# S-Series and SFTOS Release Notes

**Version 2.3.1.9 September 2006 101-00172-02**


FORCE10™

This document contains information on open caveats, caveats closed since the previous release, and operational information specific to the Force10 Networks® S-Series™ and SFTOS™ software. Caveats are unexpected or incorrect behavior and are listed in order of Problem Report (PR) number.

# Contents



For more information on hardware and software features, refer to the documents on the S-Series Product CD or visit Force10 Networks, Inc. on the web at www.force10networks.com

An updated S-Series documentation set for SFTOS version 2.3.1.5 is available on the Documentation tab of iSupport: https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx

# Important Notice About This Release

All S-Series customers should upgrade to version 2.3.1.9, including Routing Package (Layer 3) users and Switching Package (Layer 2) users.

As described below, Force10 Networks has identified a limited set of conditions under which the S50 might experience either a hang of management functions (console, telnet and SSH) and/or a failure to forward Layer 2 and/or Layer 3 traffic. A series of link flaps is most likely to precede any traffic disruption.

## Symptom 1: Only Console/Telnet access is affected

When symptom 1 is evident, the S50 cannot be accessed via the console or Telnet session (“management hang”). Network traffic might or might not continue switching.

This condition occurs when SFTOS detects an improper release of an internal buffer; the CLI task is suspended, preventing access to the system via the console, Telnet, or SSH. The failure of this task should not affect other running tasks. This symptom does not affect SFTOS version 2.2.1.9 or version 2.3.1.5 or higher.

### Symptom 2: All Layer 2 and Layer 3 traffic is affected

When symptom 2 pertains, the S50 experiences the management hang problem described for symptom 1. In addition, the switch ceases to perform Layer 2 forwarding, Layer 3 routing, and/or protocol operations ("system hang"). Specific manifestations of this symptom include:

- The switch experiences a complete system lockup; no traffic is passed through the system. A series of link flaps might precede this condition. To verify that link flaps occurred, review the syslog for a series of link up/down messages.
- The switch experiences a partial system lockup; only Layer 2 traffic passes, but routing adjacencies are lost, and Layer 3 forwarding fails. A series of link flaps might precede this condition. To verify that link flaps occurred, review the syslog for a series of link up/down messages.
- If the primary unit fails in a stacking configuration, as described in the previous scenarios, a stack member will take over the management function as the primary unit of the stack in what appears to be a successful failover. However, the failed unit might or might not continue to forward traffic. Both the failed primary and the new primary switches will illuminate the primary LED (PRI) located on the front panel.

### Issues Resolved by Upgrading SFTOS

For details on resolved issues, see Closed 2.3.1.8 Software Caveats on page 8. For the SFTOS upgrade procedure, see Upgrading and Downgrading SFTOS Versions on page 4.

For information on serviceability enhancements provided in this release, see Debug Enhancements.

## Debug Enhancements

SFTOS Version 2.3.1.9 is primarily a maintenance release to resolve console hang issues described in detail in Field Notice PN 101-00218-00. See also Important Notice About This Release, above, and Closed 2.3.1.8 Software Caveats on page 8. See also Closed 2.3.1.9 Software Caveats on page 7.

The following diagnostics and debugging features are included in this release:

- Full stack dump displayed on the console and saved to persistent memory (with boot ROM upgrade)
- A debugging console that can be used to break into a switch when the console is hung.
- Enhanced memory corruption detection and reporting mechanism. For example, when an SFTOS task attempts to free a memory block that it does not belong to, SFTOS will indicate what type of memory is being corrupted and exactly where the invalid call is being made from.

## New Software Features

- STP BPDU tunneling through S50s using DVLANs: Enable tunneling with the command **dvlan-tunnel ethertype** {**802.1Q** | **vman** | **custom** *0-65535*}. The command is enabled by default, with the **vman** value. When enabled, all STP BPDUs coming in at a customer port are sent double-tagged, while BPDUs coming in at provider ports are not.

