E-Series® and FTOS Release Notes

Version 6.5.1.9   December 2006   101-00187-05

FORCE10™

How To Use This Document

This document contains information on open and resolved caveats, and operational information specific to the Force10 Networks® E-Series® and Force10 OS (FTOS™) software. 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.

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

New Software Feature

• Flow Control (TeraScale Only)—Controls how the E-Series responds to and generates 802.3x pause frames on 1 and 10 Gig line cards.

Supported Hardware

Hardware	Catalog Number	Minimum Software Version Required
E300 Chassis	CH-E300	5.1.1.0
DC PEM	CC-E300-PWR-DC	6.2.1.1
AC Power Supply	CC-E300-PWR-AC	5.1.1.0
AC Power Supply 1200W	CC-E300-1200W-AC	6.2.1.1
Route Processor Modules—TeraScale	LC-EF3-RPM	6.2.1.1*

Hardware	Catalog Number	Minimum Software Version Required
Switch Fabric Module	CC-E-SFM	5.1.1.0
Switch Fabric Module	CC-E-SFM3	6.5.1.3**
E600 Chassis	CH-E600	3.1.1.2
AC Power Supply 1100W	CC-E600-PWR-AC	3.1.1.2
AC Power Supply 2500W	CC-E600-2500W-AC	6.1.1.1
DC PEM	CC-E600-PWR-DC	3.1.4.2
Route Processor Modules—TeraScale	LC-EF-RPM	6.2.1.1*
Switch Fabric Module	CC-E-SFM	3.1.1.2
Switch Fabric Module	CC-E-SFM3	6.5.1.3**
E600i Chassis	CH-E600i	6.5.1.3
AC Power Supply 2500W	CC-E600-2500W-AC	6.5.1.3
DC PEM	CC-E600-PWR-DC	6.5.1.3
Route Processor Modules—TeraScale	LC-EF-RPM	6.5.1.3
Switch Fabric Module	CC-E-SFM3	6.5.1.3
E1200 Chassis	CH-E1200	2.1.5.8
DC PEM	CC-E1200-PWR-DC	2.1.5.8
Route Processor Modules—TeraScale	LC-EF-RPM	6.2.1.1*
Switch Fabric Module	CC-E-SFM	2.1.5.8
Switch Fabric Module	CC-E-SFM3	6.5.1.3**

* Applies on newer version RPMs.

** Do not mix SFMs. Chassis must have the same type SFMs running the required minimum software version.

Line Cards	Catalog Number	Card Indicator	Minimum Software Version Required
E300 Line Cards			
8-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF3-10GE-8P	EXW8PF3	6.5.1.3
24-Port Gigabit Ethernet with SFP	LC-EF3-1GE-24P	E24PF3	6.2.1.3*

Line Cards	Catalog Number	Card Indicator	Minimum Software Version Required
2-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF3-10GE-2P	EXW2PF3	6.2.1.3*
48-Port 10/100/1000 BASE-T with RJ-45	LC-EF3-GE-48T	E48TF3	6.2.1.3*
E600i Line Cards			
4-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-4P	EXW4PF	6.5.1.3
16-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-16P	EXW16PF	6.5.1.3
48-Port Gigabit Ethernet with SFP	LC-EF-1GE-48P	E48PF	6.5.1.3
48-Port 10/100/1000 BASE-T with RJ-45 Interface	LC-EF-GE-48T	E48TF	6.5.1.3
48-Port 10/100/1000 Base-T High Density	LC-EF-GE-48T1	E48TF1	6.5.1.3
90-Port 10/100/1000 BASE-T Ethernet	LC-EF-GE-90M	E90MF	6.5.1.3
E600 and E1200 Line Cards			
4-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-4P	EXW4PF	6.1.2.4* or 6.2.1.1*
16-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-16P	EXW16PF	6.5.1.1
48-Port Gigabit Ethernet with SFP	LC-EF-1GE-48P	E48PF	6.1.2.4* or 6.2.1.1*
48-Port 10/100/1000 BASE-T with RJ-45 Interface	LC-EF-GE-48T	E48TF	6.1.2.4* or 6.2.1.1*
48-Port 10/100/1000 Base-T High Density	LC-EF-GE-48T1	E48TF1	6.2.1.3
90-Port 10/100/1000 BASE-T Ethernet	LC-EF-GE-90M	E90MF	6.2.1.1

* Applies on newer version RPMs.

Software Upgrade Procedures

The E-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. FTOS supports several software upgrade procedures.

- Hitless Software Upgrade — reserved for maintenance or "patch" releases beginning with FTOS release 6.3.1.1 or newer.

- Software Upgrade for a Single RPM — upgrade procedure for E-Series systems with only one RPM (Route Processor Module)

- Software Upgrade for Dual RPM — upgrade procedure for E-Series systems with two RPMs

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

Hitless Software Upgrade

The Hitless software upgrade allows you to install maintenance or "patch" releases of FTOS without reloading your E-Series chassis. Hitless software upgrade requires two RPMs (RPM0 and RPM1).

⚠ **Warning:** Hitless upgrade from 6.5.1.9 to any lower 6.5.1 build is not supported (**PR 66170**).

→ **Note:** Force10 recommends that you initiate two console sessions, one for each RPM, before beginning the Hitless upgrade procedure.

Step	Command	Command Mode	Purpose
1.	**show rpm**	EXEC privilege	View the current RPM status.
2.	**copy** *file-url* **flash://***filepath* **boot-image synchronize-rpm** Where *file-url* 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) and update the boot variables with the new image.
3.	**copy running-config startup-config**	EXEC privilege	Create a copy of the running configuration file to use as the startup configuration.
4.	**show bootvar**	EXEC privilege	View the boot configuration to verify the new parameters.

5.	**reset RPM 1 hard**
	`Force10#reset rpm 1 hard`
	`Proceed with reset? [yes/no]: yes`
		EXEC privilege	Reset the Standby RPM (1) to load the new image.

6.	**show RPM**	EXEC privilege	View the RPM status to confirm the Standby RPM (1) completed reloading and the new image is updated.

Step	Command	Command Mode	Purpose

7.	**redundancy force-failover RPM**
	
	`Force10#redundancy force-failover rpm`
	`System configuration has been modified. Save? [yes/no]: y`
	`Synchronizing data to peer RPM`
	`!!!!`
	`Peer RPM's SW version is different but HA compatible.`
	`Failover can be done by warm or hitless upgrade.`
	`Specify hitless upgrade or warm upgrade [confirm hitless/warm]:hitless`
	`Proceed with RPM failover [confirm yes/no]: yes`
		EXEC privilege	Force the Standby RPM (1) to become the Primary RPM while reloading the Primary RPM (0) with the new image.

8.	**show RPM**	EXEC privilege	View the RPM status to confirm the Primary RPM (0) completed reloading and the new image is updated.
9.	**redundancy force-failover RPM**	EXEC privilege	Return RPM 0 to the Primary RPM and RPM 1 to the Standby RPM.

Software Upgrade for a Single RPM

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-6.5.1.7.bin.

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 *file-url* 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) and update the boot variables with the new image.
3.	**dir**	EXEC privilege	The default directory for this command is the internal flash (**flash:**).
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.

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.
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

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-EF-w.x.y.z.bin (where w, x, y, and z are replaced by the current release numbers), for example FTOS-EF-6.5.1.7.bin.

⚠️ **Warning:** Both RPMs must contain the same software label number and must be of the same type.

Step	Command Syntax	Command Mode	Purpose
1.	**show rpm**	EXEC privilege	View the current RPM status.

Step	Command Syntax	Command Mode	Purpose
2.	**copy** *file-url* **flash://** *filepath boot-image synchronize-rpm* Where *file-url* 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) and update the boot variables with the new image.
3.	**show bootvar**	EXEC privilege	View the boot configuration.
4.	**reload**	EXEC privilege	Reboot the system; both RPMs will have the new image loaded.

Closed Hardware Caveats (TeraScale)

Note: A recent bootflash component change requires a bootcode upgrade for some line cards within the serial number range of 0057500 - 0063000. Please refer to the recently issued field noticed titled *E-Series TeraScale Line Cards with Serial Numbers 0057500 to 0063000 Might Fail to Boot after a Bootflash Upgrade or Line Card Crash* for complete details and workaround strategies associated with this issue.

Closed Software Caveats (TeraScale)

ARP (closed)

PR# 64351

Severity:	S1
Synopsis:	When next-hop, of a recursive route to a SNMP destination, times out on CP, the CP ARPs for SNMP destination instead of next-hop to the reach destination.
Release Note:	When next-hop, of a recursive route to a SNMP destination, times out on CP, the CP ARPs for SNMP destination instead of next-hop to the reach destination.
Workaround:	Ping the gateway or static ARP or ARP timeout zero.

PR# 64421

Severity:	S3
Synopsis:	FTOS rejects ARPs with multicast MAC (CP on TeraScale and all 3 CPUs on EtherScale). Static ARP CLI rejects multicast MAC.
Release Note:	FTOS rejects ARPs with multicast MAC (CP on TeraScale and all 3 CPUs on EtherScale). Static ARP CLI rejects multicast MAC.
Workaround:	None

BGP (closed)

PR# 64669

Severity:	S2
Synopsis:	EBGP multipath may not choose all equal cost paths when the same update with same AS path comes from IBGP peers.
Release Note:	EBGP multipath may not choose all equal cost paths when the same update with same AS path comes from IBGP peers.
Workaround:	None

Layer 3 ACL (closed)

PR# 65039

Severity:	S2
Synopsis:	Loopback ACL does not handle fragments correctly.
Release Note:	Loopback ACL only filters the first fragment. The remainder of fragments are not evaluated.
Workaround:	None

Logging (closed)

PR# 60961

Severity:	S3
Synopsis:	'show log reverse' and 'show log' entries may be different
Release Note:	The **show logging reverse** and **show logging** entries may be different. **Show log reverse** might have some entries older than **show log**.
Workaround:	None

PR# 63768

Severity:	S1
Synopsis:	EventLog task crashes in certain scenarios.
Release Note:	EventLog task crashes in certain scenarios.
Workaround:	None

PR# 64575

Severity: S1

Synopsis: EventLog task crash in certain scenarios

Release Note: EventLog task crash in certain scenarios

Workaround: None

OSPF (closed)

PR# 63895

Severity: S2

Synopsis: After reload, a part of the OSPF configuration may not be applied.

Release Note: With a large configuration, after a reload, one of the OSPF commands may be missing from the running configuration, but will still be present in the startup-configuration. This condition has been observed very rarely.

Workaround: Re-add the OSPF command to the running config. The following syslog message will be displayed to the console:

```
%RPM0-P:CP %MIB-6-SRC_TO: Task CLI send ReqType 3 ObjId 10003. Request times
out. %RPM0-P:CP %MIB-6-TIMEOUT: No response from IFMGR after 120 seconds.
Timing out....
```

PR# 64540

Severity: S2

Synopsis: In ECMP scenario all paths are not chosen in certain scenarios.

Release Note: In ECMP scenario all paths are not chosen in certain scenarios.

Workaround: None

OS / OS Infrastructure (closed)

PR# 62591

Severity: S2

Synopsis: Incorrect pointer reference of the EventLog task can result in a system crash.

Release Note: Incorrect pointer reference of the EventLog task can result in a system crash.

Workaround: None

PR# 64039

Severity: S3

Synopsis: "Show ip traffic" SNMP OIDs do not return consistent data for bcast/mcast counters.

Release Note: The new private Force10 OIDs added to reflect the Broadcast data is not consistent with the output of "show IP traffic".

Workaround: None

PR# 64140

Severity:	S3
Synopsis:	XFP power reading on a 10 gig line card might be shown as 0.0.
Release Note:	XFP power reading on a 10 gig line card might be shown as 0.0.
Workaround:	None

PR# 64276

Severity:	S2
Synopsis:	After **clear ip traffic** command followed by **clear arp cache** ARP does not get resolved in certain scenarios.
Release Note:	After **clear ip traffic** command followed by **clear arp cache** ARP does not get resolved in certain scenarios.
Workaround:	None

PR# 64339

Severity:	S2
Synopsis:	Due to vendor misprogramming, FTOS is unable to read power levels from JDSU-sourced XFPs.
Release Note:	Due to misprogramming by vendor, the power is incorrectly calculated.
Workaround:	None

PR# 64969

Severity:	S2
Synopsis:	Unable to save configuration after copying a file through SCP via SSH session.
Release Note:	Unable to save configuration after copying a file through SCP via SSH session.
Workaround:	None

PR# 65147

Severity:	S2
Synopsis:	IPC timeout on RP2 followed by chassis reboot with core dump.
Release Note:	Chassis might reboot due to IPC timeout on RP2.
Workaround:	None

PR# 65918

Severity:	S1
Synopsis:	Chassis may crash on reboot when containing a faulty line card.
Release Note:	If a chassis contains a faulty line card, the chassis may crash when bringing up the system on a reload.
Workaround:	Remove the faulty line card and reload the system again.

QoS (closed)

PR# 58916

Severity:	S2
Synopsis:	packets are being dropped for the queue that is not classified as strict priority even when there is no congestion.
Release Note:	Packets are being dropped for the queue that is not classified as strict priority even when there is no congestion.
Workaround:	None

PR# 61051

Severity:	S3
Synopsis:	Show queue statistics is showing wrong Ingress min and max WRED thresholds for 10gig linecard.
Release Note:	Ingress Min and Max WRED thresholds may be wrong for 10gig interfaces.
Workaround:	None

RTM (closed)

PR# 63968

Severity:	S3
Synopsis:	Static route pointing to next hop which is to be reached through a port-channel not added to routing table.
Release Note:	Static route pointing to next hop which is to be reached through a port-channel not added to routing table.
Workaround:	Workaround 1. Add static route with correct port-channel 1 ip route 123.0.0.0/24 port-channel 1 10.16.128.201
	Workaround 2. Remove port-channel 1 and reconfigure it again.

TFTP (closed)

PR# 63679

Severity:	S3
Synopsis:	When trying to TFTP a file from chassis there is a possibility that the TFTP task handler might crash.
Release Note:	When trying to TFTP a file from chassis there is a possibility that the TFTP task handler might crash.
Workaround:	FTP can be used replacing TFTP.

