Release Notes for Cisco Service Control Operating System (SCOS) 2.5.10

June, 2006

Release Notes for Cisco Service Control Operating System (SCOS) 2.5.10

Supports: SCOS 2.5.10, SCOS 2.5.9, SCOS 2.5.8, SCOS 2.5.7, SCOS 2.5.6, SCOS 2.5.5, SCOS 2.5.2, SCOS 2.5.1, SCOS 2.5

OL-7085-08

These release notes for the Cisco Service Control Operating System describe the enhancements provided in Cisco Release SCOS 2.5.10.

For a list of the caveats that apply to Cisco Release SCOS 2.5.10 see “Open Caveats,” page 23.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Introduction

Cisco is proud to release version 2.5.10 of the SCOS (Service Control Operating System) for its SCE platform.

SCOS 2.5.10 is a point release of SCOS 2.5. It includes some minor enhancements and various fixes of caveats that were identified as part of Cisco's on-going internal testing and during our interaction with our customers.

This document outlines the functional enhancements to the various SCOS 2.5 releases, and assumes the reader already has a good working knowledge of the Cisco solution. For additional information, please refer to the Cisco Service Control Engine documentation.

RELEASE SCOS 2.5.10

Resolved Bugs

The following bugs were fixed in this release.

Primary bandwidth controllers incorrect limitation

- Cisco Number CSCsd67973

  When more than one BWC is assigned to a Primary BWC, if one of these BWCs has an external limitation from a GC or port, the primary BWC will not give the residual bandwidth to other BWCs.

  This issue is evident when working in Subscriber aware mode, where a subscriber is being explicitly limited to a certain configurable Total BW Value and the services BW (e.g. P2P) is being limited by a Global Controller limitation.

  This bug is fixed in SCOS 2.5.10.

RDR-Formatter show function presents a clear time with one second oscillation each time

- Cisco Number CSCsd33224

  When issuing a 'show rdr-formatter' command twice, the 'last time these interfaces were cleared:' counter oscillates between two values with a gap of one second between the values.

  This bug is fixed in SCOS 2.5.10.

FTP details appear in the user log and in 'show version'

- Cisco Number CSCse10500

  On package installation, FTP details appear in the user-log and also in the 'show version' output.

  This bug is fixed in SCOS 2.5.10 by masking these details with 'ftpserver'.

Slow recovery from CPU congestion

- Cisco Number CSCse18367

  An SCE platform that works at a sustained 60-70% CPU utilization and faces a short event of CPU congestion (due to DDoS attack, routing change in the network, etc.) may remain in CPU congestion for a long period (even hours) after the original event that caused the congestion passed.

  This bug is fixed in SCOS 2.5.10 by implementing a new congestion handling that shortens the convergence time after the event that caused the congestion has passed and reduces the probability for packet dropping during the congestion.

RELEASE SCOS 2.5.9

Functional Enhancements

Show log CLI command

A new CLI command, **`show log`**, has been added. The functionality of this command is the same as the existing **`more user-Log`** command, but is a standard IOS command.

SNMP MIB forward compatibility to 3.0

The following changes have been made to SNMP traps for forward compatibility with SCOS 3.0:

- Trap *pullRequestRetryFailedTrap*: OID changed from 45 to 47
- object *pullRequestNumber* (sent along with the above trap): OID changed from 44 to 46

Resolved Bugs

The following bugs were fixed in this release.

SCE Platform Reload after Long Management Operations

- Cisco Number CSCsd41764

  In rare cases, long management operations caused an SCE platform reload.

  This issue was only relevant in SCOS 2.5.8 and is solved in SCOS 2.5.9.

Transmission Errors after Link Reestablishment

- Cisco Number CSCsd17133

  In rare cases, after reestablishment of a link, a small amount (<1%) of traffic was transmitted with errors and dropped at the gigabit interface.

  In such cases, a reboot was needed.

  This issue was only relevant in SCOS 2.5.8, and was solved in SCOS 2.5.9.

Bandwidth Controller – Direction Mismatch for Bundled Flows

- Cisco Number CSCsc94873

  In certain cases, which are arbitrary, enforcement direction of the bandwidth controller for bundled flows (e.g. RTSP, FTP) did not match the configuration.

  This bug is fixed in SCOS 2.5.9.

