Cisco AON Installation and Upgrade Guide

AON Release 2.4
March 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

AON Installation and Upgrade Guide

CONTENTS

Preface

Cisco Application-Oriented Network (AON) is a technology foundation for a class of Cisco products that embed intelligence into the network for the support of distributed application deployment. AON complements existing networking technologies by allowing increased visibility of the information passing through the network. This facilitates efforts to accomplish the following:

- Integration of disparate applications by enabling the routing of customer-specified information and message types to the appropriate destination, in the format(s) needed.
- Enforcement of security policies for information access and exchange.
- Optimization of application traffic flows, both in terms of network bandwidth and processing overheads.
- Better management of information flow, including monitoring and metering of information flow for both business and infrastructure purposes.

AON works primarily at the message-level rather than at the packet level, allowing developers and system administrators to work with the content and context of information flow. Typically, an AON node occupies the terminus of a TCP connection so that it can inspect and work with the entire message, including the "payload" and all headers. AON can work with popular application-level protocols such as HTTP, JMS, and other de facto standards.

AON Devices and Components

An application-oriented network consists of the following devices and components:

- Management Tools
- Nodes
- Other Entities

Management Tools

AON Management Console (AMC)

AMC is the software package that centralizes management of the application-oriented network. This includes:

- Configuring, managing, and monitoring AON nodes
- Deploying global and node-level properties

- Managing security, including certificates, keypairs, and users

AON Development Studio (ADS)

ADS is the tool for developers to create message-level logic using a graphical user interface (GUI). ADS provides a set of preconfigured functions, called Bladelets, that are used to construct Policy Execution Plans (PEP). Additionally, ADS includes functionality that enables developers to upload custom Bladelets to perform business functions unique to different environments.

Nodes

AON Services Modules on Catalyst 6500 Series Switches

This is the AON form factor available as a single-slot services module for the Catalyst 6500 Series Switches. Typically this node is used in a data center.

AON Network Modules on Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 Series Routers

This is the AON form factor available as a single-slot network module for several different Cisco modular access routers. Typically this type of node is used in a branch office. See *Release Notes for Cisco Application-Oriented Networking* for a detailed list of supported router platforms.

Other Entities

Depending on the configuration of your network and the needs of your business, your application-oriented network may include any of the following:

Database

When a database policy is configured, AON can store specified data in a Sybase or Oracle database.

LDAP server

Can be used to perform user authentication for both the AMC application and on individual messages traversing the application-oriented network.

Java Messaging Service (JMS)

AON devices can be configured to exchange messages between clients and JMS queues.

AON Features

Explicit and Transparent Interception

An AON node resides in the network as an inline application-aware device. The device acts as an intelligent intermediary gateway that can either be explicitly addressed by applications or as a passthrough proxy that is transparent to applications.

Access Methods and Adapters

AON understands various application access methods and provides adapters that can natively interface with commonly used protocols. The key protocols that AON supports include:

- HTTP v1.0/ v1.1 and HTTPS

- JMS
- MQ (through native adapter)

The AON software development kit (SDK) enables development of adapters for custom protocols.

Protocol Translation

AON nodes can act as protocol gateways between multiple applications that use differing protocols—as an example, a node can receive an application message through JMS and send the message information to another application as an HTTP post.

Transformation

AON supports both XML and non-XML transformation through an open transformation architecture. AON can function as an XSLT based transformation engine. You can add your own Java transformation engine to execute custom transformations.

Security

AON provides a series of intelligent services which enable message-level access and control to meet application security needs within the network. These security services include authentication, authorization, nonrepudiation, data integrity, data confidentiality, and centralized key management.

Service Virtualization

AON can act as proxy to create an abstraction layer for endpoint applications and apply policies across all of these services—in a centralized configuration, with distributed enforcement in the network. Service virtualization functionality supports execution of content-based routing, workload balancing, and message distribution operations.

Schema Validation

AON provides the ability to validate XML documents against schemas you create.

Optimization Services

AON has the capability to cache or compress messages to allow for optimization of message traffic, thus enabling reduced application response time and the conservation of network bandwidth.

External Data Access

AON enables access to or notification of other applications in parallel to the handling of the main message flow. External access is currently available using HTTP and Java Database Connectivity (JDBC).

Message Logging

AON can capture application messages for logging either synchronously, for auditing purposes, or asynchronously.

AON Installation Summary

This section summarizes installation procedures:

1. Install all switches, routers, and related AON modules and ensure they are configured for basic IP networking. Refer to documentation related to your switch or router for detailed configuration instructions.

2. Establish a relationship with a well-known certificate authority and generate a Java keystore. See the "Generating a Java Keystore" section on page 1.
3. Install AMC on a Linux server. See the "Installing and Upgrading AMC" section on page 4.
4. Configure AON nodes to register with AMC. See the "Performing Initial Node Configurations" section on page 9.

Install the AON Development Studio (ADS) on a Windows PC. See the *AON Development Studio User Guide* for detailed installation instructions.

This installation guide focuses on the AON-specific tasks for implementing an application-oriented network and includes the following chapters:

- Chapter 1, "Configuring AON Devices"

  This chapter describes the procedures you need to perform when you first install and AON system, including AMC installation, setting up a node, and performing initial node configuration. It also includes procedures to verify that the AMC and the AON devices are functioning properly.

- Chapter 2, "Upgrading AON Software"

  This chapter describes procedures for upgrading AON software on existing hardware.

Related Documentation

The AON documentation set includes the following guides:

- *Release Notes for Cisco Application-Oriented Networking*
- *AON Administration Guide*—Covers the 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

CHAPTER 1

Configuring AON Devices

This chapter includes the following sections:

- Getting Started with AMC, page 1-1
- Performing Initial Node Configurations, page 1-9

Getting Started with AMC

This section describes how to install the AON Management Console (AMC). It includes the following sections:

- Generating a Java Keystore, page 1-1 (required)
- Installing and Upgrading AMC, page 1-4 (required)
- Performing an Unattended Installation or Upgrade of AMC, page 1-6 (optional)
- Stopping, Starting, and Restarting AMC, page 1-9 (optional)

Generating a Java Keystore

Before installing or upgrading AMC, you must obtain a certificate. This certificate must be in the form of a Java Keystore (.jks) file and be compatible with JDK 1.4.2 or later releases. Additionally, AMC accepts only the well-known certificate authorities included in the Java Runtime Environment (JRE) 1.4 truststore.

Note AMC accepts class 1, class 2, and class 3 certificates. For production environments, we recommend that you use only a class 3 certificate.

Prerequisite

- Install the Java Runtime Environment and add the **/bin** directory to your path.

Step 1 To generate the key type the following on the command line of a Linux workstation:

```
[root@linux opt]# keytool -genkey -alias <name> -keyalg <algorithm> -keysize <size>
-validity <days> -keystore <filename> -storepass <password>
```

This command requires you to provide the following variables:

- *name* = Select an alias name for your keystore.
- *algorithm* = Specify either RSA or DSA. We recommend that you use RSA.
- *size* = Specify the size of the key in bits. This value must be a multiple of 64 between 512 and 1024.
- *days* = Specify the number of days your key will be valid.
- *filename* = Specify the location and filename where you want your keystore file to be generated.
- *password* = Specify he password used to protect your keystore file.