Closed Software Caveats (EtherScale)

ARP (closed)

PR# 64421

Severity: S3

Synopsis: FTOS rejects ARPs with multicast MAC (CP on TeraScale and all 3 CPUs on EtherScale). Static ARP CLI rejects multicast MAC.

Release Note: FTOS rejects ARPs with multicast MAC (CP on TeraScale and all 3 CPUs on EtherScale). Static ARP CLI rejects multicast MAC.

Workaround: None

BGP (closed)

PR# 64669

Severity: S2

Synopsis: EBGP multipath may not choose all equal cost paths when the same update with same AS path comes from IBGP peers.

Release Note: EBGP multipath may not choose all equal cost paths when the same update with same AS path comes from IBGP peers.

Workaround: None

Logging (closed)

PR# 60961

Severity: S3

Synopsis: 'show log reverse' and 'show log' entries may be different

Release Note: The **show logging reverse** and **show logging** entries may be different. **Show log reverse** might have some entries older than **show log**.

Workaround: None

OSPF (closed)

PR# 63895

Severity:	S2
Synopsis:	After reload, a part of the OSPF configuration may not be applied.
Release Note:	With a large configuration, after a reload, one of the OSPF commands may be missing from the running configuration, but will still be present in the startup-configuration. This condition has been observed very rarely.
Workaround:	Re-add the OSPF command to the running config. The following syslog message will be displayed to the console:

```
%RPM0-P:CP %MIB-6-SRC_TO: Task CLI send ReqType 3 ObjId 10003. Request times
out. %RPM0-P:CP %MIB-6-TIMEOUT: No response from IFMGR after 120 seconds.
Timing out....
```

PR# 64540

Severity:	S2
Synopsis:	In ECMP scenario all paths are not chosen in certain scenarios.
Release Note:	In ECMP scenario all paths are not chosen in certain scenarios.
Workaround:	None

OS / OS Infrastructure (closed)

PR# 62591

Severity:	S2
Synopsis:	Incorrect pointer reference of the EventLog task can result in a system crash.
Release Note:	Incorrect pointer reference of the EventLog task can result in a system crash.
Workaround:	None

PR# 64969

Severity:	S2
Synopsis:	Unable to save configuration after copying a file through SCP via SSH session.
Release Note:	Unable to save configuration after copying a file through SCP via SSH session.
Workaround:	None

PR# 65918

Severity:	S1
Synopsis:	Chassis may crash on reboot when containing a faulty line card.
Release Note:	If a chassis contains a faulty line card, the chassis may crash when bringing up the system on a reload.
Workaround:	Remove the faulty line card and reload the system again.

RTM (closed)

PR# 63968

Severity: S3

Synopsis: Static route pointing to next hop which is to be reached through a port-channel not added to routing table.

Release Note: Static route pointing to next hop which is to be reached through a port-channel not added to routing table.

Workaround: Workaround 1. Add static route with correct port-channel 1 ip route 123.0.0.0/24 port-channel 1 10.16.128.201

Workaround 2. Remove port-channel 1 and reconfigure it again.

Open Hardware Caveats (TeraScale)

Hardware caveats are not currently searchable through the BugTrack search tool on the iSupport web site. However, you can subscribe to caveat update reports which includes Hardware caveats. To subscribe to caveat update reports, visit iSupport at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx.

Hardware (TeraScale)

PR# 47839

Severity: S3

Synopsis: CRC counters may not increment when Jumbo packets with bad CRCs are sent.

Release Note: For LC-EF3-GE-48T and LC-EF3-1GE-24P, CRC counters may not increment when jumbo packets with bad CRC are sent.

Workaround: None

PR# 56638

Severity: S2

Synopsis: Packets of 65-67, 69-71, and 73-75 bytes are dropped when the packet type of 802.3, with an invalid field length, is received on the LC-EF3-10GE-2P and LC-EF-10GE-4P line card.

Release Note: Packets of 65-67, 69-71, and 73-75 bytes are dropped when the packet type of 802.3, with an invalid field length, is received on the LC-EF3-10GE-2P and LC-EF-10GE-4P line card.

Workaround: None. It is invalid length.

Open Software Caveats (TeraScale)

PR# 47782

Severity: S2

Synopsis: A port with the default MTU may still learn MAC addresses for giant packets.

Release Note: A port with the default MTU may still learn MAC addresses for giant packets.

Workaround: None

PR# 57317

Severity: S4

Synopsis: High latency may be seen during traceroute.

Release Note: High latency may be seen during traceroute.

Workaround: None

PR# 59710

Severity: S3

Synopsis: The show cam-profile command output will display L3 ingress ACL CAM size to be 1K more than what the actual size is.

Release Note: The show cam-profile command output will display L3 ingress ACL CAM size to be 1K more than what the actual size is.

Workaround: For L3 ingress ACL, calculate the actual CAM size to be 1K less than the displayed value in the **show cam**-**profile** command output.

ARP

PR# 59514

Severity: S2

Synopsis: Some ARPs/Routes do not get loaded to line cards

Release Note: When a chassis boots up with a large number of ARPs in the local networks with a large number of line cards present, some ARPs may not be loaded into the linecard FIBs.

Workaround: The **no arp ip** *ip-address* command will cause individual ARPs to get loaded into the FIBs, and resetting each line card one at a time will get all ARPs loaded into the FIB.

BGP

PR# 56659

Severity:	S2
Synopsis:	"Show ip bgp regexp" and "Show ip bgp filter-list" may take up 99% CPU and may time out.
Release Note:	The commands **show ip bgp regexp** and **show ip bgp filter-list** may take up 99% CPU and may time out.
Workaround:	None

PR# 59000

Severity:	S2
Synopsis:	"show ip bgp regexp" may cause high CPU utilization that results in CLI timeout.
Release Note:	The command **show ip bgp regexp** may cause high CPU utilization that results in CLI timeout.
Workaround:	None

PR# 60077

Severity:	S1
Synopsis:	Out of memory on CP can lead to task crash with 250+ bgp neighbors.
Release Note:	Out of memory on CP can lead to task crash with 250+ BGP neighbors.
Workaround:	None

PR# 60322

Severity:	S3
Synopsis:	Initial misconfiguration of MD5 string between BGP peers may lead to persistent authentication failure messages.
Release Note:	When the BGP MD5 string is misconfigured between two BGP peers and then the interface later shut down and/or was removed on the E-series, the following message will persist asserting in the logs:

> %RPM0-P:RP1 %KERN-6-INT: BGP md5 authentication failed from a.b.c.d:10000 to w.x.y.z:179

Workaround:	Ensure remote peer removes their misconfigured session and rebuild it with the appropriate MD5 string, or have the BGP session deleted from peer box if no longer needed.

PR# 60354

Severity:	S3
Synopsis:	BGP hidden password option does not work if the password is clear text and less than 16 characters. If hidden password option is selected on one end and configured password is less than 16 characters, the bgp session will be authenticated even if there is no password configured on other end.
Release Note:	BGP hidden password option does not work if the password is clear text and less than 16 characters. If hidden password option is selected on one end and configured password is less than 16 characters, the bgp session will be authenticated even if there is no password configured on other end.
Workaround:	Use encrypted password to authenticate the peers.

PR# 63638

Severity:	S3
Synopsis:	as-path access-list regexp expects alphanumeric after OR (pipe |)
Release Note:	Using	in regexp expects alphanumeric or whitespace to follow. Else syntax is rejected: Force10(config-as-path)# permit ^123(456|)$ % Error: Input string is not a regular expression.
Workaround:	Break OR into two statements
	Force10(config-as-path)# permit ^123 456$
	Force10(config-as-path)# permit ^123$

PR# 64109

Severity:	S3
Synopsis:	show ip bgp <prefix>" shows peer group names, as well as some peers that are actually members of the peer groups displayed already.
Release Note:	The outputs of the command "show ip bgp <prefix>" has a section "advertised to". This section should show peer-groups and individual neighbors (which don't belong to a peer-group), to which this prefix is advertised to. It has been noticed that sometimes, this output lists some individual neighbors, which already belong to a peer group. The output would then contain the peer-group names, as well as some peers that are actually members of the peer groups already displayed.
Workaround:	None

PR# 64299

Severity:	S2
Synopsis:	The BGP task "bgpRibupd" reaches CPU utilization of nearly 100% with a number of AS-path lists with a lot of regular expression matches embedded.
Release Note:	he BGP task "bgpRibupd" reaches CPU utilization of nearly 100% with a number of AS-path lists with a lot of regular expression matches embedded. This regex evaluation takes too much CPU, especially when large amount of paths need to matched.
Workaround:	None

CLI

PR# 57454

Severity: S3

Synopsis: "Login successful for user on line aux" is displayed on new primary (after failover), even though there is no connection to aux port.

Release Note: "`Login successful for user on line aux`" is displaying on new primary after failover, even though there is no connection to aux port.

Workaround: None

PR# 59468

Severity: S2

Synopsis: Console session hangs after telnet sessions hang and 'no ip telnet server enable' toggled.

Release Note: When telnet sessions hang, accessing the E-series via console and proceeding to execute a 'no ip telnet server enable' can result in a console lockup as well as a CPU spike.

Workaround: None

PR# 60104

Severity: S4

Synopsis: NTP server is not converted to IP address in configuration file.

Release Note: The configuration command "ntp server {hostname}" saves the command with the hostname, rather than converting to IP address in the configuration file. This is inconsistent with other configuration commands that reference server names.

Workaround: None

PR# 60330

Severity: S4

Synopsis: Terminal length inconsistency with lines greater than terminal width.

Release Note: Pagination does not take into account wrapped lines.

Workaround: None

PR# 60667

Severity: S3

Synopsis: No login/motd Banner Message shows up after SSH to the switch.

Release Note: No login/motd Banner Message shows up after SSH to the switch.

Workaround: None

PR# 62631

Severity: S4

Synopsis: CLI command following a "!" still takes effect

Release Note: CLI command following a "!" is not commented out. The command will still take effect.

Workaround: None

PR# 63198

Severity: S3

Synopsis: Error message is displayed due to cfg0->cfgDsync0 queue not getting flushed out.

Release Note: The cfg0->cfgDsync0 queue increments when secondary RPM gets stuck without processing messages in its SWP queue. This could result in the following error msg:

May 29 13:42:54.496: %RPM1-S:CP %CFG-3-CFG_ERROR: Cfg SWP error May 29 13:42:54.496: %RPM1-S:CP %SWP-2-NO MORE TIMEOUT: SWP: swpTimeoutCB: queue 1, cfg0 to cfgDsync0, timeouts used: 256, timeout limit: 255".

Workaround: None

PR# 63259

Severity: S3

Synopsis: show log doesn't show full log output

Release Note: When SSH to Force10 Switch from SecureCRT, if there are more than 24 logs and when user run "show log" command, user could see more than 24 lines output (default terminal length = 24) before hitting"space" bar for next 24 lines, or quit from show log after first 24 lines.

Workaround: User can use telnet/console instead, or use another software, such as Putty.

PR# 63894

Severity: S3

Synopsis: A '?" in startup-config does not get applied to running config

Release Note: A question mark in startup configuration will not get applied to running configuration correctly after a reload.

   Force10#sho run as-path test
   !
   ip as-path access-list test permit 1?$ deny .*
will change to the following on reload:
   ip as-path access-list test deny.*

Workaround: use {0,1} instead of ?

Control Plane

PR# 59526

Severity: S2

Synopsis: A Loopback ACL with "log" may let packets through.

Release Note: A Loopback ACL with "log" may let packets through.

Workaround: Do not use the "log" attribute for a Loopback ACL.

FIB

PR# 47504

Severity:	S3
Synopsis:	CAM full messages are not printed (6.3.1.2 or later).
Release Note:	CAM full messages for L3 FIB are not logged (builds 6.3.1.2 and later).
Workaround:	Use **show ip fib linecard slot summary** and **show ip cam linecard** *slot* **port-set 0/1** command to verify.

PR# 59234

Severity:	S2
Synopsis:	The **show ip flow** and **show port-channel flow** commands are not supported in lag-hash-align microcode (non default cam-profile).
Release Note:	The **show ip flow** and **show port-channel flow** commands are not supported in lag-hash-align microcode (non default cam-profile).
Workaround:	None

PR# 60101

Severity:	S3
Synopsis:	icmp ip redirect messages are not sent to source when ip redirect condition is detected and ip redirects command is enabled on the interface.
Release Note:	icmp ip redirect messages are not sent to source when ip redirect condition is detected and ip redirects command is enabled on the interface.
Workaround:	None

PR# 61175

Severity:	S1
Synopsis:	fat2NHWalker task crashed on the line card and subsequently line card failed to checkin.
Release Note:	fat2NHWalker task crashed on the line card and subsequently line card failed to checkin.
Workaround:	None

PR# 61891

Severity:	S2
Synopsis:	FIB may fail to update NH information after counter wraps with large number of unresolved recursive NHs.
Release Note:	Under rare circumstances with a large number of recursive, yet eventually unresolved next-hops, an internal variable will increase in orders of magnitude faster than normal. Eventually, this counter may wrap, at which point, the FIB is unable to update NH information.
Workaround:	Hard Reset the specific linecard with the command "reset linecard <#> hard".

PR# 62373

Severity: S1

Synopsis: fat2Mover task may crash on LC-EF-10GE-4P

Release Note: fat2Mover task may crash on LC-EF-10GE-4P. A crash log file for that linecard is created in flash:/
                   /CRASH_LOG_DIR and a trace file is created in flash://TRACE_LOG_DIR.

Workaround: None.The line card will reset itself and come online. Please contact TAC if this problem is seen.

Flow Control

PR# 66138

Severity: S3

Synopsis: On 10G Interface the configured flow-control values take effect only after shut/no shut on the
                   interface.

Release Note: On 10G Interface the configured flow-control values take effect only after shut/no shut on the
                   interface.

Workaround: Do shut/no shut on the Interface.

FTP

PR# 63388

Severity: S3

Synopsis: Able to access all files under the flash even though "ftp topdir" is not configured after ftped into
                   system.

Release Note: Able to access all files under the flash even though "ftp topdir" is not configured.

Workaround: None

FTSA

PR# 57332

Severity: S3

Synopsis: callhome will stop sending messages after hitless upgrade.

Release Note: The Call Home (FTSA) service will stop sending messages after a hitless upgrade.

