Release Notes for Cisco Service Control Operating System (SCOS) 3.0.6

March, 2007

Release Notes for Cisco Service Control Operating System (SCOS) 3.0.6.

Supports: SCOS 3.0.6, SCOS 3.0.5, SCOS 3.0.4, SCOS 3.0.3, SCOS 3.0.1, SCOS 3.0.0.

OL-8955-09

These release notes for the Cisco Service Control Operating System describe the enhancements provided in Cisco Release SCOS 3.0.6.

For a list of the caveats that apply to Cisco Release SCOS 3.0.6 see *Open Caveats*, page 32.

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

Contents

Introduction

Cisco is proud to release version 3.0.6 of the SCOS (Service Control Operating System) for its SCE platform.

SCOS 3.0.6 is a maintenance- release of SCOS 3.0. It includes fixes of issues that were identified as part of Cisco's on-going internal testing and during our interaction with our customers.

This document outlines the fixes to the SCOS 3.0.6 release. It assumes the reader already has a good working knowledge of the Cisco Service Control solution. For additional information, please refer to the Cisco Service Control Engine documentation.

RELEASE SCOS 3.0.6

Resolved Issues

The following issues were resovled in this release.

Accommodation of U.S. Daylight Saving Time policy changes

- Cisco number: CSCsh24223

  Beginning in March 2007, Daylight Saving Time (DST) in the U.S. will start three weeks earlier and end one week later. The start date will change from the first Sunday in April to the second Sunday in March. The end date will change from the last Sunday in October to the first Sunday in November. The time switch has an impact on time-based policy enforcement, the timestamps in RDRs and system logs, and the displayed time.

  The SCE platform can be configured to automatically switch to DST on a specified date, and also to automatically switch back to standard time using the **`clock summer-time recurring`** command. The default dates for this recurring automatic switch are the dates used in the U.S. However, these default values were based on the pre-2007 DST dates.

  In release 3.0.6, the **`clock summer-time recurring`** command defaults are the new U.S. DST dates.

PRPC authentication did not work with NAT/firewall

- Cisco Number CSCsh39763

  SCA BB Console PRPC authentication failed when trying to connect to the SCE platform if there was a device located between the console and the SCE platform that changed its IP address (such as an NAT). The problem occurred when PRPC security level on the SCE platform was configured to “semi” or “full”.

  This issue is fixed in SCOS 3.0.6.

RELEASE SCOS 3.0.5

Functional Enhancements

Service Control Management Protocol (SCMP)

SCMP is a protocol that integrates the SCE platform and the ISG (Intelligent Service Gateway) functionality of the Cisco routers, thereby providing a mechanism that allows the ISG and the SCE platform to manage subscriber sessions together without requiring coordination and orchestration by additional components. For further information, see the chapter "*Managing the SCMP*" in the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

CLI and MIB support for Cisco Universal Device Identifier (UDI)

UDI is a Cisco baseline feature supported by all Cisco platforms that allows network administrators to manage the assets in their network by tracing specific devices. The following features were added to SCOS 3.0.5 to support UDI:

- "**`show inventory`**" CLI command
- support for ENTITY-MIB version 2 (as defined in RFC 2737). For further information see the sections relating to MIBs in Chapter 5 "Configuring the Management Interface and Security" in the *Cisco Service Control Engine (SCE) Software Configuration Guide.*

Updated "do" CLI command

The "**do**" CLI command is supported also in line vty mode. See the "**do**" command in the *Cisco Service Control Engine (SCE) CLI Command Reference*.

MIB files

Information and proprietary MIB files that are supported by the SCOS can be downloaded from the following link under the Cisco Service Routing Products section:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

3.0.5 Backwards compatibility

The number of Global Controllers was increased to 1024 in release 3.0.5. These GCs are implemented by SW and therefore the capability of counting dropped bytes per global controller, which relies on the HW implementation of the GCs, is no longer supported. Instead, starting from release 3.0.5, all dropped bytes are counted and aggregated into GC number 0.

Note that this change has no effect on the capability of counting dropped bytes per service which is still supported under the mode: ‘no accelerate-packet-drops’.

Resolved Issues

The following bugs were fixed in this release.

’clear traffic-counter’ CLI command moved ADMIN level

- Cisco Number CSCsc01995

  Users with ADMIN authorization level privileges (most users) could not clear the traffic counters.

  In SCOS 3.0.5, the following command has been moved to the ADMIN authorization level so that users can clear the traffic counters:

  `clear interface LineCard 0 traffic-counter name` <*name*>

Retrieving support file to the local disk using "logger get support file <file>" (not FTP) caused the subscriber API to disconnect and in some cases reload of the SCE platform.

- Cisco Number CSCsd65316

  The execution of the CLI command **`’logger get support-file`**‘ to the local disk (tffs0/) caused the subscribers API to disconnect and in some cases caused the SCE platform to reload.

  This bug is fixed in SCOS 3.0.5.

SCE Subscriber API – The additive flag is ignored for VLAN login

- Cisco Number CSCsd77872

  In the SCE API functions '*login*', *'loginBulk'*, '*networkIDUpdate*', and *'networkIDUpdateBulk'*, the '*networkIdAdditive*' (or '*networkIDsAdditive*') argument had no effect for VLAN mappings. If the network ID type was VLAN, the mappings were always additive.

  This bug is fixed in SCOS 3.0.5.

CLI command “show snmp MIB pcube-SE-MIB link” displayed wrong information

- Cisco Number CSCse06539

  The ‘**`show snmp MIB pcube-SE-MIB link`**‘ command displayed wrong information for *linkNetworkSidePortIndex* and *linkSubscriberSidePortIndex.*

  This bug is fixed in SCOS 3.0.5.

Missing output in CLI command "show snmp MIB pcube-SE-MIB vas-traffic-forwarding"

- Cisco Number CSCse14198

  The CLI command '**`show snmp MIB pcube-SE-MIB vas-traffic-forwarding'`** returned information for five VAS servers instead of eight servers.

  This bug is fixed in SCOS 3.0.5.