Counted Bytes not Displayed in Readable Format

- Cisco Number CSCsc77198

  The counted bytes for the Line Interfaces statistics should display the number in standard decimal format.

  This bug is fixed in SCOS 2.5.9.

Lack of 'Service Loss' (Failure) Detection

- Cisco Number CSCsc66985 and CSCsc69289

  An SCE platform sometimes did not detect that it had gone into a failure state even though one of its processors was no longer processing traffic and thus did not provide the expected service.

  Since no failure state was detected, the SCE platform did not hand over production traffic to a standby SCE platform in cases of HA configurations.

  This bug is fixed in SCOS 2.5.9.

snmpwalk on SCE does not supply all information under tree

- Cisco Number CSCsb73297

  The following problems had been observed when executing *snmpwalk*:

  - *snmpwalk* on packageGrp (.1.3.6.1.4.1.5655.4.2.3) returns all objects under packageCounterTable (.1.3.6.1.4.1.5655.4.2.3.1) but not those under packageServiceUsageTable (.1.3.6.1.4.1.5655.4.2.3.2).
  - *snmpwalk* on pcubeEngageObjs skips packageServiceUsageTable.

  In addition, when manually running *get next* in the subtree packageCounterEntry at the end of the subtree, it skipped to serviceCounterGrp instead of continuing to the next subtree under packageGrp.

  This bug is fixed in SCOS 2.5.9.

Fragments and Filtered traffic handling vulnerability

- Cisco Number CSCsc94599

  Fragments that were classified as Ignored Traffic sometimes caused the control processor to be congested.

  This bug is fixed in SCOS 2.5.9.

RELEASE SCOS 2.5.8

Functional Enhancements

Link Reflection SNMP Trap

In SCOS 2.5.8 a trap indicating port operational status change is added. The trap contains the port's state and the reason for this state (forced down, external down etc.). The ID of the link that has failed can be extracted using the port group in the MIB.

Resolved Bugs

The following bugs were fixed in this release.

Service Loss MIB Counter

- Cisco Number CSCsc04845

This counter reported inconsistent values in certain shortage scenarios.

This bug is fixed in SCOS 2.5.8

SSH Operations Cause SCE to Reboot and other miscellaneous SSH issues

- Cisco Number CSCsb78399, CSCsb89993, CSCsb90412, CSCsb90412, CSCsb90421

SSH operations might cause SCE platform to reboot, or a direct problem with SSH connections to the SCE platform may occur.

This bug is fixed in SCOS 2.5.8.

Failure after short power outage

- Cisco Number n/a

In rare cases, after a short power outage, the SCE platform traffic ports may stop responding. In this case, links will not be established and traffic will not run through the system.

This issue was solved in SCOS 2.5.8

Zombie telnet sessions can cause a memory overrun

- Cisco Number CSCsc82102

A telnet session that was established and closed without any login attempt might have caused a memory overrun.

This bug is fixed in SCOS 2.5.8.

Subscribers synchronization between cascaded SCE platforms has a deficit

- Cisco Number CSCsc82090

In case of very high spawning rate of anonymous subscribers, a deficit could be created between the active and standby SCE platforms. This deficit will be closed if the standby becomes the active SCE platform, with the penalty of potential loss of state.

The issue is only relevant for Pull Subscriber Mode.

This bug is fixed in SCOS 2.5.8.

Telnet session might get stuck when Changing IP and Default Gateway

- Cisco Number CSCsb51681

In certain situations, configuration of the default gateway caused the telnet session to get stuck and prevented further work with the SCE platform until the SCE platform was rebooted.

A workaround was implemented in SCOS 2.5.8.

Issues with Connectivity to the SCE Platform in case Name-Server Configured

- Cisco Number CSCsb51681

If name-server was not configured correctly, ping didn’t work.

This bug is fixed in SCOS 2.5.8.

'setup' CLI Command - the SCE Platform Halts when Configuration is Saved

- Cisco Number CSCsb90338

The SCE platform rebooted when the configuration was saved via the CLI setup command.

This bug is fixed in SCOS 2.5.8.

Hardware Bypass Module Fixes for the SCE2000-4/8xFE

- Cisco Number n/a

Problems were encountered on the NICs of the SCE2000-4/8xFE that could cause an additional reboot on system startup.