## Changes in Default Behavior and Syntax

**Routing Protocols.** S-Series switches running routing software images previous to 2.3.1.8 did not conform fully to the Master VRRP router election algorithm specified by RFC 2338. If two routers in a VRRP group had the same highest priority setting, the election of the VRRP Master router was based on whichever router was booted first, rather than which router had the higher IP address. The Master VRRP router election mechanism now conforms to RFC 2338 and selects the router with the highest IP address.

However, since this behavior results in disruption of traffic during pre-emptive selection of a new master when a router with a higher IP address subsequently comes online, this behavior will be reverted to its previous behavior in the next release. This reverted behavior will also be consistant with Force10's E-Series FTOS behavior.

# Upgrading and Downgrading SFTOS Versions

Part of the software upgrade or downgrade process includes migrating the configuration files.

**Caution:** When downgrading, be aware that the existing configuration file is not automatically reapplied. If you want to use it, back it up before downgrading, and then apply it after downgrading.

However, even then, because the older version of software might not support all of the newer configuration features, some configuration elements might be lost. For example, version 2.2.1.2 did not support a 32-byte admin password, so downgrading to that version and applying a configuration that contains such a password would lose that password.

While downgrading within a branch release, there is a high possibility that the configuration could be lost. Force10 recommends that the configuration be saved to a TFTP server, deleted from the system (**clear config** command), and then reapply the running-config after the downgrade.

If the software downgrade is between two major releases, for example from 2.3.1.5 to 2.2.1.9, then the configurations are completely lost. Use the **clear config** command before downgrading.

Starting with SFTOS Version 2.3, SFTOS uses ASCII text-based configuration files (SFTOS previously used binary files). Part of the software upgrade process includes migrating the configuration files from binary to text. Therefore, to prepare for the possibility that you might need to roll back to 2.2.x.x, you should save a copy of your binary config and a current config script to the network prior to upgrading to 2.3 from 2.2.x.x. The following procedure includes those instructions.

**Note:** Do not use pre-2.3.1 scripts (scripts created to configure Version 2.2) on Version 2.3 or higher. The script will be aborted. You must update pre-2.3.1 scripts after migrating to 2.3.x release.

This upgrade procedure assumes that you are loading the new system image from a TFTP server after downloading the image from the Force10 website. See the *SFTOS Configuration Guide* for alternative methods.

| Step | Command Syntax | Purpose |
|---|---|---|
| 1. | **enable** | After logging in to the SFTOS CLI, access the Privileged Exec mode, from which you execute all of the following commands. |
| 2. | **show switch** | Check the current software level. |

| Step | Command Syntax | Purpose |
|---|---|---|
| 3. | **copy nvram:startup-config tftp://***ip_address/folder* | Back up the configuration file to the network.<br>Keep this file in case you decide to revert to the old code. |
| 4. | **show running-config config.scr** | Create a configuration script. |
| 5. | **copy nvram:script config.scr tftp://***ip_address***/config.scr** | Save the configuration script to the network. |
| 6. | **copy tftp**://*ip address/ file_name* **system:image** | Copy the system image file to the S-Series internal flash.<br>**Note:** Using TFTP requires that you first set up a management interface on the switch. For details, see *Setting the Management IP Address* in the *S50 Quick Reference* or in the *SFTOS Configuration Guide*. As an alternative, you can use the slower Xmodem method. |
| 7. | | Type "**y**" when the CLI asks **Management access will be blocked for the duration of the transfer**<br>**Are you sure you want to start? (y/n)** |
| 8. | **reload** | Reboot the switch. If a new software image is loaded into the management unit of an S50 stack, the image will be automatically propagated to all units. |
| 9. | | The **reload** command invokes a CLI response that requires you to type "**y**" to the following two statements:<br>**Management switch has unsaved changes. Would you like to save them now? (y/n)**<br>**Are you sure you want to reload the stack? (y/n)**<br>The reboot then executes an automatic configuration conversion from binary to text. Migration errors are logged on the console if there is a command that cannot be migrated. A sample of the status message is shown below. |
| 10. | **show switch** | Verify the new software level. |
| 11. | **show running-config** | Verify the configuration conversion. |

```
User:
******* Binary configuration file detected, migration in progress....  *******
  ******* To prevent loss of data, DO NOT POWER OFF MACHINE!             *******
  ******* Migration to text configuration file completed.                *******
  ******* Applying text configuration.                                   *******

  ******* Finished text configuration                                    *******
```

