Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 2.5.7A

February, 2007

Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 2.5.7A

Supports: SCMS SM 2.5.7A, 2.5.7, 2.5.6, 2.5.5, 2.5.2, 2.5.1, SCMS SM 2.5

OL-7083-07

The release notes for the Cisco SCMS SM describe the enhancements provided in Cisco Release SCMS SM 2.5.7A.

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

Contents

Introduction

Cisco is proud to release version 2.5.7A of the Subscriber Manager infrastructure.

SCMS SM 2.5.7A is a point release of SM2.5. It includes various fixes of bugs that were identified as part of Cisco's on-going internal testing and during our interaction with our customers.

This document outlines the new features and enhancements of the SM2.5 releases, and assumes the reader already has a good working knowledge of the Cisco solution. For additional information, please refer to the Cisco Service Control Engine documentation.

Release SCMS SM 2.5.7A

See Open Caveats: Release 2.5.7A.

Resolved Caveats

The following caveats were resolved in this release.

SM and SCE lose synchronization following several frequent disconnections

Cisco Number: CSCsh55436

When the Subscriber Manager (SM) is working in pull introduction-mode and a connection loss event is followed by an immediate reconnection event between the SM and the SCEs, subscriber information synchronization might be lost between the SM and SCE. In such cases the SM is unable to update subscriber information for subscribers that are pulled by the SCE and introduced to it by the SM.

The SM identifies the disconnection and connection establishment events with the SCE. On connection establishment the SM starts a task that verifies that the SCE is synchronized with the subscriber data that is in the SM database. On disconnection the SM terminates the synchronization tasks.

During frequent disconnections and reconnections it is possible that two tasks will attempt to perform two operations at the same time resulting in corruption of the SM state regarding this SCE.

This issue was fixed in the SM 2.5.7A.

Release SCMS SM 2.5.7

Resolved Caveats

The following caveats were resolved in this release.

SM Cluster Failover Issues

When two SM servers operate in cluster mode and the standby SM gets activated after a failure of the active SM, the standby SM loads from the database part of the subscriber information. This operation includes a timeout of 20 seconds. When SM manages a significant number of subscribers (half a million or more), the operation may last more than 20 seconds, so this timeout may expire.

When this happens, a fatal error is issued and the cluster fail-over does not go into action. In addition, this timeout is not configurable in SM 2.5.6. When the failure takes place, it also triggers a series of events that might cause the SCE platform to malfunction.

The following two fixes were implemented in SM 2.5.7:

- The timeout was changed to 40 seconds and was changed to be configurable (but still hidden – ask Cisco TAC for support if needed).
- A fix was implemented in the SCE platform, causing it to switch to the connection with the new active SM regardless of the current connection state.

Canceling the pcubeSync File and Mechanism

The SM uses a system file (pcubeReg, stored in the root directory), to store the PRPC port to which the SM listens. The CLU process reads this file and opens a PRPC connection accordingly. In SM 2.5.6, another system file (pcubeSync), is used for synchronizing the access to the pcubeReg file.

In SM 2.5.7, the usage of the pcubeSync file and mechanism was cancelled, since it caused various issues. The SM now operates correctly without it.

Standby SM Performs Active Operations on the SM database

In SM 2.5.6, in cases where a non-default domain is used, the Standby SM performs operations on the SM database which caused loss of information on the Active SM.

This issue was fixed in the SM 2.5.7 and now the Standby SM only performs active operations on the SM database when it becomes the Active SM.

Support for the Multi-GBE SCP Solution

SM 2.5.7 supports the solution where a Cisco 7600/6500 is used for load-balancing among several SCE platforms. When one SCE platform fails, subscriber traffic is redistributed to a different SCE platform. The SM must remove these subscribers from the failed SCE platform and send the relevant subscriber information to the new SCE platform. To support this functionality, the *force-subscriber-on-one-sce* configuration parameter is set in the p3sm.cfg configuration file.

Release SCMS SM 2.5.6

Resolved Caveats

The following caveats were resolved in this release.

Dynamic package ID assignment

The dynamic package-ID assignment functionality did not operate correctly as part of the DHCP lease query configuration.

