Release Notes for Cisco Service Control Operating System (SCOS) 2.0.10

August 10, 2005

Release Notes for Cisco Service Control Operating System (SCOS) 2.0.10

Supports: SCOS 2.0.10, SCOS 2.0.9, SCOS 2.0.8, SCOS 2.0.7, SCOS 2.0.6, SCOS 2.0.5, SCOS 2.0.3, SCOS 2.0.2, SCOS 2.0.1

OL-7015-04

These release notes for the Cisco SCOS describe the enhancements provided in Cisco Release 2.0.10. These release notes also cover releases 2.0.10, 2.0.9, 2.0.8, 2.0.7, 2.0.6, 2.0.5, 2.0.2, 2.0.2 and 2.0.1 of the SCOS.

For a list of the caveats that apply to Cisco Release SCOS 2.0.8 see “Open Caveats – Cisco Release SCOS 2.0.8,” page 15.

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

Contents

Introduction

Cisco is proud to release version 2.0.10 of the SCOS (Service Control Operating System) for its SCE platform.

SCOS 2.0.10 is a point release of SCOS2.0. It includes a bug fix that was identified at the customer site.

This document outlines the new features of, and enhancements to, the various SCOS2.0 releases, and assumes the reader already has a good working knowledge of the Cisco Service Control solution. For additional information, please refer to the Cisco Service Control Engine documentation.

New Functionality in Cisco Release SCOS 2.0.10

The following issue was fixed in SCOS 2.0.10:

Link-failure reflection problem between Catalyst6500 series and SCE 1000/2000

When the SCE 1000 or SCE 2000 is configured with link-failure reflection enabled and one of the SCE platform port links changes status to down, the link-failure reflection mode forces the reciprocal SCE platform interface to go down.

When the interface to which the failure is reflected is connected to the Cisco Catalyst6500 switch, the Catalyst6500 interface remains up.

The mechanism used in the SCE platform to force the link to go down puts the port into loopback, with the peer device in auto-negotiation mode. However, in some cases the peer device does not sense it and the link remains up.

In SCOS 2.0.10, the mechanism for forcing the link to the down state is enhanced through implementing toggling of the auto-negotiation mode before putting the port into loopback. The new mechanism allows correct sensing of the link down status by the peer box (specifically the Catalyst6500).

New Functionality in Cisco Release SCOS 2.0.9

The following issue was fixed in SCOS 2.0.9:

Reboots Due to Initialization of the TX FPGA

In some rare cases during the boot sequence, SCE platforms that are running SCOS 2.0.x may reboot unexpectedly during the initial system load. The reboot may only happen when the user reloads the SCE platform or turns on the unit.
In most cases, after this reboot, the system will self recover and load normally.

New Functionality in Cisco Release SCOS 2.0.8

Support for the Improved SCE 1000

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

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

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

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

Solved Bugs and Issues

Avoiding Unnecessary Drops of Packets

In previous SCOS 2.0 releases, the SCE platforms dropped unnecessary packets. This happened in case of flows when BW was over 50 Mbps per second.

This issue was identified and fixed in SCOS 2.0.8.

False Detection of ICMP attacks

In previous SCOS releases, the SCE platform erroneously reported on frequent attacks in the network. The reported attacks used the ICMP protocol and did not contain any specific IP address.

The causes of this phenomenon were identified and the issues were fixed in SCOS 2.0.8.

New Functionality in Cisco Release SCOS 2.0.7

The main issues that were fixed in SCOS 2.0.7 are the following:

Dropped Packets When New Flow Opens with BW Control Enforced

When a new flow opens and BW control mechanisms are enforced on this flow, some of the first packets of the flow may be dropped.

This may happen during the initial time period of 0.5 - 1 seconds of the life of the flow.

SCE Platform Fails to Return From Link Failure

The SCE platform can be programmed to enforce link failure. This may occur in the case of port failure replication, when the SCE platform identifies failure on one port, and forces link failure on the other port, or when the SCE platform is programmed to force link failure on the two ports of a link after reboot.