Figure 1 Sample of the Status Message Displayed during Migration of Binary Configuration File to Text

# Enabling HTTP

HTTP access to the switch is disabled by default. To be able to access the switch through the SFTOS Web User Interface, use the CLI to first assign an IP address to the management interface, and then execute the command **ip http server enable** from Privileged Exec mode.
To enable the secure socket layer for secure HTTP, use the **ip http secure-server enable** command.
For details on those commands, see the Security chapter in the *SFTOS Command Reference Guide*.

# Enabling SSH Server

The S50 requires an offline key generation to enable the SSH server. Use the following instructions to generate SSH keys offline using the OpenSSH tools at http://www.openssh.org/.
For details, refer to "Enabling Secure Management with Secure Shell or Secure Sockets Layer" in the Security chapter of the *SFTOS Configuration Guide*.

```
RSA key for SSHv1: ssh-keygen -q -t rsa1 -f rsa1.key -C '' -N ''
RSA key for SSHv2: ssh-keygen -q -t rsa -f rsa2.key -C '' -N ''
DSA key for SSHv2: ssh-keygen -q -t dsa -f dsa.key -C '' -N ''
```

Copy the appropriate keys with TFTP to NVRAM as follows:

```
(Force10)#copy tftp://IP_address/rsa1.key nvram:sshkey-rsa1
(Force10)#copy tftp://IP_address/rsa2.key nvram:sshkey-rsa2
(Force10)#copy tftp://IP_address/dsa.key nvram:sshkey-dsa
```

Enable the SSH server by executing the following command from Global Config mode:

```
(Force10)(Config)#ip ssh server enable
```

For additional security, disable the Telnet server by executing the following command:

```
(Force10)(Config)#ip telnet maxsessions 0
```

# Enabling Telnet

Telnet access to the switch is disabled by default.
To enable access to the switch through Telnet, enter **ip telnet server enable** from Global Config mode.

# Differences between S-Series and E-Series

This section describes the major differences in how command usage on the S-Series differs from the E-Series. Users familiar with the E-Series CLI will notice enough similarities in the CLI environment on the S-Series that they can quickly learn the variations in syntax and usage.

Of course, there are more commands with more detailed options in FTOS than in SFTOS, because FTOS supports the E-Series switches, which are larger and more complex than the S50 (currently, the only switch in the S-Series line, supported by SFTOS).

The major difference is that commands that contain a parameter in the form *slot/port* in FTOS, use a *unit/slot/port* parameter in SFTOS. In an S50 stack, the *unit* is the stack member. Because an S50 does not have a true line card, the slot is indicator is always 0 (zero). For example, 2/0/5 means stack member 2, port 5.

Examples of common commands that vary in syntax include:

- **ip route**: Both FTOS and SFTOS have the command, but the SFTOS command supports only IP addresses, not physical interfaces. In other words, the command syntax allows only for identifying the IP address of the next-hop router.
- **logging buffered**: Both FTOS and SFTOS have the command, but the FTOS command has an extra parameter for the size of the buffer. Both commands invoke debug logging with the number 7 for the severity level parameter. The SFTOS command is **logging buffered 7**.
- **show mac-address-table**: Both FTOS and SFTOS have the command, but the SFTOS command with more similar results is **show mac-addr-table**. The syntax contains the *unit/slot/port* form cited above, for example, **show mac-addr-table interface 1/0/4**:
- **show interface**: Both FTOS and SFTOS have the command, but SFTOS has fewer parameters because all ports are gigabit ports. For example, the SFTOS equivalent of **show interface gigabitethernet 2/11** (FTOS) would be **show interface 1/0/11**, where, as described above, 1/0/11 represents unit 1 in the stack, slot 0, port 11.
- **show linecard**: This FTOS command is similar to **show version** in SFTOS, which shows basic information, including the running software version and up time. **show hardware** and **show sysinfo** are similar commands, and **show tech-support** provides the results of a group of those similar commands.
- **service timestamps**: This FTOS command is not available in SFTOS. SFTOS sets timestamps automatically.
- **aaa authentication**: This FTOS command is in SFTOS as **authentication**.

