Release Notes for Cisco Application-Oriented Networking Version 2.3

November 17, 2006

Cisco Application-Oriented Networking (AON) is the first in a new line of Cisco products that embed intelligence into the network to meet the needs of application deployment. AON enables you to:

- Integrate dissimilar applications by routing information to the appropriate destination, in the format required at the destination.
- Enforce policies for information access and exchange.
- Optimize bandwidth and reduce processing overhead for application traffic.
- Increase management of information flow, including monitoring for business and infrastructure.
- Enhance business continuity by transparently backing up or rerouting critical business data.

Working at the message rather than packet level, AON provides this support by understanding more about the content and context of information flow.

Contents

These release notes cover Cisco Application-Oriented Networking Version 2.3 and include the following topics:

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

New Features in Cisco AON 2.3

AON 2.3 includes the following new features and functionality:

- Enterprise Lifecycle Management

  This feature introduces the concept of projects to partition the work performed by different development teams. Teams can manipulate the resources assigned to their projects without regard for the resources used by other projects.

- Programmatic Management Interface

  This feature provides an interface so that third-party applications can manipulate data in AMC.

- Stand-Alone Nodes with TACACS+ Support

  AON nodes can be configured to operate in an environment without AMC. In stand-alone mode, nodes are managed by a third-party application such as AlterPoint, which configures the node using SSH and the command-line interface (CLI). Additionally, nodes can be configured to use TACACS+ for authentication, authorization, and accounting of users

- Promiscuous Mode Enhancements

  Pmode now has the ability to capture UDP packets. The feature is enabled by default; no further configuration is necessary. Pmode has also been enhanced to capture packets at time-based intervals.

For more information on using these features, see the "Related Documentation" section on page 14.

AON Application System Requirements

Table 1 lists the minimum requirements for installing AON applications for AON Release 2.3.

Table 1 AON Minimum System Requirements

Application	Operating System	CPU	RAM	Hard Drive	Software Image
AON Management Console (AMC)	Red Hat Enterprise Linux 3.0 or later	Single processor; Pentium III or Xeon	1 GB	20 GB	AON 2.3.0.79
AON Development Studio (ADS)	Windows 2000 or Windows XP with latest service packs.	Pentium IV	1 GB (required) 2 GB (recommended for large adapters)	40 GB	AON 2.3.0.79

AON Supported Hardware

Table 2 lists the hardware platforms that are supported by AON version 2.3.

Table 2 Supported Hardware

AON Appliance	AON Service Module (AON-SM)	AON Network Module (AON-NM)	AON Enhanced Network Module (AON NME)
Cisco 8340 AON Appliance • APL-AON-8340-K9 Cisco 8342 AON Appliance • APL-AON-8342-K9	• WS-6503 • WS-C6503-E • WS-C6506 • WS-6506-E • WS-C6509 • WS-6509-E • WS-C6509-NEB-A • WS-6513	• Cisco 2610XM • Cisco 2611XM • Cisco 2620XM • Cisco 2650XM • Cisco 2651XM • Cisco 2691XM • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3725 • Cisco 3745 • Cisco 3825 • Cisco 3845	• Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3725 • Cisco 3745 • Cisco 3825 • Cisco 3845

AON Node Supported Software

Table 3 lists the software levels for the Cisco platforms that support AON.

Table 3 Supported Software on Nodes

Platform	Minimum Software Release Supported	Latest Software Release Supported
AON-SM Catalyst 6500 Series Switches with Supervisor Engine 720	Cisco IOS Release 12.2(18)SXE1	Cisco IOS Release 12.2(18)SXF2
AON-SM with Catalyst OS Catalyst 6500 Series Switches with Supervisor Engine 720	Cisco IOS Release 12.2(18)SXF CatOS Release 8.5(3)	CatOS Release 8.5(3) Cisco IOS Release 12.2(18)SXF
AON-SM 2 Catalyst 6500 Series Switches with Supervisor Engine 2	Cisco IOS Release 12.2(18)SXF2	Cisco IOS Release 12.2(18)SXF2
AON-SM 2 with Catalyst OS Catalyst 6500 Series Switches with Supervisor Engine 2	CatOS Release 8.4(2a) Cisco IOS Release 12.1(23)E3	CatOS Release 8.5(3) Cisco IOS Release 12.2(18)SXF2
AON-NM Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 Series Routers	Cisco IOS Release 12.3(14)T1	Cisco IOS Release 12.4(9)T
AON-NME Cisco 2800, Cisco 3700, and Cisco 3800 Series Routers	Cisco IOS Release 12.4(9)T	—
Cisco 8340 AON Appliance	AON version 1.1.0.189 AON version 2.1.2.29 (with firmware upgrade)	AON version 2.3.0.79
Cisco 8342 AON Appliance	AON version 2.1.2.29	AON version 2.3.0.79