The following is a sample entry using the above variables:

```
[root@linux]# keytool -genkey -alias test -keyalg rsa -keysize 512 -validity 365
-keystore teststore -storepass password
```

Step 2 After pressing RETURN, you are prompted for information related to your organization and location. Enter the appropriate data. The values that follow are for illustrative purposes only:

Note When prompted for your first and last name, enter the hostname for the server on which AMC is to be installed.

```
What is your first and last name?
  [Unknown]:  aon.hostname.com
What is the name of your organizational unit?
  [Unknown]:  Application-Oriented Networking
What is the name of your organization?
  [Unknown]:  Cisco Systems
What is the name of your City or Locality?
  [Unknown]:  San Jose
What is the name of your State or Province?
  [Unknown]:  California
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San Jose,
ST=CA, C=US correct?
  [no]:  yes
Enter key password for <test>
        (RETURN if same as keystore password):
```

Step 3 Enter the following command to view the details of your keypair.

```
[root@linux opt]# ./keytool -list -v -keystore teststore  -storepass password
Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: test
Creation date: April 20, 2005
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San
Jose, ST=California, C=US
Issuer: CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San
Jose, ST=California, C=US
Serial number: 42768483
Valid from: Mon May 02 12:50:27 PDT 2005 until: Tue May 02 12:50:27 PDT 2006
Certificate fingerprints:
         MD5:  8E:C8:62:5F:30:3F:DE:47:80:75:9A:84:6D:B6:0E:EF
```

```
SHA1: 28:0E:76:86:13:EC:B0:8D:B0:1E:73:A4:7D:87:D0:0F:55:81:E5:63
```

Note At this point, you do not have a keystore file with your keypair. Your keypair contains a self-signed certificate, which cannot be used with AMC until it is registered with a certificate authority.

Step 4 Generate a certificate signing request (CSR) for your keypair by entering the following command:

```
[root@linux]# keytool -certreq -v -alias <alias_name> -file <outputfile> -keystore
<keystore> -storepass <storepassword>
```

This command requires you to provide the following variables:

- <*alias_name*> = The alias you created in Step 1.
- <*file*> = The name of the file where the CSR is to be stored.
- <*keystore*> = The name of the keystore file you created in Step 1.
- <*storepassword*> = The password for the keystore file.

```
[root@linux]# keytool -certreq -v -alias test -file testcert -keystore teststore
-storepass password
Certification request stored in file <testcert>
Submit this to your CA
```

Step 5 Submit the CSR file (*testcert* in the above example) to your certificate authority. On successful submission, the CA will provide you with a .cer file that contains your production certificate.

Step 6 Import the .cer file from your CA into the keystore created in Step 1.

```
[root@linux]# keytool -import -v -alias <alias> -file <cer_file> -keystore <keystore_file>
-storepass <keystore_password>
```

This command requires you to provide the following variables:

- <*alias*> = Alias created in Step 1.
- <*cer_file*> = Path to the .cer file you received from CA.
- <*keystore_file*> = keystore file created in Step 1.
- <*keystore_password*> = The keystore password.

After you enter this command, information similar to the following is displayed:

```
Owner: CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San
Jose, ST=California, C=US
Issuer: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
Serial number: 3a7a57a56046cce564ce7cc500995b21
Valid from: Sun Feb 06 16:00:00 PST 2005 until: Tue Feb 07 15:59:59 PST 2006
Certificate fingerprints:
MD5:  8E:C8:62:5F:30:3F:DE:47:80:75:9A:84:6D:B6:0E:EF
SHA1: 28:0E:76:86:13:EC:B0:8D:B0:1E:73:A4:7D:87:D0:0F:55:81:E5:63
Trust this certificate? [no]: yes
Certificate was added to keystore
[Saving ./CreateKeystore/teststore.jks]
```

Note Note the name and location of the .jks file. You will need it each time you install or upgrade AMC.

Installing and Upgrading AMC

Cisco distributes the AMC application in two formats, a package that installs a fresh copy of AMC, and a package that upgrades an AMC but preserves the existing database of nodes, properties, logs, and other settings. The instructions that follow assume installation in the **/opt/amc** directory. However, you can install AMC in any directory of your choosing.

Requirements

- You must install AMC on a local disk. AMC cannot run on a network file system.
- You must obtain a certificate from a certificate authority before installing or upgrading AMC. The keystore information must be in the Java Keystore format with a **.jks** extension. See the "Generating a Java Keystore" section on page 1-1 for instructions. AMC accepts only the well-known certificate authorities included in the Java Runtime Environment (JRE) 1.4 truststore.
- It is possible to install multiple instances of AMC on a single server if each AMC uses a unique set of TCP ports. We recommend that this be done only in testing or training environments. A given node cannot be managed by more than one AMC, and we recommend that a production AON environment include no more than one AMC.
- If you are upgrading AMC, be sure to deactivate any active nodes.

Caution If you are upgrading AMC, be sure to read the latest AON Release Note before running the upgrade package. The new release note may contain critical upgrade procedures beyond those described below. Failure to follow the procedure described in the release note may result in data loss or corruption.

Step 1 Download the installation file and use the **chmod** command to make it executable.

```
[root@linux opt]# chmod +x aon-amc_<version>_lnx.bin
```

Step 2 Execute the installer.

```
[root@linux opt]# ./aon-amc_<version>_lnx.bin
Preparing to install...
```

Step 3 Enter the directory in which AMC is to be installed. The **/opt/amc** directory is the default, although any directory is acceptable.

```
Enter the directory to install the AMC to [/opt/amc]:
Directory "/opt/amc" does not exist - create? [y|n]:y
Extracting archive.
Configuring paths.
Configuring the ports that the AMC will listen on
If you are installing more than one AMC, these values
must be unique to each installation.
```

Step 4 Enter the port on which AMC will listen for HTTPS requests. 7010 is the default.

```
Enter a port for https [7010]:7010
```

Step 5 Enter the port on which AMC will listen for traffic from nodes. 7011 is the default.

```
Enter a port for communication with AON nodes [7011]:7011
```

Step 6 Enter the port on which AMC will listen for shutdown signals. 7025 is the default.

```
Enter a port for server shutdown signals [7025]:7025
```

Step 7 Enter the port on which AMC will listen for database transactions. 2638 is the default.

```
Enter a port for the database [2638]:2638
```

Step 8 Enter the logging level to be used while AMC runs.

```
Enter AMC logging level (TRACE|DEBUG|INFO|WARN|ERROR|FATAL) [INFO]:error
```

AMC can use one of the following logging levels:

- TRACE
- DEBUG
- INFO
- NOTICE
- WARN
- ERROR
- FATAL

Note In production environments, we recommend that only ERROR or FATAL log levels be used. More verbose log levels can have an adverse affect on the performance of AMC.

Step 9 Enter the size of the log file in kilobytes. When the log size is exceeded, AMC saves it as a backup and generates a new log file.

```
Enter log file rollover threshold size (KB) [1024]:1024
```

Step 10 Enter the number of backup logs to keep. When the number of backup logs is exceeded, AMC discards the oldest file.

```
Enter number of backup logs to keep [5]:5
```

Step 11 AMC uses a keystore file for communication with AON nodes. Enter the path and filename for this keystore.

```
The AMC requires a keystore file and password
to communicate with the AON node.
Enter the path to the keystore file:/root/amcKeystore.test.cisco.com.jks
```

Note The path to amcKeystore shown above is for illustrative purposes. You must provide the path to an actual Java keystore in order to complete the installation.

Step 12 If the keystore file has multiple keypairs, enter the name for the pair you want to use.

```
You may optionally enter a keyname within the keystore.
Enter a keyname, otherwise enter none [none]:none
```

Step 13 Enter the password associated with the keystore.

```
Enter a password for this keystore:
about to load the root certs
Loading /opt/test080107/admin/security/keystores/ciscocerts/cap-rtp-003.cer
Loading /opt/test080107/admin/security/keystores/ciscocerts/cisco-root.cer
Loading /opt/test080107/admin/security/keystores/ciscocerts/cisco-manu-ca.cer
Loading /opt/test080107/admin/security/keystores/ciscocerts/cisco-manu-ca-dev.cer
Loading /opt/test080107/admin/security/keystores/ciscocerts/cisco-test-ca-2048.cer
Using existing ciscoamc group
Using existing ciscoamc user
Setting permissions for AMC installation...
Configuring AMC service to start at boot...
```

Step 14 Enter **y** to start AMC now or **n** to start it later.

```
Would you like to run the AMC now? [y|n]:y
Starting AMC Database...Done.
Starting AMC...Done.
AMC logfile is /opt/amc/log/amc.log
Installation successful.
To uninstall, run '/opt/amc/bin/amcSetup uninstall'.
```

Step 15 Use a Web browser to navigate to the AMC log-in page to confirm that the installation was successful. The URL is **https://*hostname*:7010/amc**. Replace *hostname* in this URL with the name or IP address for the server running AMC. The default user name and password are **aonsadmin**.

