Release Notes for Cisco Service Control Operating System, Release 3.8.x

First Published: September 26, 2012
Last Updated: Oct 29, 2013
OL-26875-06

Note This document supports all the 3.8.x releases of the Cisco Service Control Operation System (Cisco SCOS).

The release notes for the Cisco SCOS describe the functional enhancements and fixes provided in the Cisco SCOS Release 3.8.x. These release notes are updated as needed.

For a list of the open caveats that are applicable to Cisco SCOS Release 3.8.x, see the "Open Caveats" section on page 6. Some caveats are applicable only to the Cisco Service Control Engine (Cisco SCE) 8000 platform, some to the Cisco SCE 2000 and Cisco SCE 1000 platforms, and others to all the Cisco SCE platforms.

Contents

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

Introduction

Cisco SCOS Release 3.8.x for Cisco SCE platforms contains new features, as well as fixes for issues that were identified during internal testing and customer interaction.

This document outlines the functional enhancements and resolved issues delivered in Cisco SCOS Release 3.8.x. It assumes that the reader has substantial knowledge of the Cisco Service Control solution. For more information Cisco SCE products and features, see the Cisco SCE documentation.

To access the new Cisco Service Control online documentation site, do the following:

1. On Cisco.com, go to http://www.cisco.com/cisco/psn/web/psa/default.html?mode=prod.
2. From the Products list, select **Service Exchange > Cisco Service Control > Cisco Service Control Product**.

Limitations and Restrictions

Upgrading from Cisco SCOS Release 3.0.0 and Earlier

Upgrading from Cisco SCOS Release 3.0.0 and earlier may result in reinitialization of the Cisco SCE 1010 or Cisco SCE 2020 hardware bypass module. This reinitialization may cause a failure of the GBE link when the system stalls for less than one second.

Port Scan on Cisco SCE

When you perform a port scan operation on the Cisco SCE platform management port, the platform may experience a reboot. This reboot occurs because of scheduling optimization for detecting failover conditions during periods of less than one second in a configuration involving two cascaded Cisco SCE platforms. We recommend the following:

- Use IP access lists to eliminate port scans that take place because of actual attacks.
- If the system administrator must perform a port scan operation as part of the security check, we recommend that you disable the Cisco SCE watchdog only for the period during which the port scan is performed.

  To disable the Cisco SCE watchdog, use the following root-level CLI commands:

```
SCE#> configure
SCE(config)#> watchdog software-reset disabled
SCE(config)#> interface linecard 0
SCE(config if)#> no watchdog
```

- To re-enable the Cisco SCE watchdog, use the following root-level CLI commands:

```
SCE#> configure
SCE(config)#> watchdog software-reset enabled
SCE(config)#> interface linecard 0
SCE(config if)#> watchdog
```

Cisco Service Control Operating System Release 3.8.5

This section describes the compatibility information, new features, resolved issues, and open issues pertaining to Cisco SCOS Release 3.8.5:

Compatibility Information

For information about the Cisco SCE platforms that are compatible with Cisco SCOS Release 3.8.5, see the *Cisco Service Control Application for Broadband Download Guide*.

Cisco SCOS Release 3.8.5 is compatible only with Cisco SCMS Collection Manager Release 3.7.5-p1 and later.

New and Enhanced Features

This section describes the major Cisco SCE platform-related new features and enhancements in Cisco SCOS Release 3.8.5:

- IPv6 subscriber support through Subscriber Manager.

Enhanced IPv6 Features

Cisco SCE supports software-based processing of IPv6 traffic on Cisco SCE 8000 devices. Cisco SCOS Release 3.8.5 introduces the following IPv6 features:

- Enhanced Raw Data Records
- Import and export of subscriber information and anonymous groups.

Raw Data Records

The following Raw Data Records are enhanced for IPv6:

- RTSP Transaction Usage RDR
- VOIP Transaction Usage RDR
- Video Transaction Usage RDR
- Flow Start RDR
- Flow Ongoing RDR
- Flow End RDR
- SPAM RDR
- Media Flow RDR
- Virtual Links Usage RDR

- Anonymized Spam RDR
- Anonymized Video Transaction Usage RDR
- Anonymized VoIP Transaction Usage RDR
- Anonymized RTSP Transaction Usage RDR
- Anonymized Flow Start RDR
- Anonymized Flow Ongoing RDR
- Anonymized Flow End RDR
- Anonymized Transaction RDR
- Anonymized Transaction Usage RDR
- Anonymized HTTP Transaction Usage RDR
- Anonymized Blocking RDR
- Anonymized Media Flow RDR

While the existing structure of the RDRs is maintained, three new fields—IP_type, ServerIPv6Address, and ClientIPv6Address—are added to the event-based RDRs and IP-type field is added to Virtual Link Usage RDR. The IP_Type field has two values—0 for IPv4 and 1 for IPv6. The subscriber ID and the subscriber IPv6 address are hashed in the Anonymous RDRs.

Import and Export of Subscriber Information and Anonymous Groups

From SCOS Release 3.8.5, you can import and export subscriber information and anonymous groups to the Cisco SCE device.

Flow-Filter Enhancements

Cisco SCOS Release 3.8.5 introduces the following flow-filter enhancements:

- Support for IPv6 advanced service configuration options.
- Rules from 0 to 63 are reserved for IPv4 flow-filters.
- Rules from 64 to 128 are reserved for IPv6 flow-filters.

Resolved Issues

This section describes the resolved caveats pertaining to Cisco SCOS Release 3.8.5:

- Resolved Issues—Cisco SCE 8000, page 4
- Resolved Issues—All Platforms, page 6

Resolved Issues—Cisco SCE 8000

This section describes the resolved caveats in the Cisco SCE 8000 platform in Cisco SCOS Release

CSCtq20627

When a PQB is pushed or any other operation is performed on the Cisco SCE 8000 platform with high CPU utilization, the platform or the CLI fails to respond.

This issue is resolved.

CSCtx51801

On Cisco SCE 8000, when the device tries a push logon for a Gx subscriber, Cisco SCE fails with timeout error messages in the CLI output.

This issue is resolved.

CSCty73906

Downgrading Cisco SCOS Release 3.7.5 to a previous release displays error messages.

While downgrading Cisco SCOC Release 3.7.5 to Release 3.7.2, an error message similar to the following is displayed:

```
"Could not allocate 7383087 bytes for Control Application XML data partition"
```

The downgrae procedure has been added to the Cisco SCE8000 GBE Installation and Configuration Guides, and the Cisco SCE8000 10GBE Installation and Configuration Guides.