Extra characters in output of "show snmp pcube-se-mib application" command

- Cisco Number CSCse16669

  The CLI command '**`show snmp MIB pcube-SE-MIB application'`** added invalid characters to the end of the strings of 'apName' and 'apType.

  This bug is fixed in SCOS 3.0.5.

SCE platform and Agent clock not in sync in summer-time

- Cisco Number CSCse16986

  The SCE platform and the management agent lost time synchronization when the SCE platform moved to daylight savings time. This sometimes caused faulty execution of time-frame-based rules.

  This bug is fixed in SCOS 3.0.5.

MIB variable tpTotalNumHandledPackets held negative values

- Cisco Number CSCse43925

  The PCUBE-SE-MIB object *`tpTotalNumHandledPackets`* sometimes held negative values when no traffic was going through the SCE platform.

  This bug is fixed in SCOS 3.0.5.

Commands were not saved correctly in the configuration file

- Cisco Number CSCse55601, CSCse82541

  The following commands were not saved correctly in the configuration file and failed to execute after reload:

  - **`dropped-bytes counting-mode {per-global-controller | per-queue}`**
  - **`snmp interface 6 alias`** *<alias-string>*
  - **`snmp interface 6 link-up-down-trap`**

  This bug is fixed in SCOS 3.0.5.

FTP user name and password were logged by the copy command

- Cisco Number CSCse63416

  FTP user name and password were logged and exposed in the log file by the '**copy**' command with ftp path.

  This bug is fixed in SCOS 3.0.5.

Default gateway was not set properly in RevG in recover mode

- Cisco Number CSCse66119

  When the SCE platform reloaded in recover mode, it failed to initialize the default gateway. As a result, the SCE platform management interface became unreachable from any subnet other than the one on which the SCE platform was located.

  This bug is fixed in SCOS 3.0.5.

SCE rebooted or stopped responding to management traffic for a short period

- Cisco Number CSCse94394

  When external subscriber aging was enabled and a large number (more than 1000) of static subscribers (generated by importing a CSV file with subscriber data) were aged at the same time, the SCE platform either rebooted or stopped responding to management traffic (such as Telnet or SSH) for a short period of time.

  This bug is fixed in SCOS 3.0.5.

MIB variable pportOperStatus held incorrect value

- Cisco Number CSCsf20374

  In platforms that support a second management port, the PCUBE-SE-MIB object *pportOperStatus* returned an incorrect status for the first traffic port.

  This bug is fixed in SCOS 3.0.5.

Second Management port not identified correctly on some MIBs queries.

- Cisco Number CSCsf20375

  In platforms that support a second management port, the following PCUBE-SE-MIB objects appeared with the wrong port index:

  - *globalControllersDescription*
  - *txQueuesDescription*
  - *txQueuesUtilization*

  This bug is fixed in SCOS 3.0.5.

High rate of warnings on 'RDR buffer is full' filled the debug log

- Cisco Number CSC sf22326

  In scenarios where the traffic processors generated a very high rate of RDRs (~300 per second, each), the debug log of the SCE platform was filled with the following warning and info messages (one per second):

  ```
  <WARNING> [0x0300:0x002a] Formatter: starting to throw RDRs -
  RDR buffer is full
  ```

  ```
  <INFO>    [0x0300:0x0029] Formatter: got to the RDR-throw-
  warning watermark of 1000000 under the full buffer size
  ```

  This bug is fixed in SCOS 3.0.5.

MIB variable tpTotalNumHandledFlows held negative values

- Cisco Number CSCsg04903

  The PCUBE-SE-MIB object *`tpTotalNumHandledFlows`* sometimes held negative values when more than 2^32 flows were accumulated.

  This bug is fixed in SCOS 3.0.5.

MIB variable tpDiscardedrPackets held negative values

- Cisco Number CSCsg05182

  The MIB variable PCUBE-SE-MIB object *`tpTotalNumDiscardedPacketsDueToBwLimit`* sometimes held negative values when more than 2^32 discarded packets were accumulated.

  This bug is fixed in SCOS 3.0.5.

High rate of "The bundle exceeded the number of allowed flows" errors may cause the SCE to reload

- Cisco Number CSCsg39419

  A high rate of the following error caused a false detection of one of the SCE sanity checks, which resulted in an SCE platform reload.

  The errors are of the following type:

  ```
  "<<ERROR>> [0x0805:0x0041] RUC high level: The bundle exceeded
  the number of allowed flows can't add a new flow to bundle,
  origin FC ID: 58974 Number of bundled flows: 40"
  ```

  This bug is fixed in SCOS 3.0.5.

SSH login sequence error caused SCE platform reboot

- Cisco Number CSCsg45088

  SCE platform rebooted after the following sequence:

  1. SSH login with SSHv2
  2. First user+password combination typed by the user was rejected due to illegal password
  3. On the second login attempt (of the same SSH session), if the user name typed was different from the first user name type, the SCE sent the following error message and then rebooted:

  ```
  'Changing the user name is not allowed'.
  ```

  This bug is fixed in SCOS 3.0.5.

The object indices are not shown in "show snmp pcube-se-mib tx-queue"

- Cisco Number CSCsf29453

  Indices of Tx queues were not displayed in CLI output, which would therefore differ sometimes from an SNMP MIB query.

  This bug is fixed in SCOS 3.0.5.

Configuring the connection mode required uninstalling the application

- Cisco Number CSCsg08178

  Changing the connection-mode while an application was loaded in the SCE platform required uninstalling the application (and then re-installing it after the connection-configuration was done).

  This bug is fixed in SCOS 3.0.5. You can now change the connection mode under either of the following conditions:

  - When there is no application loaded
  - When the LineCard is in shutdown.

SCE reloaded due to internal clock problem

- Cisco Number CSCsd56771

  On rare events the SCE platform reloaded itself due to a failure in one of the JVM modules, which caused the EM agent to time out. Prior to the reboot, the SCE platform log displayed the following error:

  ```
  "java.lang.InternalError: cannot get time at
  java.lang.System.currentTimeMillis()J [native] ".
  ```

  This bug is fixed in SCOS 3.0.5.

