



Release Notes for Cisco Service Control Operating System (SCOS) 1.5.10

Dec 8, 2004

Release Notes for Cisco Release Service Control Operating System (SCOS) 1.5.10

Supports: SCOS 1.5.10, SCOS 1.5.10, SCOS 1.5.9, SCOS 1.5.8

OL-7016-01

These release notes for the Cisco SCOS describe the enhancements provided in Cisco Release 1.5.10. These release notes also cover releases 1.5.9 and 1.5.8 of the SCOS.

For a list of the software caveats that apply to Cisco Release SCOS 1.5.10 see “Open Caveats – Cisco Release SCOS 1.5.10,” page 10



Corporate Headquarters:

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Contents

INTRODUCTION	4
NEW FUNCTIONALITY IN CISCO RELEASE SCOS 1.5.10.....	4
<i>CLI Command Displaying Incorrect MIB Variable.....</i>	4
<i>Outstanding Issues</i>	4
NEW FUNCTIONALITY IN RELEASE SCOS 1.5.9	5
<i>Support of a Hardware Change in the SCE 1010.....</i>	5
<i>Support of File Retrieving</i>	5
<i>Using a Password at Level 0</i>	5
<i>Time-Based Counters.....</i>	5
<i>GBE Link Failure</i>	5
NEW FUNCTIONALITY IN RELEASE SCOS 1.5	6
<i>Subscriber Management</i>	6
Anonymous Subscribers and Subscriber Templates	6
Importing and Exporting Subscriber Information	7
Monitoring Subscribers.....	7
Aging.....	7
<i>Global Controllers.....</i>	8
<i>Tunneling Support</i>	8
MPLS Environment Support.....	8
<i>Supporting New Protocols</i>	8
SIP	8
WAP 1.x.....	8
<i>RDR Protocol.....</i>	9
<i>Resiliency to DoS Attacks</i>	9
<i>New SNMP MIB Groups.....</i>	9
IMPORTANT NOTES	9
<i>Calendar Update.....</i>	9
CAVEATS	10
OPEN CAVEATS – CISCO RELEASE SCOS 1.5.10	10
<i>FF L4 Rules Do Not Match Non-First IP Fragments.....</i>	10
<i>Reboot the SCE to Change the SCE's IP Address.....</i>	10
<i>ToS Marking for TCP: 3 First Packets Receive the ToS Value of the Default Class.....</i>	10
<i>Saving Configurations Using SNMP Occasionally Fails</i>	10
<i>Problem with HTTP Access to Port 8082 on the SCE 1010</i>	11
<i>Telnet Sessions to the SCE Remains Open</i>	11
<i>SNMP Time-Related Variables May Become Incorrect</i>	11
<i>Executing the CLI Command 'PQI install/upgrade/...'</i>	11
<i>Changing the RMI Port Number on the SCE</i>	11
<i>Traffic with the Same IP addresses as the SCE Management Port is Bypassed.....</i>	12
<i>Operating in MPLS VPN Environment</i>	12
<i>DNS Server Configuration.....</i>	12

<i>SCE 1010 Disk Space</i>	12
<i>Packet Loss During the Application Install/Upgrade</i>	13
OBTAINING TECHNICAL ASSISTANCE	14
CISCO TECHNICAL SUPPORT WEBSITE	14
SUBMITTING A SERVICE REQUEST.....	14
DEFINITIONS OF SERVICE REQUEST SEVERITY	15
OBTAINING ADDITIONAL PUBLICATIONS AND INFORMATION	15

Introduction

Cisco is proud to release version 1.5.10 of the SCOS (Service Control Operating System) for its SCE platform. This version includes implementations of fundamental features and capabilities in the areas of subscriber management, Global Controllers, tunneling and infrastructure for supporting of new protocols.

This document outlines the new features and enhancements to the SCOS, and assumes the reader already has a good working knowledge of the Cisco's solution. For additional information, please refer to the Cisco's User Guides.

New Functionality in Cisco Release SCOS 1.5.10

The following new functionalities are supported by Cisco for Cisco Release SCOS 1.5.10

CLI Command Displaying Incorrect MIB Variable

The main change in this release relates to a CLI command that was incorrectly displaying the value of the MIB variable `tpNumCpuShortageEvents`.