Note For best results, we recommend you use Microsoft Internet Explorer 6 with AMC.

Performing an Unattended Installation or Upgrade of AMC

AMC version 2.4 includes the ability to install the application in a non-interactive fashion. By providing a text file that contains the answers to the questions asked during the installation or upgrade of AMC, you can configure the installer to perform the operation without prompting you for additional details.

Answer File

The text file used to perform an unattended installation or upgrade is called an answer file. It has the following requirements:

- The answer file must contain all of the configuration parameters and in the order listed below.
- Individual parameters must be enclosed in single quotes in order to be correctly interpreted by the shell.
- There must be no spaces on either side of the equal sign.

A sample answer file is shown in Example 1-1.

Example 1-1 Sample Answer File

```
INSTALL_DIR='/opt/amc'
CREATE_INSTALL_DIR='y'
OVERWRITE_AMC='y'
CONFIRM_BKUP='y'
BKUP_DIR='/tmp'
HTTPS_PORT='7010'
HTTPS_INT_PORT='7011'
SHUTDOWN_PORT='7025'
DB_PORT='2638'
AMC_LOG_LEVEL='INFO'
AMC_LOG_MAXFILESIZE='1024'
AMC_LOG_MAXBACKUPS='5'
KEYSTORE_PATH='/opt/amcKeystore.10.4.1.200.jks'
KEYSTORE_KEYNAME='none'
KEYSTORE_PASSWD='password'
```

```
PROJ_PRE='abc'
PROJ_NAME='USER_PROJ'
RESTORE_BKUP='y'
START_AMC='y'
```

Table 1-1 shows the parameters configured by the answer file.

Table 1-1 Answer File Parameters

Parameter	Description	Value
INSTALL_DIR	Path to be used for installation or upgrade	Valid path on the server's local file system
CREATE_INSTALL_DIR	Specifies whether to create the installation directory if it does not already exist	• **n**—causes installation to fail if directory does not exist • **y**—causes the directory to be created
OVERWRITE_AMC	Specifies whether any files found in the existing directory should be overwritten	• **n**—causes installation to fail if files exist in the directory • **y**—causes files to be deleted
CONFIRM_BKUP	Specifies whether to back up the existing installation directory	• **n**—causes installation to fail if directory does not exist • **y**—causes the directory to be created
BKUP_DIR	Location where backup file is to be written	Valid path on the server's file system
HTTPS_PORT	TCP port to be used for web access to AMC	Any unused TCP port
HTTPS_INT_PORT	TCP port to be used for communication between nodes and AMC	Any unused TCP port
SHUTDOWN_PORT	TCP port to be used by AMC shutdown	Any unused TCP port
DB_PORT	TCP port to be used by the AMC database	Any unused TCP port
AMC_LOG_LEVEL	Message severity threshold for the AMC log	One of the following values: • DEBUG • INFO • NOTICE • WARN • ERROR • FATAL
AMC_LOG_MAXFILESIZE	Maximum size of AMC log file in kilobytes	Any integer
AMC_LOG_MAXBACKUPS	Maximum number of backup logs to be kept	Any integer
KEYSTORE_PATH	Location of the keystore used to configure the certificate for node-AMC communication	Valid path on the server's file system
KEYSTORE_KEYNAME	Optional key name within the keystore	Specify the key name or use **none** if there is no key name
KEYSTORE_PASSWD	Keystore password	Keystore password
PROJ_PRE	Specifies the project prefix.	Must begin with an alphanumeric character. Can include letters, numbers, hyphens, and underscores. Not to exceed 50 characters.

Table 1-1 Answer File Parameters (continued)

Parameter	Description	Value
PROJ_NAME	Specifies the project name.	Must begin with an alphanumeric character. Can include letters, numbers, hyphens, and underscores. Not to exceed 256 characters.
RESTORE_BKUP	Specifies whether to restore from backup should the upgrade fail	• **n**—AMC installer terminates after failed upgrade • **y**—AMC installer restores from backup file after
START_AMC	Specifies whether to launch AMC after the installation completes	• **n**—AMC installer terminates after installation is complete • **y**—AMC installer launches AMC after installation completes

Launching an Unattended Installation or Upgrade

Unattended installations and upgrades are performed with same software packages you use to perform a standard installation or upgrade. This accomplished by including the path to the answer file when you execute the installation or upgrade package.

Example 1-2 shows sample output from an unattended installation.

Example 1-2 Sample Unattended Installation of AMC

```
[root@cisco root]# ./aon-amc_version_k9_lnx.bin /root/MyAnswerFile
Preparing to install...
Installation directory read from answer file: /opt/amc
Directory "/opt/amc" does not exist, and is being created.
Extracting archive.
Configuring paths.
Configuration read from answer file: /root/MyAnswerFile
INSTALL_DIR          = /opt/amc
CREATE_INSTALL_DIR   = y
OVERWRITE_AMC        = y
CONFIRM_BKUP         = n
HTTPS_PORT           = 7010
HTTPS_INT_PORT       = 7011
SHUTDOWN_PORT        = 7025
DB_PORT              = 2638
AMC_LOG_LEVEL        = INFO
AMC_LOG_MAXFILESIZE  = 1024
AMC_LOG_MAXBACKUPS   = 5
KEYSTORE_PATH        = /amcKeystore.cisco.com.jks
KEYSTORE_KEYNAME     = none
KEYSTORE_PASSWD      = <hidden>
PROJ_PRE             = abc
PROJ_NAME            = USER_PROJ
RESTORE_BKUP         = n
START_AMC            = y

The AMC requires a keystore file and password
to communicate with the AONS node.
about to load the root certs
Loading /opt/testamc/admin/security/keystores/ciscocerts/cap-rtp-003.cer
Loading /opt/testamc/admin/security/keystores/ciscocerts/cisco-root.cer
Loading /opt/testamc/admin/security/keystores/ciscocerts/cisco-manu-ca.cer
Loading /opt/testamc/admin/security/keystores/ciscocerts/cisco-manu-ca-dev.cer
Loading /opt/testamc/admin/security/keystores/ciscocerts/cisco-test-ca-2048.cer
Using existing ciscoamc group
Using existing ciscoamc user
Setting permissions for AMC installation...
Configuring AMC service to start at boot...
Finalizing installation...
Done.
AMC is being started
Starting AMC Database...Done.
Starting AMC...Done.
AMC logfile is /opt/testamc/log/amc.log
Installation successful.
To uninstall, run '/opt/testamc/bin/amcSetup uninstall'.
```

Stopping, Starting, and Restarting AMC

During the installation process, the AMC daemon (amcd) is configured to run when the server on which it is installed starts up, and it stops when the server is shut down. You might, however, have need to stop, start or restart the AMC daemon independently of the server. The examples that follow show how to do this.

Example 1-3 Shutting Down AMC

```
[root@linux]# /opt/amc/bin/amcd stop
Stopping AMC...waiting for services to complete...Done.
Stopping AMC Database...Done.
```

Example 1-4 Starting AMC

```
[root@linux]# /opt/amc/bin/amcd start
Starting AMC Database...Done.
Starting AMC...Done.
```

Example 1-5 Restarting AMC

```
[root@linux]# /opt/amc/bin/amcd restart
Stopping AMC...waiting for services to complete...Done.
Stopping AMC Database...Done.
Starting AMC Database...Done.
Starting AMC...Done.
```

Performing Initial Node Configurations

AON nodes have no direct console access, so the first configuration task for an AON service module (AON-SM), an AON enhanced service module (AON-NME), or an AON network module (AON-NM) is to define IP address and subnet masks for the AON interface. See the following sections for configuration tasks for AON nodes. Each task in the list is identified as either required or optional.