GC enforcement took 10 minutes to converge

- Cisco Number CSCpu13091

  The Global Controller enforcement took 10 minutes to converge under the following conditions:

  - The Global Controller was configured with low rate.
  - A BW controller was connected to this GC and was configured with unlimited rate.

  SCOS 3.0.5 implements a different algorithm with a faster convergence time.

  The maximum time for convergence in SCOS 3.0.5 is about 2 minutes.

GC bandwidth was breached when the required BW was less then 0.000 PIR*

- Cisco Number CSCsd20303

  The GC in a specific configuration had a problem converging to the configured rate. The GC bandwidth in this situation was breached.

  This usually happened when (PIR * 1/100000 * number_of_subscriber) > GC rate.

  This bug is fixed in SCOS 3.0.5.

globalControllersIndex reported differently in MIB and in CLI

- Cisco Number CSCsf29443

  The `globalControllersIndex` MIB object is reported differently in the MIB and in CLI show command.

  This bug is fixed in SCOS 3.0.5.

Improve the SCOS CLI / MIB counter type visibility (L1/L2/L3 visibility)

- Cisco Number CSCse63542

  Some CLI commands and MIB objects that display byte and bandwidth counters were missing a clear indication of which protocol layer they count (i.e. do they refer to L2 bytes or L3 bytes).

RELEASE SCOS 3.0.4

Resolved Issues

The following bugs were fixed in this release.

TCP flow redirection and blocking might not work in cascade mode

- Cisco Number CSCse23591

  TCP flow redirection and blocking did not work correctly in cascade setups, since the injected packets were sent on the wrong links in certain circumstances, as described below. (Note that regarding blocking on a TCP connection, packets would have been blocked even if the injected packets were not sent correctly.)

  In cascade setups, one SCE platform is configured to handle "link-0" and the other is configured to handle "link-1". The problem occurred on the box configured as "link-1", regardless of the priority configuration.

  This bug is fixed in SCOS 3.0.4.

Potential invalid memory access during Protocol Pack upgrade on top of SCOS 3.0.3

- Cisco Number CSCse72906

Protocol pack upgrade (using hitless upgrade in SCOS 3.0.3) could have potentially triggered an invalid memory access resulting in unpredictable system behavior that varied from errors reported in the debug log to a reload of the SCE platform.

This bug is fixed in SCOS 3.0.4.

Link flickering when link reflection executed in linecard aware mode

- Cisco Number CSCse16643

  The following problem was noted when an SCE platform was connected to a Cisco 7600 router on each link, as in an MGSCP topology, with link reflection and linecard aware mode enabled:

  During the recovery process of one link, a flickering was experienced on the other link, although in linecard aware mode one link should have no effect on the other.

  This bug is fixed in SCOS 3.0.4.

Applying policy might fail if the SCE platform is configured with large lists

- Cisco Number CSCse28465

  When configuring a very large number of entries (more than 10K) in more than one list (such as services, HTTP URLs, Flavors), although a first apply operation was successful, a second apply operation failed due to RPC function failure. This was a result of exhaustion of the RPC resources.

  This bug is fixed in SCOS 3.0.4.

Backup of startup configuration file not available in ADMIN Level

- Cisco Number CSCse48893

  The backup of the startup configuration file could only be done from ROOT authorization level.

  This bug is fixed in SCOS 3.0.4, and this functionality is now available in ADMIN level via the following CLI command:

  `copy startup-config` <*destination-file*>

  This bug is fixed in SCOS 3.0.4.

CLI commands for connection mode inline-cascade not supported on SCE 2000 4/8xFE

- Cisco Number CSCse38026

  CLI commands for configuring the connection mode to cascade and other related commands were not supported on the SCE 2000 4/8xFE platform.

  This bug is fixed in SCOS 3.0.4.

Quick-forwarding option not available in ADMIN level

- Cisco Number CSCse30735

  The quick-forwarding and quick-forwarding-ignore action options of the traffic-rule command were available only at the ROOT authorization level. This capability is required in order to isolate voice traffic from data, and still have DPI reporting capabilities for the voice traffic in parallel.

  This bug is fixed in SCOS 3.0.4, and these two options are available at ADMIN level.

'no link failure-reflection linecard-aware-mode' enables link-reflection

- Cisco Number CSCse63682

  The CLI command "'no link failure-reflection linecard-aware-mode" erroneously enables link reflection on all ports.

  This bug is fixed in SCOS 3.0.4.

MIB variable tpFlowsCapacityUtilization displays wrong value

- Cisco Number CSCse69009

  The value of tpFlowsCapacityUtilization does not reflect the correct utilization estimation.

  This bug is fixed in SCOS 3.0.4.

Tuning high temperature thresholds

- Cisco Number CSCse30751

  The high and low thresholds are switched incorrectly in the configuration file. This results in a detection of a temperature which is too high by five degrees compared to the specification in two out of five sensors on the SCE platform.

  This bug is fixed in SCOS 3.0.4.

Elements not displayed in running-config all-data

- Cisco Number CSCse55616
- Cisco Number CSCse55611
- Cisco Number CSCse55598

  The following commands were not displayed as output of **`{show | more} running-config all-data`** command after being set:

  - `connection-mode inline on-failure bypass`
  - `connection-mode inline-cascade physically-connected-links link-1 priority secondary on-failure bypass`
  - `no link failure-reflection linecard-aware-mode`
  - `snmp-server enable traps enterprise mpls-vpn-auto-learn`
  - `snmp-server enable traps snmp`
  - `default VAS-traffic-forwarding VAS server-id 1 VLAN`
  - `no VAS-traffic-forwarding VAS server-id 1 VLAN`
  - `snmp-server enable traps enterprise telnet`
  - `snmp-server enable traps snmp authentication`

  Since these commands are included in the default configuration of the SCOS, there was no real impact on the running configuration before or after a reload.

  This bug is fixed in SCOS 3.0.4.

RELEASE SCOS 3.0.3

Functional Enhancements

The SCOS release 3.0.3 contains all functional enhancements that were part of the 2.5.x SCOS releases, up to and including SCOS 2.5.10 (see *Release Notes for Cisco Service Control Operating System (SCOS) 2.5.10*, available at http://www.cisco.com/en/US/partner/products/ps6134/prod_release_notes_list.html).