Workaround: None

PR# 64138

Severity: S2

Synopsis: Callhome may not send out messages to recipients after failover.

Release Note: Callhome does not send out messages to recipients after failover.

Workaround: After doing a 'no enable-all' followed by 'enable-all' within callhome context on the new primary,
                   messages were sent out again.

IGMP

PR# 44218

Severity:	S2
Synopsis:	General Query is not sent out of the Root port after MSTP Topology change.
Release Note:	General Query is not sent out of the MSTP Root port after a Topology change in the network. The effect is that multicast traffic receiver will not receive traffic for the time-interval equal to the IGMP Query interval configured on the IGMP Querier.
Workaround:	None

PR# 57349

Severity:	S3
Synopsis:	With IGMP Snooping enabled, the debug ip igmp interface command for physical interface does not show incoming and outgoing general queries for that interface.
Release Note:	With IGMP snooping enabled, "debug ip igmp interface" command for physical interface does not show incoming and outgoing general queries for that interface.
Workaround:	Use **debug ip igmp vlan** command for the general queries.

PR# 58528

Severity:	S2
Synopsis:	IGMP snooping enabled switch does not detect PIM router which is not a IGMP querier.
Release Note:	If there is more than one PIM router on a VLAN, F10 detects only the port connected to the IGMP querier router as the multicast router port. It does not detect non-querier routers.
Workaround:	Use the "ip igmp snooping mrouter interface" command in VLAN context to add all multicast router ports.

IPv4

PR# 56335

Severity:	S3
Synopsis:	'Debug ip packet' does not show the forwarded packets unless explicitly configured on the ingress port.
Release Note:	'Debug ip packet' does not show the forwarded packets unless explicitly configured on the ingress port.
Workaround:	Enable **debug ip packet** on the ingress interface of the chassis.

PR# 57757

Severity:	S2
Synopsis:	With IGMP snooping enabled, 200 groups joined in one vlan can cause a memory leak.
Release Note:	With IGMP snooping enabled, 200 groups joined in one VLAN can cause a memory leak.
Workaround:	None

ISIS

PR# 57491

Severity:	S3
Synopsis:	When there are a large number of LSPs in the database, show isis database on SSH session is not returning any output.
Release Note:	When there are large number of LSPs in the database, show isis database on SSH session is not returning any output
Workaround:	Use either console or Telnet.

Layer 2

PR# 47359

Severity:	S3
Synopsis:	In TeraScale mode, the show port-channel flow and show ip flow commands are not supported when packet-based hashing is configured.
Release Note:	In TeraScale mode, the **show port-channel flow** and **show ip flow** commands are not supported when packet-based hashing is configured.
Workaround:	None

PR# 56903

Severity:	S2
Synopsis:	STP BPDU entries are improperly installed in the L2 CAM.
Release Note:	Extra STP Entries can end up being installed in the Layer 2 CAM.
Workaround:	None. These entries should not affect any feature functionality or data traffic.

PR# 56958

Severity:	S3
Synopsis:	Vlan-stack TAG is not getting removed at the access interface when vlan-stack protocol type of "0x8100" is used.
Release Note:	VLAN-Stack tag does not get removed at the access interface when VLAN-Stack protocol type of 0x8100 is configured (TeraScale only).
Workaround:	Use VLAN-Stack tag other than 0x8100.

PR# 57371

Severity:	S1
Synopsis:	Mac Manager & L2PM report out of memory and RP2 stops responding with 4K VLANs
Release Note:	With Spanning tree (STP/MSTP/RSTP/PVST) enabled, adding interfaces to a large number of vlans using the **vlan range** command is currently not supported
Workaround:	Add interfaces to the VLANs individually.

PR# 61621

Severity: S3

Synopsis: When a channel-member is removed from a LAG with mac limit, the Unknown SA Drops are getting reduced.

Release Note: When a channel-member is removed from a LAG that has mac learning-limit configured, the Unknown SA Drops will be reduced by the number equals to the drops happened on the removed member port.

Workaround: None

PR# 61708

Severity: S3

Synopsis: If there is a LAG with no members/ with members shut, the show mac learning-limit will not show the unknown SA drops incrementing for other interfaces.

Release Note: If there is a port-channel with no members/ with members shut, the show mac learning-limit will not show the unknown SA drops incrementing for other interfaces with learning-limit configured.

Workaround: Remove mac limit from the port-channel with no members/ with members shut.

PR# 61755

Severity: S2

Synopsis: After failover mac learning-limit on port-channels is not working intermittently.

Release Note: After RPM failover mac learning-limit on port-channels may not work intermittently.

Workaround: Unconfigure and configure mac-limit.

Layer 2 ACL

PR# 56866

Severity: S2

Synopsis: No option available to delete a mac access-group for a vlan

Release Note: A MAC ACL cannot be deleted per VLAN if it was applied for multiple VLANs on an interface.

Workaround: Reapply the required VLANs.

PR# 57660

Severity: S4

Synopsis: When the port channel is not created, "show mac accounting access-list" for that port channel, gives an incorrect error message.

Release Note: If an access list is created but not a port channel, "show mac accounting accesslist [name] int po [#] in" gives an incorrect error message saying that the access list does not exist.

Workaround: None

PR# 62562

Severity: S2

Synopsis: With CAM profile ipv4-320K, the LACP and FEFD won't work for the port set 0 of card E90MF.

Release Note: When the cam profile is set to ipv4-320K, the LACP and FEFD will not work for the port set 0 of card E90MF.

Workaround: None

Layer 3 ACL

PR# 57448

Severity: S2

Synopsis: If, a L2 interface and a vlan has access-lists applied to it and subsequently, interface is made a member of vlan, it is allowed.

Release Note: If a Layer 2 interface and a VLAN has access lists applied to them, and subsequently, the interface is made a member of a VLAN, it is allowed.

Workaround: Add the interface to the VLAN before applying the access list.

PR# 58950

Severity: S3

Synopsis: With inverse-mask enabled, non-contiguous mask check functionality without "bitmask" keyword in prefix-list is broken.

Release Note: With inverse-mask enabled, non-contiguous mask with "bitmask" does not work.

Workaround: Do not enable inverse-mask when non-contiguous mask is used.

PR# 60143

Severity: S2

Synopsis: rapid and repeated egress ACL configuration can lead to acl_1 task withholding memory.

Release Note: rapid and repeated egress ACL configuration can lead to acl_1 task withholding memory on RP1.

Workaround: None

PR# 60256

Severity: S3

Synopsis: Cosmetic issue of CAM Full Messages could appear after adding one more ACL.

Release Note: Cosmetic issue of CAM Full Messages after adding one more ACL, even if there is free CAM mem (12K by default) for L3ACL. It will show CAM Full message and this only happens if the added ACL Seq number is less than 10. But the added ACL will still work.

> Force10(config-ext-nacl)#seq 4 permit ip any 6.5.0.0/24 log count
> Force10(config-ext-nacl)#May 18 10:45:13.20: %E48TF3:3
> %ACL_AGENT-2-ACL_CAM_FULL: L3Acl Cam is Full.

Workaround: Ignore the CAM full message, and run show ip accounting access-list to make sure the ACL is the there.

PR# 64352

Severity: S4

Synopsis: Timestamp of running config, seen under block sync, does not get updated after a write memory.

Release Note: The 'write memory' should update the timestamp on both startup config and running config. The 'show redundancy' has a field 'last data block sync record' which has the timestamps of both these configs, at last sync. The timestamp for startup config is updated but running config is not.

Workaround: startup config timestamp could be checked to see the time of last sync.

MSDP

PR# 47323

Severity: S2

Synopsis: SA-Filters are not working under MSDP.

Release Note: SA-Filters do not work for MSDP

Workaround: None

PR# 56328

Severity: S2

Synopsis: FTOS doesn't support using the as-path information of routes to determine peer-RPF neighbor.

Release Note: FTOS doesn't support using the as-path information of routes to determine peer-RPF neighbor, which is described in item IV of section 10.1.3 "Peer-RPF Forwarding Rules" of RFC3618.

Workaround: Let the MSDP topology mirror the (m)BGP topology and make sure that MSDP peer address is the same as the (m)BGP peer address.

PR# 56828

Severity: S2

Synopsis: Prefix-list doesn't work for MSDP default peer.

Release Note: SA filtering for default peer using prefix-list does not work.

Workaround: None

PR# 57270

Severity: S2

Synopsis: 'Clear ip msdp sa-cache' sometimes fails to reconcile entries between PIM and MSDP.

Release Note: The command **clear ip msdp sa-cache** does not resolve out-of-sync problems between PIM and MSDP.

Workaround: None

PR# 59923

Severity: S2

Synopsis: MSDP will not update the existing SA entry if it receives the same SA entry from a different peer.

Release Note: MSDP will not update the existing SA entry if it receives the same SA entry from a different peer.

Workaround: Use the command "clear ip msdp sa-cache" to clear the SA entry.

PR# 61928

Severity: S3

Synopsis: Executing a 'show ip msdp sa-cache' outputs a subset of the values expected.

Release Note: When there are large numbers of multicast sources (> 1500) the output of 'show ip msdp sa-cache' may provide only a subset of the total data for a period of time.

Workaround: Waiting several minutes for the sa-cache to converge can result in correct output.

Multicast

PR# 41519

Severity: S3

Synopsis: SPT switchover still happened even when the traffic rate was below the threshold

Release Note: SPT switchover may happen immediately after **clear ip mroute** * or **clear ip pim tib** regardless of configured switchover threshold.

Workaround: None

PR# 41916

Severity: S3

Synopsis: mtrace doesn't have a complete trace output after static mroute is added in certain scenarios.

Release Note: mtrace doesn't have a complete trace output after static mroute is added in certain scenarios.

Workaround: None

PR# 44746

Severity: S2

Synopsis: 'Show ip rpf' does not show the correct Route/Mask info if route is learnt via BGP.

Release Note: The command **show ip rpf** may not show correct RPF neighbor for recursive BGP routes.

Workaround: None

PR# 47404

Severity: S2

Synopsis: The number of multicast entries supported in FTOS is limited to 15000.

Release Note: The number of multicast entries supported in FTOS is limited to 15000.

Workaround: None

PR# 47461

Severity:	S2
Synopsis:	mtrace may not work as expected.
Release Note:	mtrace may not work as expected.
Workaround:	None

PR# 47927

Severity:	S2
Synopsis:	CPU is receiving excessive control plane traffic: traffic will be rate controlled messages may be seen with multicast forwarding
Release Note:	CPU is receiving excessive control plane traffic: traffic will be rate controlled messages may be seen with multicast forwarding.
Workaround:	None

PR# 57975

Severity:	S3
Synopsis:	Reverse Path Forwarding (RPF) check algorithm needs to be retuned.
Release Note:	Currently, the FTOS algortihm performs an RPF check based on longest match and distance, as opposed to mstatic/mbgp/unicast rib.
Workaround:	None

PR# 58508

Severity:	S2
Synopsis:	When PIM is enabled on a VLAN, IGMP reports are not forwarded to another PIM router on the VLAN. If F10 is not the PIM-DR, then forwarding to that receiver won't work.
Release Note:	When PIM is enabled on a VLAN, IGMP reports are not forwarded to another PIM router on the VLAN. If F10 is not the PIM-DR, then forwarding to that receiver won't work
Workaround:	Configure only one PIM router per VLAN. If more than one PIM router is to be configured, enable IGMP Snooping on the VLAN and configure mrouter ports using the **ip igmp snooping mrouter interface** command in VLAN context.

PR# 59497

Severity:	S3
Synopsis:	The command **show ip msdp sa-cache** *group* doesn't display all the relevant SA entries
Release Note:	The command **show ip msdp sa-cache** *group* only displays a subset of the nominal list of entries when executed.
Workaround:	None

PR# 60174

Severity:	S3
Synopsis:	Stale multicast entries reside in CAM upon unconfiguring and reconfigure multicast routing.
Release Note:	On a F10 system heavily loaded (i.e w/ CPU load > 75%) with multicast traffic unconfiguring and reconfigure multicast routing may result in stale multicast entries remaining in the CAM.
Workaround:	Reduce the likelihood of high CPU load due to multicast (e.g. increase IGMP query interval, statically configure multicast groups that experience excessive amounts of join/leaves).

NTP

PR# 56256

Severity:	S4
Synopsis:	ntp port(123) should be closed when ntp is not configured.
Release Note:	ntp port(123) should be closed when ntp is not configured.
Workaround:	None

OS / OS Infrastructure

PR# 45203

Severity:	SS4
Synopsis:	If both ends of the copper link are configured with same forced master or slave settings flapping may occur.
Release Note:	If both ends of copper links are configured with "mode forced-master" or "mode forced-slave", the "show interface" command will flap between "Auto-neg-Error" and forced-master/slave states.
Workaround:	Reconfigure only one end of a connection to be "mode forced-master" or "mode forced-slave".

PR# 47319

Severity:	S3
Synopsis:	Output Unicast counters in the show interface command might give a large incorrect value, when there is output Multicast or output broadcast traffic.
Release Note:	Output Unicast counters in the show interface command might give a large incorrect value, when there is output Multicast or output broadcast traffic.
Workaround:	Clear counters

PR# 47425

Severity:	S2
Synopsis:	Configuring "no nego auto" on LC-EF-48T interfaces can lead to inconsistent port status.
Release Note:	Configuring **no nego auto** on LC-EF-48T interfaces can lead to inconsistent port status.
Workaround:	None

PR# 48038

Severity: S2

Synopsis: IPC receive fail error when LAG port is deleted in inter-vlan scenario %RPM0-P:RP2
                %IPMGR-3-DEL_INT_RB: IPM2: Interface(0x4207802b) delete Error.

Release Note: IPC receive fail error when LAG port is deleted in inter-vlan scenario %RPM0-P:RP2
                %IPMGR-3-DEL_INT_RB: IPM2: Interface(0x4207802b) delete Error.

Workaround: None

PR# 56078

Severity: S3

Synopsis: "md5 authentication failed" message is generated for shutdown neighbor.

Release Note: Even though a BGP neighbor (with MD5 authentication configured) is shutdown, BGP MD5
                authentication failure messages may be seen in the logs.

Workaround: Shutdown the peer from the remote side or remove the peer configuration from the remote peer's
                BGP configuration.