Upgrade Paths

Table 4 lists the valid upgrade paths for each AON software release. Beginning with AON 2.1, AMC can manage nodes running any previous AON 2.x release. Therefore you are not required to upgrade nodes when you upgrade AMC and ADS. However, we recommend that you do upgrade nodes whenever possible in order to benefit from the software defects resolved in each new release.

Table 4 AON Upgrade Paths

AON Release	Valid Upgrade Paths	Node Upgrade Required
AON 1.*x*	AON 2.1 only	Yes
AON 2.1	Any AON 2.*x*	No
AON 2.1.1	Any AON 2.*x*	No
AON 2.1.2	Any AON 2.*x*	No
AON 2.2	AON 2.3	No

Upgrading a Router to Cisco IOS Release 12.4(9)T

Cisco IOS Release 12.4(9)T changes the name of the AON-NM in Cisco IOS. It is now referred to as **AON-Engine** instead of AONS-Engine. Because of this change, you must perform the following additional steps as part of your upgrade:

- Back up your startup and running configurations
- After the upgrade, re-enter the AON-NM's network configuration using the AON-Engine interface.

For further details on configuring the AON-NM, see the *AON Installation and Upgrade Guide*.

Important Notes

- The AON Management Console (AMC) supports only Microsoft Internet Explorer 6. AMC pages may not render properly in other Web browsers.
- AON is implemented in Java where memory is automatically managed by the Java runtime system. This means that there might be moments in the system where the garbage collection (automatic memory management) is still working at freeing up memory. The graceful handling mechanism checks the free memory to determine if a message should be let into the system. So under high loads it is possible that AON will reject messages because the garbage collection is taking time to free up memory.
- The following issues may affect AON Development Studio installation, however, the root causes are beyond the control of Cisco:
  - Using the ALT key during ADS installation can cause some InstallShield screens to become corrupted. Despite this display problem, the ADS installer continues to function. If the display gets corrupted, minimize the ADS installer and then maximize it again. The display should return to normal. This is a known InstallShield issue when using JVMs with version 1.4.2.x.
  - In rare situations when initially launching ADS on Windows 2000, an error message may be returned indicating the database is busy or unavailable. The error can occur even though the database is listed as started in the list of Windows Services. This occurs when a database port is chosen in the ADS installer that also appears in the output of the **netstat -a** command in a loopback situation. The port is shown pointing to another server port which in turn points back to it. This behavior has only been seen with one port, though not always the same port on the system. Reboot the PC to correct this problem.

Resolved Caveats

Table 5 lists the caveats that have been resolved in this AON release.

Table 5 Resolved Caveats in AON 2.3

Defect ID	Description
CSCse76913	**show cdp** command not displaying version value
CSCek28868	Deprecate rollback feature from EMS delivery failure policy
CSCek28910	Graceful handling activates in AON-SM server proxy with few hours of 15 concurrent 600KB messages
CSCek32772	Timestamp is incorrect in AON appliance after upgrade to new image
CSCek33304	AON does not preserve original proxy host and port in implicit mode
CSCsd99036	ADS unable to create a flow with Branch bladelet inside a Loop bladelet
CSCsd99156	XPath returns value of null from rule when processed the first time
CSCsf04907	Bootloader configuration erased after log trace boot
CSCek29537	Accept error: too many open files exception with 60MB message
CSCek34255	Watchdog restarts AON when MBean server busy, unable to connect
CSCek36038	AMC Global Deployment fails if first node in AMC is inactive
CSCin98529	Unable to create scar file on Windows XP using .so without version
CSCek35365	Crash in schema validation when deploying XSD

Open Caveats

Table 6 lists the caveats for this AON release, including defect identification numbers and symptoms. When applicable, conditions under which the defects occur and workarounds are also included.