CSCty99703

If the time zone of Cisco SCE 8000 devices are modified through Cisco SCA BB Quota Manager, the device fails to adjust the aggregation period to the new time zone. The aggregation period is calculated based on the default UTC time zone even if a different time zone is configured.

This issue is resolved.

CSCtz57916

On Cisco SCE 8000 devices, when the subscribers are mapped to different UpVlink and DownVlink, the active subscribers displayed using the **show party all-party-with-open-flows** command may not match with the subscribers listed in the generated VLUR.

This issue is resolved.

CSCub72077

When the Cisco SCE devices reload because of a power off or a hardware failure, the electronic bypass fails to pass the traffic for about 40 seconds.

The Cisco SCE8000 10GBE Installation and Configuration Guides and the Cisco SCE8000 GBE Installation and Configuration Guides have been updated with the correct down time.

CSCuc05881

Cisco SCE 8000 devices add error messages to the debug log when there are IPv6 hwflows in the hwsim when the interface linecard is being shut down.

The messages state that all the allocated heap memory is not freed properly during the shutdown operation. The heap memory is completely freed when the device is shut down and does not affect the Cisco SCE devices.

This issue is resolved.

CSCuc06549

When the SNMP accelerate-query is configured and the SNMP is enabled on a Cisco SCE 8000 device, the device may restart abruptly while installing the pqi.

This issue is resolved.

CSCuc76451

Cisco SCE 8000 devices may fail after upgrading to Cisco SCOS Release 3.8.0.

This issue is observed when the default configuration is applied with Host Based Classification (HBC) enabled.

This issue is resolved.

CSCuc15960

When Diameter Gy is enabled and disabled, CCR-T fails to carry usage information when the Gx+ subscriber logs out. The quota bucket state always shows the subscriber in the breached state.

This issue is resolved.

CSCuc16315

Cisco SCE 8000 devices fail to create more than 20,000 zone indices. The devices display error when applying policies.

Cisco SCE Release 3.8.0 supports 20,000 zone indices, including IPv4 and IPv6 zones.

This issue is resolved.

CSCuc17799

Cisco SCE 8000 devices failed during a maximum flow testing for IPv6 traffic. This issue was observed when software flow aging was set to the maximum supported value, and the traffic was pushed at a higher rate and the traffic pattern tried to create flows continuously.

This issue is resolved.

CSCuc23894

The total number of active subscribers in the Package Usage RDR is more than the actual count. This issue is observed when policies contain different packages and anonymous groups, and the configuration of these anonymous groups or packages is removed when the traffic is flowing.

This issue is resolved.

Resolved Issues—All Platforms

CSCtk08011

Transmit queue overflow warnings appear when VLURs are enabled.

This issue is resolved.

Open Caveats

This section describes the open caveats pertaining to Cisco SCOS Release 3.8.x. It consists of the following sections:

- Open Caveats—Cisco SCE 8000, page 7
- Open Caveats—Cisco SCE 1000 and Cisco SCE 2000, page 11
- Open Caveats—All the Cisco SCE Platforms, page 12

Open Caveats—Cisco SCE 8000

This section describes the open caveats pertaining to the Cisco SCE 8000 platform for Cisco SCOS Release 3.8.x.

CSCui37822

IPv6 packets are corrupted if ToS marking is enabled.

This issue is observed for common services or rules that contain both IPv4 and IPv6 packets.

Workaround: Map IPv6 services to a separate package and disable ToS marking for that package.

CSCuf85505

The upgrade procedure fails on Cisco SCE devices configured in a cascade setup while upgrading from Cisco SCOS Releases 3.7.5 and 3.7.5p1 to Cisco SCOS Releases 3.8.0 and later.

Workaround: Remove the Cisco SCE devices from the cascade setup and configure the devices as standalone devices, then upgrade each devices separately. Note that this upgrade procedure may cause a service disruption.

CSCuc87456

When SNMP queries are sent to the Cisco SCE for invalid IDs, the device runs out of memory and takes more time to respond to valid IDs.

Workaround: There is no workaround.

CSCud42080

When VAS is enabled, the IPv4 fragmented traffic that enters the Cisco SCE creates a loop in VAS interfaces.

It happens when these conditions are met:

- VAS farwarding is enabled.
- The Cisco SCE detects some IPv4 fragments.
- The Cisco SCE recovers from a congestion.

Workaround: Avoid congestion.

CSCsq95048

The IP table contains entries for internal IP addresses and interfaces. This results in inconsistency in the If index representation of the following components in the IP table:

- ipAddrTable
- ipRouteTable
- ipNetToMediaTable

Workaround: Ignore all the entries in the IP tables, except for the management interface. See the following examples:

The If MIB represents five interfaces as follows:

- If index 1—mng port
- If index 2—Traffic port 0
- If index 3—Traffic port 1
- If index 4—Traffic port 2

- If index 5—Traffic port 3

The IP tables and the AT tables represent six interfaces as follows:

- If index 1—eth0 “currently simba to simba”
- If index 2—eth1 “mng port”
- If index 3—eth2 “cofico 1 that is not connected”
- If index 4—lo
- IfDescr.5—dummy0 “configure to skynet”
- IfDescr.6—skynet0

  The only relevant ifIndex in these tables is the management interface, with IfIndex 1 in the If table being equal to IfIndex 2 in the IP tables.

CSCtc28950

DDoS global attacks (such as TCP syn and UDP fragment) do not result in sending a relevant SNMP trap. Note, however, that specific IP DDoS attacks send relevant SNMP traps.

Workaround: There is no workaround.

CSCte34741

The **show interface LineCard 0 subscriber name** <*sub_name*> **bucket-state** CLI command shows the wrong bucket status for breached buckets.

This issue is observed when the command is run in the context of a subscriber with several buckets in different states (with some of them in breached status), the output shows that all the buckets are in the *not breached* state.

When you run the **show interface LineCard 0 subscriber name** <*sub_name*> **bucket-state id** <*bucket_id*> CLI command on a specific bucket in breached state, the bucket status is *breached*. If you run the general **show bucket-state** CLI command after running the **show bucket-state id** command, the output shows the status as *breached*.

Workaround: There is no workaround.

CSCtd87721

When a peer is removed from a Cisco SCE device in the high-availability forwarding mode, the device fails to replace the details in the peer list automatically. As a result, the device fails to send CCRs when the primary Gy peer is removed.

Workaround: There is no workaround.

CSCtf24792

In a chassis with two SCE8000-SCM modules installed, the management ports of the second SCM are active. If you plug a network cable into the management port of the SCE8000-SCM in slot 2, the Link LED turns on. The Link LED status may confuse you because this port has no IP address configured and should not be used.