PR# 56311

Severity: S2

Synopsis: Few packet drops are seen in Strict priority queue after Hot-Failover.

Release Note: When Strict Priority is enabled, a few packets may be dropped during Hot-Failover.

Workaround: None

PR# 57907

Severity: S2

Synopsis: Sometimes, after deleting and recreating a VLAN, OSPF NBR does not come up on it.

Release Note: Sometimes, after deleting and recreating a VLAN, OSPF NBR does not come up on it.

Workaround: Remove IP address and add IP address for the VLAN.

PR# 57945

Severity: S1

Synopsis: RP2 reset to recover from SWP timeout.

Release Note: The ACL agent on a line card experienced an SWP timeout, which triggered RP2 to reset to
                recover.

Workaround: None

PR# 58329

Severity: S3

Synopsis: The RP1 "5 second utilization" output may incorrectly display CPU utilization at 100%.

Release Note: The RP1 "5 second utilization" output may incorrectly display CPU utilization at 100%.

Workaround: None

PR# 58445

Severity: S3

Synopsis: RP1/RP2 send out packet with source ip address 0.0.0.0 for sometime when ip address is
                removed.

Release Note: RP1/RP2 may send out packet with source ip address 0.0.0.0 for a while when ip address is
                removed.

Workaround: None, system stops sending those packets after some time.

PR# 58456

Severity: S4

Synopsis: E300 RPM P/S indicator LED does not go out once P/S is extracted.

Release Note: E300 RPM P/S indicator LED does not go out once P/S is extracted.

Workaround: None

PR# 58458

Severity: S3

Synopsis: Incorrect MD5 authentication failure message for BGP is generated after RPM failover.

Release Note: Incorrect MD5 authentication failure message for BGP is printed after RPM failover.

Workaround: Ignore the message.

PR# 59454

Severity: S3

Synopsis: When a passive peer group session is configured with an MD5 password, authentication failures
                result and the BGP session does not come up.

Release Note: When a passive peer group session is configured with an MD5 password, authentication failures
                result and the BGP session never comes up.

Workaround: None

PR# 59786

Severity: S3

Synopsis: "BGP MD5 authentication failed" messages may be seen with established neighbors.

Release Note: "BGP MD5 authentication failed" messages may be seen with established neighbors.

Workaround: None. Ignore these error messages.

PR# 60270

Severity: S1

Synopsis: RP2 may crash because of loss of heartbeat between CP and RP2.

Release Note: RP2 may crash because of loss of heartbeat between CP and RP2.

Workaround: None

PR# 60311

Severity:	S3
Synopsis:	PEM down Alarm may not always generate.
Release Note:	PEM down Alarm may not always generate.
Workaround:	None, the correct status is displayed in show environment.

PR# 60381

Severity:	S2
Synopsis:	With half duplex mode, some ports on copper cards may have problems with transmitting packets.
Release Note:	In half duplex mode, the following ports may have excessive discards in transmit direction, due to collisions. The list of ports affected on the various cards are:

> E48TF - 1, 4, 10, 13, 16, 22, 25, 28, 34, 37, 40, 46
> E48TF1 - 1, 4, 10, 25, 28, 34; E48TF3 - 1, 4, 10, 25, 28, 34
> E90MF - 1, 4, 10, 25, 28, 34, 49, 52, 58, 70, 76

Workaround:	None. Avoid using these ports in half duplex mode.

PR# 60780

Severity:	S2
Synopsis:	XFP DWM : Ports take long time to come up after no shutdown, reset, reload (15 - 20 sec).
Release Note:	Ports take a long time (15 - 20 sec) to come up after no shutdown, reset, reload.
Workaround:	None

PR# 60784

Severity:	S3
Synopsis:	Phantom BGP neighbors which had been configured at one point in time w/ MD5 string will persistently output MD5 authentication message failures.
Release Note:	BGP neighbors which had been configured at one point in time w/ a MD5 string but had since been removed (i.e. phantom neighbors) will persistently output MD5 authentication message failures. Completely removing the BGP config and reapplying does not resolve the issue.
Workaround:	Reconfigure the BGP neighbor w/ its associated MD5 string and shut it down.

PR# 61149

Severity:	S2
Synopsis:	Inserting external flash device in a TeraScale RPM gave error message that "hot insertion failed" multiple times before it succeeded.
Release Note:	Inserting external flash device in a TeraScale RPM gave error message that "hot insertion failed" multiple times before it succeeded.
Workaround:	On an occasional board, a 1 in 10 insert failure is observed. To overcome: Try again.

PR# 61190

Severity: S2

Synopsis: On LC-EF-10GE-16P and LC-EF3-10GE-8P, when a port is in WAN mode and has an MTU >
5500, users may see CRC errors with traffic at or close to line rate.

Release Note: On LC-EF-10GE-16P and LC-EF3-10GE-8P, when a port is in WAN mode and has an MTU >
5500, users may see CRC errors with traffic at or close to line rate.

Workaround: 1) Reduce MTU to less than 5500
or
2) Set egress traffic shaping to 70% of line rate.

PR# 61269

Severity: S3

Synopsis: Running Config Shows "microcode default" When A Chassis Is Reloaded Without A
startup-config And With The IPv4-320k Profile.

Release Note: When a user changes the next boot cam-profile to IPv4-320k, copies the configuration to
NVRAM, deletes the startup-config and reloads, the running configuration shows - cam-profile
ipv4-320k microcode default instead of - cam-profile ipv4-320k microcode ipv4-320k.

Workaround: This bug does not affect functionality. To work around either do:

1. Do not delete startup-config after changing the next boot cam-profile to IPv4-320k.

or

2. Reconfigure the **cam-profile ipv4-320k microcode ipv4-320k** command after reload
to make sure the running-config has the right configuration statement.

PR# 61452

Severity: S3

Synopsis: Invalid MSS size advertised on BGP-MD5 (TeraScale)

Release Note: With MD5 enabled, an extra 18 bytes are not taken into account when computing MSS.

Workaround: lower IP mtu on interface

PR# 61459

Severity: S3

Synopsis: The ip unreachable functionality is not working for Layer 3 VLANs.

Release Note: The ip unreachable functionality is not working for Layer 3 VLANs. Traceroute messages will not
be generated.

Workaround: None. ip unreachable should be configured for traceroute to an ip address configured on F10
router to work.

PR# 61572

Severity: S3

Synopsis: SFM uptime resets after RPM failover

Release Note: SFM uptime may reset after RPM failover

Workaround: None

PR# 61757

Severity: S3

Synopsis: Duplicate IP address message is logged for management virtual ip address on RPM failover.

Release Note: Duplicate IP address message is printed for management virtual ip address on RPM failover
                  "%RPM0-P:CP %IP-4-DUPADDR: Duplicate IP address (A.B.C.D) sent from MAC address
                  xx:xx:xx:xx:xx:xx"

Workaround: None: Ignore the message

PR# 62194

Severity: S3

Synopsis: Ethernet-like interfaces should display the ifspeed value as the default speed when the interface
                  is down.

Release Note: Ethernet-like interfaces should display the ifspeed value as the default speed when the interface
                  is down. This currently holds true for fiber cards only.

Workaround: None

PR# 62494

Severity: S3

Synopsis: file system- while copying a file to ftp. providing an incorrect ip address, does not return error

Release Note: Error message is not given when hostname is not resolved for different applications e.g. ping,
                  logging, ftp etc.

Workaround: None

PR# 62523

Severity: S3

Synopsis: Management interface gets displayed occasionally while issuing show interfaces port-channel
                  brief command from multiple sessions.

Release Note: Management interface gets displayed occasionally while issuing show interfaces port-channel
                  brief command from multiple sessions.

Workaround: use show run interface port-channel <id> command

PR# 63206

Severity: S4

Synopsis: The output of show alarm/logs did not tally with the show chassis output with regards to PEM
                  status.

Release Note: Show alarms and logs displayed both PEMs as failed or removed.
                  JST: %RPM0-P:CP %CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module 0
                  JST: %RPM0-P:CP %CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module 1
                  JST: %RPM0-P:CP %CHMGR-5-PEM_OK: Major alarm cleared: power entry module 0 is good
                  JST: %RPM0-P:CP %CHMGR-5-PEM_OK: Major alarm cleared: power entry module 1 is good
                  Partial output of show alarms after four and six minutes are shown below
                      -- Major Alarms --
                      Alarm Type Duration

RPM 1 PEM 0 failed or rmvd 4 min

RPM 1 PEM 1 failed or rmvd 4 min

Alarm Type Duration

RPM 1 PEM 0 failed or rmvd 6 min

RPM 1 PEM 1 failed or rmvd 6 min

SWSN6#

But show chassis showed both PEMs as up.

Partial output of show chassis

-- Power Entry Modules --

Bay Status

----

0 up

1 up

Workaround:	None

PR# 63223

Severity:	S3
Synopsis:	Some log messages show interface numbers as normal numerical values rather than in slot/port format.
Release Note:	Some log messages show interface numbers as normal numerical values rather than in slot/port format. Example: #un 21 14:21:40 KST: %RPM0-P:RP1 %KERN-3-INT: giga138: arp: link address is broadcast for IP address 10.0.0.1! - repeated 3 times #Jun 21 14:21:40 KST: %RPM0-P:CP %ARP-4-BCASTMAC: MAC address is broadcast for IP address 10.0.0.1 - repeated 3 times #Jun 21 14:21:40 KST: %RPM0-P:RP2 %KERN-3-INT: giga138: arp: link address is broadcast for IP address 10.0.0.1! - repeated 3 times #Jun 21 14:20:08 KST: %RPM0-P:RP1 %KERN-3-INT: giga138: arp: link address is broadcast for IP address 10.0.0.1!
Workaround:	None

PR# 63334

Severity:	S4
Synopsis:	The output of 'show interface' for 1G port displays XFP information when the media type is unknown.
Release Note:	The output of 'show interfaces gigabitethernet slot/port-' displays ' XFP receive power reading is 0.0000' whenever the media type is 'unknown'. force10#sh int gi 0/23 GigabitEthernet 0/23 is up, line protocol is up Description: force10, gig 0/23, 1G trunk to force10-1:1/4, IT, cableid Hardware is Force10Eth, address is 00:01:e8:16:bf:85 Current address is 00:01:e8:16:bf:85 Pluggable media present, Media type is unknown Medium rate is unknown, XFP receive power reading is 0.0000 This occurs when SFPs not recommended by Force10 is used. To obtain a list of supported transceiver modules please visit http://www.force10networks.com/products/specifications.asp.
Workaround:	None

PR# 63359

Severity: S3

Synopsis: Upon catastrophic RPM failover there is a possibility of not seeing any traffic transiting the LAG.

Release Note: Upon catastrophic RPM failover there is a possibility of not seeing any traffic transiting the LAG.

Workaround: None

PR# 63662

Severity: S2

Synopsis: VRRP will preempt on reload of a system even if "no preempt" is enabled on port-channel interfaces, with SSH enabled.

Release Note: VRRP will preempt on reload of a system even if "no preempt" is enabled on port-channel interfaces, with SSH enabled.

Workaround: None

PR# 64041

Severity: S3

Synopsis: Different outputs from "show vlan" on active and standby RPM if the vlan status is 'inactive' on primary RPM.

Release Note: For the same VLAN whose status is shown as 'inactive' on the active RPM, the status on standby RPM is 'active'.

Workaround: None

PR# 64339

Severity: S2

Synopsis: Due to vendor misprogramming, FTOS is unable to read power levels from JDSU-sourced XFPs.

Release Note: Due to misprogramming by vendor, the power is incorrectly calculated.

Workaround: None

OSPF

PR# 59635

Severity: S1

Synopsis: Under stress condition with large OSPF and BGP configurations and flapping, the system may run out of memory.

Workaround: None

PR# 58706

Severity: S3

Synopsis: When static routes configured with Null 0 interface are redistributed into OSPF, the expected LSA translation does not take place.

Release Note: When a F10 acting as an ASBR has static routes pointed at a Null0 interface, redistribution into OSPF results in improper LSA type translation.

Workaround: If possible, point static route out of a legitimate physical interface w/ associated IP; otherwise there is no workaround.

PR# 60134

Severity: S3

Synopsis: The route learned from IA and E1 removed in the routing table from time to time.

Release Note: After a network statement (s) with area removed from router ospf, the area becomes un-used area stays in ospf and still participate the SPF calculation, which causes all IA and E1 removed in the routing table once SPF calculation occurs. (ABR becomes Backbone router as a good example).

Workaround: There are three workarounds:

      1.) simply remove the unused area from router ospf (no area <ID).

      2.) execute "**no router ospf** *processID* and add it back.

      3.) Reload the router.

PR# 60175

Severity: S3

Synopsis: OSPF convergence may take prolonged period of time after unconfiguring/reconfigure multicast routing.

Release Note: OSPF convergence may take an excessive amount of time to converge after removing multicast routing from a config after the F10 chassis has been heavily loaded with multicast.

Workaround: None

PR# 60640

Severity: S3

Synopsis: If a port-channel member is removed or added, then OSPF should not send Router LSA as update.

Release Note: If a port-channel member is removed or added, then OSPF should not send Router LSA as update.

Workaround: None

PR# 61743

Severity: S1

Synopsis: OSPF task may crash with multiple md5 keys or repeated addition and deletion of keys.

Release Note: OSPF task may crash with multiple md5 keys or repeated addition and deletion of keys.

Workaround: None

PIM

PR# 47552

Severity: S2

Synopsis: mtrace may not work as expected.

Release Note: mtrace may not work as expected.

Workaround: None

PR# 56238

Severity: S2

Synopsis: interface is missing from oil of SG entry present in *G entry.

Release Note: Using the as-path information of routes to determine peer-RPF neighbor (RFC3618), is not supported.

Workaround: Allow the MSDP topology mirror the (m)BGP topology and make sure that MSDP peer address is the same as (m)BGP peer address.

PR# 58240

Severity: S1

Synopsis: PIM task crashed while enabling debugging for MSDP and PIM.

Release Note: PIM task crashed while enabling debugging for MSDP and PIM.

Workaround: None

PR# 60738

Severity: S3

Synopsis: NF-PIM-DM: "show ip pim tib" displays the uptime as 1882w0d, after stopping all data traffic and reports from the igmp hosts.