MPLS-VPN Solution

This is the Cisco state-of-the-art Service Control solution for service providers offering MPLS-VPN services to their customers. The Service Control MPLS/VPN solution features:

- Complete visibility into the applications and services in MPLS-VPN tunnels for subscriber-based usage monitoring and billing
- Leveraged capacity control and differentiation of service levels
- The ability to monitor and control all the traffic in an MPLS/VPN tunnel as belonging to a single subscriber entity, including traffic with private non-routable IP addresses.

Hitless Upgrade

The SCOS can replace an application loaded on the SCE platform with a new application without forcing any traffic-processing downtime.

VAS over 10G Solution

VAS over 10G is a specific configuration of VAS traffic forwarding, using a Cisco 7600 Series router as a dispatcher. The 7600 distributes the external 10G link and also functions as the switch for the VAS servers. VAS functionality is supported over a dual 10G topology with two external 10G links, each one connected to a separate 7600 platform and VAS server array. Only one set of VAS servers is used at a time, serving the VAS traffic of both 10G links. The other set of VAS servers is reserved for failover in case of either a switch failure or VAS servers failure.

L2TP offset support

The SCE platform is able to either ignore the tunneling protocols or treat the tunneling information as subscriber information.

Proprietary MIB files are now accessible via FTP

The Cisco Service Control proprietary MIB files may be accessed on the following FTP site:

ftp://ftp.cisco.com/pub/mibs/

Show interface line card 0 subscriber all-names CLI command

A new CLI command, **`show interface line card 0 subscriber all-names`**, has been added.

Backward Compatibility Notes

Introducing subscribers with VLAN mappings is permitted only when tunneling mode is "VLAN symmetric classify"

Subscribers with VLAN mappings can be logged in only when the system tunneling mode is "VLAN symmetric classify". This restriction was added in order to prevent erroneous usage of VLAN mappings in modes that do not support this classification mode. An attempt to login a subscriber with VLAN mapping in an unsupported mode results in failure and an appropriate error message.

SNMP MIB changes affecting backward compatibility

The following changes have been made to the MIB for compatibility with SCOS 3.0.3:

- Removed attackTypeTableClearTime from attackType table OID 1.3.6.1.4.1.5655.4.1.15.1.2
- Changed subscriberPropertiesValueEntry to subscribersPropertiesValueEntry OID 1.3.6.1.4.1.5655.4.1.8.3.1

SNMP MIB changes to prevent descriptors conflict

The names of the following objects now have a ‘p’ added at the beginning of the name to prevent descriptors conflicts with CISCO-STACK-MIB.

The following table lists both the old and the current names of these objects.

Old Object Name	Current Object Name (‘p’ added)
Port Group Objects	
portGrp	pportGrp
portTable	pportTable
portModuleIndex	pportModuleIndex
portIndex	pportIndex

Old Object Name	Current Object Name ('p' added)
portType	pportType
portNumTxQueues	pportNumTxQueues
portIfIndex	pportIfIndex
portAdminSpeed	pportAdminSpeed
portAdminDuplex	pportAdminDuplex
portOperDuplex	pportOperDuplex
portLinkIndex	pportLinkIndex
portOperStatus	pportOperStatus
Module Group Objects	
moduleGrp	pmoduleGrp
moduleIndex	pmoduleIndex
moduleType	pmoduleType
moduleNumTrafficProcessors	pmoduleNumTrafficProcessors
moduleSlotNum	pmoduleSlotNum
moduleHwVersion	pmoduleHwVersion
moduleNumPorts	pmoduleNumPorts
moduleNumLinks	pmoduleNumLinks
moduleConnectionMode	pmoduleConnectionMode
moduleSerialNumber	pmoduleSerialNumber
moduleUpStreamAttackFilteringTime	pmoduleUpStreamAttackFilteringTime
moduleUpStreamLastAttackFilteringTime	pmoduleUpStreamLastAttackFilteringTime
moduleDownStreamAttackFilteringTime	pmoduleDownStreamAttackFilteringTime
moduleDownStreamLastAttackFilteringTime	pmoduleDownStreamLastAttackFilteringTime
moduleAttackObjectsClearTime	pmoduleAttackObjectsClearTime
moduleAdminStatus	pmoduleAdminStatus
Chassis Group Objects	
chassisGrp	pchassisGrp
chassisSysType	pchassisSysType
chassisPowerSupplyAlarm	pchassisPowerSupplyAlarm
chassisFansAlarm	pchassisFansAlarm
chassisTempAlarm	pchassisTempAlarm
chassisVoltageAlarm	pchassisVoltageAlarm

Old Object Name	Current Object Name ('p' added)
chassisNumSlots	pchassisNumSlots
chassisSlotConfig	pchassisSlotConfig
chassisPsuType	pchassisPsuType
chassisLineFeedAlarm	pchassisLineFeedAlarm

Resolved Issues

In addition to some new bug fixes, the SCOS release 3.0.3 contains all bug fixes that were part of the 2.5.x SCOS releases, up to and including SCOS 2.5.10 (see *Release Notes for Cisco Service Control Operating System (SCOS) 2.5.10*, available at http://www.cisco.com/en/US/partner/products/ps6134/prod_release_notes_list.html).

The following bugs were fixed in this release.

Configure speed and duplex on interface management fails with admin privilege

- Cisco Number CSCsd90973

  Configuring speed and duplex under 'interface Mng 0/1 or 0/2' configuration mode in the CLI returns with error for insufficient privilege level for users with a privilege level lower than ROOT.

  This bug is fixed in SCOS 3.0.3.

Hostname configuration with too long host name

- Cisco Number CSCsb78041

  Configuring a hostname with more than 20 characters results in an error when executing copy running-config to startup-config.

  This bug is fixed in SCOS 3.0.3 by preventing such configurations.

Cannot configure management port using interface fastEthernet 0/0

- Cisco Number CSCsd61664

  When trying to configure speed and duplex of interface *fastEthernet 0/0*, the configuration is not performed.

