis: The "show linecard" command will display the status as "cardproblem" for a line card which is not present.

Release Notes: When a line card is not fully inserted on a slot, the show linecard command will display the status as "card problem" for other slots in which no line card is present. For example, if a line card is not fully inserted in slot 1 and no line card is installed in slot 5, the status field in the show linecard command will change to "card problem" for slot 5.

Workaround: None. This is a cosmetic issue only.

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# 71278

Severity: S3

Synopsis: "txdone: transmitter resynced" message may be seen when copying a configuration file from flash to running config.

Release Notes: When using the "copy flash://test.cfg running-config" command to copy a configuration file to the running configuration, a "txdone: transmitter resynced" message may be seen.

Workaround: None. The copy operation should complete successfully.

PR# 72040

Severity: S3

Synopsis: Under rare circumstances chassis manager might declare two same linecard's on different slots.

Release Notes: On improper insertion of a line card in rare cases, chassis manager could receive messages indicating that the newly inserted line card is in a slot different from which it is really inserted. This could be confirmed if the show inventory output shows multiple slots having line cards with the same serial number.

Workaround: Insert a real card of the same type in the slot in which the line card was incorrectly detected. Then remove the line card.

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# 74419

Severity: S3

Synopsis: The "show debug" command will not indicate that the "debug rollback" command is enabled.

Release Notes: The "show debug" command will not indicate that the "debug rollback" command is enabled.

Workaround: This command is not supported.

Open C- Series Software Caveats

PR# 75005

Severity: S3

Synopsis: The "boot system default" command is not supported by configuration replace and rollback.

Release Notes: The "boot system default" command is not supported by configuration replace and rollback.

Workaround: None.

PR# 75484

Severity: S3

Synopsis: F10-IF-EXTENSION-MIB : f10IfOut512To1023BytePkts attribute does not give the right value for LAG interfaces.

Release Notes: F10-IF-EXTENSION-MIB : f10IfOut512To1023BytePkts attribute does not give the right value for LAG interfaces. It might give a value of 0 always.

Workaround: None

PR# 76925

Severity: S3

Synopsis: Configuration rollback and replace may not work correctly with some Call Home configuration statements.

Release Notes: Configuration rollback and replace may not work correctly with some Call Home configuration statements. When this condition occurs, differences between the startup- and running-config files will be seen.

Workaround: Re-apply any missing or incorrect Call Home configuration statements.

PR# 77587

Severity: S3

Synopsis: The "show cpu-traffic-stats all" command will not return any output when executed on the C-Series.

Release Notes: The "show cpu-traffic-stats all" command will not return any output when executed on the C-Series.

Workaround: Use the "show cpu-traffic-stats" (no "all" parameter) to display information for all interfaces.

PR# 77870

Severity: S2

Synopsis: Intermittently, 10-GE CX4 interfaces may not reach an interface up status after a line card is reset.

Release Notes: Intermittently, 10-GE CX4 interfaces may not reach an interface up status after a line card is reset.

Workaround: Remove and re-insert the XFPs.

PR# 78289

Severity: S2

Synopsis: Secondary RPM unable to cacheboot 7.7.1.0 after upgrading the cacheboot image on a system loaded with 7.6.1.0.

Release Notes: The secondary RPM cannot be cache-booted using 7.7.1.0 after upgrading the cacheboot image on a chassis loaded with 7.6.1.0. Instead, it will fall back to booting in download mode. To recognize that this condition has occurred, look for the message "Error: Cacheboot integrity check failed." in the bootup log.

Workaround: Update the boot parameters, save the config, and then reset the secondary RPM.

PR# 78308

Severity: S3

Synopsis: When the "archive config" command is entered for the first time, a message similar to "%Warning: Archive sync is in progress" is reported.

Release Notes: When the "archive config" command is entered for the first time, a message similar to "%Warning: Archive sync is in progress. Please try again later." will be reported.

Workaround: None. This message can be ignored as the system is simply spawning the required task within FTOS.

PR# 78529

Severity: S2

Synopsis: The "Last configuration change" timestamp displayed in the "show run" command output is not updated after some configuration changes.

Release Notes: The "Last configuration change" timestamp displayed in the "show run" command output is not updated after some configuration changes. For example, this issue has been seen when the "logging facility" command is configured.

Workaround: None.

PR# 79340

Severity: S2

Synopsis: Incorrect FTOS version shown for standby RPM when Primary RPM is loaded with 7.6.1.0 and Secondary RPM with 7.7.1.0.

Release Notes: Incorrect FTOS version shown for standby RPM when Primary RPM is loaded with 7.6.1.0 and Secondary RPM with 7.7.1.0. Specifically, the "show version" command will display as 7.6.1.0 for both RPMs.