This occurred when using the DHCP lease query LEG or when using the RDR DHCP LEG.

The problem was that these two LEG SW components did not support null-terminated strings for package-ID assignment.

Backward compatibility

When the SM is running SM 2.5.X with SCOS 2.0.X and operating in Pull mode, it replies to pull requests from the SCE platforms, but does not maintain the subscriber-ID to SCE mapping. As a result, the SM does not propagate updates on logout of subscribers and on package-ID changes to the relevant SCE.

Lease-query User Log messages

Wrong User Log messages are produced on some occasions after a DHCP server response to a lease-query request coming from the DHCP lease-query LEG. The problem that was identified is that log messages of the Lease-Query LEG contain corrupted IP address for the relay-agent and for the subscriber.

This issue occurs in the 2.5.1 to 2.5.5 SM releases, and was fixed in SM 2.5.6.

Configuration of subscriber-Id option in Lease-query

When the SM operates in DHCP environments, the MAC address of the cable modem is normally used as the subscriber ID. The MAC address of the cable modem is extracted from option 82 (Remote Id sub-option of the DHCP Relay Agent Information Option). Therefore, the DHCP server is required to support and store option 82 for each CPE. This default can now be overwritten by configuration. Furthermore, a LEG can assign the subscriber IP address as a fallback subscriber-Id (using an IP_a.b.c.d format) if the option does not exist in the server response. This fallback is disabled by default.

Release SCMS SM 2.5.5

Resolved Caveats

The following caveats were resolved in this release.

Sending VLAN mapping to the SCE

When the SM and SCE loose connection and then the connection is restored, the SM and SCE perform resynchronization of the subscriber-related information.

During this resynchronization phase, subscriber-related information of subscribers that were identified through VLAN tags was not sent correctly to the SCE.

This issue is now fixed and the information is now sent correctly to the SCE.

Supporting domain=Null at some of the API functions

Some functions in the SM API can now be used in parallel both by a LEG component and by a provisioning system. In order to allow parallel use, the ability to call the login functions with a value of Domain=null was added.

When the login function is called with Domain=null and the subscriber is already mapped to a domain, the mapping will not be affected. If, on the other hand, the subscriber still does not exist in the database, a subscriber will be created without a specific domain.

When the getSubscriberNameByMapping method is called with Domain=Null the subscriber name will be retrieved regardless of the subscriber's mapping to a domain.

Propagation of package ID updates to the SCE

In a few rare cases, the SM was not aware of the fact that a subscriber was managed by an SCE, and did not propagate package ID updates to the relevant SCE.

This issue was fixed.

SM-LEG failure handling

When the SM-LEG Handling feature is enabled (clear_all_mappings configuration parameter is set to true) and the LEG is associated to a domain (LEG-Domains Association section), the SM will start the "clear-all-mappings" timer on valid disconnections of the LEG. A "valid disconnection" is for example a situation where a LEG is restarted. In this case, if the LEG does not reconnect within the timeout, the SM clears all of the mapping in the domain.

In previous releases, in case of other types of failures, such as when the machine on which the LEG was running crashed, or in case of a networking disconnection between the LEG and the SM, the failure was ignored.

This issue was fixed.

Release SCMS SM 2.5.2

Resolved Caveats

The following caveats were resolved in this release.

SM Synchronization after SCE Reboot

A problem was found in the SM sync mechanism that is activated after an SCE unexpectedly reboots.

This issue was fixed in SM 2.5.2.

Replying to Pull Requests

In SM 2.5, when the SM receives a Pull request from the SCE (request of subscriber information issued by the SCE when new subscriber IP address was identified in the traffic), it responds with the details of the subscriber that is mapped to the IP address in the Pull request, without checking whether the lease period of the IP address was expired (this is relevant only for Cable or Satellite deployments, where IP addressees are allocated with a lease period)

In SM 2.5.2, when the SM receives a Pull request, it performs the relevant checks, and in case the IP address's lease period expired, the SM does not reply to the Pull request. The SCE then applies a default policy to this IP address.