This bug is fixed in SCOS 2.5.8.

Link Loss during Upgrade Caused by Hardware Bypass Module Re-Initialization when Configured to Auto-Negotiation

- Cisco Number CSCsc90447

When upgrading a SCE2000 that required a hardware bypass module upgrade, a temporary link loss might have been experienced when the link ports were configured to AutoNeg enabled.

This bug is fixed in SCOS 2.5.8.

SCE Management Traffic Cannot Pass through SCE Platform GBE Links

- Cisco Number CSCsc77883

SCE platform management traffic is dropped when it passes through the SCE platform GBE traffic ports.

This bug is fixed in SCOS 2.5.8.

SCE Platform Reboot due to Excessive Number of FTP Sessions

- Cisco Number CSCsc12769

When the SCE platform processes an excessive amount of FTP sessions, a reboot may occur.

This bug is fixed in SCOS 2.5.8.

Anonymous Subscriber Export Problem

- Cisco Number CSCsc61655

When exporting an anonymous-group file and deleting an anonymous-group name via CLI command, the end of the exported CSV file is also deleted. For example; when three names are deleted, the three names are deleted from the export file and an additional three names are deleted from the bottom of CSV file as well.

This bug is fixed in SCOS 2.5.8

Static Subscriber Not Saved after Boot

- Cisco Number CSCsc61656

Static subscriber configuration; that is, subscriber configuration explicitly configured via CLI, such as package ID, is not saved after system reboot.

This bug is fixed in SCOS 2.5.8

Enhanced Link Recovery after Link Reflection

- Cisco Number CSCsb51681

SCOS 2.5.8 supports an enhanced link recovery protocol that ensures port recovery after link reflection.

The link reflection function forces down the reciprocal port when the link fails. When the link is restored, the reciprocal port that had been forced down is automatically restored, also. The enhanced link recovery functionality tests the reciprocal port before restoring it. If the port is down, the enhanced link recovery procedure is applied.

The enhanced link recovery mode is supported for all link failure reflection modes (normal, all ports, and all ports linecard aware).

By default, this new mode is disabled. To enable the enhanced link recovery mode, use the following CLI command:

```
configure
interface linecard 0
link port-enhance-recovery
```

To disable the enhanced link recovery mode, use the following CLI command:

```
configure
interface linecard 0
no link port-enhance-recovery
```

Package ID Variable Not Correctly Updated in Pull Mode

- Cisco Number CSCsc04812

In the following scenario, the subscriber package ID variable may not be correctly updated:

- Package ID is configured via anonymous subscriber templates.
- A new IP address spawns a new anonymous subscriber, which triggers a pull request to the SM.
- The pull response returned by the SM includes the subscriber state, but no package ID.
- When Control receives a pull response, it updates the state and any variables that were changed by the pull response. Variables that were not updated by the pull response retain the default value. In this case, the package ID assigned by the anonymous subscriber template will NOT be retained.

This issue was identified and fixed in SCOS 2.5.8.

RELEASE SCOS 2.5.7

New Features

New link reflection mode for the SCE 2000: Link Reflection on All Ports Linecard Aware

In SCOS 2.5.7, a new mode has been added to the link failure reflection functionality of the SCE 2000: All Ports Linecard Aware mode. This mode is used when each link of the SCE 2000 (Subscriber-side interface and the corresponding Network-side interface) is connected to a different linecard.

This mode reflects a failure of one port to the other three ports of the SCE 2000, in the following manner:

- One interface of the SCE 2000 is down, indicating a problem with the SCE platform: Link failure is reflected to the other three SCE platform ports.
- Two reciprocal ports of the SCE 2000 are down, indicating a problem in the linecard to which the SCE platform is connected and not the interface: No action is taken. This allows the second link in the SCE platform to continue functioning without interruption.

Resolved Caveats

The following caveats were resolved in this release.

Failure of Subscriber Database Loading from Disk

The operation of loading the subscriber database from the SCE platform internal disc may fail when a burst of pull requests is initiated by the SCE platform after the connection with the Subscriber Manager is established.

This issue is fixed in SCOS 2.5.7.

SCOS SW Upgrade Failure of SCE platform in Cascade Topology

During a SW upgrade of a cascaded SCE pair, the SCOS enters failure mode when three consecutive reboots of the SCE platform occur within 30 minutes.