- Configuration Prerequisites, page 1-10 (required)
- Configuring a Cisco 8300 Series AON Appliance, page 1-10 (required)
- Configuring Networking Parameters on a Catalyst 6500 Series Switch, page 1-12 (required)

- Configuring Network Parameters on a Cisco Modular Access Router, page 1-15 (required)
- Configuring Nodes to Use SSH, page 1-16 (optional)
- Configuring Nodes to Register with the AMC, page 1-17 (required)

Caution AON network modules do not support online insertion and removal. Always power off the router before inserting or removing a module. You need not take this precaution before removing an AON-SM from a switch.

Configuration Prerequisites

This guide assumes that your switch, router, or AON appliance is properly installed. Additionally, switches and routers that will house AON nodes must be configured for basic IP communications and have their AON modules installed. See the following platform documentation if necessary:

- Cisco 8300 Series AON Appliance Hardware Installation Guide

  http://lbj.cisco.com/targets/ucdit/cc/td/doc/product/aon/aonmod/8300/8300hig/index.htm
- Catalyst 6500 Series Switch Installation Guide

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/inst_aug/index.htm
- Catalyst 6500 Series Switch Module Installation Guide

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/mod_inst/index.htm
- Cisco Modular Access Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/index.htm
- Cisco Network Modules Hardware Installation Guide
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/index.htm

Configuring a Cisco 8300 Series AON Appliance

A Cisco 8300 AON Appliance arrives from the factory with AON software preinstalled. In order to configure an appliance, you must connect a terminal server to the serial port on the rear of the appliance. For instructions on connecting a terminal server, see the *Cisco 8300 Series AON Appliance Hardware Installation Guide*. This section includes the following topics:

- Configuring Networking Parameters, page 1-10
- Disabling Cisco Discovery Protocol, page 1-12

Configuring Networking Parameters

Perform the following steps to configure networking parameters:

Step 1 With your terminal server connected, power on the appliance and allow it to boot. When the appliance is ready for configuration, a **Password :** prompt is displayed. Enter the default password of **aonsadmin**.

```
                   Welcome to Cisco AON Engine
                       (Version: 1.1.0.189)
```

```
Fri Nov  4 03:24:41 PST 2005
AON boot: hit RETURN to set boot flags: 0002

Available boot flags (enter the sum of the desired flags):
  0x0000 - exit this menu and continue booting normally
  0x2000 - disable login security

[AON boot - enter bootflags (type '-' to exit)]: 0x0000
You have entered boot flags = 0x0
Boot with these flags? [yes]: y
Boot with these flags? [yes]: yes

********** rc.aesop ****************
Setting timezone: No timezone configured
Loading Tarari Drivers...
SUCCESS: Loaded Tarari Drivers
Loading Cisco WCCP module
wccp: v1.00 (20000327), debug=0
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
Serial Number: 99C7523
Reading Manifest...done.
Doing Certificate Check
Certificate Check Done
INIT: Entering runlevel: 2
********** rc.post_install ****************
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal

 waiting 51 ...
Password :
```

Step 2 Enter configuration terminal mode.

```
defaulthost> configure terminal
Enter configuration commands, one per line.  End with exit.
```

Step 3 Enter interface configuration mode for Gigabit Ethernet Interface 1

```
defaulthost(config)> interface gigabitethernet 1
```

Note The appliance includes three gigabit ethernet connectors, however, only Gigabit Ethernet 1 is supported in AON version 1.1.

Step 4 Enter the IP address and subnet mask to be used by the appliance, then exit interface configuration mode.

```
defaulthost(config-interface)> ip address 192.168.56.106 255.255.255.0
WARNING!!! Changing interface IP address will disrupt connectivity and traffic!
defaulthost(config-interface)> exit
SYSTEM ONLINE
```

Step 5 Configure the default gateway to be used by the appliance. A default gateway is required even if all AON devices are on the same LAN segment.

```
defaulthost(config)> ip default-gateway 192.168.56.1
```

Step 6 Configure the domain name to be used by the appliance.

```
defaulthost(config)> ip domain-name cisco.com
```

Step 7 Configure the domain name servers to be used by the appliance.

```
defaulthost(config)> ip name-server 192.168.168.183 192.168.226.120
```

Step 8 Configure the NTP server to be used by the appliance.

```
defaulthost(config)> ntp server 192.168.156.11
```

Step 9 Configure the hostname to be used by the appliance.

```
defaulthost(config)> hostname aon-appliance
```

Step 10 Enable secure shell (SSH) access for the appliance.

```
aon-appliance(config)> ssh enable
```

Step 11 Change the default password.

```
aon-appliance(config)> login password unencrypted mypassword
```

Note For a detailed description of SSH and login passwords, see the "Configuring Nodes to Use SSH" section on page 1-16.

Step 12 Exit configuration mode, and save the new configuration.

```
aon-appliance(config)> exit
aon-appliance> write memory
```

Disabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP is enabled by default, and the appliance sends CDP Version-1 (CDPv1) advertisements. It receives both CDPv1 and CDPv2 advertisements. Example 1-6 shows CDP being disabled.

If you do not need CDP, you should disable it.

Note Only the Cisco 8300 Series AON Appliance supports CDP at this time.

Example 1-6 Disabling CDP

```
aon-appliance> configure terminal
Enter configuration commands, one per line.  End with exit.
aon-appliance(config)> no cdp run
aon-appliance(config)> exit
aon-appliance> write memory
```

Note You can use **cdp run** to enable CDP again if necessary.

Configuring Networking Parameters on a Catalyst 6500 Series Switch

You must configure a VLAN for the AON-SM, then assign an IP address to it. These tasks are covered in the following sections:

- Configuring a VLAN under the Catalyst Operating System, page 1-13 (required for Catalyst operating system)

- Configuring a VLAN under Cisco IOS, page 1-13 (required for Cisco IOS)
- Assigning IP Addresses to the AON-SM Interface, page 1-14 (required)

Configuring a VLAN under the Catalyst Operating System

You must configure a VLAN for the AON-SM by completing the following steps:

Step 1 Create a VLAN to be used by the AON node.

```
Router> (enable) set vlan 100
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 100 configuration successful
```

Step 2 Assign the VLAN to the AON node.

```
Router> (enable) set vlan 100 5/2
VLAN 100 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- -----------------------
100   5/2

Vlan 100 is active.
Router> (enable)
```

Configuring a VLAN under Cisco IOS

You must configure a VLAN for the AON-SM by completing the following steps:

Step 1 Enter configuration terminal mode.

```
MSFC# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 2 Create a VLAN to be used by the AON node.

```
MSFC(config)# vlan 100
```

Step 3 Make the VLAN active, then exit configuration terminal mode.

```
MSFC(config-vlan)#state active
MSFC(config)# exit
```

Step 4 Assign the VLAN to the AON-SM.

```
MSFC(config)# AON module 6 vlan 100
```

Step 5 Enter interface configuration mode for the VLAN.

```
MSFC(config)# interface vlan 100
```

Step 6 Assign an IP address and subnet mask to the VLAN.

```
MSFC(config-if)# ip address 192.168.22.36 255.255.255.0
```

Assigning IP Addresses to the AON-SM Interface

To assign IP addresses to the AON service module running in a Catalyst 6500 series switch, perform the following steps:

Note During start up, the AON-SM retrieves the system time from the switch. Ensure that NTP is configured on the switch before you configure the AON-SM.

Step 1 If this is an active node for which you are assigning a new IP address, use AMC to deactivate it.

Step 2 Open a session to the AON-SM, then enter configuration terminal mode.

```
Router# session slot number processor number
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open


               Welcome To Cisco AON Engine


aon-node> enable
aon-node# configure terminal
```

Step 3 Select an interface to configure.

```
aon-node(config)# interface GigabitEthernet 2
```

Note At this time, AON supports only the GigabitEthernet 2 interface.

Step 4 Specify the IP address for the interface, then exit interface configuration mode.