  This bug is fixed in SCOS 3.0.3.

"show interface LineCard 0 subscriber sm-connection-failure" generates error

- Cisco Number CSCsc90460

  The CLI command "**`show interface LineCard 0 subscriber sm-connection-failure`**" generates an error message that the privilege is wrong for the admin and viewer levels.

  This bug is fixed in SCOS 3.0.3.

Error message in case of incompatible application should be improved

- Cisco Number CSCsb78556

  If an incompatible application is installed, the following error message will appear:

  SCE1010(config if)#pqi install file eng25611.pqi

  Copying file /tffs0/app/eng25611.pqi ...

  Extracting package 'SCAS BB' ...

  Registering 'SCAS BB' ...

  Verifying installation is allowed ...

  Installing ...

  Looking for old rollback data and deleting it

  33% done.

  Assigning new SLI

  44% done.

  ***Failed to register module eng25611.pm0**: The Install process failed in assigning an SLI file: **Bad SLI format**, object format is 15, should be no less than 12 and no greater than 12.*

  Error - Cannot install SCAS BB - see errors above

  This bug is fixed in SCOS 3.0.3.

Shutdown / no application may cause HW/SW Loss of Sync

- Cisco Number CSCsd26991

  Any operation that causes Shutdown, including No Application, Debug Soft Reset, implicit change to Shutdown due to loss of connection with the SM (if this option is configured), or Implicit Shutdown operation in the CLI, may cause HW/SW loss of sync if immediately followed by other successful operations - mainly moving from Enhanced to Classical open-flow-mode.

  This bug is fixed in SCOS 3.0.3.

L2TP fragmented packets are not handled correctly

- Cisco Number CSCse01278

  Fragmented packets wrapped with L2TP tunnel are not classified to the same flow and might not get service.

  This bug is fixed in SCOS 3.0.3.

SNMP - Errors/Warnings compiling mibs

- Cisco Number CSCsc36133

  There are several error/warnings when loading MIB files with high parsing level.

  This bug is fixed in SCOS 3.0.3.

SNMP - Platform type returns incorrect value

- Cisco Number CSCsc37490

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

  This bug is fixed in SCOS 3.0.3.

SNMP - SEMib -> trafficCountersGrp->trafficCountersTable – warning & more

- Cisco Number CSCsc36175

  trafficCountersTable: Value, Name, and Type not returned. Warnings are issued to the log when snmpwalk is executed on trafficCountersGrp.

  This bug is fixed in SCOS 3.0.3.

SNMP MIBS 'pcube' names are all still included

- Cisco Number CSCsc24434

  Pcube name appears in MIB comments, contacts and documentation

  This bug is fixed in SCOS 3.0.3.

  This defect was resolved only in the context of the document, contact information and comments. The *pcube* name still appears on descriptors and MIB names until final integration with Cisco is completed

RELEASE SCOS 3.0.1

Functional Enhancements

The SCOS release 3.0.1 contains all functional enhancements that were part of the 2.5.x SCOS releases, up to and including SCOS 2.5.9 (see *Release Notes for Cisco Service Control Operating System (SCOS) 2.5.9*, available at http://www.cisco.com/en/US/partner/products/ps6134/prod_release_notes_list.html).

Resolved Issues

In addition to some new bug fixes, the SCOS release 3.0.1 contains all bug fixes that were part of the 2.5.x SCOS releases, up to and including SCOS 2.5.9 (see *Release Notes for Cisco Service Control Operating System (SCOS) 2.5.9*, available at http://www.cisco.com/en/US/partner/products/ps6134/prod_release_notes_list.html).

The following bugs were fixed in this release.

Link failure-reflection and connection mode configurations not saved correctly

- Cisco Number CSCsd36257

  After changing the default link failure–reflection mode, the following commands are not written correctly to startup/running config:

  - **`link failure-reflection [on-all-ports] [linecard-aware-mode]`**
  - **`connection-mode {inline|inline-cascade|receive-only|receive-only-cascade}`**

  This bug is fixed in SCOS 3.0.1.

An additional reload due to an initialization problem while rebooting

- Cisco Number CSCsc86784

  In very rare cases, (less than 1%) the SCE platform experienced an initialization problem that resulted in an additional reload after the SCE platform had automatically recognized this situation.

  This bug is fixed in SCOS 3.0.1.

SNMP – Unpredictable results when trying to walk/get trap objects

- Cisco Number CSCsc27396

SNMP queries for trap objects that are part of the SCE MIB sometimes yielded unpredictable results.

This bug is fixed in SCOS 3.0.1.

Release SCOS 3.0.0

New Features

For more information regarding the new features in the Cisco Service Control release 3.0.0 in general, please refer to the "New Features" section of the *Release Notes for Cisco Service Control Application Suite for Broadband (SCA BB) 3.0.0*, available on the same site as the current document.

Packet processing hardware acceleration

Several 3.0.0 features allow the SCE platform to perform under higher network load:

- Hardware flow handshake management – Offloads SW processing and makes system more resilient to traffic bursts
- Traffic is bypassed through fast-path – Offloads system ingress queues and increases resilience to traffic bursts
- Anomaly detection integrated with congestion avoidance mechanism – In case of near exhaustion, attacks are being isolated and bypassed using hardware

Expected improvement of 30%

Value Added Services (VAS) Integration

The VAS integration capability enables classification and control of services not currently supported by SCA BB. The VAS feature allows the service provider to forward selected flows to an external, third-party solution for per-subscriber value-added functionality. A specified part of the traffic streams can be diverted to an individual VAS server or appliance, or a cluster of them. The diversion is based on the subscriber package, flow type and the availability of the VAS servers.

For more information, refer to "*Value Added Services (VAS) Traffic Forwarding*" in the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

Dual Link BW Control

This feature enables Global Controllers (GCs) to enforce BW control over traffic that spans two links. Using an SCE 2000 4xGBE platform for controlling these two links, the administrator can define the GC limit on the total throughput of both links.

This extends the functionality of previous SCA BB releases where GCs are defined separately for each link, and the administrator is only able to set a separate limit value for each of the link-specific controllers.