Workaround: Use only the management ports of the SCE8000-SCM in slot 1.

CSCtf43847

The **snmpget** command returns the message `No Such Object available on this agent at this OID` even if you request for a correct OID. This issue is observed when getting the support file or when applying a policy. The issue is observed more often when you request multiple OIDs in one **snmpget** command.

Workaround: Request only one OID per **snmpget** command.

CSCth82475

After package change, CCR-U messages continue to be sent every 30 seconds.

Workaround: There is no workaround.

CSCti15865

The Cisco SCE 8000 crashes during Gx/Gy capacity testing while having 250,000 active sessions with long VSAs, with all VSAs being more than 200 bytes.

Workaround: Use normal VSAs rather than long VSAs.

CSCtj37754

No SNMP trap is sent when the **external-bypass** command is issued on Cisco SCE 8000 GBE when the OPB-SCE8K-2L-SM optical bypass modules are installed.

Workaround: There is no workaround.

CSCtj46134

Cisco SCE 8000 uses software to process the VAS, and this impacts the performance of the device. Therefore, VAS processing is not supported for delay-sensitive, bundled, flow handling.

This issue is a known limitation.

Workaround: There is no workaround.

CSCtj50046

The *on-failure cutoff* option of the **connection-mode** command does not block traffic for a few minutes when Cisco SCE 8000 is rebooted.

Workaround: There is no workaround.

CSCtk67558

The notification of the first QuotaStatus RDR is delayed after subscriber logon. Subsequent notifications come through correctly.

Workaround: There is no workaround.

CSCtl10121

SNMP traps are not sent when only one of the eight fans fail.

Workaround: There is no workaround.

CSCts94869

In the **show interface linecard 0 counter** command output, the IPv6 packets are accounted as non-IP packets.

Workaround: Use IPv6 bytes counter or Link Usage RDRs (LURs).

The IPv6 bytes are available from the IPv6 bytes counter and from the Link Usage RDRs. The Non-IP Packets field shows both the IPv6 packets and the non-IP packets.

CSCtu12409

In the **show interface linecard 0 counter** command output, the DP L2TP Control Packet Count field shows DP IPv6 byte sizes. The L2TP packet count is not displayed.

Workaround: There is no workaround.

CSCty13726

The Cisco SCE 8000 platform that is configured in the IP-Tunnel L2TP Skip mode does not process traffic on the first traffic processor.

The device fails to process traffic because of bad handling of non-first-fragment packets. Therefore, in networks with some IP fragmentation, it is likely that the problem may not be observed even if IP-Tunnel L2TP Skip is configured.

The appropriate workaround depends on whether L2TP tunneled traffic must be processed based on the internal IP layer.

Note This workaround is not applicable to a cascade configuration.

- If L2TP tunneled traffic need not be processed based on the internal IP layer.

  Workaround: Disable L2TP Skip.

- If L2TP tunneled traffic must be processed based on the internal IP layer.

  Workaround:

  Run the following root-level CLI command:

  ```
  debug slot 0 ppc 0 func SimbaDPT[0].4DP[0].RegWr16 0x28 0x1000
  ```

  This command provides an immediate solution to the problem, but it is not persistent across reboots. To make this **debug** command run during the Cisco SCE 8000 boot-up process, add the command to the genstart.txt file.

  The genstart.txt file is located at /apps/data/scos/system/p3hidden/config/ (or /system/p3hidden/config/ from the Cisco SCE CLI). The genstart.txt file must exist on your Cisco SCE disk space and must be empty. If the file does not exist, create it under /apps/data/scos/system/p3hidden/config/.

  To edit the file, copy the file from the Cisco SCE platform to an FTP server using FTP. Add the following line to the file:

  ```
  do debug slot 0 ppc 0 func SimbaDPT[0].4DP[0].RegWr16 0x28 0x1000
  ```

  After editing, copy the file back to the Cisco SCE platform using FTP.

  The following sample CLI session shows how to copy the file to an FTP server and how to copy the file back to the appropriate folder in the SCE platform:

  ```
  copy ftp://username:password@10.1.1.30/./genstart.txt
  /system/p3hidden/config/genstart.txt
  ```

  After copying the file to the SCE platform, verify whether the appended line appears in the file:

  ```
  more /system/p3hidden/config/genstart.txt
  do debug slot 0 ppc 0 func SimbaDPT[0].4DP[0].RegWr16 0x28 0x1000
  ```

CSCtz74897

The Total Link Limit feature fails on Cisco SCE 8000 devices when multiple global controllers are configured.

Workaround: Use only one global controller while using the Total Link Limit feature.

CSCua98956

Cisco SCE 8000 devices in a cascade setup running Cisco SCOS Release 3.7.2 and later, fail to replicate the anonymous subscribers created in an active device to the standby device. This issue is observed when using the **clear interface line 0 subscriber anonymous all** command.

Workaround: There is no workaround.

CSCub42442

When two Cisco SCE 8000 devices running Cisco SCOS Release 3.7.5 and later, are configured as active and standby for redundancy, the active device fails to sustain in the standby mode after a reload.

Workaround: There is no workaround.

CSCub93514

On Cisco SCE 8000 devices running Cisco SCOS Release 3.7.5-p1 and later, the Gy interface may be enabled after you restart the device even if the Gy interface is disabled and the configuration is saved to the startup configuration.

Workaround: Disable the Gy interface again and restart the device.

Open Caveats—Cisco SCE 1000 and Cisco SCE 2000

This section describes the open caveats pertaining to Cisco SCE 1000 and Cisco SCE 2000 platforms for Release 3.8.x.

CSCud38306

The Framed-IPv6-Prefix field was added to the following RDRs for Cisco SCE 8000 device in Cisco SCOS Release 3.8.0:

- Subscriber Usage RDR
- HTTP Transaction Usage RDR
- Video Transaction Usage RDR

Although the Cisco SCE 2000 does not support IPv6, this field has to be added to the three RDRs.

Workaround: There is no workaround.

CSCtd18312

Cascade links may remain down when link failure-reflection is configured if:

- Link failure-reflection is configured on both the SCE platforms.
- Both the cascade links are disconnected and then connected again.

Workaround: Disable and enable link failure-reflection on the secondary Cisco SCE platform. Execute the following CLI command sequence on the secondary SCE:

```
# configure
(config)# interface LineCard 0
(config if)# no link failure-reflection
(config if)# link failure-reflection
(config if)# exit
(config)# exit
```

CSCti17836

When SSH sessions are rapidly opened and closed and FTP sessions are run simultaneously, the Cisco SCE 2000 crashes with a fatal SafeFdManager error. Note that this issue is not observed in Cisco SCOS Release 3.6.x.