```
aon-node(config-interface)#ip address 192.168.3.11 255.255.255.0
aon-node(config-interface)#end
```

Step 5 Specify the IP address for the default gateway, then exit configuration terminal mode. A default gateway is required even if all AON devices are on the same LAN segment.

```
aon-node(config)#ip default-gateway 192.168.3.1
aon-node(config)#end
```

Step 6 Save the configuration in NVRAM.

```
aon-node# write memory
```

Step 7 Proceed to the "Configuring Nodes to Register with the AMC" section on page 1-17 to continue configuring the AON-SM.

Configuring Network Parameters on a Cisco Modular Access Router

To assign IP addresses to the AON network module running in a router, perform the following steps:

Note During start up, the AON-NM retrieves the system time from the router. Ensure that NTP is configured on the router before you configure the AON-NM.

Step 1 If this is an active node for which you are assigning a new IP address, use AMC to deactivate it.

Step 2 Establish a session to the router and enter configuration mode for the AON network module interface.

For AON-NME:

```
Router(config)# interface integrated-service-engine 1/0
```

For AON-NM:

```
Router(config)# interface AON-engine 1/0
```

Note If your router is running a version of Cisco IOS prior to Cisco IOS Release 12.4(9)T, the AON-NM interface is referred to as **AONS-Engine**.

Step 3 Specify that FastEthernet 0/0 interface is unnumbered.

```
Router(config-if)# ip unnumbered FastEthernet 0/0
```

Step 4 Configure an IP address for the interface used by the AON network module.

```
Router(config-if)# service-module ip address 10.4.1.184 255.255.255.0
```

Step 5 Specify the default gateway used by the AON network module. A default gateway is required even if all AON devices are on the same LAN segment.

```
Router(config-if)# service-module ip default-gateway 10.4.1.183
```

Step 6 Bring up the AON network module interface.

```
Router(config-if)# no shutdown
```

Step 7 Exit configuration mode.

```
Router(config-if)# exit
```

Step 8 Configure IP routing on the router.

```
Router(config)# ip routing
```

Step 9 Define a static IP route to the AON network module.

For AON-NME:

```
Router(config)# ip route 10.4.1.184 255.255.255.255 integrated-service-engine 1/0
```

For AON-NM:

```
Router(config)# ip route 10.4.1.184 255.255.255.255 AON-engine 1/0
```

Step 10 Define a static IP route to the default gateway.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 10.4.1.1
```

Step 11 Exit configuration mode.

```
Router(config)# exit
```

Step 12 Save the configuration in NVRAM.

```
Router# write memory
```

Configuring Nodes to Use SSH

Using the default configuration, you connect to a node’s command-line interface using telnet or a serial interface. AON nodes running release 1.1 and later versions can be configured to use secure shell (SSH). When SSH is used, all traffic between the node and your SSH client is encrypted. Additionally, SSH enables users to configure a node without providing access to the switch or router command-line interface. To configure a node to use SSH, perform the following steps:

Step 1 In the node’s configuration terminal mode, use the **ssh enable** command to enable ssh.

```
aon-node(config)> ssh enable
```

Note Until you complete Step 2, the default password to gain secure access to a node is **aonsadmin**.

Step 2 Use the login password command to configure a password for SSH access. This command accepts either encrypted or plaintext passwords.

- To enter a plain text password:

```
aon-node(config)> login password unencrypted cisco
```

- To enter an MD5 encrypted password

```
aon-node(config)> login password encrypted $1$7v.O130F$xGo.LUNGt0eYxWTCZ/McQ
```

Step 3 Exit configuration terminal mode and save the configuration.

```
aon-node(config)> exit
aon-node> write memory
```

Step 4 Verify the configuration by using an SSH client to connect to the IP address assigned to the node.

```
[root@linux root]# ssh admin@10.4.1.92
The authenticity of host '10.4.1.92 (10.4.1.92)' can't be established.
RSA key fingerprint is 50:fa:d4:7e:46:e3:7b:2f:17:0d:e6:9f:d0:b4:1e:d5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.4.1.92' (RSA) to the list of known hosts.
admin@10.4.1.92's password:
```

Note The only username permitted to connect to an AON node is **admin**.

Configuring Nodes to Register with the AMC

In order to register with the AMC, the AON node must be configured with connection details for both itself and the AMC. To complete this task, perform the following steps:

Step 1 Enter configuration terminal mode on the AON node, then create an AON configuration ID. A configuration ID can be any combination of letters and numbers.

```
AON-node (config)# AON config abc create
```

Step 2 Configure the hostname or IP address of AMC. This is used by the AON node to communicate with AMC.

```
AON-node (config)# AON config abc amc host 10.1.1.1
```

Step 3 Assign an IP address to the AON management agent.

```
AON-node (config)# AON config abc ama host 10.1.1.2
```

Step 4 Activate the AON configuration.

```
AON-node (config)# AON config abc activate
```

Step 5 Specify a network time protocol (NTP) server that the node can use to maintain accurate time.

```
AON-node (config)# ntp server 10.1.1.10
```

Step 6 Specify the domain name of the node.

```
AON-node (config)# ip domain-name cisco.com
```

Step 7 Specify the DNS server to be used by the node.

```
AON-node (config)# ip name-server 10.1.10.10
```

Step 8 Exit configuration terminal mode. When AON asks to restart, enter **n**.

```
AON-node (config)# exit
CAUTION!! Configuration changed. Need to restart AON.
Confirm restart[y]? n
```

Step 9 Use the **write memory** command to save the AON configuration to nonvolatile memory, then restart AON.

```
AON-node> write memory
AON-node> AON restart force
!!CAUTION!! Restarting all processes right away.
Are you sure[n]? y
Start counting down before restart


This may take a while longer...
```

After the AON restart is complete, the node attempts to register with the AMC. The AMC ignores these attempts until a node with the proper credentials has been added.

Step 10 Use the **show version** command to obtain the module serial number (highlighted below). You need this information when you create a new node in AMC.

```
    AON-node> show version
    CPU Model:                    Pentium III (Coppermine)
    CPU Speed (MHz):              498.675
    CPU Cache (KByte):            256
    Chassis Type:                 C2691
    Chassis Serial:               12345678901
    Module Type:                  NM-AON-K9
    Module Serial:                FOC082313YY
    AON:                          0.0.0.409
    AMA:                          0.0.0.409
```

Step 11 Use the **write memory** command to save the configuration

```
AON-node> write memory
```

CHAPTER 2

Upgrading AON Software

The procedure that follows explains how to upgrade your Application-Oriented Networking (AON) environment to Cisco Application-Oriented Networking 2.2. It includes the following sections:

Caution Data loss may occur if you attempt to upgrade from a 1.*x* release to AON version 2.1.1 or later. You must first upgrade from 1.*x* to version 2.1.

Obtaining AON Software

AON software is available at the following URL:

http://www.cisco.com/kobayashi/sw-center/aon.shtml

Upgrade Paths

Table 2-1 lists the valid upgrade paths for each AON software release.

Table 2-1 AON Upgrade Paths

Current AON Release	Valid Upgrade Paths	Node Upgrade Required
AON 1.*x*	AON 2.1 only	Yes
AON 2.1.0	Any AON 2.*x*	Only if upgrading to AON 2.4
AON 2.1.*x*	Any AON 2.*x*	Only if upgrading to AON 2.4
AON 2.2	AON 2.4	Yes[1]

[1] If you are upgrading an AON Appliance from version 2.1.1 or earlier, you must first upgrade firmware and BIOS on the appliance. See the "Upgrading Firmware on the AON Appliance" section on page 2-19.

Upgrading AON 1.*x* Releases

AON version 2.1 includes a new software architecture to improve the process of upgrading nodes for future AON software releases. Consequently, this upgrade has several unique steps that differ from previous upgrade procedures. After this migration, future upgrades will be delivered in smaller files, and upgrades will require less downtime to complete.

Note Be sure to read this procedure completely before beginning the upgrade. The upgrade procedure for version 2.*x* releases is different from that of version 1.*x* releases.