TACACS+

TACACS+ (Terminal Access Control Access Control System) is a Cisco sponsored access control protocol that allows customers to use one or more external servers to provide AAA services in a modular and independent way.

SCA BB release 3.0.0 supports the TACACS+ protocol on the SCE platform and provides the following functionality via the TACACS+ protocol:

- User authentication by a AAA server
- Privilege level and command authorization by a AAA server
- Accounting by a AAA server

For more information, refer to "*TACACS+ Authentication, Authorization and Accounting*" in the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

Second management port

Starting with SCOS 3.0.0, the second management port on the SCE platform is available, providing management interface redundancy. A virtual IP approach is implemented; only one port is active at any time, and the same IP and MAC addresses are used on both ports.

Upon failure of the active management port, the SCE platform detects a link problem on the active port and switches to the MAC address of the standby port. An SNMP trap is then generated indicating the event.

For more information, refer to "*Configuring the Management Interface and Security*" in the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

Management port resiliency

SCA BB release 3.0.0 improves the ability of the SCE platform to remain stable under flooding attacks on its management port. It also addresses vulnerabilities related to the TCP/IP stack control protocol. Identified attacks on the management port are reported in the form of an RDR.

For more information, refer to "*Management Interface Security*" in the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

Flow Filter Traffic Rules - Protocol Field Enhancement

Flow filter traffic rules, which enable hardware filters to by pass specified IP protocols, can be defined for any IP protocol in the range of 0 to 255. For example, it is possible to define flow filter rules to bypass all GRE, XTP, or IGP traffic. Configuration is done through the *SCA BB* console.

Dynamic RDR Routing

SCA BB 3.0.0 enables external configuration of RDR destinations based on their tag value. This provides the user with the flexibility to select the external systems the SCE platform works with and sends RDRs to (Subscriber Manager, Collection Manager, Billing Server, Policy Server, URL database, etc.) even if those external systems are running on separate machines.

For more information, refer to "*Dynamic Mapping of RDRs to Categories*" in the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

Additional CLI Privilege (Viewer)

A new CLI privilege level, called CLI VIEWER, is provided with SCOS 3.0.0. This level is enabled using the "enable 5" CLI command, but allows access to all 'show' commands enabled at level 10 (ADMIN level).

For more information, refer to "*CLI Authorization Levels"* in the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

SCE Platform Serviceability

A number of features have been implemented as part of SCOS 3.0.0 in order to increase the serviceability level of the SCE platform. The following are some of these serviceability features:

- Flow capture
- Support file retrieval in recover mode

Flow Capture

The Flow Capture capability allows the capturing of packets from the traffic stream in real time and storing them for later analysis using a standard capture file format. The classification of the captured traffic is based on Transport layer (layer 4) attributes.

Support File Retrieval in Recover Mode

The ability to generate a support file in recover mode is added to SCOS 3.0.0 using the same CLI command. It is important to note that the support file generated in recover mode may not contain some of the information that typically exists in the support files, since many device interfaces and HW drivers are blocked while in recover mode.

Features not Supported on All Platforms

Refer to the following table for a summary of new features that are supported only on the specific platforms listed.

Feature Name	Supported Platforms
2nd MNG port	SCE 2000 4xGBE SCE 1000 2xGBE 2U SCE 2000 4/8xFE
VAS	SCE 2000 4xGBE (Single device configuration)
Dual-Link BW Control	SCE 2000 4xGBE SCE 2000 4/8xFE

Resolved Issues

In addition to a number of new bug fixes, the SCOS release 3.0.0 contains all bug fixes that were part of the 2.5.x SCOS releases, up to and including SCOS 2.5.8 (see *Release Notes for Cisco Service Control Operating System (SCOS) 2.5.8*, available at http://www.cisco.com/en/US/partner/products/ps6134/prod_release_notes_list.html).

The following bugs were fixed in this release.

No timeout for current telnet session

- Cisco Number CSCsa94259

  When **`no timeout`** is configured for telnet sessions, the new configuration is applied only to new telnet sessions and not the current session.

  This bug is fixed in SCOS 3.0.0.

False duplex status detected for Fast Ethernet interfaces

- Cisco Number CSCsb86150

  When duplex status of Fast Ethernet interfaces (management interfaces and FE line interfaces) is configured to “auto”, it was reported by the SCOS as being “full”, as indicated by the **`show interface`** command and the SNMP interface.

  This bug is fixed in SCOS 3.0.0.

Link mode is cached even if the command fails

- Cisco Number CSCpu14006

  The configured link mode is cached in the line card even if the RPC fails. Thus, the command effectively succeeds even though the RPC failed.

  This bug is fixed in SCOS 3.0.0.

Detailed description for Link Down reason

- Cisco Number CSCpu13638

  The detailed reason for a link going down (such as link failure reflection or self box failure) was not indicated in the user log or SNMP interfaces

  This bug is fixed in SCOS 3.0.0.

Close all flows of anonymous subscriber when pull response is received

- Cisco Number CSCpu13530

  When anonymous subscriber context was updated during pull, all the flows were not properly closed.

  This bug is fixed in SCOS 3.0.0.

Cascade system upgrade documentation is misleading

The documentation of the SCE platform upgrade for cascaded solution is not clear enough and can be misleading.

This issue is fixed in SCOS 3.0.0.

Limitations and Restrictions

The upgrade to the SCOS 3.0.5 release 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 this 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	3.0.0	3.0.1	3.0.3	3.04	3.0.5	3.0.6
2.5.0	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.1	-	-	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.2	-	-	-	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.5	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.6	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.7	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.8	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.9	-	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes
3.0.0	-	-	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes
3.0.1	-	-	-	-	-	-	-	-	-	-	No	No	No	No
3.0.3												No	No	No
3.0.4													No	No
3.0.5														No

- The SCE platform may experience a reboot when a port scan operation is performed on the SCE platform 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 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

Problems may be encountered in downgrading from Release 3.0.5 to a previous release

- Cisco Number CSCse74400

  Downgrading from a system running SCOS 3.0.5 to a previous SCOS release may be unsuccessful until a second reload is performed. This is due to subscriber database incompatibility between 3.0.5 and previous versions resulting from the increase in the subscriber name size.