This issue is fixed in SCOS 2.5.7.

Failure of the Connection with the Subscriber Manager

In some rare cases applying a SCAS BB configuration file to the SCE platform causes the connection with the Subscriber Manager to fail.

This issue is fixed in SCOS 2.5.7.

Anonymous Subscriber Pull Rate Limit Failure

The pull rate limit mechanism fails to limit anonymous subscribers spawning rate. The failure may cause loss of the pull messages and lack of subscriber resolution in the pull mode.

This issue is fixed in SCOS 2.5.7.

SCE 2000 4/8xFE Issues

Various platform-related issues in SCE 2000 4/8xFE were fixed in SCOS 2.5.7.

SCE 2000 4/8xFE should not be used with SCOS 2.5.5 or SCOS 2.5.6 due to issues related to the support of SCE 2000 4/8xFE in these SCOS releases.

These issues were fixed in SCOS 2.5.7.

SCE 2000 4/8xFE should be used with SCOS 2.5.7 or with future SCOS releases.

RELEASE SCOS 2.5.6

Inject after packets with short TCP header

SCEs that were running earlier SCOS releases failed to inject packets triggered by the reception of TCP packets with a header smaller than 20 bytes. In those circumstances, sanity checks caused a reboot of the SCE.

This issue is fixed in SCOS 2.5.6.

Incorrect counting in the tpServiceLoss MIB-Object

The counting in the tpServiceLoss MIB-Object was incorrect.

This issue is fixed in SCOS 2.5.6.

Missing CLI command

The CLI command for enabling sniffing mode on the SCE2000-4/8xFE was missing. The CLI command was added in 2.5.6. This CLI command is:

```
con
in li 0
link mode <all, link1, link2> sniffing
```

Reboots due to initialization of the TX FPGA

In some rare cases during the boot sequence, SCE platforms that are running SCOS 2.5.x may reboot unexpectedly during initial system load. The reboot may only happen when the user reloads the SCE or turns on the unit.

In most cases, after this reboot the system will self recover and load normally.

This issue was fixed in SCOS 2.5.6.

RELEASE SCOS 2.5.5

Reduced latency for delay-sensitive traffic

SCOS 2.5.5 includes an improvement that allows for reducing the level of latency that SCE platform adds to delay-sensitive traffic.

Delay-sensitive traffic can be any media traffic such as VoIP packets or Video packets.

The reduced latency improvement was implemented by duplicating the packets of delay-sensitive traffic to Traffic Processor 0, in addition to processing the packets in Traffic Processors 1 to 3, as is done for normal traffic. Traffic Processor 0 is responsible for transmitting this type of traffic, and since the queues of Traffic Processor 0 are normally empty, it only adds minimal delay.

This improvement assures that the SCE platforms will not add delays of more than several hundred micro-seconds to delay-sensitive traffic.

Cisco-related changes in CLI

Minor changes were implemented in CLI for making the SCEs system more compliant regular Cisco practices

- The P-Cube logo was omitted
- The prompt name of the platforms was changed to "SCE"
- The default password was changed to the normal Cisco default password. The old P-Cube default password is also supported.

Changing the values of VLAN tags

The SCE 2000 platform now includes the ability to change the values of the VLAN tags of VLAN-tagged packets that flow through the platforms.

Changing the VLANs is useful in various network scenarios where the SCE 2000 is deployed in a link where the traffic is tagged with VLANs, and the changing of the VLAN tag is required for directing the packets to a specific destination.

The user can specify some increment or some decrement that will be applied to all of the tags of all of the VLAN tagged packets.

Link-failure reflection on all ports

The functionality of link-failure reflection on all ports extends the normal link-failure reflection functionality. It allows the user to determine whether all ports should be taken down if the link fails on a single port of the SCE 2000.

In certain topologies, when a failure state occurs on one link, the link state must be reflected to all of the other ports (3) of the SCE 2000 in order to signal to the network elements that are connected to these ports that one of the links of the SCE 2000 has failed.

Support for SCE2000s with boards of type 'G002'

SCOS 2.5.5 supports SCE 2000 platforms with boards of type 'G002' without requiring any configuration changes. This is different from previous SCOS versions where configuration changes were required in order to support boards of type 'G002'.