This issue is fixed, and the CLI command displays the correct value of this MIB variable.

Outstanding Issues

The following list is outstanding issues that you should be aware of:

- The upgrade procedure to SCOS 1.5.10 from SCOS 1.5.8 or earlier SCOS releases includes re-initialization of SCE 1010's hardware Bypass module. This re-initialization process can cause a failure of the GBE link where the SCE 1010 is installed for a period of less than 1sec.
- We have identified a problem with the SCE's DNS configuration (The CLI command for that is `(config)#>ip name-server`). When the IP address of the DNS server is of a server that does not exist, the SCE experiences various communication problems, including a failure to ping other network entities from the SCE (even when the Ping address is provided explicitly and not as domain name).

New Functionality in Release SCOS 1.5.9

The following new functionalities are supported by Cisco for Cisco Release SCOS 1.5.9

Support of a Hardware Change in the SCE 1010

The L2 cache device that is used in the SCE 1010 is being discontinued. Therefore, Cisco moved to using another L2 cache device. This release includes the required change in the relevant driver to support the new cache device.

Support of File Retrieving

Some of the issues that the user sometimes experiences when retrieving the Support File from the SCE platform to an FTP server are identified and fixed.

Using a Password at Level 0

When a password is configured for CLI Level 0, in certain cases the login attempts to the SCE fails, and the connection to the box is lost.


This issue is fixed.

Time-Based Counters

An issue was identified with the maintenance of time-based counters in the SCE platform. This also caused failures in performing PING operations to SCE platforms that were running continuously for 49 days.

This issue is fixed.

GBE Link Failure

	
Note	The upgrade procedure to SCOS 1.5.9 includes re-initialization of SCE 1010's hardware Bypass module. This re-initialization process can cause a failure of the GBE link where the SCE 1010 is installed for a period of less than 1second.

New Functionality in Release SCOS 1.5

Subscriber Management

This release introduces major enhancements in the SCE Platform's subscriber related functionality.

The SCE Platforms include an infrastructure for subscriber awareness that has the ability to relate traffic and usage to specific subscribers. This ability to map between IP flows and specific subscribers permits the SCE to do the following:

- Maintain the state of each subscriber that's transmitting traffic through the SCE.
- Provide usage information for specific subscribers
- Enforce the appropriate policy on subscriber's traffic

Each traffic session (single IP flow, or a group of related IP flows) processed by the SCE device is assigned to a single subscriber on the basis of the configured subscriber mappings. These mappings usually represent the IP address or group of IP addresses that are currently assigned to a specific logged-in customer of the service provider.

The mappings can be one of the following:

- IP address
- Range of IP addresses
- Group of IP addresses or ranges
- VLAN tag
- Group of VLAN tags.

Anonymous Subscribers and Subscriber Templates

The SCE Platform handles two types of subscribers:

- Introduced Subscriber – a subscriber whose Subscriber ID was introduced to the SCE by an external system.

Introduced subscribers can map to more than a single IP address.

- Anonymous subscribers - subscribers with Subscriber-ID that was generated by the SCE according to an anonymous subscriber group specification.

An anonymous subscriber is always mapped to a single IP address.

An anonymous subscriber group is a specified IP range, possibly assigned to a subscriber template. When an anonymous group is configured, the SCE Platform generates anonymous subscribers for that group when it detects traffic with an IP address that is in the specified IP range. If a subscriber template has been assigned to the group, the anonymous subscribers generated have properties as defined by that template. If no subscriber template has been assigned, the default template is used.

This release includes the CLI commands: managing Introduced, Anonymous subscribers, Anonymous subscriber groups, and templates.

Importing and Exporting Subscriber Information

Individual subscribers, anonymous groups, and subscriber templates may all be defined in *csv* files. A *csv* file is a text file in a comma-separated-values format. Microsoft Excel™ can be used to view and create such files. The subscriber data is imported into the system using the appropriate CLI command. The SCE device can also export the currently configured subscribers, subscriber templates and anonymous groups to *csv*-formatted files

This release includes CLI commands for importing and exporting subscriber information.