After enforcing such a link failure, the SCE platform may attempt to cancel this forced failure and restore normal operation of the port or ports. When this occurs, the MAC device of the port may get stuck. Even though the SCE platform signals the network element to which it is connected that the link is up, the SCE platform actually drops all the packets that it receives from this port.

This issue occurs only on the SCE 1000 and SCE 2000.

RDR Accuracy

The accuracy of the reported information in RDRs during subscriber logout is improved.

Introduction of New Subscribers Fails During SM Resynchronization

When a SCE platform loses connection with the SM, and then the connection is renewed, the SM attempts to resynchronize the subscriber information of the SCE platform.

During the resynchronization process, any attempt to introduce new subscribers to the SCE platform fails.

New Functionality in Cisco Release SCOS 2.0.6

The following new software features are supported by Cisco for Cisco Release SCOS 2.0.6

Granular Activation of the Anti-DDos Mechanism

An option was added to activate the SCE platform anti-DDoS mechanism per protocol. The mechanism can now be activated and deactivated for TCP, UDP, ICMP and Other types of traffic.

Better Handling of SM-Connection-Down Event

The following two improvements were added to the SCE platform handling of an event when the connection between the SCE platform and the SM is down:

- An option was added to configure the SCE platform to cut the traffic link when the SCE platform detects that the connection with the SM is down. This was implemented for a SCOS 2.0.x Beta customer who uses Cisco for implementing prepaid billing for mobile. The CLI command for activating this configuration option is:

  `subscriber SM-connection-failure action`

- The SNMP trap that notifies that there is a failure of the SCE platform connection with the SM had a bug.

  This bug is fixed in SCOS 2.0.6.

RDR Mechanism

Two improvements were added to the RDR mechanism:

- The number of RDR categories was increased to four.
- The SCE platform connection time to an RDR collector was reduced from 30 secs to 10 secs.

Link Reflection Improvements

Two improvements were implemented in the SCE platform mechanism of reflecting link failures on one port to the other port:

- The time for detection of a failure on a port was reduced.

  The test of the link status occurs every 200 milliseconds and the link on the port is declared as failed after two consecutive failures.

- The SCE platform behavior after the link has revived was improved: a grace period of 15 seconds was added, before trying to detect a failure again.

This is required in order to prevent a situation of toggling between the two elements to which the SCE platform is connected.

Number of Multi-IP Subscribers on the SCE 1010

A bug was found which prevented the SCE 1010 from supporting 8K multi-IP subscribers.

This bug is fixed in SCOS 2.0.6.

Wrong Duplex Indication in the Show Interface CLI Command

When running the CLI command *`show interface FastEthernet 0/0`*, the indication in the reply of the actual duplex status of the port was wrong. The reply provided the opposite information from the actual status (the reply was 'half' when the port was in 'full duplex', and the reply was 'full', when the port was in 'half duplex'.)

This bug is fixed in SCOS 2.0.6.

Wrong SNMP Traps on Fan Failure

A bug was found in the SNMP trap from the SCE platform produces when it identifies a fan failure. The SCE platform wrongly produced a systemResetTrap.

This bug is fixed in SCOS 2.0.6.

New Functionality in Cisco Release SCOS 2.0.5

The following new functionalities are supported by Cisco for Cisco Release SCOS 2.0.5

SCE 2020 Reboot Due to PPC Exception

The SCE 2020 is currently equipped with Motorola PPC 7457 V1.1 processors.

The Motorola errata specify that in this version of the PPC, the Branch target instruction cache (BTIC) must not be used and should be disabled, and that the symptoms of processor failures when BTIC is enabled include unexpected exceptions that eventually cause a system reboot.

In SCOS 2.0.3 the BTIC was enabled, and we observed a reboot phenomenon with SCOS 2.0.3 that can be explained by this PPC problem. This occurred during a customer beta trial, where the SCE 2020 experienced a reboot every few days.

This issue was fixed by disabling the BTIC mechanism.

