



Release Notes for Cisco Application-Oriented Networking Version 2.1

March 24, 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 and include the following topics:

- [AON Application Requirements, page 2](#)
- [AON Node Supported Hardware, page 2](#)
- [AON Node Supported Software, page 3](#)
- [Important Notes, page 3](#)
- [Resolved Caveats, page 4](#)
- [Open Caveats, page 5](#)
- [Upgrade Instructions, page 19](#)
- [Downgrade Instructions, page 19](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, page 20](#)
- [Documentation Feedback, page 21](#)
- [Cisco Product Security Overview, page 21](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Obtaining Technical Assistance, page 22](#)

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.

Table 2 *Supported Hardware*

| AON Appliance | AON Service Module (AON-SM) | AON Network Module (AON-NM) |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco 8340 AON Appliance | <ul style="list-style-type: none"> • WS-6503 • WS-C6503-E • WS-C6506 • WS-6506-E • WS-C6509 • WS-6509-E • WS-C6509-NEB-A • WS-6513 | <ul style="list-style-type: none"> • 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 8342 AON Appliance | AON version 2.1.0.173 | — |
| 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*

| Defect ID | Description |
|------------|----------------------------------------------------------------------------------------------------|
| CSCei85094 | Ordered delivery fails; messages received out of sequence after Discard bladelets on client proxy. |
| CSCej26320 | Keywords do not have any affect on show cdp command output. |
| CSCeh97036 | tcpdump needs to be upgraded to resolve security vulnerability. |
| CSCei08853 | Security bladelets should throw exception when key is expired. |
| CSCei34579 | TTL value for cache object changes after node is reloaded. |
| CSCej41786 | ADS fails to return error when synchronizing with AMC when DR is staged. |
| CSCej43486 | Unable to reclaim memory after around 48 hours of run time. |
| CSCej43550 | Message classification not matching cookie header rules correctly. |
| CSCei68004 | EMS,MDS: NPE in JMSSendMessageHandler.initialize() |
| CSCej09320 | Errors occur when message size exceeds 35 MB. |
| CSCej43039 | Buffer leak occurs on two-node MQ scenario when CacheData bladelet is in PEP. |
| CSCej57256 | Retry fails to send exception on AON-SM with message of 20 MB |
| CSCei58010 | EMS,MDS: SP cant deliver JMS response, get stuck if CP restarts |
| CSCei73370 | Multi-send bladelet fails to deliver all messages. |
| CSCei34579 | TTL value for Cache object changes after reloading of node. |
| CSCej54752 | Buffer not released when “out of buffers” error occurs in server proxy. |

Open Caveats

[Table 5](#) 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 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1