  Workaround: Clear the subscribers database after package installation of the downgraded version and prior to the reload by deleting all files under the directory */tffs0/system/p3hidden/partydb/*.

Errors in the debug log after loosing connection with the SM

- Cisco Number CSCsg61739

  The following error may appear in the SCE log in complex scenarios, where the SCE platform is configured to work with Quota Manager and the connection to the SM is down:

  "`<<ERROR>> [0x0920:0x000c] Logger: EM Agent: Error occurred during quotaUpdate operation on subscriber Subscriber is not logged in`".

Link failure may be reflected to all ports if a port is flickering due to a HW problem

- Cisco Number CSCsg46885

  When link reflection on all ports with linecard aware is configured, the link failure may be reflected to all ports (rather than only to the relevant link) if one of the ports that is connected to the failed linecard is flickering due to a hardware problem.

FTP operations fail if the username contains slash characters

- Cisco Number CSCsg46931

  FTP operations from the SCE platform fail when trying to access an FTP server with a username that contains slash characters. The following error message is received:

  `"host unreachable"`

"show snmp MIB pcube-SE-MIB port" returns wrong number of ports

- Cisco Number CSCsg45606

  The CLI command "**`show snmp MIB pcube-SE-MIB port`**" returns the wrong number of ports, because Mng port 2 is treated as traffic port instead of 2nd management port.

  Workaround: Use SNMP browser rather than CLI command.

Access violations

- Cisco Number CSCsg37325

  The following two scenarios may cause an access violation:

  - Configure: **`subscriber anonymous-group name sub1 IP-range 0.0.0.0/32`** and transmit traffic. Then remove this group and wait for the flow to end.

    Then configure: **`subscriber anonymous-group name sub1 IP-range 0.0.0.0/0`** and transmit traffic.

  - Configure **`anonymous-group name sub1 IP-range 0.0.0.0/32`** and **`anonymous-group name sub2 IP-range 0.0.0.0/0`**

    Then remove sub1.

BWC controller gives less bandwidth than configured

- Cisco Number CSCsg32201

  When BWC has many short UDP flows associated with it, such as eMule flows with very few packets each, the bandwidth given to all flows is lower than configured.

  Workaround: Configure Global Controllers to control the bandwidth

  There is no workaround when working with Service Bandwidth Controllers.

Subscriber with many mappings does not send all lease time expiration notifications

- Cisco Number CSCsg02338

  A subscriber with many mappings does not send lease time expiration notification on some mappings.

CLI "subscriber anonymous-group" appears in a different section in the running-config

- Cisco Number CSCse68542

  The CLI command "**`subscriber anonymous-group name <string> IP-range <string>`**" appears in the running/startup-config in a different '*interface linecard 0*' section from all the other commands.

This may create confusion for a user when verifying the configuration, however the order of the command in the configuration file has no effect on its execution after reload or the SCE platform behavior.

The IP of internal interfaces of the SCE is externalized in SNMP

- Cisco Number CSCsf28704

  SNMP walk on the MIB objects *ipAdEntIfIndex* and *ipAdEntAddr* return information on the internal IP interfaces, which are not accessible outside of the SCE platform.

PCUBE-SE-MIB logger counters are not correct

- Cisco Number CSCse34857

  PCUBE-SE-MIB logger counters are wrong.

  Use the CLI command **`show logger counters`** instead.

Part of the quota information not exchanged between two cascaded SCE platforms

- Cisco Number CSCsf97557

  Part of the quota information is not exchanged between two cascaded SCE platforms. This causes the failover in SCE cascade topology to be stateless with regard to quota. On SCE failover, all of the subscribers go into an immediate breach state. As a result, the external server has to provide quota to all active subscribers immediately after the failover.

  In addition, the first quota notification after failover contains a wrong quota report that the quota manager has to ignore

Output of "show snmp MIB pcube-SE-MIB application" differs from MIB response for the application group

- Cisco Number CSCsf29433

  CLI output differs from MIB response for the application group (*`apName`* and `apType`) the results are not the same. In the MIB response, the results for both *`apName`* (.1.3.6.1.4.1.5655.4.1.13.2.1.2) and *`apType`* (.1.3.6.1.4.1.5655.4.1.13.2.1.3) contain both the name and the type, while in the CLI output, each section holds only the name or type respectively.

destConnectionStatus of the rdr-formatter group is missing in " show snmp MIB pcube-SE-MIB rdr-formatter" command

- Cisco Number CSCsf29452

  The MIB object *`destConnectionStatus`* of the rdr-formatter group is missing in CLI '**`show snmp MIB pcube-SE-MIB rdr-formatter`**' command.

Potential memory overrun in cascaded environment with a high number of subscribers

- Cisco Number CSCsc96282

  Under rare conditions, the standby SCE platform of a cascaded pair crashes and restarts. This may happen in a scenario involving a heavy load of anonymous subscribers in cascade topology.

  In such a case, only the standby box is affected, and therefore:

  - overall service is not compromised
  - fault tolerance is compromised only for the time it takes the standby box to restart.

Consecutive connect /disconnect when SSH is enabled may cause reboot of the SCE platform

- Cisco Number CSCse16759

  Many SSH sessions in rapid succession may cause one of the following in the SCE platform:

  - reboot
  - loss of the Flash File System (for example, "**`dir`**" returns "`Error - Could not open /tffs0/`"). Can be accessed again after reboot.

Second Management port is not identified correctly on some MIBs queries.

- Cisco Number CSCsf20375

  In platforms that support a second management port, the following PCUBE-SE-MIB objects appear with the wrong port index:

  - *globalControllersDescription*
  - *txQueuesDescription*
  - *txQueuesUtilization*

Explicit NULL not supported for non-VPN traffic in MPLS/VPN auto-learn

- Cisco Number CSCsd61202

  In MPLS/VPN auto-learn mode, explicit NULL on non-VPN traffic from the P side prevents the SCE platform from learning non-VPN mappings. This only occurs when the system is configured to **MPLS VPN auto-learn**, and the P router sends explicit NULL label on the downstream non-VPN traffic.