RELEASE SCOS 2.5.2

Support for the improved SCE 1000

Cisco is enhancing the functionality, serviceability and failure-resiliency of the SCE 1000 platform.

The following functions will be made available on the new SCE 1000:

- The power supply units of the new SCE 1000, whether AC or DC, will be Field Replaceable Units
- The FAN module of the new SCE 1000 will be a Field Replaceable Unit
- A second management port will be added to the new SCE 1000 enabling future support of fail-over of management ports
- The new SCE 1000 will support Single Mode transmission, in addition to the existing support for Multi Mode transmission

Note that the new SCE 1000 will now have a form factor of 2 Rack Units.

Support for the improved SCE 2000 4/8xFE

Cisco is releasing a new SCE platform that provides a solution for FE connectivity. The SCE2000 4/8xFE includes 8 FE interfaces, while only 4 of them are SW-supported in this release.

The SCE 2000 4/8xFE enables a Service Control solution for 1 or 2 FE links. The 2 FE links can be active-standby or active-active. In addition, a fail-over solution using 2 cascaded SCE 2000 4/8xFE platforms is also supported.

Solved bugs and issues

Avoiding unnecessary drops of packets

In previous SCOS 2.0 releases, the SCEs were dropping unnecessary packets. This mainly happened in case of flows with very high BW of over 50 Mbps per second.

This issue was identified and fixed in SCOS 2.5.2.

False detection of ICMP attacks

In previous SCOS releases, the SCE reported on frequent attacks in the network while there was no reason to believe that these attacks actually occur. The protocol of the reported attacks us usually ICMP, and he reported attack did not contain any specific IP address.

The causes for this phenomenon were identified and the issue was fixed in SCOS 2.5.2.

Counting correctly dropped packets in Global BW Controllers

The counters of dropped packets in Global BW Controllers were counting incorrectly in previous SCOS 2.5 releases.

This issue was fixed in SCOS 2.5.2.

Issue with the More Filter

When using the CLI command ‘debug slot 0 ppc <0-3> func <someFunc>’, and this function generates more than 24 lines of output, and the user takes more than a few seconds to respond to the - - more - - prompt, various subscriber related functionalities of the SCE are malfunctioning.

This issue was fixed in SCOS 2.5.2.

RELEASE SCOS 2.5.1

The main issues that are fixed in the scope of SCOS 2.5.1 are the following:

- Packet drop on open flow when BW control enforced
- Failure to return from of enforced link failure state
- Introduction of new subscribers during SM resynchronization
- Management port presents wrong duplex

Packets dropped when a Flow Opens and Bandwidth Control is Enforced

When a new flow opens, and bandwidth control mechanisms are enforced on this flow, some of the first packets of the flow were dropped during the initial time period of 0.5–1 seconds.

This caveat was resolved.

SCE Fails to Return from an Enforced Link Failure State

The SCE can be programmed to enforce link failure. For example, if there is port failure replication, and the SCE identifies failure on one port, forcing link failure on the other port. Another example is that the SCE can be programmed to force link failure on the 2 ports of a link after reboot.

Normally, after enforcing such link failure, the SCE attempts to cancel this forced failure and restore normal operation of the port or ports. When this happens, in some cases the MAC device of the port may get stuck, and although the SCE signals to the network element to which it is connected that the link is up, the SCE actually drops all the packets that it receives from this port.

This occurred only on the SCE 1000 and SCE 2000, and the caveat was resolved in this version.

Introduction of New Subscribers During SM Resynchronization

When a SCE loses the connection with the SM, and then the connection is renewed, the SM attempts to resynchronize the subscriber information of the SCE. In past versions, it was not possible to introduce new subscribers during resynchronization.

In this version, this caveat was resolved, and subscribers now can be added during resynchronization.

SCE 2000's Management Port Presentation of Duplex Mode

When the SCE 2000's management port operates in 1000 Mbps, the response to the **`show interface`** CLI command presented an incorrect output.

This caveat was resolved.

RELEASE SCOS 2.5

Multi CPE Management in Cable Environments

In a cable environment, the SCE platforms now allows association of a number of Customer Premises Equipment (CPE) devices into a single home network (that is, behind a single cable modem). This allows attributing a number of CPEs to a single subscriber-context and applying a single policy to this subscriber context. This is also relevant for cases where each CPE uses multiple global IP addresses (unlike a residential gateway NAT setup allowing all CPE machines to share an IP address).