Monitoring Subscribers

A set of CLI commands was added to this release for monitoring the status of the subscribers in the SCE. These commands can be used to display information regarding the following:

- Subscriber Database
- All the subscribers that meet certain criteria
- Individual subscriber information, such as properties and mappings
- Information that relates to Anonymous subscribers

Aging

The SCE device can age subscribers automatically. ‘Aging’ is the automatic removal of a subscriber entry from the SCE’s database that is performed when no traffic flows with IP addresses that are mapped to this subscriber have been detected for a certain amount of time. The most common usage for aging is for managing Anonymous subscribers, since this is the easiest way to ensure that anonymous subscribers that have logged-out of the network are removed from the SCE device, and are no longer occupying resources in the SCE’s database.

This release includes CLI commands for configuring aging parameters for Anonymous and Introduced subscribers.

Global Controllers

The 1.4.x SCOS releases have the ability to control BW per all the flows of a subscriber, or per the flows of a group of protocols (service) of the subscriber. This release includes a mechanism to control BW of a certain type of flows per the whole link of SCE 1010. The new mechanism is called Global Controller. The SCE 1010 supports up to 16 Global Controllers per traffic direction (upstream and downstream).

SCAS BB2.0 makes use of this new capability. For each service in SCAS BB, a rule can be defined to associate that service's traffic with a particular Global Controller.

Tunneling Support

This release includes the following Tunneling Support:

- MPLS Environment Support

MPLS Environment Support

The SCE platform can now be deployed in network segments with MPLS tagged traffic.

The various Cisco applications can classify IP flows and perform their normal Service Control functionality in MPLS environment.

Supporting New Protocols

This release supports the following new protocols:

- SIP
- WAP 1.x

SIP

The SCE platform now supports complete layer7 analysis and control of SIP flows. SIP (Session Initiation Protocol) is commonly used as the communication protocol for Voice & Instant-Messaging applications and typically involves multiple simultaneous TCP & UDP connection on dynamically negotiated ports.

WAP 1.x

Support of the WTP transport layer is now added to the SCE Platform for analyzing and controlling WAP 1.x flows.

WAP 1.x is used in wireless network for enabling a variety of content-based services.

RDR Protocol

The RDR protocol is now enhanced for making it a better vehicle for the reporting functionality in the various Cisco solutions.

The following improvements are implemented:

- High availability – a history buffer and sequence numbers are now added
- Keep-alive messages are now added to the protocol
- RDR records can now be routed to multiple logical and physical entities
- The RDR record is enlarged for allowing reporting of increased number of parameters

The SCE platform is backward compatible and supports the old RDR protocol as well.

Resiliency to DoS Attacks

Being a stateful entity, the SCE platform is potentially vulnerable to DoS attacks, in which case the platform might face difficulties with providing the desired analysis & control functionality. This occurs because the IP flows that establish such attacks interfere with the correct functionality of the SCE platform, by consuming internal resources of the platform. These resources can be processing power, and memory resources, which are devoted to classification of flows, and to other aspects of the SCE functionality.

The SCE platform now has an internal mechanism for protecting itself from attacks, by detecting and identifying DoS attacks that threaten the platform's correct functionality.

New SNMP MIB Groups

Two new SNMP MIB groups are now added:

- Generic application MIB group for monitoring Encharge and SCAS BB variables
- Global BW Controllers MIB groupNew Functionality in Cisco

Important Notes

The following section contains an important note about Cisco SCOS Release 1.5.10.

Calendar Update

Following the updating of the SCE's clock, it is recommended to also update the calendar, using the CLI command:

```
'clock update-calendar'
```

Caveats

Open Caveats – Cisco Release SCOS 1.5.10

FF L4 Rules Do Not Match Non-First IP Fragments

- Cisco number 3975

A non-first fragment packet doesn't include any L4 information. This implies that when setting Flow Filter rules using L4 attributes (such as port numbers and TCP flags) they will not work for Non-First-Fragment packets. When using counters or any other rules for L4 information, this phenomenon should be taken into account.

There are no known workarounds.

Reboot the SCE to Change the SCE's IP Address

- Cisco number 4989

Modifying the IP address on an SCE using CLI will not take effect.

Workaround: Reboot the SCE after changing the IP address

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

- Cisco number 6139

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

There are no known workarounds.