# Caveats

SFTOS is available as a base Layer 2 image (the “Switching Package”) and as an optional, extra-cost image, augmented with Layer 3 functionality (the “Routing Package”) . A separate subsection, Layer 3 Open Software Caveats, handles open caveats that are specific to the Layer 3 functionality.

## Closed 2.3.1.9 Software Caveats

The following PR pertains to the Layer 3 (Routing) package only:

Packets will not be forwarded through a VRRP master router with port-based routing only (VLAN-based routing is not affected). [700051700]

## Closed 2.3.1.8 Software Caveats

The following PR pertains to the Layer 3 (Routing) package only:

- The election of the VRRP Master router is based on whichever router is booted first if two routers in the VRRP group have the highest priority setting. This is in conflict with RFC 2338, which specifies that the router with the higher IP address should win the tie. However, since this behavior results in disruption of traffic during pre-emptive selection of a new master when a router with a higher IP address subsequently comes online, this behavior will be reverted to its previous behavior in the next release. This reverted behavior will also be consistant with Force10's E-Series FTOS behavior. Since it has been re-opened, this PR also appears in the Open Caveats section. [700052047]

The following PRs pertain to both the Layer 2 (Switching) and Layer 3 (Routing) packages:

- When IGMP is enabled, a large amount of multicast traffic might lead to a Spanning Tree loop. [700043784]
- After failover of a management unit in a switch stack or power down of a management unit, pings to the management IP address may fail, and the ARP cache may take up to 60 seconds to refresh. [700039303]
- Removal of secondary IP address causes loss of VLAN configuration. [700049201]
- The RMON task — one of a set of SFTOS application and kernel tasks running on the S50 — might become stuck in an execution loop, while assuming a high priority, preventing other software tasks from accessing the SFTOS scheduler. [700046481]

  Workaround: None
- An SFTOS task might stall while attempting to release an invalid memory block. When this condition is occurring, a console message is generated similar to the following:

  ```
  0xe85e158 (nim_t): memPartFree: invalid block 0xffffffff in partition 0x12e60fc.
  ```

  The task name appears as nim_t, SNMPTask, or lvl7TaskUtilMonitorTask. [700050240]
- A system hang can result from a race condition that occurs when a rapid series of link up/down events is experienced with SNMP traps enabled on those links. SNMP traps are enabled by default in SFTOS. [700047528]

  Workaround: Disable SNMP link traps by executing the command **no snmp trap link-status all.**
- The EmWeb process, which serves console and telnet, can free an invalid buffer pointer. When this condition is occurring, the following message might be generated on the console:

  ```
  EmWeb: invalid buffer pointer freed
  ```

  This error condition results in a console-only hang, production traffic should continue to flow unaffected. [700047916]

  Workaround: None
- The macro, LOG_MSG(), might cause memory to be overwritten or exceed its buffer size, leading to memory corruption. [700050229]

  Workaround: None

## Layer 2/Layer 3 Open Software Caveats

The following caveats are logged against the Switching Package ("Layer 2 image") of SFTOS (listed in ascending order by PR#):

- Saving the start-up configuration to NVRAM might take longer than expected. [700028364]
- Logout does not prompt to save some configuration changes. [700028794]

  Workaround: For ports to operate in 1G speed, do not issue the **no auto-negotiate** command.
- TCN count increments in the root switch when the alternate LAG is shut on the non-root switch. [700031045]
- The ifMtu object, in the Interface MIB, is not displaying the correct value. [700031420]
- An inappropriate help message appears in response to attempt to remove ipmask/ipaddr from a particular community name. [700031450 / 700031585]