  If non-vpn traffic is not managed, then this has no effect.

  Workaround: Make sure that the MPLS router performs penultimate hop popping.

The configured attack threshold is set for each PPC separately

- Cisco Number CSCsd48922

  For certain types of attacks, an attack is detected by the SCOS attack-filter module only if it is three times stronger (as measured by flow rate per second) than the configured value.

  This happens when the IP address common to all the flows of the attack is on the network side of the SCE platform, so all attacks of type 'single-side-network' have this problem.

When the VAS Health Check initializes, the CLI command "show interface LineCard 0 VAS-traffic-forwarding VAS server-id <id>" shows the server being UP even if it is actually Down

- Cisco Number CSCse05325

  The operative state of a VAS server while the Health Check is in Init state is considered to be Up as shown in the CLI command "show interface LineCard 0 VAS-traffic-forwarding VAS server-id <id>". In addition, during this time, the SCE platform may forward VAS traffic to this server.

Service Loss should be computed using the bypass-all FF rule counter

- Cisco Number CSCse04182

  The MIB counter *service-loss* is estimated using the *Rx-Congested packets* counter. It should use the *bypass-all flow-filter rule* counter instead.

CM - SCE TCP connection problem

- Cisco Number CSCsd87239

  Network connectivity on the management port may become intermittent. This might happen when the RDR-formatter destination is configured to connect to a device that cannot handle the rate of RDRs generated by the SCOS and also keep the TCP connection open.

  Workaround: The RDR-formatter destination should be configured to connect only to a proper CM device.

MPLS/VPN subscribers - only 2014 are used, instead of 2015

- Cisco Number CSCsd16031

  After the first logout of an MPLS/VPN subscriber, only 2014 MPLS/VPN subscribers can be simultaneously logged in. This is relevant to MPLS/VPN auto-learn mode.

  Workaround: Assume that the system only supports 2014 simultaneous MPLS/VPN subscribers, and design the deployment accordingly.

SCE1000 - Applying large policy causes "Out of Memory" error message

- Cisco Number CSCse17118

  Attempting to apply a policy that exceeds 10k entries of approximately 70 characters in length on an SCE 1000 (for example, an http URL flavor table) will cause the LUT (lookup table) to get full and a error message (“out of memory”) will be sent from the SCA BB console.

  Trying to apply a different policy afterwards (even with no LUT entries) will fail and give various error messages of the same type (“out of memory”).

  Recovery: Clear the LUT table manually by removing all the entries from it. Use the following (ROOT level) command.

  ```
  (config if)#lookup lookup-name remove-all
  ```

snmpwalk on mgmt.mib-2.at.atTable returns error

- Cisco Number CSCsd06743

  snmpwalk on mgmt.mib-2.at.atTable returns with the following error message:

  “Error – OID not increasing.”

Disk space issue during upgrade

- Cisco Number CSCsb68145

  Symptom: Installation of SCOS package is prevented due to insufficient disk space.

  Cause: Since some SCE 1000-1.5U platforms have disk space of 144MB, and the SCOS package size for 3.0.0 has been increased to approximately 65MB, there are many scenarios in which there would not be sufficient disk space for installing the new SCOS on the specific SCE 1000 device.

  In pre-3.0.0 versions, the size is about 10MB lower, but the symptoms might also be experienced due to disk maintenance related issues.

  To find out what disk capacity is on the SCE platform, use the **dir** command on the SCE platform, and add the amount of used and free disk space.

  Workaround: Use the following workaround until the problem is fixed:

Step 1. Login as ROOT on the SCE platform.

Step 2. Clear the logger files.

```
SCE1000#>clear logger device Debug-File-Log
Are you sure? y
SCE1000#>clear logger device Statistics-File-Log
Are you sure? y
SCE1000#>clear logger device Line-Attack-File-Log
Are you sure? y
SCE1000#>clear logger device Statistics-Archive-File-Log
Are you sure? y
SCE1000#>clear logger device SCE-agent-Debug-Log
```

Step 3. Delete the following files

```
SCE1000#>cd  /tffs0/system/p3hidden
SCE1000#>del vxworks
SCE1000#> cd /tffs0/system/p3hidden/fpga
SCE1000#> delete. /recursive
24 files and 1 directory will be deleted.
Are you sure? y
```

Step 4. Install the new SCOS package file.

Note If reboot occurs during this procedure, the box will get into recovery mode and only then will it be possible to perform the last step of package installation.

Non-coherent progress bar indication when extracting SCOS PKG

- Cisco Number CSCsc36110

  When running the command **`boot system ....pkg`** there is no visual indication of the progress of the installation. The progress bar halts for few minutes and then splashes all dots to the screen instantly.

  When running the command **`'copy running-config startup-config`**', the progress bar works properly.

Flow "opened from VAS" is misrouted if there is a FF rule to bypass

- Cisco Number CSCsc49573

  When VAS mode is enabled, the system generally assumes that traffic with a VLAN tag is VAS traffic coming from the VAS servers, and therefore forwards it to the non-VAS link. However, under the following conditions, a flow will be forwarded by the SCE platform on the same link on which it was received and with no VLAN tag:

  - VAS mode is enabled
  - The FIF packet has a VLAN tag
  - There is a traffic rule to bypass the flow *or* the SCE platform is in congestion

  In some topologies this behavior may cause VAS traffic to be incorrectly routed back to the VAS link.

Saving Configuration using SNMP Sometimes Fails

- Cisco Number CSCpu07664

  Cisco's proprietary SNMP allows saving of the SCE platform 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.)

SNMP Time-related Variables May Become Incorrect

- Cisco Number CSCpu09409

  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 CSCpu09565

  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 CSCpu11798

  When a PQI application file is installed or upgraded on the SCE, the SCE may lose a few packets for a few seconds. The overall percentage of this phenomenon is very low.

  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 install pqi is completed, use:
    `(config if)#default link mode`

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* (on page 41) 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 41), 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.