Saving Configurations Using SNMP Occasionally Fails

- Cisco number 7664

Cisco's proprietary SNMP allows saving of the SCE's configuration. In certain cases this set operation fails due to short time out of the MIB viewer.

Workaround: Increase the default timeout value of the MIB viewer. In HPoV the timeout is 0.8 seconds; this should be increased to ~15 seconds.

Problem with HTTP Access to Port 8082 on the SCE 1010

- Cisco number 8308

When password encryption is enabled HTTP access to port 8082 on the SCE 1010 is not possible.

Workaround: If you need to work with HTTP access to port 8082, you should not enable password encryption.

Telnet Sessions to the SCE Remains Open

- Cisco number 8749

When the SCE is configured with 'no timeout' for Telnet sessions, and there is an open telnet session when a network disconnection occurs, the telnet session in the SCE remains open, and never closes.

Workaround: It is recommended to specify a timeout for Telnet sessions.

SNMP Time-Related Variables May Become Incorrect

- Cisco number 9409

The SNMP variables that are time related may become incorrect after around 45 days, as a result of wraparound of the internal counters

There are no known workarounds.

Executing the CLI Command 'PQI install/upgrade/...'

- Cisco number 9565

After executing the CLI command 'PQI install/upgrade/...', the user sees the progress on the screen, and then the CLI prompt returns, even though the installation has a few more minutes to complete. Then, the following message appears: "Now please wait 5 minutes before attempting to do anything else."

Workaround: Wait until the operation is completed to continue using the CLI.

Changing the RMI Port Number on the SCE

- Cisco number 10734

Modifying the RMI port number on the SCE will not take effect.

- Workaround: Reboot the SCE after changing the RMI port number.

Traffic with the Same IP addresses as the SCE Management Port is Bypassed

- Cisco number 10757

The SCE box bypasses traffic with the IP of its management port (this occurs if the traffic traverses through the SCE). This ensures that the SCE will never block the management port traffic.

When working in an environment with private IP addresses over VLANs / tunnels environment, this IP address might belong to a valid subscriber (over a different VLAN). If this occurs, the subscriber's traffic is bypassed and is not serviced.

There are no known workarounds.

Operating in MPLS VPN Environment

When operating in MPLS VPN environment, various capabilities that require injecting packets, such as redirection, are not operational.

There are no known workarounds.

DNS Server Configuration

There is a problem with the SCE's DNS configuration (which the CLI command for it is (config)#>ip name-server). When the IP address of the DNS server is from a server that does not exist, the SCE experiences various communication problems, including failure to ping other network entities from the SCE (even when the Ping address is provided explicitly and not as domain name).

Workaround: Verify that you configured a DNS server that actually exists. As a general recommendation, if configuring a DNS server is not essential, try avoiding such a configuration.

SCE 1010 Disk Space

In certain cases the SCE 1010 runs out of disk space. Since the SCE 1010 requires free 40Mbytes for correct operation, this can cause severe problems.

The symptoms of running out of disk space can be one of the following:

- The SCE's operational status is "warning", indicating in the CLI that it does not have sufficient disk space.
- You are unable to extract a new package.
- You have problems interpreting your logs.
- You are unable to Zip a diagnostics image.

Workaround: Perform the following steps:

Step 1. Package files should not be copied to the SCE 1010 disk and should be installed directly from the network.

To install package files:

- a. configure
- b. boot system `ftp://user:password@host/drive:/dir/new-package-name.pkg`
- c. exit
- d. copy running-config startup-config
- e. reload

Step 2. Uninstall the previous PQI before installing a new one.

Step 3. Create the logs and support-files directly on a network drive.

Packet Loss During the Application Install/Upgrade

- Cisco number 11798

When a PQI application file is installed or upgraded on the SCE, the SCE may cause a loss of traffic packets for several seconds.

Workaround: It is recommended to move the SCE to bypass, before installing a PQI application.

The following CLI commands should be used:

- For the SCE 1010:
`(config if)#link mode port1-port2 bypass`
- For the SCE 2020:
`(config if)#link mode all-links bypass`
- After insult pqi is completed, use: `(config if)#default link mode`

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>

- iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0411R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.