Non-UNIX Veritas Configuration File

The configuration file of the ProcessOnOnly Veritas cluster agent was not in the correct UNIX format. This causes the Veritas cluster server to fail during startup.
This issue was fixed in SM 2.5.2

Support Lease Renewals in the CNR LEG without Requiring Option 82

When the CNR LEG operates in “CM as Subscriber” mode, it used to require the existence of option 82 in the DHCP renewal transaction. This was required for being able to associate the IP address whose lease is being extended with a specific Cable Modem MAC address. In SM 2.5.2 this is no longer required, as extending the lease is solely based on the IP address. Option 82 is still required for the first login of the subscriber.

Release SCMS SM 2.5.1

Two new LEG components were added to the SM infrastructure.

New LEG Component: DHCP Lease Query LEG & DHCP Forwarder

The DHCP Lease Query LEG is an extension to the SM software and runs as part of the SM.

The DHCP Lease Query LEG handles pull-requests from the SCE platforms that the SCMS SM was unable to handle. The LEG queries the DHCP server using a DHCP Lease-Query transaction.

The following figure shows a sequence diagram representing the operation of the DHCP Lease Query LEG & DHCP Forwarder LEG:

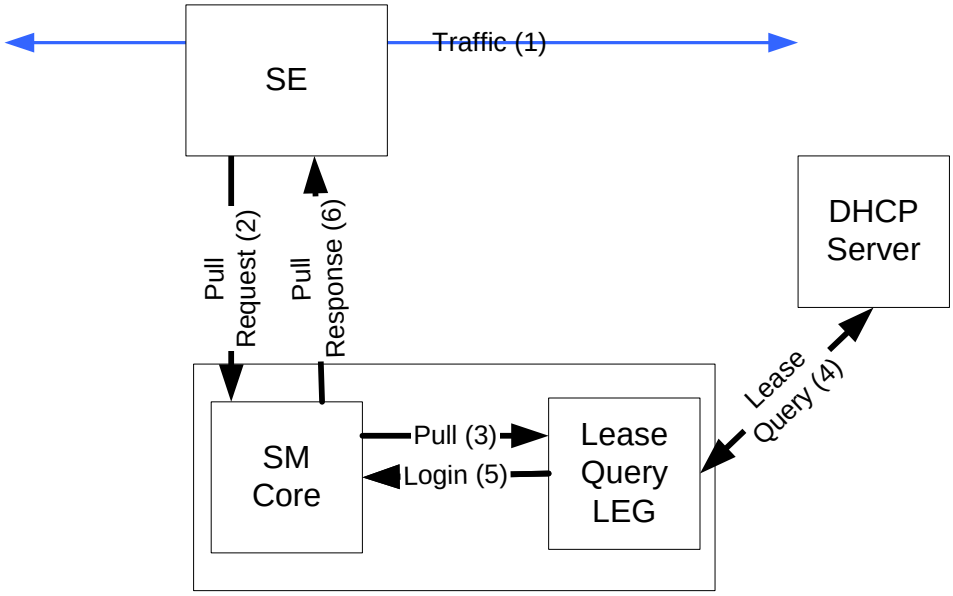

Figure 1: DHCP Lease Query LEG & DHCP Forwarder LEG

The subscriber traffic (1) triggers a pull-request from the SCE and (2) the SCMS SM receives the request for processing. If the SCMS SM does not find a subscriber with a matching IP address in the subscriber database it passes the pull request to the DHCP Lease Query LEG (3). The LEG queries the DHCP server. If the server finds a match for the IP in its database, the server replies with the subscriber information (4). The LEG performs a login operation. (5) Based on the received information, this operation updates the subscriber database and logs the subscriber into the SCE (6) which triggered the pull request.

The DHCP Lease-Query LEG includes a component called the DHCP forwarder, which acts as a bridge between the DHCP Lease-Query LEG and the DHCP servers.

The DHCP Lease-Query transaction is defined as an IETF draft. The LEG supports version 7 of the draft. For more information see http://www.ietf.org/internet-drafts/draft-ietf-dhc-leasequery-07.txt.