Release Note: Intermittently, **show ip pim tib** displays the uptime as 1882w0d.

Workaround: The **clear ip pim tib** command will clear the TIB.

PR# 60792

Severity: S2

Synopsis: Interface may remains in "Forward" state when Force10 is the assert winner and the assert loser is Cisco or Juniper.

Release Note: Interface remains in "Forward" state for assert winner, even after another router on the same link that loses assert on the link. This is seen for interfaces with a Cisco or Juniper neighbor. This problem happens when there is an assert between Cisco and Force10 on the same link. The draft says " Receive Preferred Assert or State Refresh". The received Assert or State Refresh has a better metric than this router's, and therefore the Assert state machine MUST transition to the "I am Assert Loser" state and store the Assert Winner's address and metric. If CouldAssert(S,G,I) == TRUE, the router MUST also multicast a Prune(S,G) to the Assert winner with a Prune Hold Time equal to the Assert Timer and evaluate any changes in its Upstream(S,G) state machine. " However, we do not see the cisco router sending out a prune msg on the Lost Assert interface. It puts the interface in the pruned list though.

Workaround: None

PR# 62114

Severity: S2

Synopsis: Show ip pim interface displays deleted VLANs in the output

Release Note: Show ip pim interface displays deleted VLANs in the output

Workaround: Ignore the deleted VLANs.

PR# 62184

Severity: S2

Synopsis: PIM may not install some of the SA entries learned from MSDP.

Release Note: PIM may not install some of the SA entries learned from MSDP

Workaround: Clear ip msdp sa-cache

PR# 62492

Severity: S1

Synopsis: RP2 may crash while switching over between PIM-SM and PIM-DM.

Release Note: If configurations on interfaces are configured back and forth between PIM-SM and PIM-DM, RP2 may crash.

Workaround: None

PR# 63166

Severity: S3

Synopsis: For PIM-SM there is a delay of 1.6s for joining a Multicast group and 2.5s for leaving a Multicast group.

Release Note: IF PIM-SM is configured and a host sends join request for a MC group, there is a delay of about 1.6s after which host starts receiving packets from the MC group. Similarly for leave, there is delay of about 2.5s.

Workaround: None

Port Mirroring

PR# 60079

Severity: S3

Synopsis: %RPM0-P:CP %SWP-2-NO MORE TIMEOUT: SWP: swpTimeoutCB: queue 24, portmirr0 to aclAgent0, timeouts used: 11, timeout limit: 10

Release Note: When the linecard is down and port-mirroring is configured, there may be SWP timeout messages between the port-mirroring and ACL tasks.

Workaround: These messages can be ignored as functionality is not affected.

PVST

PR# 47135

Severity: S3

Synopsis: PVST does not converge when more than 70 VLAN interfaces are created with redundant interfaces.

Release Note: PVST does not converge when more than 70 VLAN interfaces are created with redundant interfaces.

Workaround: None

PR# 63426

Severity: S3

Synopsis: Output of "show spanning-tree pvst vlan <vlan-id>" shows incorrect Designated Port ID

Release Note: Output of "show spanning-tree pvst vlan <vlan-id>" shows incorrect Designated Port ID

Workaround: Use the command show spanning-tree pvst vlan <vlan-id> brief" to show the correct Designated Port ID

QoS

PR# 47533

Severity: S2

Synopsis: A PBR rule can potentially redirect Protocol traffic destined to the F10 to get redirected out the incorrect interface.

Release Note: PBR applied on interface potentially redirect the protocols multicast control traffic destined to the switch out of the wrong interface. As a result, the protocol's adjacencies may not come up.This is when "any" keyword is used as destination prefix.

Workaround: None

PR# 55971

Severity: S2

Synopsis: With rate police policy-aggregate applied to an interface, arp entry for the interface maybe missing in RP2 after "clear arp-cache".

Release Note: Upon executing the **clear arp-cache** command, ARP information may be missing from RP2 on an interface with aggregate input policy configured.

Workaround: Unconfigure and then re-configure the policy.

PR# 56752

Severity: S3

Synopsis: If CAM is in middle of updating and RPM failover happens, CAM will not finish the remaining updates.

Release Note: CAM will stop updating if RPM failover happens while CAM is updating.

Workaround: After failover, remove and re-configure service-policy under interfaces.

PR# 56770

Severity: S2

Synopsis: A rate-shape value may not take effect if a greater rate-limit value is already configured.

Release Note: A rate-shape value may not take effect if a greater rate-limit value is already configured.

Workaround: Configure the rate shape first.

PR# 56805

Severity: S2

Synopsis: An output service policy, having aggregate and per-queue rate limit, may not take effect if an output policy with bandwidth was already applied.

Release Note: An output service policy, having aggregate and per-queue rate limit, may not take effect if an output policy with bandwidth was already applied.

Workaround: Unconfigure the output service policy and configure it again.

PR# 59827

Severity: S3

Synopsis: Clear qos statistics will not clear the counters during CAM updation.

Release Note: Clear qos statistics may not clear QoS statistics during CAM updation.

Workaround: Issue the "clear qos statistics" command after CAM updation is done.

PR# 59829

Severity: S3

Synopsis: Input and output qos-policies and output policy-map may not take effect, when CAM updation is in progress.

Release Note: While CAM update is in progress with loading QoS ACL, input and output qos-policies and output policy-map may not take effect.

Workaround: Will take effect after CAM update is done.

PR# 59947

Severity: S2

Synopsis: No rules will be installed in the QoS CAM if the rules to be installed per port-pipe is greater than 30k.

Release Note: When input service-policy is applied on interfaces, if more rules are added to ACL, none of the rules are installed in the QoS CAM if the rules to be installed per port-pipe is greater than 30k.

Workaround: Remove and add service-policy on interfaces.

PR# 60019

Severity: S3

Synopsis: May see "No response from linecard 3" message when ACL rules > QoS CAM size are pushed.

Release Note: "No response from linecard 3" might display when rules > QoS CAM size are pushed.

Workaround: Ignore the message; it doesn't affect the functionality.

PR# 61426

Severity: S2

Synopsis: The "storm-control unknown-unicast" command will rate limit the L2 IP multicast traffic

Release Note: The **storm-control unknown-unicast** command will rate limit the L2 IP multicast traffic

Workaround: Turn on igmp snooping if possible.

RMON

PR# 58447

Severity: S3

Synopsis: A large rmon alarm config causes CPU utilization of the rmon task to go up to 50%.

Release Note: Large RMON configuration (of the order of several thousand) can lead to non-trivial (>50%) CP CPU utilization.

Workaround: None

RTM

PR# 43904

Severity: SS2

Synopsis: Not all BGP routes are showing up in RTM after multiple consecutive **clear ip ro** *

Release Note: When you do consecutive **clear ip ro** *, all BGP routes don't show up in RTM

Workaround: Wait until the network converges and re-issue one **clear ip ro** * again.

PR# 47536

Severity: S4

Synopsis: RTM reports bad gateway error message when a static route is configured and redistributed into BGP after clearing the routes and bgp sessions.

Release Note: RTM reports bad gateway error message when a static route is configured and redistributed into BGP after clearing the routes and bgp sessions.

Workaround: None

PR# 58353

Severity: S2

Synopsis: "clear ip bgp *" in an out of memory condition may cause a software crash.

Release Note: Executing a **clear ip bgp** * in an out of memory condition may cause a software crash.

Workaround: None

PR# 58840

Severity:	S2
Synopsis:	SNMP OID ".1.3.6.1.2.1.4.24.4.1.4" is not handled properly for ECMP next-hops. For static routes having ECMP Next-Hops, only 1 Next-Hop is sent in response to SNMP query. For default route ECMP, only 3 Next-Hops are sent in response to SNMP query. For non-default route ECMP case, only first 12 Next-Hops are sent in response to SNMP query.
Release Note:	SNMP OID ".1.3.6.1.2.1.4.24.4.1.4" is not handled properly for ECMP next-hops. For static routes having ECMP Next-Hops, only 1 Next-Hop is sent in response to the SNMP query. For default route ECMP, only 3 Next-Hops are sent in response to SNMP query. For non-default route ECMP case, only first 12 Next-Hops are sent in response to SNMP query.
Workaround:	None

PR# 61508

Severity:	S3
Synopsis:	concurrent 'clear ip fib' on multiple line cards may result in RTM/FIB out of sync.
Release Note:	If 'clear ip fib' is issued on multiple line cards at the same time, the FIB databases across line cards may not be in sync with RTM (Route Table Manager).
Workaround:	Wait for FIB to synchronize on one linecard before clearing another.

sFlow

PR# 60324

Severity:	S1
Synopsis:	SfLp task may crash on LC-EF-10GE-4P
Release Note:	SfLp task crashed on LC-EF-10GE-4P.
Workaround:	None. The line card will reset itself. Please contact TAC if this issue is seen.

PR# 62409

Severity:	S3
Synopsis:	After LC replacement inbound sFlow traffic stats not being reported to data collection tool.
Release Note:	After replacement of a faulty LC, the input traffic data for the LC ports in production was not getting propagated to the offline software.
Workaround:	Hard resetting the line card, or powering it off and back on, resolves the issue.

SNMP

PR# 57569

Severity:	S3
Synopsis:	TeraScale 10GE Linecard with WAN port configured do not generate alarms/SNMP traps for SONET alarms.
Release Note:	TeraScale 10GE line card with WAN port configured does not generate alarms/SNMP traps for SONET alarms.
Workaround:	None

PR# 60407

Severity: S4

Synopsis: Cannot selectively enable generic trap types with the "snmp-server enable traps snmp" command, once "snmp authentication" has been enabled.

Release Note: Cannot selectively enable generic trap types with the **snmp-server enable traps snmp** command, once "snmp authentication" has been enabled.

> Force10(conf)#do sh run snmp
>
> !
>
> snmp-server community xxx ro
>
> snmp-server contact "xxx"
>
> snmp-server enable traps bgp
>
> snmp-server enable traps snmp authentication coldstart linkdown linkup
>
> snmp-server enable traps envmon fan supply temperature
>
> snmp-server location "xxx"
>
> From this point forward no matter what combination is used all options are added to "traps snmp..."
>
> Force10(conf)#no snmp-server enable traps snmp authentication coldstart linkdown linkup
>
> Force10(conf)#
>
> Force10(conf)#do sh run snmp
>
> !
>
> snmp-server community xxx ro
>
> snmp-server contact "xxx"
>
> snmp-server enable traps bgp
>
> snmp-server enable traps envmon fan supply temperature
>
> snmp-server location "xxx"
>
> Force10(conf)#
>
> Re-added "traps snmp..." with only "coldstart"
>
> Force10(conf)#snmp-server enable traps snmp coldstart
>
> Force10(conf)#
>
> Force10(conf)#do sh run snmp
>
> !
>
> snmp-server community xxx ro
>
> snmp-server contact "xxx"
>
> snmp-server enable traps bgp
>
> snmp-server enable traps snmp authentication coldstart linkdown linkup
>
> snmp-server enable traps envmon fan supply temperature
>
> snmp-server location "xxx"
>
> Force10(conf)#

Workaround: Use the **no snmp-server enable traps snmp** [*notification-option*] command to disable generic trap types.

> Force10(conf)#do sh run snmp
>
> !
>
> snmp-server community xxx ro

```
                    snmp-server contact "xxx"
                    snmp-server enable traps bgp
                    snmp-server enable traps snmp authentication coldstart linkdown linkup
                    snmp-server enable traps envmon fan supply temperature
                    snmp-server location "xxx"
                    Force10(conf)#
                    Force10(conf)#no snmp-server enable traps snmp authentication
                    Force10(conf)#
                    Force10(conf)#do sh run snmp
                    !
                    snmp-server community xxx ro
                    snmp-server contact "xxx"
                    snmp-server enable traps bgp
                    snmp-server enable traps snmp coldstart linkdown linkup
                    snmp-server enable traps envmon fan supply temperature
                    snmp-server location "xxx"
                    Force10(conf)#
```

PR# 63083

Severity:	S4
Synopsis:	dot1dTpFdbTable should report on MAC addresses learned on default as well as non-default VLANs.
Release Note:	dot1dTpFdbTable currently reports the MAC addresses learned on default VLANs. It does not report on MAC addresses learned on non-default VLANs
Workaround:	To obtain MAC addresses learned by non default VLANs use dot1qTpFdbPort(1.3.6.1.2.1.17.7.1.2.2.1.2).

PR# 64130

Severity:	S3
Synopsis:	'snmp walk' on RPM Memory Usage doesn't show RP1 and RP2 value in % rather shows entire current Used value
Release Note:	>snmpwalk -v 2c -c test 10.16.128.171 1.3.6.1.4.1.6027.3.1.1.3.7.1.6
	SNMPv2-SMI::enterprises.6027.3.1.1.3.7.1.6.1 = INTEGER: 13
	SNMPv2-SMI::enterprises.6027.3.1.1.3.7.1.6.2 = INTEGER: 120827904
	SNMPv2-SMI::enterprises.6027.3.1.1.3.7.1.6.3 = INTEGER: 149573632
	memory usage value on RP1 and RP2 for RPM's doesn't show in percentage(%) but shows the entire Current Used value.
Workaround:	None

Spanning Tree

PR# 41689

Severity: S2

Synopsis: Root bridge cost changes (to depreference root) can cause transient MSTP loops.

Release Note: In a "triangle" switch topology (i.e. two core switches — with one acting as root and one secondary — with access switches connected to each core) changing the cost of the root switch to depreference may cause access switches from third-party vendors to go into a designated forwarding state. This transient designated forwarding state can cause temporary loops in an MSTP topology.

Workaround: None

SSH

PR# 60103

Severity: S3

Synopsis: sh lc console disconnects ssh session with bad packet length.

Release Note: The **show lc console** command will disconnect an SSH session.

Workaround: None

PR# 62544

Severity: S1

Synopsis: ssh task may crash trying to access an invalid channel leading to an RPM failover

Release Note: SSH task may crash trying to access an invalid channel, leading to an RPM failover.

Workaround:

Telnet

PR# 58012

Severity: S4

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

Release Note: 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 another vertical length.

PR# 65131

Severity: S2

Synopsis: Telnet sessions may remain open, but inaccessible, when TACACS is enabled.