SCOS 2.5 removes previous limitations of the number of subscribers assigned multiple IP addresses in the SCE 1000 and SCE 2000. The system ensures that all IP addresses used by each CPE come from a common pool of addresses, typically assigned with their downstream CMTS / SMTS device/ blade. The system requires that the subscriber with multiple CPEs be configured to a single traffic processor (a single PPC in the SCE).

Assigning subscribers to a specific traffic processor can be implemented in either of the following ways:

- Configure all IP ranges of a given CMTS / SMTS to be processed by the same traffic processor. This can be performed only if one SCE platform handles several CMTS/SMTS units, otherwise load-balancing cannot be performed properly.
- The service provider controls the IP range from which the subscriber IP address is allocated based on additional criteria such as the subscriber type. In this case, the range can be used by the SCE platform to assign subscribers to a particular traffic processor, independent of the definition of the subscriber network ID.

  The SCE platform can be configured such that the IP address range of each subscriber is actually handled by the same traffic processor. This is achieved by assigning the IP addresses or range to a configured Traffic Processor IP Range (TIR) and the corresponding traffic processor. All IPs of a specific subscriber must be assigned to the same traffic processor at any given time.

The introduction of the TIR functionality provides two possible modes of subscriber mapping:

- Legacy subscriber mapping: ensures that all mappings of a single subscriber reach the same traffic processor by internal means, using a hash on the subscriber IP and/ or using specific subscriber rules on the IP/ range when required.
- TIR subscriber mapping: generally configures all mappings for subscribers in a specific range to reach the same traffic processor, reducing the need for internal specific rule resources per subscriber.

TIRs functionality can be applied only to relevant subscribers. That is, some subscribers are assigned to traffic processors via TIR, while the subscribers without multiple CPE equipment are processed as usual (legacy subscriber mapping).

New SNMP MIB Objects

The following new MIB objects were added in SCOS 2.5:

- **tpServiceLoss** in the traffic processor group. This MIB object reports the relative amount of service loss in this traffic processor, in units of 0.001%, since last reboot or last time this counter was cleared.
- **globalControllersDroppedBytes** in the Global BW Controllers group. This MIB object reports the number of dropped bytes in this Global BW Controller.

SSH Management

SCOS 2.5 supports management of the SCEs using SSH. This functionality prevents insecure transfer of unencrypted passwords and data over the Internet.

Where security is a concern, using a Secure Shell (SSH) server rather than Telnet is recommended. An SSH server is similar to a Telnet server, but it uses cryptographic techniques that allow it to communicate securely with any SSH client over an insecure network, to ensure privacy. CLI commands are executed over SSH in exactly the same manner as over Telnet.

The SSH server supports both the SSH- 1 and SSH- 2 protocols.

Increased number of Global BW Controller in the SCE 2000

The SCE 2000 now supports 64 Global BW Controllers per link and direction (a total of 256 Global BW Controllers).

More filter in the CLI

SCOS 2.5 supports the ability to filter the output of **show** and **more** commands in the following ways:

- *more file-name | include <regexp>*
- *more file-name | exclude <regexp>*
- *more file-name | begin <regexp>*
- *show <command> | include <regexp>*
- *show <command> | exclude <regexp>*
- *show <command> | begin <regexp>*

include is similar to **grep**, **exclude** is similar to **grep -v** (shows all lines not containing the expression) and **begin** filters everything until there is a line with the keyword, and then it shows everything.

In this context, **regexp** is a form of ***keyword***. That is, it searches for the sub-string "keyword" in the line.

Note that the **include**, **exclude** and **begin** options are case sensitive

More / Show output redirection

SCOS 2.5 allows directing the output of **show** and **more** commands to a file, either overwriting the file or appending to it:

- *more file-name | redirect <file-name>*
- *more file-name | append <file-name>*
- *show 'command' | redirect <file-name>*
- *show 'command' | append <file-name>*

Support for daylight saving time

The SCE platform can now be configured to automatically switch to and from daylight savings time on specified dates.

In addition, the three-letter time zone code can be configured to indicate daylight savings time if required. For example, in the eastern United States, standard time is designated EST, and daylight savings time is designated EDT.