Downloading Files

To perform this upgrade, make sure you have downloaded the files listed in Table 2-2.

Table 2-2 Files Required to Upgrade from an AON 1.x Release

Platform	Required files
AON Management Console	aon-amc_2.1.0.173_k9_lnx.upgrade.bin
AON Development Studio	aon-ads_2.1.0.173_k9_installer_win.exe
Cisco 8340 AON Appliance • APL-AON-8340-K9	Helper files: • aon-apl-8340_2.1.0.173_k9_helper_lnx.pkg • aon-apl-8340_2.1.0.173_k9_helper_lnx • aon-apl-8340_2.1.0.173_k9_helper_lnx.prt1 Image files: • aon-apl-8340_2.1.0.173_k9_lnx.pkg • aon-apl-8340-full_2.1.0.173_k9_lnx.prt1 • aon-apl-8340-installer_2.1.0.173_k9_lnx.prt1

Table 2-2 Files Required to Upgrade from an AON 1.x Release (continued)

Platform	Required files
AON Service Module	Migration files: • aon-svc_1.x_to_2.1.0.173_k9_helper_lnx.pkg • aon-svc_1.x_to_2.1.0.173_k9_helper_lnx.prt1 • aon-svc_1.x_to_2.1.0.173_k9_helper_lnx.manifest Helper files: • aon-svc_2.1.0.173_k9_helper_lnx.pkg • aon-svc_2.1.0.173_k9_helper_lnx.prt1 Image files: • aon-svc_2.1.0.173_k9_lnx.pkg • aon-svc-full_2.1.0.173_k9_lnx.prt1 • aon-svc-installer_2.1.0.173_k9_lnx.prt1
AON Network Module	Helper file • aon-nm_2.1.0.173_k9_helper_lnx Image files: • aon-nm_2.1.0.173_k9_lnx.pkg • aon-nm-full_2.1.0.173_k9_lnx.prt1 • aon-nm-installer_2.1.0.173_k9_lnx.prt1

Upgrading to from AON 1.*x* to AON 2.1

The steps that follow cover the tasks required for upgrading AMC and AON nodes and the order in which the must be performed. For more detailed instructions on the individual tasks that comprise this upgrade, see the following sections in this document:

- Upgrading the AON Management Console, page 2-5
- Upgrading the AON Appliance, page 2-6
- Upgrading the AON-SM, page 2-9
- Upgrading the AON-NM, page 2-12

Note This procedure refers to the default installation directory of **/opt/amc**. If your AMC is installed in a different directory, substitute that location when performing the steps below.

Upgrade Prerequisites

Before beginning, be sure to complete the following steps:

- Download all of the files needed to upgrade your AON environment. See Table 2-2 for a list of necessary files.
- Develop a backup and recovery strategy for the devices in your environment. At minimum you should have a TFTP server to store node configurations and external storage to back up your version 1.1 AMC installation.

- Verify that the Cisco IOS and CatOS versions for the switches and routers that host AON nodes, and upgrade any platforms as required. See the Release Notes for Cisco Application-Oriented Networking Version 2.1 for software requirements.

Caution You must ensure that any existing deployment requests are in the open (unstaged) state before you shut down AMC for the upgrade. Failure to do so may result in data loss.

To complete the upgrade, perform the following steps:

Step 1 Ensure that all users of ADS have synchronized PEP and message type changes before you begin the upgrade. Deploy these changes to nodes if necessary.

Step 2 Use **tar** or a similar command to back up the directory in which AMC is installed.

a. For example: **tar cvzf amc1_1_backup.tar.gz /opt/amc**

b. Copy the backup file to an external device.

Step 3 On each node being upgraded, copy the system and start-up configurations to a TFTP server.

a. Use **copy running-config startup-config** to save the current system configuration.

b. Use **copy running-config tftp** to copy the configuration to a TFTP server.

Step 4 Use the following steps to upgrade AMC to version 2.1.0.173.

a. Deactivate any active nodes.

b. Log in to the server running AMC as root.

c. Run **aon-amc_2.1.0.173_k9_lnx.upgrade.bin**. Near the end of the upgrade, it prompts you to start AMC. You must enter **no** here.

Note Do not start AMC until instructed to do so in Step 6.

For detailed instructions on upgrading AMC, see the "Upgrading the AON Management Console" section on page 2-5.

Step 5 Run the data upgrade script.

a. Change to the **/opt/amc/bin** directory.

b. Use **./upgradeData** to run the script

Step 6 Use **./amcd start** to launch AMC.

Step 7 Upgrade each node to version 2.1.0.173.

a. See the following sections of this document for detailed instructions:

– Upgrading the AON Appliance, page 2-6

– Upgrading the AON-SM, page 2-9

– Upgrading the AON-NM, page 2-12

b. After each node restarts, use configuration terminal mode to enter a new AON configuration so that the node can register with AMC.

c. Restart AON. Nodes will be shown as Registered on AMC, and you must activate each node.

Note You may see errors in aons.log when an upgraded node restarts. This occurs because the upgrade changes have not yet been deployed from AMC.

Step 8 Deploy the upgrade changes from Step 5.

a. Use AMC to deploy the property set changes to all nodes. There should be a global deployment request and a deployment request for each node.

b. Restart the nodes.

The initial bundle sent to the nodes contains the fully upgraded configuration.

Note Ensure that all AON Development Studio users uninstall all previous versions of ADS before they install ADS version 2.1.0.173.

Upgrading the AON Management Console

To upgrade AMC, perform the following steps.

Step 1 Copy the file to the local machine and make it executable.

```
[root@localhost root]# chmod +x aon-amc_2.1.0.173_k9_lnx.upgrade.bin
```

Step 2 Execute the upgrade package and enter the information requested by the application.

```
[root@localhost root]# ./aon-amc_2.1.0.173_k9_lnx.upgrade.bin
Preparing to install...
Enter the directory to install the AMC to [/opt/amc]:/opt/amc
Directory "/opt/amc" exists.
Upgrade existing installation? [y|n]:y
Attempting to stop any AMC processes in /opt/amc
Stopping AMC...Waiting for services to complete...Killing process with id 14221
Done.
Stopping AMC Database...Done.
Extracting archive.
Configuring paths.
Configuring the ports that the AMC will listen on.
If you are installing more than one AMC, these values
must be unique to each installation.
Enter a port for https [7010]:
Enter a port for communication with AONS nodes [7011]:
Enter a port for server shutdown signals [7025]:
Enter a port for the database [2638]:
Enter AMC logging level (DEBUG|INFO|NOTICE|WARN|ERROR|FATAL) [INFO]:
Enter log file rollover threshold size (KB) [1024]:
Enter number of backup logs to keep [5]:
The AMC requires a keystore file and password
to communicate with the AONS node.
Enter the path to the keystore file [/root/amcKeystore.localhost.cisco.com.jks]:
You may optionally enter a keyname within the keystore.
Enter a keyname, otherwise enter none [none]:
Enter a password for this keystore:
about to load the root certs
Loading /opt/amc/admin/security/keystores/ciscocerts/cap-rtp-003.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-root.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-manu-ca.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-manu-ca-dev.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-test-ca-2048.cer
Setting permissions for AMC installation...
Finalizing installation...
Done.
Would you like to run the AMC now? [y|n]:n
```

Note Do not run AMC until you run the upgradeData script. See Step 5 for details.