Release Note: Telnet session does not exit cleanly in certain scenarios with TACACS authentication enabled. If there are frequent connectivity issues with the TACACS server, it may result in the telnet sessions being always open, but not accessible. In this scenario, we are left with fewer active VTY lines.

Workaround: Remove the TACACS configuration and reconfigure.

PR# 65261

Severity: S3

Synopsis: CLI task is stuck at 99%, though the VTY session has cleared out on the system.

Release Note: CLI task is stuck at 99%, though the VTY session has cleared out on the system.

Workaround: None

VLAN Stack

PR# 44901

Severity: S2

Synopsis: MSTP BPDUs are not tunnelled across VMAN even though MSTP is disabled on the chassis.

Release Note: Spanning Tree BPDUs (STP/RSTP/MSTP) are not tunnelled across VMAN even though Spanning Tree Protocol is disabled on the chassis.

Workaround: Disable and then enable the port.

VRRP

PR# 56618

Severity: S3

Synopsis: When VRRP group is deleted, static arp for the deleted group's virtual address is not re-installed.

Release Note: When a VRRP group is deleted, static ARP for the deleted group's virtual address is not re-installed.

Workaround: None

Open Software Caveats (EtherScale)

ARP (EtherScale)

PR# 59514

Severity:	S2
Synopsis:	Some ARPs/Routes do not get loaded to linecards
Release Note:	When a chassis boots up with a large number of ARPs in the local networks with a large number of line cards present, some ARPs may not be loaded into the linecard FIBs.
Workaround:	The **no arp ip** *ip-address* command will cause individual ARPs to get loaded into the FIBs, and resetting each line card one at a time will get all ARPs loaded into the FIB.

BGP (EtherScale)

PR# 56659

Severity:	S2
Synopsis:	"Show ip bgp regexp" and "Show ip bgp filter-list" may take up 99% CPU and may time out.
Release Note:	The commands **show ip bgp regexp** and **show ip bgp filter-list** may take up 99% CPU and may time out.
Workaround:	None

PR# 59000

Severity:	S2
Synopsis:	"show ip bgp regexp" may cause high CPU utilization that results in CLI timeout.
Release Note:	The command **show ip bgp regexp** may cause high CPU utilization that results in CLI timeout.
Workaround:	None

PR# 60077

Severity:	S1
Synopsis:	Out of memory on CP can lead to task crash with 250+ bgp neighbors.
Release Note:	Out of memory on CP can lead to task crash with 250+ BGP neighbors.
Workaround:	None

PR# 60322

Severity: S3

Synopsis: Initial misconfiguration of MD5 string between BGP peers may lead to persistent authentication failure messages.

Release Note: If the BGP MD5 string is misconfigured between two BGP peers and then the interface later shutdown and/or removed on the E-series, the following message will persist asserting in the logs-: %RPM0-P:RP1 %KERN-6-INT: BGP md5 authentication failed from a.b.c.d:10000 to w.x.y.z:179

Workaround: Ensure remote peer removes their misconfigured session and rebuild it with the appropriate MD5 string, or have the BGP session deleted from peer box if no longer needed.

PR# 60354

Severity: S3

Synopsis: BGP hidden password option does not work if the password is clear text and less than 16 characters. If hidden password option is selected on one end and configured password is less than 16 characters, the bgp session will be authenticated even if there is no password configured on other end.

Release Note: BGP hidden password option does not work if the password is clear text and less than 16 characters. If hidden password option is selected on one end and configured password is less than 16 characters, the bgp session will be authenticated even if there is no password configured on other end.

Workaround: Use encrypted password to authenticate the peers.

PR# 60322

Severity: S3

Synopsis: Initial misconfiguration of MD5 string between BGP peers may lead to persistent authentication failure messages.

Release Note: When the BGP MD5 string is misconfigured between two BGP peers and then the interface later shut down and/or was removed on the E-series, the following message will persist asserting in the logs:

    %RPM0-P:RP1 %KERN-6-INT: BGP md5 authentication failed from a.b.c.d:10000 to w.x.y.z:179

Workaround: Ensure remote peer removes their misconfigured session and rebuild it with the appropriate MD5 string, or have the BGP session deleted from peer box if no longer needed.

PR# 63638

Severity: S3

Synopsis: as-path access-list regexp expects alphanumeric after OR (pipe |)

Release Note: Using | in regexp expects alphanumeric or whitespace to follow. Else syntax is rejected: Force10(config-as-path)# permit ^123(456|)$ % Error: Input string is not a regular expression.

Workaround: Break OR into two statements
    Force10(config-as-path)# permit ^123 456$
    Force10(config-as-path)# permit ^123$

PR# 64109

Severity: S3

Synopsis: show ip bgp <prefix>" shows peer group names, as well as some peers that are actually
                      members of the peer groups displayed already.

Release Note: The outputs of the command "show ip bgp <prefix>" has a section "advertised to". This section
                      should show peer-groups and individual neighbors (which don't belong to a peer-group), to which
                      this prefix is advertised to. It has been noticed that sometimes, this output lists some individual
                      neighbors, which already belong to a peer group. The output would then contain the peer-group
                      names, as well as some peers that are actually members of the peer groups already displayed.

Workaround: None

PR# 64299

Severity: S2

Synopsis: The BGP task "bgpRibupd" reaches CPU utilization of nearly 100% with a number of AS-path lists
                      with a lot of regular expression matches embedded.

Release Note: he BGP task "bgpRibupd" reaches CPU utilization of nearly 100% with a number of AS-path lists
                      with a lot of regular expression matches embedded. This regex evaluation takes too much CPU,
                      especially when large amount of paths need to matched.

Workaround: None

CLI (EtherScale)

PR# 57454

Severity: S3

Synopsis: "Login successful for user on line aux" is displayed on new primary (after failover), even though
                      there is no connection to aux port.

Release Note: "`Login successful for user on line aux`" is displaying on new primary after failover, even
                      though there is no connection to aux port.

Workaround: None

PR# 59468

Severity: S2

Synopsis: Console session hangs after telnet sessions hang and 'no ip telnet server enable' toggled.

Release Note: When telnet sessions hang, accessing the E-series via console and proceeding to execute a 'no
                      ip telnet server enable' can result in a console lockup as well as a CPU spike.

Workaround: None

PR# 60104

Severity: S4

Synopsis: NTP server is not converted to IP address in configuration file.

Release Note: The configuration command "ntp server {hostname}" saves the command with the hostname, rather than converting to IP address in the configuration file. This is inconsistent with other configuration commands that reference server names.

Workaround: None

PR# 60330

Severity: S4

Synopsis: Terminal length inconsistency with lines greater than terminal width.

Release Note: Pagination does not take into account wrapped lines.

Workaround: None

PR# 60667

Severity: S3

Synopsis: No login/motd Banner Message shows up after SSH to the switch.

Release Note: No login/motd Banner Message shows up after SSH to the switch.

Workaround: None

PR# 62631

Severity: S4

Synopsis: CLI command following a "!" still takes effect

Release Note: CLI command following a "!" is not commented out. The command will still taike effect.

Workaround: None

PR# 63894

Severity: S3

Synopsis: A '?" in startup-config does not get applied to running config

Release Note: A question mark in startup configuration will not get applied to running configuration correctly after a reload.

   Force10#sho run as-path test

   !

   ip as-path access-list test permit 1?$ deny .*

will change to the following on reload:

   ip as-path access-list test deny.*

Workaround: use {0,1} instead of ?

Control Plane (EtherScale)

PR# 59526

Severity:	S2
Synopsis:	A Loopback ACL with "log" may let packets through.
Release Note:	A Loopback ACL with "log" may let packets through.
Workaround:	Do not use the "log" attribute for a Loopback ACL.

FIB (EtherScale)

PR# 47504

Severity:	S3
Synopsis:	CAM full messages are not printed (6.3.1.2 or later).
Release Note:	CAM full messages for L3 FIB are not logged (builds 6.3.1.2 and later).
Workaround:	Use **show ip fib linecard slot summary** and **show ip cam linecard** *slot* **port-set 0/1** command to verify.

PR# 57510

Severity:	S3
Synopsis:	"Show process memory lp" command shows incorrect memory utilization for the FA task.
Release Note:	In the output from the "**show process memory lp**" command, the FA process is shown utilizing more memory than it is.
Workaround:	None

PR# 61891

Severity:	S2
Synopsis:	FIB may fail to update NH information after counter wraps with large number of unresolved recursive NHs.
Release Note:	Under rare circumstances with a large number of recursive, yet eventually unresolved next-hops, an internal variable will increase in orders of magnitude faster than normal. Eventually, this counter may wrap, at which point, the FIB is unable to update NH information.
Workaround:	Hard reset the specific linecard with the command **reset linecard <#> hard**.

FTP (EtherScale)

PR# 63388

Severity:	S3
Synopsis:	Able to access all files under the flash even though "ftp topdir" is not configured after ftped into system.
Release Note:	Able to access all files under the flash even though "ftp topdir" is not configured.
Workaround:	None

FTSA (EtherScale)

PR# 57332

Severity: S3

Synopsis: callhome will stop sending messages after hitless upgrade.

Release Note: The Call Home (FTSA) service will stop sending messages after a hitless upgrade.

Workaround: None

IGMP (EtherScale)

PR# 44218

Severity: S2

Synopsis: General Query is not sent out of the Root port after MSTP Topology change.

Release Note: General Query is not sent out of the MSTP Root port after a Topology change in the network. The effect is that multicast traffic receiver will not receive traffic for the time-interval equal to the IGMP Query interval configured on the IGMP Querier.

Workaround: None

PR# 57349

Severity: S3

Synopsis: With IGMP Snooping enabled, the debug ip igmp interface command for physical interface does not show incoming and outgoing general queries for that interface.

Release Note: With IGMP snooping enabled, "debug ip igmp interface" command for physical interface does not show incoming and outgoing general queries for that interface.

Workaround: Use **debug ip igmp vlan** command for the general queries.

PR# 58528

Severity: S2

Synopsis: IGMP snooping enabled switch does not detect PIM router which is not a IGMP querier.

Release Note: If there is more than one PIM router on a VLAN, F10 detects only the port connected to the IGMP querier router as the multicast router port. It does not detect non-querier routers.

Workaround: Use the "ip igmp snooping mrouter interface" command in VLAN context to add all multicast router ports.

IPv4 (EtherScale)

PR# 56335

Severity: S3

Synopsis: 'Debug ip packet' does not show the forwarded packets unless explicitly configured on the ingress port.

Release Note: 'Debug ip packet' does not show the forwarded packets unless explicitly configured on the ingress port.

Workaround: Enable **debug ip packet** on the ingress interface of the chassis.

PR# 57757

Severity: S2

Synopsis: With IGMP snooping enabled, 200 groups joined in one vlan can cause a memory leak.

Release Note: With IGMP snooping enabled, 200 groups joined in one VLAN can cause a memory leak.

Workaround: None

ISIS (EtherScale)

PR# 57491

Severity: S3

Synopsis: When there are a large number of LSPs in the database, show isis database on SSH session is not returning any output.

Release Note: When there are large number of LSPs in the database, show isis database on SSH session is not returning any output

Workaround: Use either console or Telnet.

Layer 2 (EtherScale)

PR# 56903

Severity: S2

Synopsis: STP BPDU entries are improperly installed in the L2 CAM.

Release Note: Extra STP Entries can end up being installed in the Layer 2 CAM.

Workaround: None. These entries should not affect any feature functionality or data traffic.

PR# 57371

Severity: S1

Synopsis: Mac Manager & L2PM report out of memory and RP2 stops responding with 4K VLANs

Release Note: With Spanning tree (STP/MSTP/RSTP/PVST) enabled, adding interfaces to a large number of vlans using the **vlan range** command is currently not supported

Workaround: Add interfaces to the VLANs individually.

Layer 2 ACL (EtherScale)

PR# 56866

Severity: S2

Synopsis: No option available to delete a mac access-group for a vlan

Release Note: A MAC ACL cannot be deleted per VLAN if it was applied for multiple VLANs on an interface.

Workaround: Reapply the required VLANs.

PR# 57660

Severity: S4

Synopsis: When the port channel is not created, "show mac accounting access-list" for that port channel, gives an incorrect error message.

Release Note: If an access list is created but not a port channel, "show mac accounting accesslist [name] int po [#] in" gives an incorrect error message saying that the access list does not exist.

Workaround: None

Layer 3 ACL (EtherScale)

PR# 57448

Severity: S2

Synopsis: If, a L2 interface and a vlan has access-lists applied to it and subsequently, interface is made a member of vlan, it is allowed.

Release Note: If a Layer 2 interface and a VLAN has access lists applied to them, and subsequently, the interface is made a member of a VLAN, it is allowed.

Workaround: Add the interface to the VLAN before applying the access list.

PR# 58950

Severity: S3

Synopsis: With inverse-mask enabled, non-contiguous mask check functionality without "bitmask" keyword in prefix-list is broken.

Release Note: With inverse-mask enabled, non-contiguous mask with "bitmask" does not work.

Workaround: Do not enable inverse-mask when non-contiguous mask is used.

PR# 60143

Severity: S2

Synopsis: rapid and repeated egress ACL configuration can lead to acl_1 task withholding memory.

Release Note: rapid and repeated egress ACL configuration can lead to acl_1 task withholding memory on RP1.

Workaround: None

PR# 60256

Severity: S3

Synopsis: Cosmetic issue of CAM Full Messages could appear after adding one more ACL.

Release Note: Cosmetic issue of CAM Full Messages after adding one more ACL, even if there is free CAM mem (12K by default) for L3ACL. It will show CAM Full message and this only happens if the added ACL Seq number is less than 10. But the added ACL will still work.

> Force10(config-ext-nacl)#seq 4 permit ip any 6.5.0.0/24 log count
> Force10(config-ext-nacl)#May 18 10:45:13.20: %E48TF3:3
> %ACL_AGENT-2-ACL_CAM_FULL: L3Acl Cam is Full.

Workaround: Ignore the CAM full message, and run show ip accounting access-list to make sure the ACL is the there.

Logging (EtherScale)

PR# 64352

Severity: S4

Synopsis: Timestamp of running config, seen under block sync, does not get updated after a write memory.

