Release Notes for Cisco Application-Oriented Networking Version 2.1.1

June 7, 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.

These release notes cover Cisco Application-Oriented Networking Version 2.1.1 and include the following topics:

Cisco Systems

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

AON Application Requirements

Table 1 lists the minimum requirements for installing AON applications.

Table 1 AON Minimum System Requirements

Application	Operating System	CPU	RAM	Hard Drive
AON Management Console (AMC)	Red Hat Enterprise Linux 3.0 or later	Single processor; Pentium III or Xeon	1 GB	20 GB
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 Node Supported Hardware

Table 2 lists the hardware platforms that are supported by AON version 2.1.1.

Table 2 Supported Hardware

AON Appliance	AON Service Module (AON-SM)	AON Network Module (AON-NM)
Cisco 8340 AON Appliance	• 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

AON Node Supported Software

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

Table 3 Supported Software

Platform	Minimum Software Release Supported	Latest Software Release Supported
Cisco 8340 AON Appliance	AON version 1.1.0.189	AON version 2.1.1.53
Native Catalyst 6500 Series Switches with Supervisor Engine 720	Cisco IOS Release 12.2(18)SXE1	Cisco IOS Release 12.2(18)SXF2
Hybrid 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
Native Catalyst 6500 Series Switches with Supervisor Engine 2	Cisco IOS Release 12.2(18)SXF2	Cisco IOS Release 12.2(18)SXF2
Hybrid 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
Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 Series Routers	Cisco IOS Release 12.3(14)T1	Cisco IOS Release 12.4(3)

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

Table 4 Resolved Caveats for Cisco Application-Oriented Networking Version 2.1.1

Defect ID	Description
AMC	
CSCek36891	Enhancements on AMC Package size reduction and AMC DB security.
AON	
CSCek39791	JMS queue properties changes take effect only after AON restart.
CSCse03361	Dynamically listen for change in JMS resource file (.bindings).
CSCse03363	Dynamic update to SSL configuration is required.
CSCse01517	Loop Bladelet does not reset counters if called from within another loop.

Open Caveats

Table 5 lists the caveats for this AON release. These caveats are in addition to the open caveats listed in the *Release Notes for Cisco Application-Oriented Networking Version 2.1*

Table 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1.1

Defect ID	Description
CSCsd99156	**Symptom** When the flow has multiple SetDestination Bladelets (with XPath rules) or if there are Find Bladelets ahead of SetDestination Bladelet (with XPath Rules), SetDestination's XPath evaluation returns NULL for the first request message. **Workaround** Send another message.

Table 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1.1

Defect ID	Description
CSCse35371	**Symptom** If there is an existing or new sequence in the schema, the message log writing and viewing in AMC fails. **Workaround** For Oracle, do not change the schema after it is created using the scripts in appendix A. This information is found in “Create a Message Log Database” section of Chapter 4, Step 1, in the *Cisco AON Installation and Administration Guide.* **Note** If changes are added, it may cause the message log feature to fail. For example, as reported in this defect, existing or new sequences to the schema can cause older version before 2.1.1 to fail.
CSCse41928	**Symptom** Multiple modifications to JMS/SSL Property & Single deployment doesn't work correctly. The changes notification did not happen on the corresponding nodes. Only some of the modifications had done to the JMS/SSL property take effect and sometimes AON stops listening to the modified JMS queues. **Conditions** Make a series of changes to a JMS property and do a single deployment from AMC to nodes. The changes notification did not happen on the corresponding nodes. **Workaround** Either deploy one JMS property change at a time, or restart AON.

Upgrade Instructions

For detailed instructions on upgrading to Cisco Application-Oriented Networking Version 2.1.1, see the following document:

Upgrading the Cisco Application-Oriented Networking Environment

Backward Compatibility

Cisco Application-Oriented Networking 2.1 and above releases are backward compatible.

Note You must install the latest Cisco AON Management Console (AMC) release and AON Developer Studio (ADS) software on your node. Both these software versions must match for the node to work.

Cisco Application-Oriented Networking Version 2.1.1 will work with any node with Cisco AON Version 2.1.

Related Documentation

The AON documentation set includes the following guides:

- *AON Installation and Administration Guide*—covers the installation and administration of the AON Management Console and AON nodes.
- *AON Development Studio User Guide*—covers the AON Development Studio, 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