Workaround: Log directly into the secondary RPM and execute the "show version" command to view the correct FTOS version. This issue is expected to be resolved when doing a warm upgrade between 7.7.1.1 and the next 7.7.1 maintenance release.

PR# 79693

Severity: S2

Synopsis: Config Rollback does not work when the member ports are removed from a VLAN & then rollback is done.

Release Notes: Config Rollback does not work when the member ports are removed from a VLAN & then rollback is done.

Workaround: Reconfigure the VLAN Members

PR# 79924

Severity: S2

Synopsis: Drop in traffic and pause frames generation may be observed if flowcontrol is enabled at line rate traffic flow.

Release Notes: Drop in traffic and pause frames generation may be observed if flowcontrol is enabled at line rate traffic flow.

Workaround: Disable flowcontrol for line-rate port usage.

PR# 80022

Severity: S3

Synopsis: The command "upgrade system-image all B booted" does not work with "booted" option.

Release Notes: The "upgrade system-image all B booted" command, when executed with the booted option to specify that the cache boot image should be upgraded using the booted FTOS image, will fail and return an error message of "% Error: Invalid input: syntax error" and "% Error: Invalid System image URL".

Workaround: Upgrade the cache boot image using a copy from flash or from the network.

PR# 80144

Severity: S4

Synopsis: The packet-per-second rate shown in "monitor interface" output is more than the actual rate.

Release Notes: The packet-per-second rate shown in "monitor interface" output is more than the actual rate.

Workaround: Use "show interface" output for correct packet-per-second rate.

PR# 80413

Severity: S2

Synopsis: A line card may drop to a card-problem state if inserted in a system configured with a different CAM-profile.

Release Notes: When a C-Series line card is inserted in a system with a cam-profile configuration different from the linecard CAM-profile, the linecard will drop down to a card-problem state.

Workaround: The line card can be recovered by configuring it to have the same cam-acl configuration as that of the chassis and then resetting the card. Use the "cam acl linecard" privilege mode CLI to change the CAM profile.

PR# 81202

Severity: S3
Synopsis: Uptime of chassis will be abnormally huge after warm upgrade from 7.6.1.x to 7.8.1.0
Release Notes: Uptime of chassis will be abnormally huge after warm upgrade from 7.6.1.x to 7.8.1.0.
Workaround: A reload will solve it.

OSPF (Open)

PR# 71537

Severity: S3
Synopsis: After hot failover or clear ip ospf, OSPF adjacencies may flap continuously in large-scale config with 60 adjacencies and RFC-2328 flooding enabled.
Release Notes: After hot failover or clear ip ospf, OSPF adjacencies may flap continuously in large-scale config with 60 adjacencies and RFC-2328 flooding enabled.
Workaround: Do not enable this feature with this configuration.

PR# 71822

Severity: S2
Synopsis: After failover of RPM, OSPF route calculation will not happen when there are static routes with 16 ECMP.
Release Notes: After failover of RPM, OSPF route calculation will not happen when there are static routes with 16 ECMP.
Workaround: Use 14 ECMP routes.

Port Monitoring (Open)

PR# 76833

Severity: S2
Synopsis: Inbound mirroring enabled on 10-GE port on which traffic is ingressing at 70% line rate or more can affect normal forwarding or flooding of traffic.
Release Notes: Inbound mirroring enabled on a 10-GE port on which traffic is ingressing at 70% line rate or more can affect the normal forwarding or flooding traffic, and some packets may be lost.
Workaround: None.

PR# 76907

Severity: S2
Synopsis: When port monitoring is enabled on a 10-GE interface, all packets may not be mirrored to the MG port.

Open C- Series Software Caveats

Release Notes: When port monitoring is enabled on a 10-GE interface, all packets may not be mirrored to the MG port.

Workaround: None.

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.

Power Over Ethernet (PoE) (Open)

PR# 70965

Severity: S3

Synopsis: Spurious messages like "%POEMGR-5-POE_INLINE_PWR" might appear on Standby console during bootup.

Release Notes: During bootup, "%POEMGR-5-POE_INLINE_PWR_ZERO: Not enough power supplies for inline power" messages may be reported on the standby RPM console, although sufficient power supply units for inline power are installed and working.

Workaround: None. This message is a spurious report. Functionality is not affected.

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 config.

QoS (Open)

PR# 68440

Severity: S3

Synopsis: The "show qos statistics" command will display that packets which should go to Queue 0 due to an ACL deny entry instead are sent to queue 1, 2, or 3.

Release Notes: The "show qos statistics" command will display that packets which should go to Queue 0 due to an ACL deny entry instead are sent to queue 1, 2, or 3.

Workaround: None. This is a display issue only.

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.

PR# 76987

Severity: S2

Synopsis: Strict priority queueing and bandwidth management as part of any outbound QoS service policy will not work as expected.