Release Note: The 'write memory' should update the timestamp on both startup config and running config. The 'show redundancy' has a field 'last data block sync record' which has the timestamps of both these configs, at last sync. The timestamp for startup config is updated but running config is not.

Workaround: startup config timestamp could be checked to see the time of last sync.

MSDP (EtherScale)

PR# 47323

Severity: S2

Synopsis: SA-Filters are not working under MSDP.

Release Note: SA-Filters do not work for MSDP

Workaround: None

PR# 56328

Severity: S2

Synopsis: FTOS doesn't support using the as-path information of routes to determine peer-RPF neighbor.

Release Note: FTOS doesn't support using the as-path information of routes to determine peer-RPF neighbor, which is described in item IV of section 10.1.3 "Peer-RPF Forwarding Rules" of RFC3618.

Workaround: Let the MSDP topology mirror the (m)BGP topology and make sure that MSDP peer address is the same as the (m)BGP peer address.

PR# 56828

Severity: S2

Synopsis: Prefix-list doesn't work for MSDP default peer.

Release Note: SA filtering for default peer using prefix-list does not work.

Workaround: None

PR# 57270

Severity: S2

Synopsis: 'Clear ip msdp sa-cache' sometimes fails to reconcile entries between pim and msdp.

Release Note: The command **clear ip msdp sa-cache** does not resolve out-of-sync problems between PIM and MSDP.

Workaround: None

PR# 59923

Severity: S2

Synopsis: MSDP will not update the existing SA entry if it receives the same SA entry from a different peer.

Release Note: MSDP will not update the existing SA entry if it receives the same SA entry from a different peer.

Workaround: Use the command "clear ip msdp sa-cache" to clear the SA entry.

Multicast (EtherScale)

PR# 41519

Severity: S3

Synopsis: SPT switchover still happened even when the traffic rate was below the threshold

Release Note: SPT switchover may happen immediately after clear ip mroute * or clear ip pim tib regardless of configured switchover threshold.

Workaround: None

PR# 41916

Severity: S3

Synopsis: mtrace doesn't have a complete trace output after static mroute is added in certain scenarios.

Release Note: mtrace doesn't have a complete trace output after static mroute is added in certain scenarios.

Workaround: None

PR# 44746

Severity: S2

Synopsis: 'Show ip rpf' does not show the correct Route/Mask info if route is learnt via BGP.

Release Note: The command show ip rpf may not show correct RPF neighbor for recursive BGP routes.

Workaround: None

PR# 47404

Severity: S2

Synopsis: The number of multicast entries supported in FTOS is limited to 15000.

Release Note: The number of multicast entries supported in FTOS is limited to 15000.

Workaround: None

PR# 47461

Severity: S2

Synopsis: mtrace may not work as expected.

Release Note: mtrace may not work as expected.

Workaround: None

PR# 47927

Severity: S2

Synopsis: CPU is receiving excessive control plane traffic: traffic will be rate controlled messages may be seen with multicast forwarding

Release Note: CPU is receiving excessive control plane traffic: traffic will be rate controlled messages may be seen with multicast forwarding.

Workaround: None

PR# 57975

Severity: S3

Synopsis: Reverse Path Forwarding (RPF) check algorithm needs to be retuned.

Release Note: Currently, the FTOS algortihm performs an RPF check based on longest match and distance, as opposed to mstatic/mbgp/unicast rib.

Workaround: None

PR# 58508

Severity: S2

Synopsis: When PIM is enabled on a VLAN, IGMP reports are not forwarded to another PIM router on the VLAN. If F10 is not the PIM-DR, then forwarding to that receiver won't work.

Release Note: When PIM is enabled on a VLAN, IGMP reports are not forwarded to another PIM router on the VLAN. If F10 is not the PIM-DR, then forwarding to that receiver won't work

Workaround: Configure only one PIM router per VLAN. If more than one PIM router is to be configured, enable IGMP Snooping on the VLAN and configure mrouter ports using the **ip igmp snooping mrouter interface** command in VLAN context.

PR# 59497

Severity: S3

Synopsis: The command **show ip msdp sa-cache** *group* doesn't display all the relevant SA entries

Release Note: The command **show ip msdp sa-cache** *group* only displays a subset of the nominal list of entries when executed.

Workaround: None

PR# 60174

Severity: S3

Synopsis: Stale multicast entries reside in CAM upon unconfiguring and reconfigure multicast routing.

Release Note: On a F10 system heavily loaded (i.e w/ CPU load > 75%)with multicast traffic unconfiguring and reconfigure multicast routing may result in stale multicast entries remaining in the CAM.

Workaround: Reduce the likelihood of high CPU load due to multicast (e.g. increase IGMP query interval, statically configure multicast groups that experience excessive amounts of join/leaves).

NTP (EtherScale)

PR# 56256

Severity: S4

Synopsis: ntp port(123) should be closed when ntp is not configured.

Release Note: ntp port(123) should be closed when ntp is not configured.

Workaround: None

OS / OS Infrastructure (EtherScale)

PR# 45203

Severity: SS4

Synopsis: If both ends of the copper link are configured with same forced master or slave settings flapping may occur.

Release Note: If both ends of copper links are configured with "mode forced-master" or "mode forced-slave", the "show interface" command will flap between "Auto-neg-Error" and forced-master/slave states.

Workaround: Reconfigure only one end of a connection to be "mode forced-master" or "mode forced-slave".

PR# 47319

Severity: S3

Synopsis: Output Unicast counters in the show interface command might give a large incorrect value, when there is output Multicast or output broadcast traffic.

Release Note: Output Unicast counters in the show interface command might give a large incorrect value, when there is output Multicast or output broadcast traffic.

Workaround: Clear counters

PR# 48038

Severity:	S2
Synopsis:	IPC receive fail error when LAG port is deleted in inter-vlan scenario %RPM0-P:RP2 %IPMGR-3-DEL_INT_RB: IPM2: Interface(0x4207802b) delete Error.
Release Note:	IPC receive fail error when LAG port is deleted in inter-vlan scenario %RPM0-P:RP2 %IPMGR-3-DEL_INT_RB: IPM2: Interface(0x4207802b) delete Error.
Workaround:	None

PR# 48060

Severity:	S3
Synopsis:	You may encounter message "Error while getting Peer Ip for MSDP rc is 0 While configuring MSDP".
Release Note:	You may encounter the message "`Error while getting Peer Ip for MSDP rc is 0 While configuring MSDP`" while configuring MSDP.
Workaround:	Re-configure MSDP.

PR# 56078

Severity:	S3
Synopsis:	"md5 authentication failed" message is generated for shutdown neighbor.
Release Note:	Even though a BGP neighbor (with MD5 authentication configured) is shutdown, BGP MD5 authentication failure messages may be seen in the logs.
Workaround:	Shutdown the peer from the remote side or remove the peer configuration from the remote peer's BGP configuration.

PR# 56311

Severity:	S2
Synopsis:	Few packet drops are seen in Strict priority queue after Hot-Failover.
Release Note:	When Strict Priority is enabled, a few packets may be dropped during Hot-Failover.
Workaround:	None

PR# 57907

Severity:	S2
Synopsis:	Sometimes, after deleting and recreating a VLAN, OSPF NBR does not come up on it.
Release Note:	Sometimes, after deleting and recreating a VLAN, OSPF NBR does not come up on it.
Workaround:	Remove IP address and add IP address for the VLAN.

PR# 57945

Severity:	S1
Synopsis:	RP2 reset to recover from SWP timeout.
Release Note:	The ACL agent on a linecard experienced an SWP timeout, which triggered RP2 to reset to recover.
Workaround:	None

PR# 58145

Severity: S2

Synopsis: Jumbo frames will not pass across 10GE interfaces on an EtherScale chassis when upgrading to 6.2.1.1 code or hotswapping LCs on 6.x code.

Release Note: Due to code changes between 5.x and 6.x, EtherScale customers upgrading to 6.2.1.1 may run into issues where jumbo frames on certain interfaces may fail to pass across 10GE links despite the MTU value being set appropriately.

Workaround: Please contact the Force10 TAC to provide workaround assistance.

PR# 58308

Severity: S3

Synopsis: ARP resolved based on /32 static route default static route pointing to interface is not removed when static route is removed.

Release Note: ARP resolved based on static route pointing to interface is not removed when static route is removed.

Workaround: The **clear arp no-refresh** command can be used to fix this. Use static routes with next-hop ip address. Avoid static routes pointing to an interface. In othe rwords, use the static route : ip route 10.1.1.1/32 11.1.1.2. Avoid : ip route 10.1.1.1/32 gi 0/0.

PR# 58329

Severity: S3

Synopsis: The RP1 "5 second utilization" output may incorrectly display CPU utilization at 100%.

Release Note: The RP1 "5 second utilization" output may incorrectly display CPU utilization at 100%.

Workaround: None

PR# 58445

Severity: S3

Synopsis: RP1/RP2 send out packet with source ip address 0.0.0.0 for sometime when ip address is removed.

Release Note: RP1/RP2 may send out packet with source ip address 0.0.0.0 for a while when ip address is removed.

Workaround: None, system stops sending those packets after some time.

PR# 58456

Severity: S4

Synopsis: E300 RPM P/S indicator LED does not go out once P/S is extracted.

Release Note: E300 RPM P/S indicator LED does not go out once P/S is extracted.

Workaround: None

PR# 58458

Severity: S3

Synopsis: Incorrect MD5 authentication failure message for BGP is generated after RPM failover.

Release Note: Incorrect MD5 authentication failure message for BGP is printed after rpm failover.

Workaround: Ignore the message.

PR# 59454

Severity: S3

Synopsis: When a passive peer group session is configured with an MD5 password, authentication failures result and the BGP session does not come up.

Release Note: When a passive peer group session is configured with an MD5 password, authentication failures result and the BGP session never comes up.

Workaround: None

PR# 59553

Severity: S3

Synopsis: On etherscale E300 'sh envmon pem' & 'sh inventory' shows one pem as absent even though its physically present and working fine.

Release Note: On EtherScale E300, **show envmon pem** and **show inventory** show one PEM as absent even though it's physically present and working fine.

Workaround: None

PR# 59786

Severity: S3

Synopsis: "BGP MD5 authentication failed" messages may be seen with established neighbors.

Release Note: "BGP MD5 authentication failed" messages may be seen with established neighbors.

Workaround: None. Ignore these error messages.

PR# 60270

Severity: S1

Synopsis: RP2 may crash because of loss of heartbeat between CP and RP2.

Release Note: RP2 may crash because of loss of heartbeat between CP and RP2.

Workaround: None

PR# 60784

Severity: S3

Synopsis: Phantom BGP neighbors which had been configured at one point in time w/ MD5 string will persistently output MD5 authentication message failures.

Release Note: BGP neighbors which had been configured at one point in time w/ a MD5 string but had since been removed (i.e. phantom neighbors) will persistently output MD5 authentication message failures. Completely removing the BGP config and reapplying does not resolve the issue.

Workaround: Reconfigure the BGP neighbor w/ its associated MD5 string and shut it down.

PR# 61269

Severity: S3

Synopsis: Running Config Shows "microcode default" When A Chassis Is Reloaded Without A startup-config And With The IPv4-320k Profile.

Release Note: When a user changes the next boot cam-profile to IPv4-320k, copies the configuration to NVRAM, deletes the startup-config and reloads, the running configuration shows - cam-profile ipv4-320k microcode default instead of - cam-profile ipv4-320k microcode ipv4-320k.

Workaround: This bug does not affect functionality. To work around do one of the following:

- Do not delete startup-config after changing the next boot cam-profile to IPv4-320k.

     or

- Reconfigure the **cam-profile ipv4-320k microcode ipv4-320k** command after reload to make sure the running-config has the right configuration statement.

PR# 61452

Severity: S3

Synopsis: Invalid MSS size advertised on BGP-MD5 (TeraScale)

Release Note: With MD5 enabled, an extra 18 bytes are not taken into account when computing MSS.

Workaround: lower IP mtu on interface

PR# 61459

Severity: S3

Synopsis: The ip unreachable functionality is not working for Layer 3 VLANs.

Release Note: The ip unreachable functionality is not working for Layer 3 VLANs. Traceroute messages will not be generated.

Workaround: None. ip unreachable should be configured for traceroute to an ip address configured on F10 router to work.

PR# 62494

Severity: S3

Synopsis: file system- while copying a file to ftp. providing an incorrect ip address, does not return error

Release Note: Error message is not given when hostname is not resolved for different applications e.g. ping, logging, ftp etc.

Workaround: None

OSPF (EtherScale)

PR# 58706

Severity:	S3
Synopsis:	When static routes configured with Null 0 interface are redistributed into OSPF, the expected LSA translation does not take place.
Release Note:	When a F10 acting as an ASBR has static routes pointed at a Null0 interface, redistribution into OSPF results in improper LSA type translation.
Workaround:	If possible, point static route out of a legitimate physical interface w/ associated IP; otherwise there is no workaround.

PR# 59635

Severity:	S1
Synopsis:	Under stress condition with large OSPF and BGP configurations and flapping, the system may run out of memory.
Workaround:	None

PR# 60134

Severity:	S3
Synopsis:	The route learned from IA and E1 removed in the routing table from time to time.
Release Note:	After a network statement (s) with area removed from router ospf, the area becomes un-used area stays in ospf and still participate the SPF calculation, which causes all IA and E1 removed in the routing table once SPF calculation occurs. (ABR becomes Backbone router as a good example).
Workaround:	There are three workarounds:

      1.) simply remove the unused area from router ospf (no area <ID).

      2.) execute "no router ospf <processID>" and add it back.

      3.) Reload the router.

PR# 60175

Severity:	S3
Synopsis:	OSPF convergence may take prolonged period of time after unconfiguring/reconfigure multicast routing.
Release Note:	OSPF convergence may take an excessive amount of time to converge after removing multicast routing from a config after the F10 chassis has been heavily loaded with multicast.
Workaround:	None

PR# 60640

Severity: S3

Synopsis: If a port-channel member is removed or added, then OSPF should not send Router LSA as update.

Release Note: If a port-channel member is removed or added, then OSPF should not send Router LSA as update.

Workaround: None

PR# 61743

Severity: S1

Synopsis: OSPF task may crash with multiple md5 keys or repeated addition and deletion of keys.

Release Note: OSPF task may crash with multiple md5 keys or repeated addition and deletion of keys.