Workaround: Disable SSH.

CSCti18005

When SSH sessions are rapidly opened and closed, traffic rate is 1 GBE, and FTP sessions are run simultaneously, Cisco SCE 2000 crashes with a critical Section error. Note that this occurs only in Cisco SCOS Release 3.6.1 and is not observed in Cisco SCOS Release 3.6.5.

Workaround: Disable SSH.

Open Caveats—All the Cisco SCE Platforms

This section describes the open caveats pertaining to all the platforms of Cisco SCE for Release 3.8.x.

CSCud35704

An access control list configured using the CLI is deleted when applying a policy even after disabling anomaly-based detection of malicious traffic.

Workaround: Disable anomaly-based detection from the Service Security Dashboard.

CSCuc93224

When there is a package switch from the Subscriber Manager, the Cisco SCE does not update the package ID in RDRs. This is because the device continues to use the old package ID even after the internal package of the device changes.

Workaround: There is no workaround.

CSCtc56711

Cisco SCE fails to authenticate subscriber logon through the TACACS server when the shared key contains spaces. This causes the login operation to the SCE to fail although a valid user name and password is used. Cisco SCE does not treat the space as a valid character in the key and terminates the key at the first space.

For example, if the configured key is 3b663ea010446e 72ecea2f1244853f73, Cisco SCE takes the key as 3b663ea010446e.

Workaround: Do not use keys that contain spaces.

CSCtd94013

Cisco SCE fails to control the bandwidth properly if fragmented UDP packets from the subscriber side arrive at the device at a rate that is higher than the Permitted Information Rate (PIR) because the fragmented packets are not dropped at the network side.

Workaround: Avoid using fragmented packets. Use the **no accelerate-packet-drops** CLI command to throttle fragmented packets at the software level.

CSCtl22778

The Gy reports lower volume consumption because of delay in quota allocations. The volume reported through RDR varies from the volume reported by the Gy.

This issue is observed when the Gy quota profile is configured for the subscriber and quota is requested based on the classification. HTTP flow creation takes a few seconds from the time of request submission to Cisco SCE.

Workaround: There is no workaround.

CSCtn31028

HTTP redirection does not work with GRE tunnel external fragmentation.

Workaround: There is no workaround.

CSCtq67752

Quota breach is enforced only after the completion of file download. For example, a large file with a size that exceeds the available quota limit gets downloaded, but the next download gets blocked.

Workaround: There is no workaround.

CSCts66524

When there are many short-lived subscribers, Cisco SCE raises CAT 4 RDRs even at a low RDR rate.

Workaround: Disable or increase the remaining quota RDR timing so that the CAT 4 RDR rate is lowered.

CSCtt70539

HTTP redirection does not work in the HTTP 404 error code pages.

Workaround: There is no workaround.

CSCtw34069

During the installation of a new Cisco protocol update in Cisco SCOS, the subscribers may lose their mappings and be assigned with package 0 mappings.

Workaround: Clear the subscribers using the following CLI commands:

```
SCE# configure terminal
SCE(config)> interface lineCard 0
SCE(config if)> no subscribers all
```

CSCtx47997

On Cisco SCE devices, when a port-based classification is applied using Cisco SCA BB, the following issues are observed:

- Link Usage RDR with global usage counter ID 0 is always generated, even though there are no matching flows, along with the specific global usage counter ID on which there is a matching flow.
- Zero RDRs, which are supposed to be generated at the time of pushing the traffic, are generated at the next fifth minute.
- Link Usage RDRs are generated with the value 0 for all metrics, except for total active subscribers.
- Link Usage RDR is different for TCP and UDP.

Workaround: There is no workaround.

CSCty18403

On Cisco SCE devices, packet drops are observed while upgrading the protocol pack (SPQI).

Workaround: There is no workaround.

CSCty38340

Cisco SCE devices running Cisco SCOS Release 3.5.5 may report incorrect quota consumption information when used with multiple buckets and time frames.

Workaround: There is no workaround.

Cisco Service Control Operating System Release 3.8.0

This section describes the compatibility information, new features, resolved issues, and open issues pertaining to Cisco SCOS Release 3.8.0:

Compatibility Information

For information about the Cisco SCE platforms that are compatible with Cisco SCOS Release 3.8.0, see the *Cisco Service Control Application for Broadband Download Guide*.

Cisco SCOS Release 3.8.0 is compatible only with Cisco SCMS Collection Manager Release 3.7.5-p1 and later.

New and Enhanced Features

This section describes the major Cisco SCE platform-related new features and enhancements in Cisco SCOS Release 3.8.0:

- Enhanced IPv6 features
- SNMP Walk Acceleration for linkServiceUsage Queries

Enhanced IPv6 Features

Cisco SCE supports software-based processing of IPv6 traffic on Cisco SCE 8000 devices. The features that are available for IPv4, such as traffic processing, application classification and control, and management APIs, are available for IPv6 too.

Cisco SCOS Release 3.8.0 enhances the IPv6 capabilities of Cisco SCE 8000 devices by providing support to both IPv4 and IPv6 traffic simultaneously on all traffic processors, based on the system mode configuration.

Note From Cisco SCOS Release 3.8.0, IPv6 traffic works on the subscriber awareness mode.

Cisco SCOS Release 3.8.0 introduces the following IPv6 features:

- Subscriber-based classification for IPv6 traffic
- Subscriber-based bandwidth control
- Content filtering for IPv6 traffic flows
- Dual stack support on all traffic processors
- Reporting and monitoring of IPv6 traffic
- Support for IPv6 fragmentation and zones
- IPv6 Bundling support in DS Lite
- Introduce IPv6 subscribers through Gx

- Enhanced Raw Data Records
- New system mode configuration for Cisco SCE 8000 devices

Raw Data Records

The following Raw Data Records are enhanced for IPv6:

- Package Usage RDR
- Zone Usage RDR
- Subscriber Usage RDR
- Real-time Subscriber RDR

While the existing structure of the RDRs is maintained, a new field—IP_type—is added as the last field in the RDR.

System Modes

The system mode configuration replaces the IPv6 environment configuration used in the Cisco SCOS Release 3.7.5. Cisco SCE 8000 devices work on the following three system modes:

- IPv4 only system mode
- IPv6 only system mode
- Dual Stack system mode

SNMP Walk Acceleration for linkServiceUsage Queries

SNMP walk acceleration enables Cisco SCE 8000 devices to perform SNMP queries for linkServiceUsage MIB queries in the background, and cache the results. This enhancement makes SNMP walks considerably faster.