Release Notes: Strict priority queueing and bandwidth management as part of any outbound QoS service policy will not work as expected. A larger than expected share of bandwidth is scheduled for the non-strict-priority queues. This issue has been seen only with packets larger than 1150 bytes.

Workaround: None.

PR# 78114

Severity: S2

Synopsis: Buffer profile commands appear to be accepted and applied for non-existing port pipes.

Release Notes: Buffer profile commands appear to be accepted and applied for non-existing port pipes. However, the configuration is not actually programmed in hardware. A "% Error" message will not be printed. Instead, a syslog message similar to "%DIFFSERV-2-DSA_DEVICE_BUFFER_UNAVAILABLE: Unable to allocate dedicated buffers" will be reported. In FTOS release 7.7.1.0, no error is reported for both actual policies and dummy policies (the policy exists only in name -- no policy commands are configured). In FTOS release 7.7.1.1, only dummy policies do not have an error message.

Workaround: Take care to ensure that these commands are applied to the correct port pipe number.

PR# 80476

Severity: S2

Synopsis: After a linecard configured with buffer-profile is moved to a new slot it retains the buffer-profile configurations instead of having default values.

Release Notes: When a linecard having buffer-profile applied on its interface/fp-uplink is removed and inserted in a new slot, it should come up with default values of its buffersizes i.e it should discard the earlier applied buffer-profile on the linecard.

Workaround: Manually reconfigure the buffers to default if needed so.

PR# 80826

Severity:	S3
Synopsis:	The "test cam-usage" command does not count ICMP ACL rules while calculating "Estimated CAM per Port" value
Release Notes:	An ICMP ACL, such as "seq 5 permit icmp host 10.10.45.56 any", configured as part of a rule set for a QoS class map is not factored into the " Estimated CAM per Port" calculation by the "test cam-usage" feature. The entries for the rule are present in the CAM, and the "Available CAM" field of the test cam-usage command shows the correct number of entries available. Estimated CAM per port will display as 0, instead of true value.
Workaround:	None.

RMON (Open)

PR# 64502

Severity:	S4
Synopsis:	An snmpwalk of RMON's 'etherStatsTable' returns max counter32 value for all of the counters momentarily for few seconds.
Release Notes:	An snmpwalk of RMON's 'etherStatsTable' returns max counter32 value for all of the counters. momentarily for few seconds.
Workaround:	Query again after few (5) seconds.

PR# 64911

Severity:	S3
Synopsis:	When RMON alarms for InOctets is configured and the interface receives more than 1 billion packets the SNMP trap will be sent as negative value.
Release Notes:	When RMON alarms for InOctets is configured and the interface receives more than 1 billion packets, the SNMP trap is sent with negative value
Workaround:	None.

PR# 68442

Severity:	S3
Synopsis:	RMON events will not generate log messages if only the "rmon event number [log]" command is configured.
Release Notes:	RMON events will not generate log messages if only the "rmon event number [log]" command is configured.
Workaround:	Add the trap CLI option with the "rmon event number [log] [trap community]" command.

PR# 80395

Severity: S2

Synopsis: RMON etherHistoryTable -> etherHistoryUtilization is not implemented.

Release Notes: RMON etherHistoryTable -> etherHistoryUtilization is not implemented and will always return a value of 0.

Workaround: None.

Security (Open)

PR# 66964

Severity: S3

Synopsis: With a username greater than 25 characters, an authentication request will not be forwarded to a RADIUS server. 802.1X authentication may fail.

Release Notes: When a username greater than 25 characters is used, an authentication request will not be forwarded to the RADIUS server, and 802.1X authentication may fail. Debug output will indicate "EAP Id exceeded Username limit."

Workaround: Apply a username which is 25 characters or less.

PR# 71764

Severity: S3

Synopsis: The "show running-config" command displays only the last configured AAA accounting method (either default method or name method).

Release Notes: The "show running-config" command displays only the last configured AAA accounting method (either default method or name method). It doesn't display the default method until the configured method is removed.

Workaround: None.

PR# 74058

Severity: S2

Synopsis: A configured static MAC address (in addition to the authenticated MAC address) will be accepted on a dot1x authenticated port.

Release Notes: A configured static MAC address (in addition to the authenticated MAC address) will be accepted on a dot1x authenticated port. Only the authenticated MAC address should be allowed.

Workaround: None.

PR# 74217

Severity: S3

Open C- Series Software Caveats

Synopsis:	Reauthentication may not take place for a port which is part of a guest or authentication fail VLAN until the reauth timer expires.
Release Notes:	Reauthentication may not take place for a port which is part of a guest or authentication fail VLAN until the reauthentication timer expires.
Workaround:	Execute the "shutdown" and "no shutdown" commands on the interface to restart reauthentication.

sFlow (Open)

PR# 73066

Severity:	S3
Synopsis:	An extended switch sFlow datagram will have dot1p information for untagged traffic sampled in untagged interfaces on ingress and egress.
Release Notes:	An extended switch sFlow datagram will have dot1p information for untagged traffic sampled in untagged interfaces on ingress and egress.
Workaround:	None.