The transition times into and out of daylight savings time may be configured in one of two ways, depending on how the dates for the beginning and end of daylight savings time are determined for the particular location:

- Recurring: If daylight savings time always begins and ends on the same day every year, (as in the United States), the clock summer-time recurring command is used. The beginning and ending days for daylight savings time can be configured once, and the system will automatically perform the switch every year.
- Not recurring: If the start and end of daylight savings time is different every year, the clock summer-time command is used. In this case, the transitions must be configured every year for that particular year. (Note that "year" is not necessarily a calendar year. If the transition days are determined in the fall, the transitions for that fall and the next spring may be configured.)

Limitations and Restrictions

- The upgrade to the various SCOS 2.5.x releases may include re-initialization of the SCE 1000 or SCE 2000 hardware Bypass module. This re-initialization process may cause a failure of the GBE link where the system stalls for a period of less than 1 sec.

  The table below states the various cases when these re-initialization may occur (marked as "Yes")

To / From	2.5.0	2.5.1	2.5.2	2.5.5	2.5.6	2.5.7	2.5.8	2.5.9	2.5.10
2.5.0	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.1	-	-	No	No	Yes	Yes	Yes	Yes	Yes
2.5.2	-	-	-	No	Yes	Yes	Yes	Yes	Yes
2.5.5	-	-	-	-	Yes	Yes	Yes	Yes	Yes
2.5.6	-	-	-	-	-	Yes	Yes	Yes	Yes
2.5.7	-	-	-	-	-	-	Yes	Yes	Yes
2.5.8								Yes	Yes
2.5.9									Yes

- The SCE platform may experience a reboot when a port scan operation is performed on the SCEs management port. This reboot is initiated by the SCE platform due to scheduling optimization for detecting failover conditions in periods of less than 1 second in a configuration of two cascaded SCE platforms.

The following is recommended:

- Use IP access lists to eliminate port scans that take place due to actual attacks.
- If the system administrator needs to perform a port scan operation as part of a security check, it is advisable to disable the SCE platform watchdog only for the period of time in which the port scan is performed, using the following CLI commands:

```
configure/interface linecard 0/0 no watchdog
configure/watchdog software-reset disabled
```

Open Caveats

Link flickering using link reflection with linecard aware mode

- Cisco Number CSCse16643

  When an SCE platform is connected to 7600 on each link, as in a MGSCP topology, and link reflection is used with line card aware mode, during the recovery process on one link a flickering may be experienced on the other link, although in linecard aware mode the first link should have no effect on the second one.

SNMP - chassis type returns incorrect value

- Cisco Number CSCsc91840

  The SEMib does not return the correct value indicating the type of chassis. In addition, the possible types defined do not reflect the current naming conventions of the existing chassis types.

Unsupported Counter on the SNMP Management Interface MIB

- CSCsc43972

  The ifInOctets and ifOutOctets MIB object for the management interfaces of the SCE platform are not supported and always return 0.

  This is fixed in SCOS 3.0.0.

FF L4 Rules Don't Match Non-First IP Fragments

- Cisco Number 3975

  A non-first fragment packet doesn’t include any L4 information. This implies that when setting Flow Filter rules using L4 attributes (such as port number and TCP flags) they will not work for Non-First-Fragment packets.

  Workaround: When using counters or other rules for L4 information, this phenomenon should be taken into account.

Changing SCEs IP Requires Manual Reboot

- Cisco Number 4989

  The system does not automatically reboot when the IP address is changed.

  Workaround: After changing the IP address on an SCE using CLI, manually reboot the SCE.

ToS Marking for TCP: 3 First Packets Receive the ToS Value of Default Class

- Cisco Number 6139

  ToS marking is performed after the Class of Service of the flow is determined, that is, only when the first applicative packet is received and analyzed. In TCP, the 3 first packets (SYN, SYN-ACK, ACK) have no applicative meaning and therefore cannot have a specific CoS. Therefore, their ToS receives the value of the default class, which is AF4

Saving Configuration using SNMP Sometimes Fails

- Cisco Number 7664

  Cisco's proprietary SNMP allows saving of the SCEs configuration. The set operation can fail due to a short timeout of the MIB viewer.