Resolved Issues

This section describes the resolved caveats pertaining to Cisco SCOS Release 3.8.0:

- Resolved Issues—Cisco SCE 8000, page 16
- Resolved Issues—Cisco SCE 1000 and Cisco SCE 2000, page 18
- Resolved Issues—All Platforms, page 19

Resolved Issues—Cisco SCE 8000

This section describes the resolved caveats in the Cisco SCE 8000 platform in Cisco SCOS Release 3.8.0.

CSCtc63059

The SNMP responses for the MIBs under pcube Enterprise MIB tree 1.3.6.1.4.1.5655 from Cisco SCE 8000 devices are slower than the responses from the Cisco SCE 2000 or Cisco SCE 1000 devices. This behavior is not observed on standard MIBs.

Cisco SCOS Release 3.8.0 provides a better response time.

CSCtu02839

Cisco SCE 8000 devices with Cisco SCOS Release 3.7.0 failed to send the Framed IP address in CCR-T messages.

This issue is resolved.

CSCtx10148

Cisco SCE 8000 devices with dual SCM modules failed to support 16 million bidirectional flows when there were 250,000 subscribers.

This issue is resolved.

CSCtx53825

On Cisco SCE 8000 devices, the SNMP agent failed to start while restarting the SNMP process after the SNMP agent timer was increased to 30. This issue was observed on devices running Cisco SCOS Release 3.6.5 in a dual SCM scenario.

This issue is resolved.

CSCty21517

On Cisco SCE devices, TCP/UDP fragmented packets on non-VAS links created a layer 2 loop condition on VAS links (link-0/link-1).

This issue is resolved.

CSCty32405

The *Cisco Service Control Application for Broadband Reference Guide, Release 3.7.x,* with part number OL-24174-03, showed an unknown data type “ADDRESS” for the RDR fields 3GPP2-PCF-IP-Address and 3GPP2-Home-Agent-IP-Address.

The data type “ADDRESS” is equivalent to UINT32.

This issue is resolved.

CSCty42786

The Gx/Gy implementation sent VALIDITY time expired message before the expiry of the time that was passed in AVP to the OCS. This issue was observed when the remaining quota RDR was enabled.

This issue is resolved.

CSCty64289

During a normal bootup of Cisco SCE 8000 devices, errors similar to the following appeared:

```
"some hardware versions are incompatible with this software!"
```

This issue is resolved.

CSCty65884

The Cascade setup did not work when the first traffic processor card on the Cisco SCE 8000 was configured for IPv6, and the second for IPv4.

This issue is resolved.

CSCty72702

Subscribers were not visible in Cisco SCE when there were UDP unidirectional flows or TCP unidirectional flows from the network side to the subscriber side.

This issue is resolved.

CSCty78963

When media flow, flow start RDRs, and flow end RDRs were enabled for IPv6 traffic, and at least one traffic processor card was configured for IPv6, messages similar to the following were seen in the debug log:

```
03/20/12  15:02:52 [000000942820:187:298] | 004 | 0000000349 | 0000000 | <<ERROR>>
[0x0814:0x00a4] Function Pool Flow Handling Nodes: FncplFlow::funcGetFlowTuple- Wrongly
invoked for IPv6 Flow - tupleType = 1
```

This issue is resolved.

CSCty99812

The Cisco SCE Diameter CCR-T messages contained invalid characters in the session-id field. This issue was observed on devices running Cisco SCOS Release 3.7.0,

This issue is resolved.

CSCua56086

The Cisco SCE devices initialized after a series of peer failures, and the TCP sessions flapped continuously.

This issue is resolved.

CSCua99181

High resource utilization and device reload were observed when Cisco SCE 8000 devices with Cisco SCOS Release 3.7.5 failed to free the memory heap that the device consumed.

This issue was observed when there was a high logon rate from Cisco Service Control Subscriber Manager Release 3.7.5 with the RADIUS listener configured.

This issue is resolved.

Resolved Issues—Cisco SCE 1000 and Cisco SCE 2000

This section describes the resolved caveats in the Cisco SCE 1000 and Cisco SCE 2000 platforms in Cisco SCOS Release 3.8.0.

CSCtz20343

The IP_TYPE field was missing in LUR RDRs sent from Cisco SCE 2000. The Cisco SCE 2000 failed to insert the IP_TYPE field when the field was not received from the Cisco SCMS Collection Manager RDR handler for LUR.

This issue is resolved.

Resolved Issues—All Platforms

CSCtu92802

The Cisco SCE devices with Cisco SCOS Release 3.6.1 and later restarted while the subscribers were logging out. Most of the instances were observed when the subscribers with multiple IP addresses were logging out.

This issue is resolved.

CSCtw48261

Cisco SCE devices moved to the recovery mode while upgrading from Cisco SCE Release 3.6.5 and Cisco SCE Release 3.7.0. This issue was observed when an application programming interface (API) initiated a connection during the reboot.

This issue is resolved.

CSCtx33874

Cisco SCA BB failed to apply policies on Cisco SCE devices. The following message appeared while trying to apply policies:

```
Error Code = 8, Description: "Party 'N/A' already exists.", Detailed: ""
(PRT_setDefaultPartyNameCfg:{name=N/A})
```

This issue was observed while applying policies after the Cisco SCE was reset to the factory default using the **erase startup config** command.

This issue is resolved.

CSCty38051

On Cisco SCE devices, when the Vlink mode was enabled and the link global controllers were set to unlimited for each link, the AGC failed to control the traffic.

This issue is resolved.

Open Caveats

This section describes the open caveats pertaining to Cisco SCOS Release 3.8.x. It consists of the following sections:

- Open Caveats—Cisco SCE 8000, page 20
- Open Caveats—Cisco SCE 1000 and Cisco SCE 2000, page 27
- Open Caveats—All the Cisco SCE Platforms, page 28

Open Caveats—Cisco SCE 8000

This section describes the open caveats pertaining to the Cisco SCE 8000 platform for Cisco SCOS Release 3.8.x.

CSCuf85505

The upgrade procedure fails on Cisco SCE devices configured in a cascade setup while upgrading from Cisco SCOS Releases 3.7.5 and 3.7.5p1 to Cisco SCOS Releases 3.8.0 and later.

Workaround: Remove the Cisco SCE devices from the cascade setup and configure the devices as standalone devices, then upgrade each devices separately. Note that this upgrade procedure may cause a service disruption.