  Workaround: Use correct syntax:
  **no snmp-server community ipaddr public**
  **no snmp-server community ipmask public**
- The "Packets RX and TX 1523-2047 Octets" field is miscounting counters. [700031778]
- Local traffic frame counters are not incrementing. [700031923]
- After a reload, if another reload command is issued without saving the configuration, a prompt is generated to save the current configuration, even if nothing has changed. [700032113]
- The S50 reboots itself when MSTP is configured with 1024 VLANs. [700032812]
- Counters under RMON MIB (statistics group) are returning values of both transmitted and received packets instead of the expected received packets only. [700032946]
- When MAC ACL has a permit rule and an IP ACL has a deny rule for the same packets, packets are not denied. [700032953]
- The root switch does not send RSTP BPDUs when the non-root is forced to RSTP from MSTP. [700032969]
- SNMP trap community configured with versions does not display the version in the running configuration. [700034322]
- Pagination for **show tech-support** is not working. [700038703]
- While uploading files, msg.txt, trap.txt, and asciilog.bin are created in NVRAM. [700039420]
- Broadcast Storm Recovery counters are not getting incremented [700039552]
- Member ports are not getting added to a port channel using the **interface range** command. [700039867]

  Workaround: This can be done by going to the individual interfaces and making them part of the port channel.
- Script-apply errors occur for LAG members during migration and port channel configuration [700039873, 700040043, 700040338]

  Workaround: The error message is misleading; the configuration is applied and functionality is not affected.
- Traplogs and log files cannot be uploaded to a TFTP server. [700040001]
- ACL lines are displayed twice after the 2.3.1 upgrade [700040232, 700040233]

- In SNMP, the S-Series and E-Series have identical OIDs but they refer to different names. [700040602]
- Remove from the **police-simple** CLI command all the options for nonconforming traffic other than **drop**. [700040842]

  Workaround: The only action that can be accurately done on the non confirming traffic is a “drop”. So specifically configure the non-conforming traffic to be dropped.
- Migration from SFTOS Version 2.1.x to 2.3.x makes an untagged port part of more than 1 VLAN. [700040883]

  Workaround: Do a **reload** after the migration to get the correct behavior.
- A port channel and the port channel members are displayed in different VLANs. [700040892]
- Configuring a port as tagged (with old VLAN commands) in one VLAN, which is already untagged in another VLAN, is giving an error. [700041244]

  Workaround: Tag the port under Interface VLAN mode and untag the VLAN in Interface Config mode (the same as the pre-2.3.1 configuration).
- After executing the command **no vlan port tagging all <y>** , all ports are configured to be in untagged mode for VLAN y. [700041252]

  Workaround: For each VLAN member, untag the port from the Interface VLAN mode.
- The **show vlan** command displays incorrectly when tagging is removed from a port with PVID set. [700041258]
- After migration from SFTOS versions 2.1 or 2.2 to 2.3.1.5, ACL mapping is not saved after a reload. [700041365]
- After migrating from SFTOS version 2.2.1.9 to 2.3.1.5, **show port all** makes the switch hang. [700041365]

  Workaround: Another reload is required after migration to achieve the expected behavior.
- Configuring a secondary IP address on an S50 interface running RIP does not remove the route learned through RIP if the secondary IP address and the RIP entry are on the same network. [700041440]
- No END line at the end of the configuration [700042767]
- S50 accepts an uncompleted Enable Password that causes the enable to fail. [700042826]
- Enable Password does not support '{' ' }' '~' characters. [700043193]
- The interface description field is missing after a reload. [700043322]
- `-Err-` message against speed in the display of **show interface ethernet** *vlan interface* [700043635]
- MSTP settings disappear when upgrading from 2.2.1.2 to 2.3.1.5. [700044253]
- The Web UI allows ports to be added tagged to (default) VLAN 1. [700044538]
- The **spanning tree edgeport** command does not work in the **Interface Range** mode. [700044596]
- Failure of the root forwarding link on an S50 connected to an E-Series switch results in a 30-second convergence time. [700044671]
- The port untagged/tagged configuration is lost after a reload. [700045355]
- When logging via SSH into an S50, “`User Login Failed for admin`” is sometimes displayed in the console capture even before the password prompt appears. [700045894]