New Functionality in Cisco Release SCOS 2.0.3

The following new functionalities are supported by Cisco for Cisco Release SCOS 2.0.3

Support for a HW Change in the SCE 2020

In release SCOS 2.0.3, the SCE 2020 includes a new version of the CAM (Content Addressable Memory) device. The CAM is an advanced memory device in the SCE 2020, where its main function is to allow handling of multi-IP subscribers as a single entity.

Configuring Traffic Rules and Counters

SCOS 2.0.3 includes a new capability of configuring traffic rules and counters through CLI. This capability allows the user to define specific operations on the traffic that is flowing through the SCE Platform, such as blocking or ignoring certain flows or counting certain packets. The configuration of traffic rules and counters is independent of the application that is running in the SCE platform, and is preserved when the application is changed.

The uses for traffic rules and counters include:

- Enabling the user to count packets according to various criteria.

  Since the traffic counters are readable via the SNMP MIB, these might be used to monitor various types of packets, according to the requirements of the specific deployment.

- Ignoring certain types of flows.

  When a traffic rule includes an “ignore” action, packets matching the rule criteria will pass through the SCE platform without being processed. This is useful when a particular type of traffic should be ignored by the SCE platform. Examples include, ignoring traffic from a certain IP range or traffic belonging to a certain protocol.

- Blocking certain types of flows.

  When a traffic rule includes a “block” action, packets matching the rule criteria (and not belonging to an existing flow) are dropped and not passed to the other interface. This is useful when a particular type of traffic should be blocked by the SCE platform. Examples include, performing ingress source address filtering (dropping packets originating from a subscriber port whose IP address does not belong to any defined subscriber- side subnet), or blocking specific ports.

Note Using traffic rules and counters does not affect performance. It is possible to define the maximum number of both traffic rules and counters without causing any degradation in the SCE platform performance.

New Functionality in Cisco Release SCOS 2.0.1

The following new functionalities are supported by Cisco for Cisco Release SCOS 2.0.1

SCE 2020

The SCE 2020 is Cisco's new high-end platform supporting 4 GBPS throughput and deployments in active- active load- sharing links. The SCE 2020 represents a breakthrough in Service Control technology with unprecedented performance and functionality specifically tuned to address the needs of service- providers networks. Building on the award- winning, patented architecture of the Service- Engine product- line, the SCE 2020 represents a breakthrough in Service Control technology and introduces the following key enhancements

- Support for 4 Gigabit- Ethernet ports, suitable for deployments in active-active load-sharing networks
- Support for either single SCE 2020 deployment in 2 GBE links, or deployments or 1 + 1 redundancy with full subscriber-state sharing and coordinated bandwidth control
- Increase in device performance, scaling up to 4 GBPS processing
- Increase in device capacity with support for up to 80,000 subscriber- contexts and 1,400,000 flows
- Field- replaceable, hot- swappable components: Fans, PSU & Air- filters

Load Shared Links with Asymmetrical Routing

The SCE 2020 can be deployed in two load-shared GBE links, and sustains high-utilization on both links. The SCE 2020 is the only solution in the market that supports wire-speed deep-packet-inspection of an aggregated of 2 fully-utilized GBE links.

In load-shared links, asymmetrical routing might occur, and some of the flows may be split, i.e. the upstream packets of the flow go on one link, and the downstream packets go on the other link.

When deployed in this topology, the SCE 2020 completely overcomes this phenomenon, and provides its normal functionality as if asymmetrical routing were not occurring in the two links.

Two Cascaded SCE 2020s for Fail Over

Two SCE 2020s can be deployed on 2 GBE links (one on each link). In this configuration the two SCE 2020s devices operate in coordination, so that when one SCE 2020 fails, the solution functionality is maintained. This includes the ability to perform global and per- subscriber bandwidth- control on both links as well as to maintain the subscriber-state even when one of the devices fails (i.e. no single point of failure).

The two SCE 2020s are in cascaded topology, so the primary SCE 2020 processes the traffic of the two links, while the secondary SCE 2020 only bypasses the traffic of its links to the primary SCE 2020 for processing, and then bypasses the processed traffic back to the link. The two SCE 2020s also exchange keep-alive messages and subscriber state information.