| Defect ID | Description |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCei10353 | <p>Symptom</p> <p>Changes to WCCP load balancing do not take affect due to conflicting masks.</p> <p>Conditions</p> <p>User changes the load balancing for WCCP service group from the default source-IP to other values, including source port and source IP port on the AMC.</p> <p>Workaround</p> <p>If possible, keep the default load balancing configuration. If a conflict happens, remove and recreate the WCCP service group.</p> |
| CSCej53322 | <p>Symptom</p> <p>Encryption or decryption of large messages gives Java Out-of-memory error in AON log, with the following entry:</p> <pre> WARN [MEC-Q-4] aons.mec.core OutOfMemoryError in PoolWorker.run().Will notify VM to run GC java.lang.OutOfMemoryError: Java heap space Condition This could happen when the original message is a large message (around 80MB) and the structure of the message (that is being encrypted or decrypted) falls into the following descriptions (or increases the complexity of the message more than what are given) Type 1: Huge number of nodes (around or more than 500,000), each node may have children and namespaces or attributes. In the following message template, the 'add' element falls into this category. <?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <SOAP-ENV:Body> <add xmlns="http://calculator.examples.soap.webtool"> <in0 xmlns="">DATA</in0> <in1 xmlns=""> DATA </in1> </add> <add xmlns="http://calculator.examples.soap.webtool"> <in0 xmlns="">DATA</in0> <in1 xmlns=""> DATA </in1> </add> <add xmlns="http://calculator.examples.soap.webtool"> <in0 xmlns="">DATA</in0> <in1 xmlns=""> DATA </in1> </add> </SOAP-ENV:Body> </SOAP-ENV:Envelope> Type 2: Huge number of nodes (around or more than 500, 000), each node has only CDATA (no children), but the nodes may have namespaces or attributes. In the following message template, the 'add' element falls into this category. <?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <SOAP-ENV:Body> <add xmlns="http://calculator.examples.soap.webtool"> CDATA </add> <add xmlns="http://calculator.examples.soap.webtool"> CDATA </add> <add xmlns="http://calculator.examples.soap.webtool"> CDATA </add> </SOAP-ENV:Body> </SOAP-ENV:Envelope> </pre> <p>Workaround</p> <p>The following approaches can be used for overcoming this problem:</p> <ol style="list-style-type: none"> 1. Verify if indeed the entire message needs to be encrypted, if only parts of the message need be encrypted, this problem can be overcome regardless of the total size of the message. 2. If the message can be split, then it can be sent as multiple messages that are smaller in size. 3. If the message structure can be altered, then determine if the number of nodes can be decreased. |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCej55045 | <p>Symptom</p> <p>There are various symptoms for this problem depending upon configuration, including:</p> <ul style="list-style-type: none"> • A message is delivered after it has expired. • EMS adapter causes an exception. • “Duplicate message” error appears in the AON log. <p>Conditions</p> <p>Messages created in the PEP with CreateMessage and CreateResponse when MDS is configured.</p> <p>Workaround</p> <p>Replace the CreateMessage bladelet with CreateContent and UpdateMessage bladelets to achieve the similar effect.</p> |
| CSCej57944 | <p>Symptom</p> <p>Message processing in a three-node scenario does not work correctly. Request and response paths do not traverse the same set of nodes.</p> <p>Workaround</p> <p>Three-node configurations are not supported in AON release 2.1. Use 2-node setup.</p> |
| CSCej61795 | <p>Symptom</p> <p>On rare occasions, a user will be unable to edit bladelet properties dialog windows in ADS. This problem has not been consistently reproducible.</p> <p>Workaround</p> <p>Restart ADS.</p> |
| CSCej69080 | <p>Symptom</p> <p>The show interfaces command on the AON-NM command-line interface does not show the MAC address of the Ethernet interface. This information is needed in order to configure promiscuous mode.</p> <p>Workaround</p> <p>To determine the MAC address of the internal data port on an AON-NM, you can enter the show arp command on the router command-line interface.</p> |
| CSCek10570 | <p>Symptom</p> <p>When logging object type of PEP variables, the string representation of the Object(toString) should be used and logged.</p> <p>Condition</p> <p>Using a PEP with Message Log configured to log content type PEP variable, AON logs the object as it is, which is not readable. Instead, it would be more useful to log the string representation of the object.</p> <p>Workaround</p> <p>None.</p> |

Table 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)