CSCsq95048

The IP table contains entries for internal IP addresses and interfaces. This results in inconsistency in the If index representation of the following components in the IP table:

- ipAddrTable
- ipRouteTable
- ipNetToMediaTable

Workaround: Ignore all the entries in the IP tables, except for the management interface. See the following examples:

The If MIB represents five interfaces as follows:

- If index 1—mng port
- If index 2—Traffic port 0
- If index 3—Traffic port 1
- If index 4—Traffic port 2
- If index 5—Traffic port 3

The IP tables and the AT tables represent six interfaces as follows:

- If index 1—eth0 “currently simba to simba”
- If index 2—eth1 “mng port”
- If index 3—eth2 “cofico 1 that is not connected”
- If index 4—lo
- IfDescr.5—dummy0 “configure to skynet”
- IfDescr.6—skynet0

  The only relevant ifIndex in these tables is the management interface, with IfIndex 1 in the If table being equal to IfIndex 2 in the IP tables.

CSCtc28950

DDoS global attacks (such as TCP syn and UDP fragment) do not result in sending a relevant SNMP trap. Note, however, that specific IP DDoS attacks send relevant SNMP traps.

Workaround: There is no workaround.

CSCte34741

The **show interface LineCard 0 subscriber name** <*sub_name*> **bucket-state** CLI command shows the wrong bucket status for breached buckets.

This issue is observed when the command is run in the context of a subscriber with several buckets in different states (with some of them in breached status), the output shows that all the buckets are in the *not breached* state.

When you run the **show interface LineCard 0 subscriber name** <*sub_name*> **bucket-state id** <*bucket_id*> CLI command on a specific bucket in breached state, the bucket status is *breached*. If you run the general **show bucket-state** CLI command after running the **show bucket-state id** command, the output shows the status as *breached*.

Workaround: There is no workaround.

CSCte92800

When a peer is removed from a Cisco SCE device in the high-availability forwarding mode, the device fails to replace the details in the peer list automatically. As a result, the device fails to send CCRs when the primary Gy peer is removed.

Workaround: There is no workaround.

CSCtf24792

In a chassis with two SCE8000-SCM modules installed, the management ports of the second SCM are active. If you plug a network cable into the management port of the SCE8000-SCM in slot 2, the Link LED turns on. The Link LED status may confuse you because this port has no IP address configured and should not be used.

Workaround: Use only the management ports of the SCE8000-SCM in slot 1.

CSCtf43847

The **snmpget** command returns the message `No Such Object available on this agent at this OID` even if you request for a correct OID. This issue is observed when getting the support file or when applying a policy. The issue is observed more often when you request multiple OIDs in one **snmpget** command.

Workaround: Request only one OID per **snmpget** command.

CSCth55499

The actual maximum rate for the Zone Usage RDR (ZUR) is greater than the configured value.

ZURs are sent separately from each PPC instead of one aggregated ZUR for all PPCs. As a result, the maximum rate for ZURs is not properly enforced.

Workaround: There is no workaround.

CSCth82475

After package change, CCR-U messages continue to be sent every 30 seconds.

Workaround: There is no workaround.

CSCti15865

The Cisco SCE 8000 crashes during Gx/Gy capacity testing while having 250,000 active sessions with long VSAs, with all VSAs being more than 200 bytes.

Workaround: Use normal VSAs rather than long VSAs.

CSCti18334

The VAS Health Check feature introduced in Cisco SCE 8000 causes minor performance degradation even if the VAS is not enabled.

Workaround: There is no workaround.

CSCtj37754

No SNMP trap is sent when the **external-bypass** command is issued on Cisco SCE 8000 GBE when the OPB-SCE8K-2L-SM optical bypass modules are installed.

Workaround: There is no workaround.

CSCtj46134

Cisco SCE 8000 uses software to process the VAS, and this impacts the performance of the device. Therefore, VAS processing is not supported for delay-sensitive, bundled, flow handling.

This issue is a known limitation.

Workaround: There is no workaround.

CSCtj50046

The *on-failure cutoff* option of the **connection-mode** command does not block traffic for a few minutes when Cisco SCE 8000 is rebooted.

Workaround: There is no workaround.

CSCtj58409

NALA MIP max node interrupts are generated even if subscriber ranges are present in NALA RAM. This issue does not affect functionality and is harmless.

Workaround: There is no workaround.

CSCtk67558

The notification of the first QuotaStatus RDR is delayed after subscriber logon. Subsequent notifications come through correctly.

Workaround: There is no workaround.

CSCtl10121

SNMP traps are not sent when only one of the eight fans fail.

Workaround: There is no workaround.

CSCtq20627

When a PQB is pushed or any other operation is performed on the Cisco SCE 8000 platform with high CPU utilization, the platform or the CLI fails to respond.

Workaround: When performing new operations on the Cisco SCE 8000 platform, ensure that the CPU utilization is low.

CSCts94869

In the **show interface linecard 0 counter** command output, the IPv6 packets are accounted as non-IP packets.

Workaround: Use IPv6 bytes counter or Link Usage RDRs (LURs).

The IPv6 bytes are available from the IPv6 bytes counter and from the Link Usage RDRs. The Non-IP Packets field shows both the IPv6 packets and the non-IP packets.

CSCtu12409

In the **show interface linecard 0 counter** command output, the DP L2TP Control Packet Count field shows DP IPv6 byte sizes. The L2TP packet count is not displayed.

Workaround: There is no workaround.

CSCtx51801

On Cisco SCE 8000, when the device tries a push logon for a Gx subscriber, Cisco SCE fails with timeout error messages in the CLI output.

Workaround: There is no workaround.

CSCty13726

The Cisco SCE 8000 platform that is configured in the IP-Tunnel L2TP Skip mode does not process traffic on the first traffic processor.

The device fails to process traffic because of bad handling of non-first-fragment packets. Therefore, in networks with some IP fragmentation, it is likely that the problem may not be observed even if IP-Tunnel L2TP Skip is configured.

The appropriate workaround depends on whether L2TP tunneled traffic must be processed based on the internal IP layer.

Note This workaround is not applicable to a cascade configuration.

- If L2TP tunneled traffic need not be processed based on the internal IP layer.

  Workaround: Disable L2TP Skip.

- If L2TP tunneled traffic must be processed based on the internal IP layer.

  Workaround:

  Run the following root-level CLI command:

  ```
  debug slot 0 ppc 0 func SimbaDPT[0].4DP[0].RegWr16 0x28 0x1000
  ```

  This command provides an immediate solution to the problem, but it is not persistent across reboots. To make this **debug** command run during the Cisco SCE 8000 boot-up process, add the command to the genstart.txt file.

  The genstart.txt file is located at /apps/data/scos/system/p3hidden/config/ (or /system/p3hidden/config/ from the Cisco SCE CLI). The genstart.txt file must exist on your Cisco SCE disk space and must be empty. If the file does not exist, create it under /apps/data/scos/system/p3hidden/config/.