This fail-over solution preserves the SCE 2020 functionality and the network link:

- The two SCE 2020s are simultaneously aware of the subscriber contexts, and subscriber states are constantly exchanged between them, such that if the primary SCE 2020 fails, the secondary can take over with minimum state loss.
- When one SCE 2020 fails (depending on the type of failure) its link traffic is still bypassed to the functioning SCE 2020 and processed there, so the traffic processing continues for both the links.
- The bypass of the traffic through the failed SCE 2020 is configurable, and the user may choose to always cutoff the line that goes through the failed SCE 2020. In this case network redundancy protocols like HSRP are responsible for identifying the line cutoff and switching all the traffic to go through the functioning SCE 2020.

Configuring Topology-Related Parameters

SCOS 2.0.1 introduces some changes in the CLI commands for configuring topology-related parameters. The main motivation for making these changes is the need to configure the new topology of two cascaded SCE 2020s:

- connection-mode command change

  (config if)#connection-mode *[inline / receive-only]*

  This command is now extended to include the topology of two cascaded SCE 2020s, including the priority of the SCE 2020 in a cascaded pair, the index of the link to which the SCE 2020 is connected, and the link failure behavior.

  In case of non-cascade topology, the only parameter added to this command is the link failure behavior (*on-failure)* that can be set to either *bypass* or *cutoff* (the default is bypass).

- Link bypass command change

  SCOS 1.5.x link-bypass command (under *interface linecard* configuration*)* was removed and a new "*link mode*" command was added.

  The link mode command enables the user to set the link mode of an active box to the following modes:

  - Forwarding
  - Bypass
  - Cutoff
  - Sniffing (sniffing is available in SCE 1010/2000 only and in SCE 2020 only when configuring Sniffing for all links at the same time).

Note The link mode command is relevant only for an active SCE 2020, which means that when working in cascade topology the standby SCE 2020 will only change its link mode if it becomes active.

The configuration for failure and reboot cases is done via the *on-failure* parameter in the connection-mode command.

Protection from DDoS attacks

The SCE platforms now include enhanced capabilities of identifying DoS and DDoS attacks, and protecting against them. Previous versions of the SCOS provided a means to monitor the entire link and identify a global increase in flow-open rate, indicative of a DoS attack.

SCOS 2.0.1 extends this concept by improving the detection mechanism, adding individual IP address granularity, and providing a set of actions to report (to the operator), block, and notify (the subscriber) of the attack.

The system tracks the following two metrics in an attempt to identify abnormal flow or connection increase:

- **open-flows**: Total number of flows (TCP, UDP, ICMP, other) that are concurrently open
- **ddos-suspected-flows**: Total number of flows that are possible suspects of being part of a denial- of- service attack because they are un- established (in TCP the 3-way handshake is incomplete, in UDP/ ICMP/ OTHER, less than three packets have been transmitted on a flow).

The above two metrics are maintained for each IP address, and the system tracks the values against pre- defined (and user- configurable) thresholds (an attack is defined when the threshold is breached for a certain IP address).

The system makes a distinction between an Attack- Source and Attack-Destination. As each attack is associated with an IP address, the IP- address is classified as either the attack source (i.e. it is generating the attack traffic) or its destination (i.e. it is being attacked). This parameter is later reported, and can also be used in creating filtering and action rules for the DoS mechanism.

Once an attack is identified, the system can be instructed to perform any of the following actions:

- Report: The system generates an SNMP trap each time an attack ‘starts’ and ‘stops’.
- Block: The system blocks all suspected traffic from or to the attack IP address (depending on whether the IP address is an Attack- Source or Attack-Destination)
- Subscriber notification: When the IP address identified is mapped to a particular subscriber context, the system can be configured to notify the subscriber of the attack (or a machine in the network is generating such an attack), using HTTP Redirect.