| Defect ID | Description |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek18587 | <p>Symptom Message delivered even when TTL expired.</p> <p>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.</p> <p>Workaround None.</p> |
| CSCek20178 | <p>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.</p> <p>Workaround Use batch size = 1.</p> |
| CSCek25145 | <p>Symptom Errors occur when a MQ client or endpoint uses the same correlation-ID for multiple messages.</p> <p>Workaround Configure the MQ client to use a unique correlation-ID for each message.</p> |
| CSCek25514 | <p>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.</p> <p>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.</p> |
| CSCek25614 | <p>Symptoms Coldstart trap is not generated when blade is reloaded; it is generated when SNMP is disabled and enabled.</p> <p>Workaround None</p> |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek25745 | <p>Symptom JVM reload unexpectedly on both client proxy and server proxy after more than 75 hours longevity run.</p> <p>Condition This occurs when client proxy and server proxy have complex PEPs with more than 15 bladelets involved with 10 to 40 concurrency of 100KB message size.</p> <p>Work-Around Reduce the aggregate message size (combination of message size plus concurrency) not to exceed 20MB. Here is the general guidelines of aggregate message size for all platform:</p> <ul style="list-style-type: none"> • AON SM—20MB • AON NM—5MB • AON Appliance—40MB |
| CSCek25788 | <p>Symptom MQ Adapter with SOAP message content is not being handled properly. MQ Adapter inbound queue message content supports only “Stream Content” and “XML Content.” Accessing the content as SOAPContent in the PEP causes errors.</p> <p>Workaround Convert message content to SOAPContent within a PEP. A sample PEP using Create Content Bladelet and Update Message Bladelet achieves this functionality.</p> |
| CSCek26871 | <p>Symptom AON does not recognize messages that use HTTP/1.1 pipelining.</p> <p>Workaround None. HTTP/1.1 pipelining is not supported in the AON environment.</p> |
| CSCek27572 | <p>Symptom Endpoint receives HTTP HEAD request with body but with content length header value of zero.</p> <p>Workaround None.</p> |
| CSCek28411 | <p>Symptom Signature Verification Fails after decrypting a signed encrypted message. The message was created using the same X509 certificate for both signing and encryption operations.</p> <p>Condition Created a PEP that has Signature Verification and Decryption bladelets on the response path. After the request path PEP was successfully executed, the endpoint server should have responded back with encrypted signed message. Signature verification fails on response path after decrypting an encrypted message from end server. When only Signature Verification is used without any Decryption bladelet, the verification works fine. This is observed with Weblogic 8.1.</p> <p>Workaround None.</p> |

Table 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)

| Defect ID | Description |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek28868 | <p>Symptom “Rollback Only” as a delivery failure policy in the JMS adapter configuration policy is no longer supported.</p> <p>Workaround None.</p> |
| CSCek28910 | <p>Symptom Graceful handling causes the following WARN level log message is generated: "...WARN...STOP_REQUEST_THRESHOLD hit...".</p> <p>This indicates that the available free heap memory is too low to allow new messages into AON. When the amount of free heap memory increases, the following and a WARN level log message is generated: "...WARN...START_REQUEST_THRESHOLD cleared...".</p> <p>Condition The problem was seen while doing a test involving two-node MQ-to-JMS messages. The two nodes were an AON-NM and AON-SM. Five clients were sending 600-KB messages, maintaining 15 messages in the system at any time. On the AON-NM, graceful handling caused request messages to be denied. Later the system garbage collection freed up heap memory and messages were admitted.</p> <p>Workaround The request and response thresholds that govern graceful handling can be enhanced by editing the values of some properties in the aonsFactoryDefaults.properties file. The properties are:</p> <ul style="list-style-type: none"> • aonsSystem.StopReqThreshold=0.3 • aonsSystem.StopRespThreshold=0.2 • aonsSystem.StopStartReqThresholdDiff=0.03 • aonsSystem.StopStartRespThresholdDiff=0.04 <p>Each of the above decimal values represents the percentage at which the given threshold is reached. These settings can be customized for the customer application to avoid graceful handling. These properties can also be set in the aons startup shell script to override the factory defaults.</p> |
| CSCek29537 | <p>Symptom Too many files open.</p> <p>Condition AON system receives very large messages (~60MB) over a long period of time.</p> <p>Workaround None.</p> |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek29556 | <p>Symptom Rows in the database for the CN_, SP_, and DY_ tables are not removed.</p> <p>Condition Occurred in a multi-node deployment requiring reliable/ordered delivery and using HTTP adapter on inbound and/or outbound.</p> <p>Workaround Manually drop old rows in these tables.</p> |
| CSCek29582 | <p>Symptom Unable to parse XML/SOAP documents. Manifestation of this problem appears in the form of security bladelet exception.</p> <p>Condition Under rare condition, contents of a HTTP body are corrupted. The root cause is unidentified.</p> <p>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.</p> |
| CSCek29630 | <p>Symptom AON fails to establish connection to Tibco EMS server.</p> <p>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. In this situation, AON occasionally fails to establish connection to Tibco EMS server.</p> <p>Workaround Restart AON System. In case of VC setup, restart all AON systems participating in the VC.</p> |
| CSCek29803 | <p>Symptom Messages are sometimes lost and do not appear in the dead letter queue or the destination queue.</p> <p>Condition This occurs when the inbound source batch size is greater than 1 in JMS adapter configuration.</p> <p>Workaround Change the batch size of the inbound source (including replyTo source) to 1.</p> |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek29828 | <p>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.</p> <p>Condition This happened when source and destination queues are defined on two different JMS brokers and they are statically linked via the JMS adapter configuration.</p> <p>Workaround Define the source and destination on the same brokers.</p> |
| CSCek29892 | <p>Symptom EMS broker running out of resources when EMS adapter is configured incorrectly.</p> <p>Condition EMS queue type is Send and EMS adapter is configured as Receive or vice- versa. In this misconfiguration, adapter continues to try to connect to the broker to register itself, causing resource issues on the broker side.</p> <p>Workaround Correct the EMS adapter configuration.</p> |
| CSCek30721 | <p>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:</p> <pre data-bbox="321 1087 1474 1167">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.</pre> <p>Workaround No Workaround. This problem does nor occur when caching HTTP messages.</p> |