  To edit the file, copy the file from the Cisco SCE platform to an FTP server using FTP. Add the following line to the file:

  ```
  do debug slot 0 ppc 0 func SimbaDPT[0].4DP[0].RegWr16 0x28 0x1000
  ```

After editing, copy the file back to the Cisco SCE platform using FTP.

The following sample CLI session shows how to copy the file to an FTP server and how to copy the file back to the appropriate folder in the SCE platform:

```
copy ftp://username:password@10.1.1.30/./genstart.txt
/system/p3hidden/config/genstart.txt
```

After copying the file to the SCE platform, verify whether the appended line appears in the file:

```
more /system/p3hidden/config/genstart.txt
do debug slot 0 ppc 0 func SimbaDPT[0].4DP[0].RegWr16 0x28 0x1000
```

CSCty73906

Downgrading Cisco SCOS Release 3.7.5 to a previous release displays error messages.

While downgrading Cisco SCOC Release 3.7.5 to Release 3.7.2, an error message similar to the following is displayed:

```
"Could not allocate 7383087 bytes for Control Application XML data partition"
```

Workaround:

Reload the device again and install the 3.7.2 PQI file from Cisco SCA BB Release 3.7.2.

Alternatively, follow these steps to downgrade to Cisco SCOS Release 3.7.2:

Step 1 Copy the Cisco SCOS Release 3.7.5 PQI file to the /apps/data/scos/app/ folder:

```
SCE8000#> copy ftp://ftpdefaultdirectory/ 3.7.5/pqi_file.pqi /apps/data/scos/app/
```

Step 2 Uninstall the Cisco SCOS Release 3.7.5 PQI file:

```
SCE8000(config if)#> pqi
```

Step 3 Uninstall the **pqi_file.pqi.**

Step 4 Copy the running configuration to the startup configuration:

```
SCE8000#> copy running-config-application startup-config-application
```

Step 5 Install Cisco SCOS Release 3.7.2 PKG file from Cisco SCA BB Release 3.7.2.

Step 6 Install Cisco SCOS Release 3.7.2 PQI file from Cisco SCA BB Release 3.7.2.

CSCty99703

If the time zone of Cisco SCE 8000 devices are modified through Cisco SCA BB Quota Manager, the device fails to adjust the aggregation period to the new time zone. The aggregation period is calculated based on the default UTC time zone even if a different time zone is configured.

Workaround: There is no workaround.

CSCtz57916

On Cisco SCE 8000 devices, when the subscribers are mapped to different UpVlink and DownVlink, the active subscribers displayed using the **show party all-party-with-open-flows** command may not match with the subscribers listed in the generated VLUR.

Workaround:

The following configuration works for a device setup with 37,500 subscribers, 128 services, and 1500 Vlinks:

- Set the *time to wait for reports* value to 200 seconds. (In effect, 400 seconds at the control master.)
- Set the *maximum RDR in one run per traffic processor* value to 1000
- Using the debug function, set the *maximum RDR in one run at control agent* value to 1000. The default value is 450.
- Using the Cisco SCA BB, set the *RDR interval* value to 10 minutes.

The following configuration works for a configuration with maximum (128 services, and 4096) Vlinks:

- Set the *time to wait for reports* value to 540 seconds.
- Set the *maximum RDR in one run per traffic processor* value to 1000.
- Using the debug function set the *maximum RDR in one run at control agent* value to 1000.
- Using the Cisco SCA BB, set the *RDR interval* value to 20 minutes.

To set the value of *time to wait for reports*, use the following **const-db** command:

```
# EngageConstDb.ControlPlane.Reporting.TimeToWaitForReports 200
```

To set the value of *maximum RDR in one run per traffic processor*, use the following const-db command:

```
# EngageConstDb.Common.Reporting.maxRDRsInOneRunPerTP 1000
```

To set the value of *maximum RDR limit at control agent* in the dual traffic processor card, use the following **debug** command:

```
# debug slot 0 ppc 13 func setMaxRDRLimitAtControlAgent 1000
```

To set the value of *consecutive not sent RDRs threshold*, use the following **const-db** command:

```
# ccConstDb.formatter.myConsecutiveNotSentRdrsThreshold 100000
```

CSCtz74897

The Total Link Limit feature fails on Cisco SCE 8000 devices when multiple global controllers are configured.

Workaround: Use only one global controller while using the Total Link Limit feature.

CSCua98956

Cisco SCE 8000 devices in a cascade setup running Cisco SCOS Release 3.7.2 and later, fail to replicate the anonymous subscribers created in an active device to the standby device. This issue is observed when using the **clear interface line 0 subscriber anonymous all** command.

Workaround: There is no workaround.

CSCub42442

When two Cisco SCE 8000 devices running Cisco SCOS Release 3.7.5 and later, are configured as active and standby for redundancy, the active device fails to sustain in the standby mode after a reload.

Workaround: There is no workaround.

CSCub67640

Cisco SCE 8000 devices fail to update the subscriber details with GGSN and SGSN VSA attributes even if the attributes are mapped to the corresponding subscriber in the Cisco Service Control Subscriber Manager.

Workaround: There is no workaround.

CSCub72077

When the Cisco SCE devices reload because of a power off or a hardware failure, the electronic bypass fails to pass the traffic for about 40 seconds.

Workaround: Use the external optical bypass.

CSCub93514

On Cisco SCE 8000 devices running Cisco SCOS Release 3.7.5-p1 and later, the Gy interface may be enabled after you restart the device even if the Gy interface is disabled and the configuration is saved to the startup configuration.

Workaround: Disable the Gy interface again and restart the device.

CSCuc05881

Cisco SCE 8000 devices add error messages to the debug log when there are IPv6 hwflows in the hwsim when the interface linecard is being shut down.

The messages state that all the allocated heap memory is not freed properly during the shutdown operation. The heap memory is completely freed when the device is shut down and does not affect the Cisco SCE devices.

Workaround: There is no workaround.

CSCuc06549

When the SNMP accelerate-query is configured and the SNMP is enabled on a Cisco SCE 8000 device, the device may restart abruptly while installing the pqi.

Workaround: Disable the SNMP before you install the pqi, and enable it only after completing the installation.

CSCuc76451

Cisco SCE 8000 devices may fail after upgrading to Cisco SCOS Release 3.8.0.

This issue is observed when the default configuration is applied with Host Based Classification (HBC) enabled.

Workaround: After applying the PQB on the device, disable the host based classification using the following commands:

```
SCE8000# config
SCE8000(config)> interface line 0
SCE8000(config if)> tunable GT_PL_MODULE__HBC_ENABLED value false
```

CSCuc15960

When Diameter Gy is enabled and disabled, CCR-T fails to carry usage information when the Gx+ subscriber logs out. The quota bucket state always shows the subscriber in the breached state.