Workaround: None

PIM (EtherScale)

PR# 47552

Severity: S2

Synopsis: mtrace may not work as expected.

Release Note: mtrace may not work as expected.

Workaround: None

PR# 60738

Severity: S3

Synopsis: NF-PIM-DM: "show ip pim tib" displays the uptime as 1882w0d, after stopping all data traffic and reports from the igmp hosts.

Release Note: Intermittently, "show ip pim tib" displays the uptime as 1882w0d.

Workaround: clear ip pim tib command will clear the TIB.

PR# 62184

Severity: S2

Synopsis: PIM may not install some of the SA entries learned from MSDP.

Release Note: PIM may not install some of the SA entries learned from MSDP

Workaround: Clear ip msdp sa-cache

Port Mirroring (EtherScale)

PR# 57502

Severity:	S3
Synopsis:	All packets are not received on MG port for outbound mirroring when MG and MD ports are on different linecards and for the pkt sizes > 4500 bytes as
Release Note:	All packets are not received on MG port for outbound mirroring when MG and MD ports are on different linecards and for the pkt sizes > 4500 bytes due to limited bandwidth in hardware.
Workaround:	None

PVST (EtherScale)

PR# 47135

Severity:	S3
Synopsis:	PVST does not converge when more than 70 VLAN interfaces are created with redundant interfaces.
Release Note:	PVST does not converge when more than 70 VLAN interfaces are created with redundant interfaces.
Release Note:	None

QoS (EtherScale)

PR# 47533

Severity:	S2
Synopsis:	A PBR rule can potentially redirect Protocol traffic destined to the F10 to get redirected out the incorrect interface.
Release Note:	PBR applied on interface potentially redirect the protocols multicast control traffic destined to the box out of the wrong interface. As a result the protocols adjacencies may not come up.This is when "any" keyword is used as destination prefix.
Workaround:	None

PR# 55971

Severity:	S2
Synopsis:	With rate police policy-aggregate applied to an interface, arp entry for the interface maybe missing in RP2 after "clear arp-cache".
Release Note:	Upon executing the **clear arp-cache** command, ARP information may be missing from RP2 on an interface with aggregate input policy configured.
Workaround:	Unconfigure and then re-configure the policy.

PR# 56398

Severity: S3

Synopsis: Duplicate entries may be seen in the CAM Etherscale chassis when startup-config is copied to running-config.

Release Note: ISSUE: Duplicate entries are sometimes seen in the CAM when policy QoS is applied on 1.5 linecards.

Workaround: None

PR# 56752

Severity: S3

Synopsis: If CAM is in middle of updating and RPM failover happens, CAM will not finish the remaining updates.

Release Note: CAM will stop updating if RPM failover happens while CAM is updating.

Workaround: After failover, remove and re-configure service-policy under interfaces.

PR# 56770

Severity: S2

Synopsis: A rate-shape value may not take effect if a greater rate-limit value is already configured.

Release Note: A rate-shape value may not take effect if a greater rate-limit value is already configured.

Workaround: Configure the rate shape first.

PR# 56805

Severity: S2

Synopsis: An output service policy, having aggregate and per-queue rate limit, may not take effect if an output policy with bandwidth was already applied.

Release Note: An output service policy, having aggregate and per-queue rate limit, may not take effect if an output policy with bandwidth was already applied.

Workaround: Unconfigure the output service policy and configure it again.

PR# 59827

Severity: S3

Synopsis: Clear qos statistics will not clear the counters during CAM updating.

Release Note: Clear qos statistics may not clear QoS statistics during CAM updating

Workaround: Issue the "clear qos statistics" command after CAM update is done.

PR# 59829

Severity: S3

Synopsis: Input and output qos-policies and output policy-map may not take effect, when CAM updation is in progress.

Release Note: While CAM update is in progress with loading QoS ACL, input and output qos-policies and output policy-map may not take effect.

Workaround: Will take effect after CAM update is done.

PR# 59947

Severity: S2

Synopsis: No rules will be installed in the QoS CAM if the rules to be installed per port-pipe is greater than 30k.

Release Note: When input service-policy is applied on interfaces, if more rules are added to ACL, none of the rules are installed in the QoS CAM if the rules to be installed per port-pipe is greater than 30k.

Workaround: Remove and add service-policy on interfaces.

PR# 60019

Severity: S3

Synopsis: May see "No response from linecard 3" message when ACL rules > QoS CAM size are pushed.

Release Note: "No response from linecard 3" might display when rules > QoS CAM size are pushed.

Workaround: Ignore message - doesn't effect the functionality.

RMON (EtherScale)

PR# 58447

Severity: S3

Synopsis: A large rmon alarm config causes CPU utilization of the rmon task to go up to 50%.

Release Note: Large RMON configuration (of the order of several thousand) can lead to non-trivial (>50%) CP CPU utilization.

Workaround: None

RTM (EtherScale)

PR# 43904

Severity: SS2

Synopsis: Not all BGP routes are showing up in RTM after multiple consecutive **clear ip ro** *

Release Note: When you do consecutive **clear ip ro** *, all BGP routes don't show up in RTM

Workaround: Wait until the network converges and re-issue one **clear ip ro** * again.

PR# 58353

Severity: S2

Synopsis: "clear ip bgp *" in an out of memory condition may cause a software crash.

Release Note: Executing a "clear ip bgp *" in an out of memory condition may cause a software crash.

Workaround: None

PR# 58840

Severity:	S2
Synopsis:	SNMP OID ".1.3.6.1.2.1.4.24.4.1.4" is not handled properly for ECMP next-hops. For static routes having ECMP Next-Hops, only 1 Next-Hop is sent in response to SNMP query. For default route ECMP, only 3 Next-Hops are sent in response to SNMP query. For non-default route ECMP case, only first 12 Next-Hops are sent in response to SNMP query.
Release Note:	SNMP OID ".1.3.6.1.2.1.4.24.4.1.4" is not handled properly for ECMP next-hops. For static routes having ECMP Next-Hops, only 1 Next-Hop is sent in response to SNMP query. For default route ECMP, only 3 Next-Hops are sent in response to SNMP query. For non-default route ECMP case, only first 12 Next-Hops are sent in response to SNMP query.
Workaround:	None

PR# 61508

Severity:	S3
Synopsis:	concurrent 'clear ip fib' on multiple line cards may result in RTM/FIB out of sync.
Release Note:	If 'clear ip fib' is issued on multiple line cards at the same time, the FIB databases across line cards may not be in sync with RTM (Route Table Manager).
Workaround:	Wait for FIB to synchronize on one linecard before clearing another.

sFlow (EtherScale)

PR# 60324

Severity:	S1
Synopsis:	SfLp task may crash on LC-EF-10GE-4P
Release Note:	SfLp task crashed on LC-EF-10GE-4P.
Workaround:	None. Linecard will reset itself. Please contact TAC if this issue is seen.

SNMP (EtherScale)

PR# 57569

Severity:	S3
Synopsis:	TeraScale 10GE Linecard with wanport configured do not generate alarms/SNMP traps for SONET alarms.
Release Note:	TeraScale 10GE Linecard with wanport configured do not generate alarms/SNMP traps for SONET alarms.
Workaround:	None

PR# 60407

Severity: S4

Synopsis: Cannot selectively enable generic trap types with the "snmp-server enable traps snmp" command, once "snmp authenication" has been enabled.

Release Note: Cannot selectively enable generic trap types with the "snmp-server enable traps snmp" command, once "snmp authenication" has been enabled.

    Force10(conf)#do sh run snmp

    !

    snmp-server community xxx ro

    snmp-server contact "xxx"

    snmp-server enable traps bgp

    snmp-server enable traps snmp authentication coldstart linkdown linkup

    snmp-server enable traps envmon fan supply temperature

    snmp-server location "xxx"

    From this point forward no matter what combination is used all options are added to "traps snmp..."

    Force10(conf)#no snmp-server enable traps snmp authentication coldstart linkdown linkup

    Force10(conf)#

    Force10(conf)#do sh run snmp

    !

    snmp-server community xxx ro

    snmp-server contact "xxx"

    snmp-server enable traps bgp

    snmp-server enable traps envmon fan supply temperature

    snmp-server location "xxx"

    Force10(conf)#

    Re-added "traps snmp..." with only "coldstart"

    Force10(conf)#snmp-server enable traps snmp coldstart

    Force10(conf)#

    Force10(conf)#do sh run snmp

    !

    snmp-server community xxx ro

    snmp-server contact "xxx"

    snmp-server enable traps bgp

    snmp-server enable traps snmp authentication coldstart linkdown linkup

    snmp-server enable traps envmon fan supply temperature

    snmp-server location "xxx"

    Force10(conf)#

Workaround: Use the "no snmp-server enable traps snmp [notification-option]" to disable generic trap types.

    Force10(conf)#do sh run snmp

    !

    snmp-server community xxx ro

    snmp-server contact "xxx"

```
                    snmp-server enable traps bgp
                    snmp-server enable traps snmp authentication coldstart linkdown linkup
                    snmp-server enable traps envmon fan supply temperature
                    snmp-server location "xxx"
                    Force10(conf)#
                    Force10(conf)#no snmp-server enable traps snmp authentication
                    Force10(conf)#
                    Force10(conf)#do sh run snmp
                    !
                    snmp-server community xxx ro
                    snmp-server contact "xxx"
                    snmp-server enable traps bgp
                    snmp-server enable traps snmp coldstart linkdown linkup
                    snmp-server enable traps envmon fan supply temperature
                    snmp-server location "xxx"
                    Force10(conf)#
```

Spanning Tree (EtherScale)

PR# 41689

Severity: S2

Synopsis: Root bridge cost changes (to depreference root) can cause transient MSTP loops.

Release Note: In a "triangle" switch topology (i.e. two core switches - with one acting as root and one secondary - with access switches connected to each core) changing the cost of the root switch to depreference may cause access switches from third-party vendors to go into a designated forwarding state. This transient designated forwarding state can cause temporary loops in an MSTP topology.

Workaround: None

PR# 61246

Severity: S1

Synopsis: Extended port flapping may cause RP2 to run out of memory.

Release Note: If multiple interfaces flap continuously for several days, certain processes on the RP2 processor may take a large amount of memory and have high CPU utilization.

Workaround: Shut down the interfaces that are experiencing the flapping issues.

SSH (EtherScale)

PR# 60103

Severity: S3

Synopsis: sh lc console disconnects ssh session with bad packet length.

Release Note: The **show lc console** command will disconnect an SSH session.

Workaround: None

PR# 62544

Severity: S1

Synopsis: ssh task may crash trying to access an invalid channel leading to an RPM failover

Release Note: SSH task may crash trying to access an invalid channel, leading to an RPM failover.

Workaround:

Telnet (EtherScale)

PR# 58012

Severity: S4

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

Release Note: 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 another vertical length.

VRRP (EtherScale)

PR# 56618

Severity: S3

Synopsis: When VRRP group is deleted, static arp for the deleted group's virtual address is not re-installed.

Release Note: When a VRRP group is deleted static arp for the deleted group's virtual address is not re-installed.

Workaround: None

flowcontrol

Control how the E-Series responds to, and generates 802.3x pause frames on 1 and 10 Gig line cards.

Syntax   **flowcontrol rx** {**off** | **on**} **tx** {**off** | **on**}

To return to the default **(rx on tx on)**, use the **no flowcontrol rx** {**off** | **on**} **tx** {**off** | **on**} command.

Parameters

rx on	Enter the keywords **rx on** to process the received flow control frames on this port. This is the default value for the receive side.
rx off	Enter the keywords **rx off** to ignore the received flow control frames on this port.
tx on	Enter the keywords **tx on** to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.
tx off	Enter the keywords **tx off** so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.

Defaults   **rx on tx on**

Command Modes   INTERFACE

Command History

Version 6.5.1.9	Introduced

Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full duplex flow control, stations implementing the pause operation instruct the MAC to enable reception of frames with destination address equal to this multicast address.

Important Points to Remember

- Asymmetric flow control (**rx on tx off** or **rx off tx on**) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

  Can't configure Asymmetric flowcontrol when speed <1G, config ignored

- The only configuration applicable to half duplex ports is **rx off tx off**. The following error is returned:

  Can't configure flowcontrol when half duplex is configure, config ignored

  Half duplex can not be configured when Flow control configuration is on (default is **rx on tx on**). The following error is returned:

  Can't configure half duplex when flowcontrol is on, config ignored

  ➡   **Note:** The flow control must be off (**rx off tx off**) before configuring the half duplex.

• Speeds less than 1 Gig can not be configured when the asymmetric flow control configuration is on. The following error is returned:

Can't configure speed <1G when Asymmetric flowcontrol is on, config ignored

FTOS only supports **rx on tx on** and **rx off tx off** for speeds less than 1 Gig (Symmetric).

Example

```
Force10(conf-if-gi-0/1)#show config
!
interface GigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...
```

Figure 1 show running config (partial)

Table 1 displays how FTOS negotiate the flow control values between two Force10 chassis connected back-to-back using 1 Gig Copper Ports.

Table 1 Negotiated Flow Control Values

Configured				Negotiated			
LocRxConf	**LocTxConf**	**RemoteRxConf**	**RemoteTxConf**	**LocNegRx**	**LocNegTx**	**RemNegRx**	**RemNegTx**
off	off	off	off	**off**	**off**	**off**	**off**
		off	on	**off**	**off**	**off**	**off**
		on	off	**off**	**off**	**off**	**off**
		on	on	**off**	**off**	**off**	**off**
off	on	off	off	**off**	**off**	**off**	**off**
		off	on	**off**	**off**	**off**	**off**
		on	off	**off**	**on**	**on**	**off**
		on	on	**off**	**off**	**off**	**off**
on	off	off	off	**off**	**off**	**off**	**off**
		off	on	**on**	**off**	**off**	**on**
		on	off	**on**	**on**	**on**	**on**
		on	on	**on**	**on**	**on**	**on**
on	on	off	off	**off**	**off**	**off**	**off**
		off	on	**off**	**off**	**off**	**off**
		on	off	**on**	**on**	**on**	**on**
		on	on	**on**	**on**	**on**	**on**

Related Commands

show running-config	Display the flow configuration parameters (non-default values only)
show interfaces	Displays the negotiated flow control parameters