New LEG Component: RDR DHCP LEG

The new DR DHCP LEG software module receives RDR (Raw Data Report) messages containing DHCP information from SCE devices configured with a DHCP sniffer service.

The SCE device analyzes DHCP traffic, and reports the DCHP transactions to the SCMS SM device using the RDR protocol. The DHCP transactions that are relevant for the operation of the LEG are *`initial login`*, *`lease extension`*, and *`release`*.

The SCMS SM extracts the modem MAC address, the CPE IP address, and optionally the subscriber package information from the RDR, and triggers a logon or logout operation to the SCMS SM.

The following figure shows a sequence diagram representing the operation of the RDR DHCP LEG:

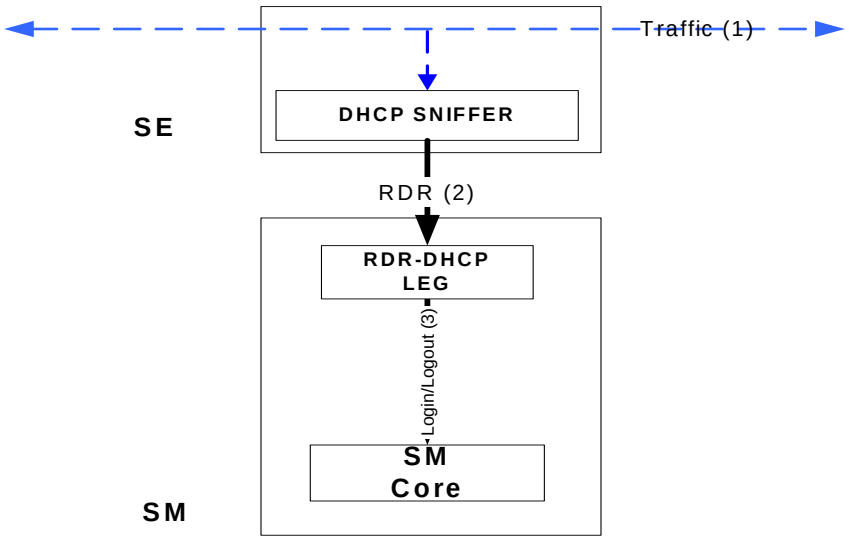

Figure 2: RDR DHCP LEG Sequence Operation

Release SCMS SM 2.5

Porting the SCMS SM to Linux

Previous versions of the SCMS SM ran only on Solaris 8. Version 2.5 offers the option of running the SCMS SM software on Red Hat Linux AS 3.0 and ES 3.0 (and up).

The following components of the SCMS SM SW package were ported to Linux:

- SCMS SM SW and the Command Line Utilities (CLU)
- SCMS SM Java and C / C++ APIs
- RADIUS Listener LEG
- Upgrade and installation procedures and Veritas agents
- 3rd party SW packages, such as the TimesTen In-Memory database and the Veritas Cluster Server

The CNR LEG was NOT ported and it continues to run on Solaris and Windows only.

SCMS SM Capacity Increase

Cisco is currently involved in very large deployments were the SCMS SM is required to support more than 1 million active subscribers in a single SCMS SM machine.

SCMS SM 2.5 supports deployments of up to 3 million subscribers on a single SCMS SM machine. This number of subscribers requires a strong machine with more than 2Gbyte of RAM.

This capability of increased number of subscribers requires a 64-bit machine for the SCMS SM. The increased capacity is supported on Solaris\Sparc machines, while Linux\X86 is normally used with 32-bit machines.

Reliable SCMS SM Java API

In SCMS SM 2.5 the Java SCMS SM API was updated to support a reliable connection. That is, if the connection fails, the logon operations are stored in a buffer and re-sent when the connection is re-established. Furthermore, the Java SCMS SM API now includes a feature of automatic re-connect to the SCMS SM with no intervention needed by the API user.

Issues to Note in Version SCMS SM 2.5

Backward Compatibility with SCOS

SCMS SM 2.5 can operate with SCE platforms that run SCOS versions 2.0.6 and up . This was implemented for cases were the service provider wants to deploy SCMS SM 2.5 (for Linux support for example), but continue to operate SCE platforms with SCOS 2.0.6 and up.