- Sending some garbage data while logging into S50 via SSH makes the session hang. [700045895]
- Inconsistent behavior when VRRP and spanning-tree protocols are enabled, resulting in traffic being dropped. [700046823]
- Even if Java mode is enabled, the S50 switch navigation icon might not appear at the top of the Web UI. [700047361]
- No reply for ping with jumbo size packets [700047656]
- 4-digit code version is not shown for **show switch** *unit-id*. [700047900]
- An SNTP server can be pinged, but is not recognized. The **show sntp** command displays the SNTP server status as "unknown". [700048634]
- MTU cannot be configured on 10GE interfaces via the Web User Interface [700048705]

### Stacking

- The **switch renumber** command keeps the old unit as detached. [700028826]
- The **mgmt unit renumber** command causes RPC to time out to CPU. [700028828]
- Disabling administration capabilities, for all units in a stack using the **switch *unit id* priority 0** command, will execute the disable without warning. Upon stack reload, all units will come up in a disabled state. [700030354]

  Workaround: Ensure that at least one unit in the stack has the administrative priority of 1 to 15.
- When removed from a stack, secondary members stay as stack members. [700031197]

  Workaround: Execute the **switch renumber** command.

## Layer 3 Open Software Caveats

The following list applies only to the Routing Package (“Layer 3 image”). (For caveats that apply to both images, see Layer 2/Layer 3 Open Software Caveats on page 9.)

- The election of the VRRP Master router is based on whichever router is booted first if two routers in the VRRP group have the highest priority setting. This is in conflict with RFC 2338, which specifies that the router with the higher IP address should win the tie. However, since this behavior results in disruption of traffic during pre-emptive selection of a new master when a router with a higher IP address subsequently comes online, this behavior will be reverted to its previous behavior in the next release. This reverted behavior will also be consistant with Force10’s E-Series FTOS behavior. Since this PR was officially closed for this release, but has been re-opened, this PR also appears in the Closed Caveats section. [700052047]

  Workaround: None
- Performing an SNMPwalk on the RMON MIB gives a response only for statistics and history groups, not all groups. [700032834]

  Workaround: None
- ARP is not getting cleared for high values of ARP time-out [700034139]

  Workaround: Use a lower ARP time-out value.

- Creating a loopback address is not possible. [700034140]

  Workaround: None

- The switch cannot do a recursive route lookup. (A recursive route is one where the route is not pointed directly to the next hop, but, instead, to a hop for which a route is already present in the routing table.) [700034187]

  Workaround: Create specific routes.

- The **show ip route bestroutes** command displays all possible routes. [700034258]

  Workaround: None

- Routing CLI options under logical interfaces are not supported. [700034369]

  Workaround: Routing should be enabled on individual interfaces or VLAN interface.

- Characters print twice after doing an outbound telnet back to the switch. [700034580]

  Workaround: Use 'noecho' in the CLI command **telnet** *host-ip* **noecho**.

- When the routes are changed for the same major network, old routes are reinstated. [700034619]

  Workaround: None

- The neighbor table is not cleared and new routes are learned when an area ID is changed on one interface. [700034676]

  Workaround: None

- The OSPF MD5 key does not support "!". [700043192]
- Switch ARPs are not flushed on link failure. [700044585]
- Saving and reloading the switch with VRRP configurations causes errors. [700045944]
- VRRP/STP issue: VRRP and spanning-tree protocols being enabled can result in traffic being dropped. [700046823]
- The **ip pimsm staticrp** command cannot be reversed. [700047424]
- Unable to ping router interface when a VRRP group is removed [700052155]
- Unable to ping virtual IP address when there is more than 1 VRRP group [700052156]