Table 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)

| Defect ID | Description |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek30950 | <p>Symptom</p> <p>A MsgType exists in AMC without its associated PEP in AMC. A series of exceptions are thrown because of the nonexistent PEP in the AON MsgType.</p> <p>Condition</p> <p>This bug occurs in the following sequence of steps:</p> <ol style="list-style-type: none"> 1. Create a PEP F1 and MsgType M1 and associate this MsgType to F1. 2. Synchronize the PEP F1 and MsgType M1 to AMC. 3. Create another PEP F2 and associate MsgType M1 to this new PEP F2. 4. Now delete PEP F1 from ADS. 5. Synchronize the newly created PEP F2 and the deleted PEP F1; but do not delete the MsgType M1. 6. In AMC, F1 gets deleted and F2 gets created and the old record of MsgType M1 exists and still remains associated with the PEP F1 (which does not exist anymore). <p>Workaround</p> <p>Delete this MsgType on ADS and synchronize it to AMC, so that the MsgType also gets deleted on the AMC and deploy it. Then, AON is able to run successfully without any exception.</p> |
| CSCek31535 | <p>Symptom</p> <p>After invoking the amcd stop command to stop AMC, the command never seems to complete.</p> <p>Conditions</p> <ol style="list-style-type: none"> 1. Run the amcd stop command. 2. The terminal shows: <pre># ./amcd stop Stopping AMC Database...</pre> <p>(Script hangs here waiting for a prompt)</p> 3. The aondb.log file shows the message: <pre>There are still active connections. Stop anyway? (Y/N)</pre> <p>The amcd shell script that stops the AMC database fails to properly handle the active connections prompt.</p> <p>Workaround</p> <p>Entering “Y” or “N” at the terminal will answer the prompt and cause the amcd command to complete.</p> |

Table 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)