Table 6 Open Defects in Cisco AON Version 2.3

Defect ID	Description
CSCek18587	**Symptom** Message delivered even when TTL expired. **Condition** The associated PEP introduced an artificial delay of 60 seconds. The TTL was set for 30 seconds, yet the message was still delivered to the server proxy. The message should have been dropped. **Workaround** None.
CSCek20178	**Symptom** EMS adapter with inbound batch size greater than 1 does not work properly. Success and failure notifications do not occur properly, causing incorrect message delivery notifications to occur. **Workaround** Use batch size = 1.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCek25145	**Symptom** Errors occur when a MQ client or endpoint uses the same correlation-ID for multiple messages. **Workaround** Configure the MQ client to use a unique correlation-ID for each message.
CSCek25514	**Symptom** Optimization does not support wild cards in URI for message type classification. In a message type URI, if a string such as /index* is specified, then Optimization classification does not classify messages with URIs /index.html and /index1.html to that message type. **Workaround** Use complete URI for message type classification. If more than one URI needs to be classified to a single message type, and hence execute the same PEP, define a message type for each URI and map all of these message types to the same PEP.
CSCek29582	**Symptom** Unable to parse XML/SOAP documents. Manifestation of this problem appears in the form of security bladelet exception. **Conditions** Under rare condition, contents of a HTTP body are corrupted. The root cause is unidentified. **Workaround** The client is notified of error by sending appropriate HTTP error code and it is expected that the client re-tries the message again.
CSCek29630	**Symptom** AON fails to establish connection to Tibco EMS server **Condition** This happens when Tibco EMS server is re-started multiple times after AON system has bootstrapped. It has been observed mostly in virtual cluster (VC) setup. **Workaround** Restart AON System. In case of VC setup, re-start all AON nodes participating in the VC
CSCek29803	**Symptom** Messages are sometimes lost and do no appear in the dead letter queue (DLQ) or the destination queue. **Conditions** This happens when the inbound source batch size is greater than 1 in JMS adapter configuration. **Workaround** Change the batch size of the inbound source (including replyTo source) to 1.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCek29828	**Symptom** Unable to classify a JMS message on the destination URI even though source and destination policies are statically linked via the JMS adapter configuration. **Conditions** This happened when source and destination queues are defined on two different MS brokers and they are statically linked via the JMS adapter configuration. **Workaround** Define the source and destination on the same brokers.
CSCek29892	**Symptom** EMS broker running out of resources when EMS Adapter is configured incorrectly. **Conditions** EMS queue type is Send and EMSAdapter is configured it as Receive or vice- versa. In this misconfiguration, adapter continues to try to connect to the broker to register itself. This is causing resource issues on the broker side. **Workaround** Correct EMS Adapter configuration to have a proper valid configuration.
CSCek30721	**Symptom** Caching MQ and JMS messages causes buffer leaks which eventually results in buffer exhaustion. System is unable to process any messages after this condition. The following message is logged: `11-Oct-2005 17:51:54 DEBUG [MEC-Q-1] aons.mec.monitor *** Buffer space utilized = 6.686 Under steady state conditions (when no messages are being processed) Buffer space utilized should be zero.` **Workaround** No Workaround. This problem does nor occur when caching HTTP messages.
CSCek31626	**Symptom** URI-based classification does not seem to work correctly. Messages are rejected even if there is an entry for that URI. This could happen if there are other message types that are classified based on 5-Tuple. This issue can be reproduced only in the following scenario. **Condition** Classification based on URI /index.html does not work correctly. Message type 't1' based on 5-Tuple 'a' and URI '/index-nomatch.html' and message type 't2' based just on URI '/index.html' Client messages that match 5-Tuple 'a' and URI '/index.html' does not get classified to type 't2'. Then the message is rejected. **Workaround** Add a message type 't3' that is based on 5-Tuple 'a' and URI '/index.html' Or If 5-Tuple based classification is not required for 't1' classification, remove the 5-Tuple detail from message type 't1'.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCek34188	**Symptom** On a two-node queue based adapter test, a memory leak was observed for reliable and ordered messages. Eventually this leak causes graceful handling too kick in and all new messages are rejected. **Condition** Observed in a two-node scenario (AON-NM as the client and AON-SM as the server proxies) for MQ-to-JMS translation. The messages were being sent on reliable and ordered queues. The concurrency for 5 and message size for 600 KB. Due to the limited heap size on the AON SM, after few hours graceful handling kicks in and a few messages are rejected. The inbound side slows down considerably as the memory keeps increasing (due to the leak). Due to this leak, almost 1000 messages drop down to less than 100 messages in eight hours. **Workaround** There is no workaround for the two-node case. Switching to a single node setup will eliminate the leak. Note This problem does not happen for HTTP cases or translation from HTTP to queue based adapters.
CSCek35429	**Symptom** Request message does not reach its destination in a queue-to-queue based message interaction. **Condition** In a multi-blade virtual cluster (VC) setup, AON replyTo queues do not get equitably distributed among all the blades. It is possible that some of the blades may not acquire any AON replyTo queues. **Workaround** Configure the number of AON replyTo queues equal to or greater than twice the number of blades in the VC setup.
CSCek36378	**Symptom** Cookie headers in 302 direction response are not correctly handled by AON. The cookie headers are not forwarded to the directed URL or sent to the client. **Conditions** It only happens for 302 redirection response containing cookie headers. **Workaround** None.