Upgrading the AON Appliance

To upgrade the AON Appliance, perform the following steps:

Step 1 Use AMC to deactivate the node, then reboot the appliance. Wait for the bootloader prompt, then enter ***.

```
GRUB Loading stage2...


Please enter '***' to change boot configuration: ***

Probing pci nic...
[tg3-5704]Ethernet addr: 00:14:5E:1C:20:60
Tigon3 [partno(BCM95704A6) rev 2100 PHY(5704)] (PCIX:100MHz:64-bit)
Link is up at 10 Mbps, half duplex.


 Cisco Bootloader Version : 2.0.0.6


Cisco Bootloader>
```

Step 2 Use the **config** command to update the IP information as necessary and enter the name of the helper image.

```
Cisco Bootloader> config
IP Address > 192.168.51.2
IP Netmask > 255.255.255.0
TFTP Server > 192.168.1.1
Gateway IP Address > 192.168.50.1
Default Helper-file > aon-apl-8340_2.1.0.173_k9_helper_lnx
Default Boot [none|disk] [disk] >
```

Step 3 Use the boot network command to boot the new helper image from the TFTP server.

```
Cisco Bootloader> boot network
Me: 192.168.51.2, Server: 192.168.1.1, Gateway: 192.168.50.1
Netbooting aon-apl-8340_2.1.0.173_k9_lnx.pkg (CTRL-C aborts)


Downloading aon-apl-8340_2.1.0.173_k9_lnx.pkg
Bytes downloaded :  94436

Validating package signature ... done
type:  application
WARNING:: Software installation will clear disk contents
Continue [n]? y
```

```
cleaning fs
prepfs.sh: olympus reiser /mnt clean
check_partition_count: 0
check_partition_flag: 1

The number of cylinders for this disk is set to 4306.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): Partition number (1-4):
Command (m for help): Command action
   e   extended
   p   primary partition (1-4)
Partition number (1-4): First cylinder (1-4306, default 1): Using defa
1
Last cylinder or +size or +sizeM or +sizeK (1-4306, default 4306):
Command (m for help): The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.

<-------------mkreiserfs, 2003------------->
reiserfsprogs 3.6.8

mkreiserfs: Guessing about desired format..
mkreiserfs: Kernel 2.4.24 is running.
Initializing journal - 0%....20%....40%....60%....80%....100%
Starting payload download
```

Step 4 Once the helper loads, enter **1** to install software.

```
Welcome to Cisco Systems Helper Software

Please select from the following choices:
1       Install software
2       Install certificate
3       Reload module
4       Disk cleanup
5       Configure IP parameters
6       Display status of RAID array
(Type '?' at any time for help)
Choice: 1
```

Step 5 Enter the package name of the version 2.1 image and the URL for the server hosting the helper image. If the server is password-protected, enter the user and password required to gain access to the file. If no password is required, leave these fields blank.

```
Package name: aon-apl-8340_2.1.0.173_k9_lnx.pkg
Server url: http://192.168.1.1/aonimages/
Username:
Password:
Downloading  aon-apl-8340_2.1.0.173_k9_lnx.pkg
Bytes downloaded :  94436

Validating package signature ... done
type:  application
WARNING:: Software installation will clear disk contents
Continue [n]? y
cleaning fs
prepfs.sh: olympus reiser /mnt clean
check_partition_count: 0
```

```
check_partition_flag: 1
```

Note The output during software installation and startup is extensive. It has been removed here for brevity.

```
                Welcome to Cisco AON Engine
                    (Version: 2.1.0.173)

AON boot: hit RETURN to set boot flags: 0001

********** rc.aesop ****************
Setting timezone: timezone is America/Los_Angeles
Loading Tarari Drivers...
SUCCESS: Loaded Tarari Drivers
Loading Cisco WCCP module
wccp: v1.00 (20000327), debug=0
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
Serial Number: KQGYY1M
Reading Manifest...Processing: /sw/installed/manifest/gpl_infrastructure_manifes
t.sig
Processing: /sw/installed/manifest/installer_manifest.sig
Processing: /sw/installed/manifest/oscore_manifest.sig
Processing: /sw/installed/manifest/global_manifest.sig
Processing: /sw/installed/manifest/aon_manifest.sig
Processing: /sw/installed/manifest/infrastructure_manifest.sig
Retrieved 4 sysdb nodes
Populating internal database .. complete.
[16640 refs]
Doing Certificate Check
Certificate Check Done
Loading Cisco CDP module
INIT: Entering runlevel: 2
********** rc.post_install ****************

****************************************
           post_install.sh
****************************************
Changing owners and file permissions.
Change owners and permissions complete.
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal
STARTED: NameService
STARTED: CLIFrontEnd
STARTED: NTPMonitor
STARTED: CacheService
STARTED: ManagementAgent
STARTED: WCCPSubsystem
STARTED: CLIBackEnd
STARTED: StunnelServer
STARTED: StunnelClient
STARTED: RAIDMonitor
STARTED: dwnldr_startup.sh

 waiting 9 ...
Password :
```

Step 6 Enter your administrator password and go to configuration terminal mode, then create an AON configuration so the node can register with AMC.

Upgrading the AON-SM

In order to make the transition to the new architecture described in the "Upgrading AON 1.x Releases" section on page 2-2, the AON-SM requires a migration image that serves as a bridge from the old architecture to the new. To complete the upgrade, you will:

1. Reload and enter the version 1.1 helper.
2. Install the migration image. This will install a version 2.1 helper image into flash.
3. Reload and enter the version 2.1 helper.
4. Install the version 2.1 application image.

Note The AON-SM contains two helper images, the primary helper image on cf:4 and the secondary helper image on cf:5. For the transition to version 2.1, we recommend you dedicate one of these helper image to be an AON 2.1 helper image and the other helper image to contain the AON 1.1 helper image. This will enable the ability to install either AON 1.1 images or AON 2.1 images as desired.

This procedure assumes that you will use the primary helper (cf:4) for version 2.1 and the secondary helper (cf:5) for version 1.1.

To upgrade the AON-SM to version 2.1, complete the following steps:

Step 1 Use AMC to deactivate the node, then set the boot device to cf:4 and reset the module:

- CatOS:

```
Router> (enable) reset module_number cf:4
This command will reset module 5.
Unsaved configuration on module 5 will be lost
Do you want to continue (y/n) [n]? y
Module 5 shutdown in progress.
Do not remove module 5 until shutdown completes.
```

- Cisco IOS:

```
Router# hw-module module module_number reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.
Proceed with reload of module? [confirm]y
```

Step 2 When the module finishes reloading, establish a session to it.

- CatOS:

```
Router# (enable) session module_number
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open
Starting Config
```

- Cisco IOS:

```
Router# session slot module_number processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open
Starting Config
```

Step 3 Enter the IP configuration details in the version 1.1 helper.

```
                    Welcome To Cisco AON Installer
                        (Version: 1.1.0.189)


**********************************
* AON Installer IP Configuration *
**********************************

Please enter the IP address of your module: 10.94.0.20
Please enter the netmask of your module: 255.255.255.0
Please enter the default gateway for your module: 10.94.0.1

The following IP configuration is set:
  IP     : 10.94.0.20
  NETMASK: 255.255.255.0
  GATEWAY: 10.94.0.1

Do you wish to use this configuration (y,n) [n] y

Config Done.
Starting Client
SYSTEM ONLINE
```

Step 4 Use the **software install** command to install the migration image from your HTTP or FTP server.

- FTP:

```
AONinstaller#> software install package url
ftp://server_ip_address/path_to_images/aon-svc_1.x_to_2.1.0.173_k9_helper_lnx.pkg
user username password password
```

- HTTP:

```
AONinstaller#> software install package url
http://server_ip_address/path_to_images/aon-svc_1.x_to_2.1.0.173_k9_helper_lnx.pkg
```

Note The installer cannot resolve domain names. Be sure to use only an IP address when you enter a URL.

```
Connecting to host...
  % Total    % Received % Xferd  Average Speed          Time             Curr.
                                 Dload  Upload Total    Current  Left    Speed
100 27768  100 27768    0     0  27768      0  0:00:01  0:00:00  0:00:00 7712k
File listing is signed
Retrieving aon-svc_2.1.0.173_k9_lnx_slim_migration.manifest from 10.47.0.2
Manifest Version retrieved is 1.0
Manifest Version matches package version
WARNING: This is an unrecoverable operation!
WARNING: This will completely replace the existing AON helper image.

Do you wish to continue (y,n) [n] y
Which Helper would you like to update primary or secondary (p,s) [p] p
mke2fs 1.27 (8-Mar-2002)
Retrieving aon-svc_2.1.0.173_k9_lnx_slim_migration.prt1 from 10.47.0.2
Connecting to host...
  % Total    % Received % Xferd  Average Speed          Time             Curr.
                                 Dload  Upload Total    Current  Left    Speed
100 12.1M  100 12.1M    0     0  10.9M      0  0:00:01  0:00:01  0:00:00 10.9M
complete.
Validating security header...done
Extracting files from package...done
Installing software onto the system...
Wed Jan 25 00:56:01 UTC 2006
100% complete.
```

```
Done.
Installing bootloader...
done.

Cleaning up...complete.
```