| Defect ID | Description |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek31626 | <p>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.</p> <p>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.</p> <p>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'.</p> |
| CSCek32197 | <p>Symptom WCCP does not work with GRE encapsulation on the AON appliance. Therefore, GRE WCCP bits are set to 0. AON (appliance form factor) cannot decipher how to handle these packets and the packets are returned to the router. This leads to a AON application layer not receiving any packets at all. Therefore, AON appliance is not usable with Catalyst switch when GRE forwarding is used (which is the preferred mode for appliance). This problem does not occur when Layer 2 forwarding is used for AON appliance.</p> <p>Workaround Change the encapsulation type to L2.</p> <p>Note Older images do not have this problem. s72033-ipservices_wan-mz.122-18.SXE1 works fine.</p> |
| CSCek32601 | <p>Symptom AON Appliance reloads unexpectedly when a user tries to validate a message of size 20MB</p> <p>Condition This situation occurs when the schema validation engine reaches its memory limit which then results in invalid memory page reference.</p> <p>Workaround None.</p> |
| CSCek32772 | <p>Symptom AON Appliance log timestamp is different from the system clock.</p> <p>Condition This happens after loading a new AON image. Due to the AON bootstrap, time is out of sync with the system time, certain scheduled AON tasks might not start according to scheduler, this could result with issues. In the worse case, under heavy load, it may cause system to be out of memory.</p> <p>Workaround Restart AON one more time from CLI.</p> |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek33285 | <p>Symptom: Client receives a 303 response instead of 200 OK.</p> <p>Conditions This happens when AON receives a 303 response from the endpoint and does not handle it as expected.</p> <p>Workaround None.</p> |
| CSCek34188 | <p>Symptom On a 2 node queue based adapters test, a memory leak was observed for reliable and ordered messages. Eventually this leak causes graceful handling too kick in and all new messages to be rejected.</p> <p>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.</p> <p>Workaround There is no workaround for the two-node case. Switching to a single node setup will eliminate the leak.</p> <p>Note This problem does not happen for HTTP cases or translation from HTTP to queue based adapters.</p> |

Table 5 Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)

| Defect ID | Description |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek34255 | <p>Symptom</p> <p>1. ama.log shows that the Mbean watchdog restarted AON.</p> <pre>2006-03-04 06:01:06,846 [Thread-38] ERROR ama.watchdog.MAgentWatchdog - Exception connecting to MBean Server. AONS must be dead. com.cisco.aons.ama.jmx.adaptor.http.HttpException: Connection refused at com.cisco.aons.ama.jmx.adaptor.http.HttpAdaptor.processAonsProxyRequest(HttpAdaptor.java:639) at com.cisco.aons.ama.watchdog.MAgentWatchdog.isAONSHealthy(MAgentWatchdog.java:741) at com.cisco.aons.ama.watchdog.MAgentWatchdog.access\$100(MAgentWatchdog.java:40) at com.cisco.aons.ama.watchdog.MAgentWatchdog\$HeartbeatRunnable.run(MAgentWatchdog.java:624) at EDU.oswego.cs.dl.util.concurrent.ClockDaemon\$RunLoop.run(Unknown Source) at java.lang.Thread.run(Unknown Source) 2006-03-04 06:01:06,852 [Thread-38] INFO ama.watchdog.MAgentWatchdog - Triggering recovering action RESTART_PROCESS</pre> <p>2. various java (JVM) core dumps appear upon logging into the command line interface on the AON module.</p> <p>3. show aon health and other commands that make calls to the Mbean server may be unresponsive or display the following:</p> <pre>aon-module> show aon health Request Timeout</pre> <p>Condition</p> <p>This occurred due to many events sent to the MBean server in a short period of time. For example, over 16 events per minute for many hours or days. Correcting the root cause of whatever is causing so many events to be sent to the Mbean is one way to prevent this watchdog case from occurring.</p> <p>Workaround</p> <p>None.</p> |
| CSCek35365 | <p>Symptom</p> <p>AON does not work when user tries to load schema with invalid path to imported or included schemas.</p> <p>Condition</p> <p>This occurs when the schema package contains schemas that has invalid path to imported or included schemas.</p> <p>Workaround</p> <p>Make sure all path to imported or included schemas are valid in the schema package.</p> |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek35399 | <p>Symptom AON network module shows as “Shutdown” when using the service-module AONS-Engine interface number status Cisco IOS command. However, when you session to the module, the AON CLI is still fully functional and the blade is not really shutdown.</p> <p>Condition This occurs when the service-module AONS-Engine interface number shutdown Cisco IOS command is used on the router hosting your AON network module.</p> <p>Workarounds Reload the AON network module and perform the following:</p> <ol style="list-style-type: none"> 1. On the network module, enter the AON shutdown command and wait for the system to halt. This puts the module into the state the router expects it to be in. 2. On the router, enter the Cisco IOS service-module AONS-Engine interface number reset command to reset the AON network module. <p>Note When the module and the router come back up, the status is correct.</p> |
| CSCek35429 | <p>Symptom Request message do not reach its destination in a queue-to-queue based message interaction.</p> <p>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.</p> <p>Workaround Configure the number of AON replyTo queues equal to or greater than twice the number of blades in the VC setup.</p> |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek36038 | <p>Symptom</p> <p>After upgrading AMC to a new Cisco-internal build of release 2.1, user attempted to perform a global deployment. The operation failed with the error: Node not active. In the amc.log file, the following messages were seen:</p> <pre>INFO [http7010-Processor23] AMC.Deploy.GlobalDeploymentRequestLogic Executing global deployment request, DR ID: (801) NOTICE [http7010-Processor23] AMC.Deploy.GlobalDeploymentRequestLogic Deploying global deployment request to all nodes using transactional, 2-phase deploy ... ERROR [http7010-Processor23] AMC.Deploy.GlobalDeploymentRequestLogic Exception while preparing nodes. Rolling back nodes. ERROR [http7010-Processor23] AMC.Deploy.GlobalDeploymentRequestLogic AMCEXception deploying global deployment request, DR ID: 801. Error message: node.not.activated INFO [http7010-Processor23] AMC.Deploy.GlobalDeploymentRequestLogic Value of Message Key: node.not.activated NOTICE [http7010-Processor23] AMC.Deploy.GlobalDeploymentRequestLogic Successfully changed deployment request state to 'Error' ERROR [http7010-Processor23] AMC.Deploy.DRACTION DRACTION: unable to deploy global DR</pre> <p>Condition</p> <p>This occurs when the AMC was managing a network of 29 nodes. All were initially in the Registered state. The global deployment was attempted. It failed (correctly) with the “Node not active” message because it is required that at least one node be in the Active state in order to perform a global deployment. User then activated one of the nodes, and re-tried the deployment. It still failed with the same error.</p> <p>Workaround</p> <p>Activate THE FIRST NODE IN THE LIST on the “Activate/Deactivate Network Nodes” page. There is apparently an unexpected dependency within the AMC code on the position within the list.</p> |
| CSCek36267 | <p>Symptom</p> <p>AON module was not able to boot up due to “No space left on device” error.</p> <p>Condition</p> <p>When Caching bladelets are in the PEP and lot of messages are going through the PEP.</p> <p>Workaround</p> <p>None.</p> |