Workaround: Reload the box or enable the Diameter Gy again.

CSCuc16315

Cisco SCE 8000 devices fail to create more than 20,000 zone indices. The devices display error when applying policies.

Cisco SCE Release 3.8.0 supports 20,000 zone indices, including IPv4 and IPv6 zones.

Workaround: There is no workaround.

CSCuc17799

Cisco SCE 8000 devices failed during a maximum flow testing for IPv6 traffic. This issue was observed when software flow aging was set to the maximum supported value, and the traffic was pushed at a higher rate and the traffic pattern tried to create flows continuously.

Workaround: While using a large number of IPv6 flows, increase the limit of free memory available in the system to 40 Mb using the **const-db lcConstDb.mem.minMarginForFlowCreationIssueStop** command.

CSCuc23894

The total number of active subscribers in the Package Usage RDR is more than the actual count. This issue is observed when policies contain different packages and anonymous groups, and the configuration of these anonymous groups or packages is removed when the traffic is flowing.

Workaround: There is no workaround.

Open Caveats—Cisco SCE 1000 and Cisco SCE 2000

This section describes the open caveats pertaining to Cisco SCE 1000 and Cisco SCE 2000 platforms for Release 3.8.x.

CSCtd18312

Cascade links may remain down when link failure-reflection is configured if:

- Link failure-reflection is configured on both the SCE platforms.
- Both the cascade links are disconnected and then connected again.

Workaround: Disable and enable link failure-reflection on the secondary Cisco SCE platform. Execute the following CLI command sequence on the secondary SCE:

```
# configure
(config)# interface LineCard 0
(config if)# no link failure-reflection
(config if)# link failure-reflection
(config if)# exit
(config)# exit
```

CSCti17836

When SSH sessions are rapidly opened and closed and FTP sessions are run simultaneously, the Cisco SCE 2000 crashes with a fatal SafeFdManager error. Note that this issue is not observed in Cisco SCOS Release 3.6.x.

Workaround: Disable SSH.

CSCti18005

When SSH sessions are rapidly opened and closed, traffic rate is 1 GBE, and FTP sessions are run simultaneously, Cisco SCE 2000 crashes with a critical Section error. Note that this occurs only in Cisco SCOS Release 3.6.1 and is not observed in Cisco SCOS Release 3.6.5.

Workaround: Disable SSH.

Open Caveats—All the Cisco SCE Platforms

This section describes the open caveats pertaining to all the platforms of Cisco SCE for Release 3.8.x.

CSCtc56711

Cisco SCE fails to authenticate subscriber logon through the TACACS server when the shared key contains spaces. This causes the login operation to the SCE to fail although a valid user name and password is used. Cisco SCE does not treat the space as a valid character in the key and terminates the key at the first space.

For example, if the configured key is 3b663ea010446e 72ecea2f1244853f73, Cisco SCE takes the key as 3b663ea010446e.

Workaround: Do not use keys that contain spaces.

CSCtd94013

Cisco SCE fails to control the bandwidth properly if fragmented UDP packets from the subscriber side arrive at the device at a rate that is higher than the Permitted Information Rate (PIR) because the fragmented packets are not dropped at the network side.

Workaround: Avoid using fragmented packets. Use the **no accelerate-packet-drops** CLI command to throttle fragmented packets at the software level.

CSCtk08011

Transmit queue overflow warnings appear when VLURs are enabled.

Workaround: Disable the VLUR aggregation using the **no periodic-records aggregate-by-cpu vlur** command in the interface line 0 configuration mode.

CSCtl22778

The Gy reports lower volume consumption because of delay in quota allocations. The volume reported through RDR varies from the volume reported by the Gy.

This issue is observed when the Gy quota profile is configured for the subscriber and quota is requested based on the classification. HTTP flow creation takes a few seconds from the time of request submission to Cisco SCE.

Workaround: There is no workaround.

CSCtn31028

HTTP redirection does not work with GRE tunnel external fragmentation.

Workaround: There is no workaround.

CSCtn64912

Intermittently, the Duration field values are not populated correctly in the Subscriber Usage RDRs (SUR). Total consumption of the allocated bandwidth causes delay in updating the SURs within the configured duration. This issue is observed on the Cisco SCE 2020 and Cisco SCE 8000 platforms. This symptom is mostly visible when using custom reporting tools or when evaluating the RDRs manually. However, the effect of the delay is nominal with the Cisco SCA BB reporter tool.

Workaround: To resolve the condition temporarily, clear the affected subscriber mappings and reintroduce the affected subscribers.

CSCtq67752

Quota breach is enforced only after the completion of file download. For example, a large file with a size that exceeds the available quota limit gets downloaded, but the next download gets blocked.

Workaround: There is no workaround.

CSCts66524

When there are many short-lived subscribers, Cisco SCE raises CAT 4 RDRs even at a low RDR rate.

Workaround: Disable or increase the remaining quota RDR timing so that the CAT 4 RDR rate is lowered.

CSCts69555

Without a P2P time-based rule, limiting works as expected. However, with the same configuration for P2P limiting that is configured in a time-based rule, the P2P traffic exceeds the configured traffic.

Workaround: There is no workaround.

CSCtt70539

HTTP redirection does not work in the HTTP 404 error code pages.

Workaround: There is no workaround.

CSCtw34069

During the installation of a new Cisco protocol update in Cisco SCOS, the subscribers may lose their mappings and be assigned with package 0 mappings.

Workaround: Clear the subscribers using the following CLI commands:

```
SCE# configure terminal
SCE(config)> interface lineCard 0
SCE(config if)> no subscribers all
```

CSCtx47997

On Cisco SCE devices, when a port-based classification is applied using Cisco SCA BB, the following issues are observed:

- Link Usage RDR with global usage counter ID 0 is always generated, even though there are no matching flows, along with the specific global usage counter ID on which there is a matching flow.
- Zero RDRs, which are supposed to be generated at the time of pushing the traffic, are generated at the next fifth minute.

- Link Usage RDRs are generated with the value 0 for all metrics, except for total active subscribers.
- Link Usage RDR is different for TCP and UDP.

Workaround: There is no workaround.

CSCty18403

On Cisco SCE devices, packet drops are observed while upgrading the protocol pack (SPQI).

Workaround: There is no workaround.

CSCty38340

Cisco SCE devices running Cisco SCOS Release 3.5.5 may report incorrect quota consumption information when used with multiple buckets and time frames.

Workaround: There is no workaround.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.