  Workaround: Increase the default timeout value of the MIB viewer to approximately 15 seconds. (The original setting in HPoV the timeout is 0.8 sec.)

Telnet Sessions to the SCE May Not Close

- Cisco Number 8749

  When the SCE is configured with *`no timeout`* for Telnet sessions, and a disconnect occurs during an open Telnet session, the telnet session in the SCE will not close.

  Workaround: Specify a timeout for Telnet sessions.

SNMP Time-related Variables May Become Incorrect

- Cisco Number 9409

  The SNMP variables that are time related may set themselves incorrectly approximately every 45 days, due to wraparound of the internal counters.

  Workaround: Check time-related values every month to make sure they are correct.

PQI Upgrade Requires User to Wait

- Cisco Number 9565

  After executing the CLI command `PQI install/upgrade/...`, the user sees the progress on the screen, and then the CLI prompt returns before the system has completed the upgrade. Nevertheless, the installation is not finished for additional several minutes. The following message appears: `Now please wait 5 minutes before attempting to do anything else`. Although it appears that the user can continue to perform CLI functions, it is necessary to wait.

Note The user must wait until the operation is complete before continuing to use the CLI.

Packet Loss During Application Installation or Upgrade

- Cisco Number 11798

  When a PQI application file is installed or upgraded on the SCE, the SCE may lose packets for a few seconds.

  Workaround: During install and upgrade, it is recommended to set the SCE to bypass mode, using the following CLI commands:

  - For the SCE 1000:

```
(config if)#link mode port1-port2 bypass
```

  - For the SCE 2000:

```
(config if)#link mode all-links bypass
```

  - After insult pqi is completed, use:

```
(config if)#default link mode
```

Inject Failure for Packets with the SCE 2000 in 2 GBE Links with Tunneling and Split-Flows

- Cisco Number: n/a

  Inject may fail under the following circumstances:

  - When the 2 GBE links in the SCE 2000 experience split-flows

    AND

  - When the links are tunneled (L2TP or MPLS)

    AND

  - The SCE 2000 performs injection of a packet

  An example of this occurrence might be when implementing HTTP Redirect

Error in Attack Filter CLI Command

- Cisco Number 13034

  The CLI command Show interface linecard 0 attack-filter query IP current returns an error message when the attack filter is enabled only for part of the protocols.

Loss of Import Information on Reboot

- Cisco Number: n/a

  If the SCE reboots while a user is performing several **`import CSV`** operations, the imported information is not preserved.

SCE Platform may Fail during Upgrade of a Cascaded System

During the upgrade of a pair cascaded SCE platforms, one of the SCE platforms may experience three consecutive reboots, causing a failure of the platform. The reboots are due to the fact that at some point during the upgrade, the two cascaded SCE platforms are each running a different version of SCOS, which results in RPC protocol incompatibility between the two SCE platforms.

The following procedure should be used for upgrading a cascaded system with SCOS versions lower than 2.5.7 (either old or new).

Note This issue is resolved in SCOS 2.5.7, and the upgrade procedure for cascaded systems that is documented in the *Cisco Service Control Engine Software Configuration Guide* can be used.

SOLUTION

To upgrade a cascaded system for SCOS 2.5.6 or lower, use the following procedure:

Step 1. Shutdown both SCE platforms by running the following commands:

```
SCE# configure
SCE (config)# interface linecard 0
SCE (config if)# shutdown
```

Step 2. Change connection mode for both boxes to 'inline' rather than 'inline-cascade'. This prevents inter connection communication between the two SCE platforms, thus preventing the original problem.

```
SCE (config if)# connection-mode inline
```

Step 3. Upgrade both SCE platforms independently as described in the *Cisco Service Control Engine Software Configuration Guide*.

Step 4. Reload both SCE platforms.

Step 5. Change connection mode for both boxes back to 'inline-cascade'.

```
SCE (config if)# connection-mode inline-cascade
```

Step 6. Verify that communication between the two SCE platforms has been re-established.

Step 7. Activate both SCE platforms using the following command:

```
SCE (config if)# no shutdown
```

Obtaining Technical Assistance

Cisco provides *Cisco.com* as a starting point for all technical assistance. Customers and partners can obtain documentation., troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for *Cisco.com* (on page 27), go to the following website:

http://tools.cisco.com/RPF/register/register.do

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.