CSCek37187	**Symptom** When an image upgrade is done, as designed, the AON optimization log level resets to default behavior. However, the running config shows the previously set non-default level. **Condition** This situation occurs only when an image upgrade is done. **Workaround** Reconfigure the desired log level after each upgrade.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCek37408	**Symptom** AON stops picking message from JMS IN queue **Conditions** This happens in a two-blade single-node VC when client uses unlimited dynamic reply queues. **Workaround** Use static queues instead of dynamic queues.
CSCse41928	**Symptom** Multiple modifications to JMS/SSL property and single deployment do not work correctly. The change notification did not happen on the corresponding nodes. Only some of the modifications done to the JMS/SSL property take effect and sometimes AON stops listening to the modified JMS queues. **Conditions** Made a series of changes to a JMS property and did a single deployment from AMC to nodes. The change notification did not happen on the corresponding nodes. **Workaround** Either deploy one JMS property change at a time or restart AON.
CSCse46613	**Symptom** The following adapter exception is encountered in a two-node setup: `No destination could be found` **Conditions** This happens if the same reply queue is being used in the following scenario: JMS message is processed in a request-response flow by a JMS adapter on an AON client proxy and a JMS adapter on an AON server proxy, this is followed by an MQ message processed in a request-response flow by an MQ adapter on the AON client proxy and a JMS adapter on the AON server proxy. **Workaround** Use different reply queues for the JMS-to-JMS flow and the MQ-to-JMS flow.
CSCse46778	**Symptom** In a two-node reliable/ordered scenario, some of the requests do not reach the end point (as a result the corresponding the responses are not received by the client). On server proxy, the following warning message appears on the log: `aons.mec.core %%FAILURE% %%received% 2006-06-08 03:25:22.963 %%source% null %%dest% http://httpserver.aontest.com:80/echo.php %%corrid %` **Conditions** Reliable/Ordered, two node, JMS/MQ at inbound on client proxy and HTTP at outbound on server proxy. The end point should close the connection while AON writes a message to it. **Workaround** None.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCse47151	**Symptom** Execution of PEP is really slow to finish, at the same time when checking node events, will see Log bladelet have error exceptions. **Conditions** If the database is down or if Msg Log Policy has incorrect information, AON cannot establish connection to the database. The Log bladelet, even in Asynchronous mode, will take a long time, approximately 30 seconds, to execute. During the execution of the PEP, it will pause in the Log bladelet until it times out before moving on to the next bladelet. **Workaround** Fix the incorrect information in the message log policy and deploy. Restart the database if it is down.
CSCse55758	**Symptom** When the URI is http:cisco.com/index.html, then instead of sending the data to http://cisco.com/index.html, the request is going to destination specified in “host” header field. **Conditions** This condition happens when URI is incorrect. Though http:www.cisco.com is a correct form of URI, as per Fastpath it is incorrect. Hence Fastpath tries to reconstruct the URL from the “host” header field and tries to connect to it. **Workaround** None.
CSCse67323	**Symptom** O/R message processing with EMS in a two-blade scenario virtual cluster (VC) is very slow, almost at the rate of 1 message every two minutes. **Conditions** EMS adapter at inbound in a two-blade VC. A number of messages are deposited in the inbound queue at once. First few messages get processed quickly, but later the message processing slows down considerably. Eventually the messages get processed. No related error or warning messages are in the log. **Workaround** None.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCsf25346	**Symptom** Messages are rejected due to graceful handling under heavy load, high concurrency, and a large number of messages. **Conditions** When there is a heavy load in terms of concurrency and number of messages, if the depositing of messages to the outbound queue is slow for any reason (end point behavior, load characteristics on AON), a backlog could ensue, resulting in dropping of messages at the inbound queue due to graceful handling. **Workaround** Reduce the load. Ensure that the calculations of load take into effect the time required to process a message. If running at debug level change it to NOTICE or WARN, if appropriate as debug level logging by itself could slow down the overall PEP processing
CSCsg32611	**Symptom** Output of the **show users** CLI command shows more users than are currently logged into the AON CLI. **Conditions** CLI sessions have been abnormally terminated at the client side rather than terminated by using the CLI **exit** command. **Workaround** None.
CSCsg36209	**Symptom** MDS fails to redeliver message over HTTPS in an AON multi-node scenario if the destination end point goes down and is brought back up before time to live (TTL) expires. **Conditions** This occurred in a multi-node scenario where MDS is enabled on both the client proxy (CP) and the server proxy (SP). The CP and SP use HTTPS to communicate. If the destination end point goes down, the HTTPS connection gets closed by the client. When the end point is up again, the message does not get redelivered even though the TTL has not expired. **Workaround** None.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCsg55520	**Symptom** User starts a deployment, and it hangs indefinitely. If user retries the deployment from a different browser window, or if the user attempts to deploy a different DR to one of the nodes involved in the hung deployment, the deployment fails with the error "another user is currently deploying to node." **Conditions** This situation has been observed when an AON-SM was in a non-running state (neither the AMA or AON processes were running on the node). **Workaround** Try restarting the node, then restart AMC. This will remove the deployment locks held on the node. Try to deploy again. **Further Problem Description** This problem is believed to be caused by a defect in the Web service remote procedure call framework used by AMC. Under normal circumstances, calls to unresponsive nodes should timeout, and the deployment should terminate with an error. The defect in the framework is preventing this from happening.
CSCsg72965	**Symptom** Node health is unknown on the Node Details page of AMC. There is no up or down triangle next to the node in the State column. **Conditions** Occurs if the node is down when AMC starts up. After the initial polling attempt, AMC continues to wait for a response and makes no further attempt to poll the node. **Workaround** Restart AMC once the node is online again.