Installing SCMS SM 2.5

In SM 2.5, the installation script checks which operating system it runs on, and installs the relevant components accordingly.

The following parameters are available for the installation:

Usage: **`install-sm.sh [-h] [[-d INSTALLDIR] | -o] [-v VARDIR] [-n] [-m] [-j]`**

Options (switches):

`-d INSTALLDIR`

Select install directory for ~pcube the default is *<default_installdir>*. The directory must not exist prior to installation.

-o

Use an existing home of user pcube. The flags **-d** and **-o** cannot be used together

-v VARDIR

Indicate a directory for data storage. The default is *INSTALLDIR/var*. The directory should not exist prior to installation, and must be on a partition with at least 1GB of free space.

-n

Do not install TimesTen.

-m

Do not install SM DSN for TimesTen.

-j

Do not install JRE (Java Runtime).

-32

Install 32bit version.

-h

Print this help and exit.

Note The 64-bit TimesTen/JRE versions will be installed unless '-32' option was used

Note **-j** and **-32** are new installation options

Note When installing SM 2.5, a JRE package is installed under the *pcube h*ome directory.

Upgrading to a New Software Release

SM 2.5 includes upgrade procedures from SM 1.5, 2.0 and 2.2 to the SM 2.5 version. Please refer to the SM 2.5 User Guide for a detailed description of these procedures.

The following table summarizes upgrade support from different versions to various distributions of SM 2.5:

Table 1 Upgrade Support Table

To: From:	Solaris 32bit 2.5	Solaris 64 bit 2.5	Linux 32 bit 2.5
Solaris 32bit 1.5	×	✓	×
Solaris 32bit 2.0	×	✓	×
Solaris 32bit 2.2	✓	✓	×
Solaris 32bit 2.5	✓	✓	×
Solaris 64bit 2.5	×	✓	×
Linux 32bit 2.5	×	×	✓

Note SM 2.5 supports upgrade to a newer version of TimesTen 32bit version for customers with existing 32bit deployments and no need for a subscriber database larger than 2GB RAM.

Note When upgrading to ANY distribution of Solaris, a 64bit JRE 64bit package is installed.

Note To upgrade from 32bit to 64bit TimesTen database, a 64bit version installation is required. Therefore, the subscribers are exported and imported again after the 64bit version is installed.

Note Default upgrade option: 32bit for 32 bit versions, and 64bit for 64bit versions. The exception is upgrade from SM 2.0 (32bit) when the TimesTen version needs upgrade from 4.5 to 5.0. In this case, the 64bit version is installed by default.

Note It is not possible to downgrade from the 64bit version to the 32bit version.

Upgrade Options

Syntax:

`./upgrade-sm.sh [-d] [-p] [-64] [-h]`

Options (switches):

- **`-d`** destroy database during upgrade
- **`-p`** pause the upgrade for PQI installation
- **`-64`** upgrade to 64bit version
- **`-h`** show this message

Changes in the CLU

p3net

- The *domain* option was removed
- A new **`–detail`** option was added. This option is used with **`–show-all`** option order to display detailed info about all SCE platforms in table format

p3sm

- The **`--show-logging`** option was removed. The information it presented is now presented under **`p3sm –show CLU`**.
- A **`--remote=IP[:port]`** option was added. It is used with the **`--load-config`** option for loading the local configuration file to the local and remote SMs.
- A **`--detail`** option was added. It is used with the **`–sm-status`** option to display a detailed view of the status of the SCMS SM.
- A **`--wait`** option was added. It is used with **`--start`** or **`--restart`** for signaling to the CLU that it should return only when the SCMS SM is up.

p3db

- A **`--keep-in-mem`** SECS option was added. This option sets a timeout for saving the database in the shared-memory from the time the last connection to the DB is down. This improves the SCMS SM restart time.
- A **`--duplicate --local=<LOCAL_MACHINE> --remote=<REMOTE_MACHINE>`** option was added. This option copies the data-store from the “remote” machine to the “local” machine

Caveats

Open Caveats: Release 2.5.7A

Veritas Cluster Server Version 4.x Agent Name Clash

- Cisco Number: n/a

  Veritas Cluster Server 4.x introduced a ProcessOnOnly bundled agent that causes a clash of agent names with Cisco ProcessOnOnly custom cluster agent. The two agents have a slight difference in functionality that requires the use of the Cisco agent with the SM clusters.