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# 78310

Severity:	S2
-----------	----

Synopsis:	On the C-Series, Layer 3 and Layer 2 multicast traffic is not collected with sFlow sampling.
Release Notes:	On the C-Series, Layer 3 and Layer 2 multicast traffic is not collected with sFlow sampling. This issue does not impact the E-Series.
Workaround:	None.
PR# 78533	
Severity:	S3
Synopsis:	Incorrect sFlow sampled length packet
Release Notes:	In the current implementation, the sFlow "sampledPacketSize" field refers to the stripped-out packet size of the sampled packet. According to RFC 3671, this field must refer to the total length of the sampled packet.
Workaround:	None. This issue does not impact the S-Series.

SNMP (Open)

PR# 65995	
Severity:	S2
Synopsis:	Cold/warm start traps are transmitted ~30 seconds after bootup if using a non-management interface to transmit the SNMP information.
Release Notes:	If a linecard interface instead of a management port is used for SNMP queries or traps, then the cold start or warm start trap will take around 30 seconds to be sent out after the chassis comes up. The SNMP configuration then is applied afterwards.
Workaround:	None
PR# 79522	
Severity:	S3
Synopsis:	chSysSwModuleTable of f10-chassis.mib and f10-cs-chassis.mib do not return entries for RPMs.
Release Notes:	chSysSwModuleTable of f10-chassis.mib and f10-cs-chassis.mib do not return entries for RPMs.
Workaround:	None.

Spanning Tree (Open)

PR# 78212

Severity: S3

Synopsis: dot1qTpFdbPort might not match with the dot1dStpPort value.

Release Notes: The port ID values as read by the dot1qTpFdbPort OID and the dot1dStpPort OID may not be the same.

Workaround: None.

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

Telnet (Open)

PR# 58012

Severity: S4

Synopsis: Telnet session does not accept input if vertical length is 255.

Release Notes: If the vertical length of a telnet session is set to 255, the telnet session will not accept any input, or show any output.

Workaround: Use a different vertical length, such as 254 or 256.

TFTP (Open)

PR# 62494

Severity: S3

Synopsis: When copying a file via FTP, no error is returned if an incorrect IP address is given.

Release Notes: When copying a file via FTP, no error message ("% Error: Unrecognized host or address.") is returned if an incorrect IP address is given. Instead, the system will attempt to translate the address, fail, and return to the CLI prompt. In addition, an error message is not given when the hostname cannot be resolved for other applications, such as ping and logging.

Workaround: None.

PR# 65407

Severity: S3

Synopsis: "ip tftp source-interface" functionality is incorrect when a loopback interface is configured as a source interface.

Release Notes: If the interface specified in the "ip tftp source-interface" command is loopback interface the TFTP process continues to use the interface as the source IP even though the loopback interface is shut down. As a result, a copy run tftp operation fails.

Workaround: None.

VLAN (Open)

PR# 80780

Severity: S3

Synopsis: Multicast group learned via secondary VLAN will not be populated to primary VLAN and vice versa.

Release Notes: Multicast group learned via secondary VLAN will not be populated to primary VLAN and vice versa.

Workaround: None.

PR# 80972

Severity: S3

Synopsis: GVRP-enabled ports may not be added dynamically to a VLAN after removing the PVLAN mode of the same VLAN.

Open C- Series Software Caveats

Release Notes:	GVRP-enabled ports may not be added dynamically to a VLAN after removing the PVLAN mode of the same VLAN.
Workaround:	A port can be added to the VLAN by either bouncing the port or the GVRP process of the system.

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.

VRRP (Open)

PR# 73787

Severity:	S2
Synopsis:	Interface may not be reachable, if VRRP virtual IP address is configured similar to interface IP address on port-channel interface.
Release Notes:	Interface may not be reachable, if VRRP virtual IP address is configured similar to interface IP address on port-channel interface.
Workaround:	None

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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> •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.	<p>Request a Return Materials Authorization (RMA) number from TAC by opening a support case. Open a support case by:</p> <ul style="list-style-type: none"> • Using the Create Service Request form on the iSupport page (see Contacting the Technical Assistance Center on page 46). • Contacting Force10 directly by E-mail or by phone (see Contacting the Technical Assistance Center on page 46). Provide the following information when using E-mail or phone: • Part number, description, and serial number of the component. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.	<p>Pack the component for shipment, as described in the hardware guide for your system. Label the package with the component RMA number.</p>

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 be reset.