Table 6 Open Defects in Cisco AON Version 2.3 (Continued)

Defect ID	Description
CSCsg76213	**Symptom** On a two-node HTTP adapter test, a memory leak was observed for reliable and ordered messages. Eventually this leak caused AON to run out of buffers and no further messages were processed. **Conditions** The problem was observed while running two-node tests (AON-NM and AON-SM as the client and server proxies) using HTTP adapters. The messages were being sent using reliable and ordered delivery semantics. **Workaround** There is no workaround for the two-node case. Switching to a single node setup will eliminate the leak. **Further Problem Description** The leak is in the metadata maintained by AON for each message to ensure ordering (delivery entry). This leak happens on the inbound side of the message. For request messages it happens on the client proxy, and for response messages on the server proxy
CSCsg83737	**Symptom** AMC allows next hop domain to be configured in projects other than the system project. **Condition** Next hop domain is a system-level policy and should only be configured in the system project. If next hop is configured in another project, the new configuration will fail. **Workaround** None. Configure this policy only in the system project.

Related Documentation

The AON documentation set includes the following guides:

- *AON Installation and Upgrade Guide*—covers the installation and upgrade of the AON environment.
- *AON Administration Guide*—covers the administration of AMC and AON nodes.
- *AON Development Studio User Guide*—covers ADS, bladelets, and PEP creation.
- *AON Programming Guide*—covers the development of custom bladelets, custom adapters, and other features related to extending AON functionality.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation by using the embedded feedback form next to the document on Cisco.com or by writing to the following address:

Cisco Systems, Inc.
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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 provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is 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/

- *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