Solution

To be able to work with Cisco’s agent the following procedure should be performed:

Step 1 Install Veritas Cluster Server version 4.0

Step 2 Rename\move the directory /opt/VRTSvcs/bin/ProcessOnOnly.

Step 3 Install Cisco’s Veritas Cluster Agents from the SCMS-SM installation distribution by running the following command:

```
# <SM-installation-dir>/install-vcs-agents.sh
```

This overwrites the content of the */opt/VRTSvcs/bin/ProcessOnOnly* directory.

Step 4 Remove the type definition of the bundled agent by running the following CLU:

```
# /opt/VRTSvcs/bin/hatype –delete ProcessOnOnly
```

Note When you have a resource using this agent you will have to run the */opt/VRTSvcs/bin/hares –delete <resource-name>* CLU before the *hatype*.

Step 5 Import the ProcessOnOnly agent type definition by importing the */opt/VRTSvcs/bin/ProcessOnOnly/ProcessOnOnly.cf* file using the Veritas Cluster Manager GUI (see the SCMS-SM User Guide)

Step 6 Configure the ProcessOnOnly resources as described in the SCMS-SM User Guide.

Restart of SCMS SM Sun Machine Required after Time Change

- Cisco number 7426

  After changing the time on the machine running the SCMS SM, the operator must manually restart the SCMS SM. If the machine is not restarted, it may not be possible to log into the SCMS SM from any of Cisco's Management clients.

Deleted Subscribers Manually Configured

- Cisco Number 9134

  If an SCE platform is part of an SCMS SM domain, and it is also configured directly with subscriber through CLI, the SCMS SM will perform synchronization of the SCE platform subscriber database and will erase the subscribers that were manually configured.

  Workaround: Be aware of this caveat when designing and configuring the system.

Clearing the Subscriber Information in the SCMS SM

- Cisco Number 9570

  When the `SM-LEG Failure Handling` parameter in the SCMS SM's configuration file is configured to `Clear_ all_ mappings= true`, the subscriber information that was manually entered using CLU commands is also erased.

  Workaround: Be aware of this caveat when designing and configuring the system.

Solaris Time Zone and Locale Prerequisites

- Cisco Number: n/a

  Setting the time zone and locale should be done through editing the /etc/TIMEZONE configuration file.

  Note that changes in this file require a reboot to take effect.

Time zone

- Cisco Number: n/a

  Setting the OS time zone as offset from GMT in POSIX format is not supported and may lead to corrupted log files.

  It is best to set the time zone by country name, for example:

  TZ=Israel

Note If GMT offset must be used, use the "zoneinfo" format by attaching a **`:Etc/`**' prefix, for example **`TZ=:Etc/GMT+5`**

Locale

- Cisco Number: n/a

  For correct SCMS SM operation, English locale must be used. The easiest way to set it is by adding the line

  `LANG=en_US`

  To the **`/etc/TIMEZONE`** configuration file

Standby SCMS SM Failure Status

- Cisco Number 12383

  When the standby SCMS SM fails, the Veritas agent notes the user on that through a “monitor time-out” status notification.

SM-LEG Failure Handling is Not Operational in SM 2.5.1 & 2.5.2.

- Cisco Number 13682

  When SM-LEG Handling feature is enabled (*`clear_all_mappings`* is set to true) and the LEG is associated to a domain (LEG-Domains Association section), the SM will start the “clear-all-mappings” timer on valid disconnections of the LEG.. A “valid disconnection” is, for example, when a LEG is restarted. In this case, if the LEG does not reconnect within the timeout, the SM clears all of the mapping in the domain.

  For other types of failures, for example, a crash of the machine running the LEG, or a network disconnect between the LEG and the SM, the failure is ignored!

  Based on this caveat, it is recommended not to use this functionality. Note that this functionality is disabled by default.

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