Table 5 *Open Caveats for Cisco Application-Oriented Networking Version 2.1 (Continued)*

| Defect ID | Description |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek37187 | <p>Symptom</p> <p>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.</p> <p>Condition</p> <p>This situation occurs only when an image upgrade is done.</p> <p>Workaround</p> <p>Reconfigure the desired log level after each upgrade.</p> |
| CSCin98529 | <p>Symptom</p> <p>SCAR file packaging causes error when the NativeVersion for the lib file (.so file) is not given. This has occurred on only one Windows XP PC and cannot be reproduced elsewhere.</p> <p>Condition</p> <p>This occurred when the nativeVersion is present in the bladelet-info.xml file, the SCAR file packaging looks for the lib file (.so file) with the appropriate version number and the packaging proceeds. When the nativeVersion is not given, an error occurs, and the SCAR file is not packaged.</p> <p>Workaround</p> <p>Try another Windows PC, or try using the nativeVersion tag in bladelet-info.xml.</p> |

Upgrade Instructions

For detailed instructions on upgrading to Cisco Application-Oriented Networking Version 2.1, see the following document:

[Upgrading the Cisco Application-Oriented Networking Environment](#)

Downgrade Instructions

For detailed instructions on downgrading Cisco Application-Oriented Networking Version 2.1 to Version 1.1, see the following document:

[Downgrading Cisco Application-Oriented Networking Version 2.1 to Version 1.1](#)

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_inpk/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>

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply partnership relationship between Cisco and any other company. (0609R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.