Additional Tunneling Support – L2TP

In cases where the SCE platform is deployed in the L2TP cloud, the SCE platform must "ignore" the L2TP headers while performing the Service Control functionality. Otherwise, all traffic would be classified as L2TP traffic between the LAC and LNS, and the true application and subscriber nature of traffic would remain unveiled.

To address this, the SCE Platform can be configured to perform the above action. In this case, the Service Control functionality is performed starting from the IP header of the internal packet encapsulated inside the L2TP packet. Once selected, the system skips the tunnel (outer IP headers and tunnel headers) and uses the internal TCP/UDP headers, and the starting point for processing.

Note This is an internal process and the SCE platform does not modify the packet (or its tunnels), allowing the L2TP tunneling mechanism to function.

When deployed in an L2TP environment, the SCE platform must be configured to enable its L2TP header processing. This is done using the CLI, and can optionally set the port numbers used by the LAC or LNS (the default is 1701). The following example shows how to configure an SCE platform to ignore L2TP headers for all traffic between a LAC (typically the BRAS device) and an LNS device.

SCE> IP-tunnel L2TP skip - to enable L2TP skip mode

SCE> L2TP identify-by port-number *1701*

Important Notes

- The upgrade to SCOS 2.0.9 will include re-initialization of the SCE 1010 / SCE 2020 hardware Bypass module. This re-initialization process can cause a failure of the GBE link where the SCE 1010 / SCE 2020 is installed for a period of less than 1sec.
- The number of subscribers with IP ranges that the SCE 1010 and SCE 2020 can support was increased to 8,000.
- Cisco has identified a situation in which the SCE box might experience a reboot when a port scan operation is performed on the SCE management port. We decided not to fix this issue, since this reboot is initiated by the SCE platform as a result of scheduling optimization for detecting failover conditions in periods of less than 1 second (in a configuration of two cascaded SCE platforms)

The following is recommended:

- Use IP access lists - they should eliminate the occurrence of port scans that occur as a result of actual attacks.
- If the system administrator performs a port scan operation as part of a security check, it is suggested to disable the SCE watchdog only for the period of time in which the port scan is performed.

The CLI commands for this are: *'configure/interface linecard 0/no watchdog'* and *'configure/watchdog software-reset disabled'.*

Caveats

Open Caveats – Cisco Release SCOS 2.0.8

FF L4 Rules Do not Match Non-First IP Fragments

- Cisco number 3975

  A non-first fragment packet does not 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 IP Address

- Cisco number 4989

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

  Workaround: Reboot the SCE platform after changing the IP address

ToS Marking for TCP: Three 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 three first packets (SYN, SYN-ACK, and 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 supports saving of the SCE 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 sec; this should be increased to ~15 sec.

Telnet Sessions to the SCE Stays Open

- Cisco number 8749

  When the SCE platform 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 platform stays open, and will never close.

  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.

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 which occurs when the traffic traverses through the SCE platform). This ensures that the SCE platform never blocks the management port traffic.

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

  There are no known workarounds.

SCE 1010 and SCE 2020 Disk Space

In certain cases the SCE 1010 or SCE 2020 runs out of disk space. Since the SCE platform requires 40Mbytes of free space for correct operation, this can cause severe problems.

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

- The SCE 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 platform 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 platform, the SCE platform may cause a loss of traffic packets for several seconds.

  Workaround: It is recommended to move the SCE platform 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`**

DNS Server Configuration

There is a problem with the SCE platform DNS configuration (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 platform experiences various communication problems, including failure to ping other network entities from the SCE platform. This occurs 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.

Injecting Packets with the SCE 2020 in Two GBE links with Tunneling in Split-Flows Environment

When the two GBE links where the SCE 2020 is installed experience split-flows, and the links are tunneled (L2TP or MPLS), performs injection of a packet (for example for implementing HTTP Redirect) may fail.

There are no known workarounds.

Error in CLI Command

- Cisco number 13034

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

  There are no known workarounds.

Importing Subscribers to the SCE

When you perform several 'import CSV' operations on the SCE platform, and then the SCE platform reboots for any reason, the imported information is not saved.

There are no known workarounds.

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

.