Step 5 Once the migration image finishes loading, exit the session and reset the module.

```
AONinstaller#> exit
```

- CatOS:

```
Console> (enable) reset module_number cf:4
This command will reset module 5.
Unsaved configuration on module 5 will be lost
Do you want to continue (y/n) [n]? y
Module 5 shutdown in progress.
Do not remove module 5 until shutdown completes.
```

- Cisco IOS:

```
Router# hw-module module module_number reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.
Proceed with reload of module? [confirm]y
```

Step 6 When the module resets, establish a session to the version 2.1 helper and enter 1 to install the version 2.1 software.

```
                   Welcome To Cisco AON Installer
                       (Version: 2.1.0.173)
              Welcome to Cisco Systems Helper Software
Please select from the following choices:
1       Install software
2       Install certificate
3       Exit session
4       Disk cleanup
5       Configure IP parameters
6       Temporarily disable login (for password recovery)
(Type '?' at any time for help)
Choice: 1
```

Step 7 Enter the IP configuration details in the migration helper.

```
The following IP configuration is set:
  IP     : 10.94.0.20
  NETMASK: 255.255.255.0
  GATEWAY: 10.94.0.1

Do you wish to use this configuration (y,n) [n] y
```

Step 8 Enter **1** to install software

```
Please select from the following choices:
1       Install software
2       Install certificate
3       Exit session
4       Disk cleanup
5       Configure IP parameters
6       Temporarily disable login (for password recovery)
(Type '?' at any time for help)
Choice: 1
```

Note The output produced during software installation and startup is extensive. It has been removed here for brevity.

Step 9 Enter the package name for the version 2.1 application image and the HTTP or FTP URL for the server hosting the files. Include any username or password needed to access the server.

```
Package name:  aon-svc_2.1.0.173_k9_lnx.pkg
Server url: http://10.47.0.2/aonimages/
Username:
Password:

Downloading  aon-svc_2.1.0.173_k9_lnx.pkg
Bytes downloaded :  95612
Validating package signature ... done
type:  application
WARNING:: Software installation will clear disk contents
Continue [n]? y
cleaning fs
prepfs.sh: kplus reiser /mnt clean
check_partition_count: 0
check_partition_flag: 1
```

Step 10 When the module reloads, reset the boot device to hdd:1.

- CatOS:

```
Console> (enable) reset module_number hdd:1
This command will reset module 5.
Unsaved configuration on module 5 will be lost
Do you want to continue (y/n) [n]? y
Module 5 shutdown in progress.
Do not remove module 5 until shutdown completes.
Console> (enable)
```

- Cisco IOS:

```
Router# hw-module module module_number reset hdd:1
Device BOOT variable for reset = <hdd:1>
Warning: Device list is not verified.

Proceed with reload of module? [confirm]
```

Step 11 When the module reloads, establish a session and use configuration terminal to create an AON configuration to enable the node to register with AMC.

Upgrading the AON-NM

To upgrade an AON-NM, perform the following steps:

Step 1 Use AMC to deactivate the node, then reboot the AON-NM. Wait for the bootloader prompt, then enter ***.

```
Please enter '***' to change boot configuration: ***

Cisco Bootloader Version : 2.0.0.4
```

Step 2 Use the **config** command to change IP configuration as necessary and to enter the name of the new helper image.

```
Cisco Bootloader> config

IP Address [192.168.169.92] >
IP Netmask [255.255.255.0] >
TFTP Server [192.168.1.1] >
Gateway IP Address [192.168.169.65] >
Default Helper-file [aon-nm_2.1.0.173_k9_helper_lnx] >
Ethernet Interface [internal] >
Default Boot [none|disk] [disk] >
Default Bootloader [primary|secondary] [primary] >
Updating flash with bootloader configuration
```

Step 3 Use the **boot network** command to load the helper from the TFTP server.

```
Cisco Bootloader> boot network
Me: 192.168.169.92, Server: 192.168.1.1, Gateway: 192.168.169.65
Netbooting aon-nm_2.1.0.173_k9_helper_lnx (CTRL-C aborts)
Dbg: Final image size: 11962750
Debug: bl_sz: 126496
in verifysignature_md5, MD5 hash generated now, str format:hexmd5:15ab0186f45a4
0b01cd5a4719b811a11
Verifying signature now...
calling RSA decrypt now
RSA decrypt returned:33
verifysignature_md5, Orig MD5 hash generated during encryption:15ab0186f45a40b0
1cd5a4719b811a11
Image signature verified successfully
```

Note The output produced during software installation and startup is extensive. It has been removed here for brevity.

Step 4 Once the helper loads, enter **1** to install software.

```
        Welcome to Cisco Systems Helper Software

Please select from the following choices:
1       Install software
2       Install certificate
3       Reload module
4       Exit session
5       Disk cleanup
(Type '?' at any time for help)

Choice:1
```

Step 5 Enter the package name of the version 2.1 image and the URL for the server hosting the helper image. If the server is password-protected, enter the user and password required to gain access to the file. If no password is required, leave these fields blank.

```
Package name: aon-nm_2.1.0.173_k9_lnx.pkg
Server url: http://192.168.1.1/aonimages/
Username:
Password:

Downloading  aon-nm_2.1.0.173_k9_lnx.pkg
Bytes downloaded :  92817

Validating package signature ... done
```

```
                Welcome to Cisco AON Engine
                    (Version: 2.1.0.173)

Mon Mar  6 11:48:28 UTC 2006
AON boot: hit RETURN to set boot flags: 0001

****************************************
           post_install.sh
****************************************
Changing owners and file permissions.
Change owners and permissions complete.
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal
STARTED: NameService
STARTED: CLIFrontEnd
STARTED: NTPMonitor
STARTED: CacheService
STARTED: ManagementAgent
STARTED: WCCPSubsystem
STARTED: CLIBackEnd
STARTED: StunnelServer
STARTED: StunnelClient
STARTED: dwnldr_startup.sh

 waiting 40 ...
Password :
```

Step 6 Enter your administrator password and go to configuration terminal mode, then create an AON configuration so the node can register with AMC.

Upgrading AON 2.1 Releases

Version 2.1.1 of Cisco Application-Oriented Networking provides you the ability to upgrade only AMC, while leaving some or all nodes at version 2.1. A mix of 2.1 and 2.1.1 nodes can interact with one another and with a version 2.1.1 AMC.

Additionally, AON 2.1.1 supports online upgrade of nodes. You can upgrade a node from within the AON application. It will download only the data needed to perform an incremental upgrade, then reboot, resulting in a much smaller period of downtime compared to previous AON releases.

Upgrading from AON 2.1 to AON 2.1.1

The steps that follow cover the tasks required for upgrading AMC and AON nodes from version 2.1 to version 2.1.1.

Caution Data loss may occur if you attempt to upgrade from a 1.*x* release to AON version 2.1.1. You must first upgrade from 1.*x* to version 2.1.

Note This procedure refers to the default installation directory of **/opt/amc**. If your AMC is installed in a different directory, substitute that location when performing the steps below.

Upgrade Prerequisites

Before beginning, be sure to complete the following steps:

- Download all of the files needed to upgrade your AON environment. If you are upgrading nodes, copy the appropriate files to an FTP server.
- Develop a backup and recovery strategy for the devices in your environment. At minimum you should have a TFTP server to store node configurations and external storage to back up your AMC installation.
- Verify that the Cisco IOS and CatOS versions for the switches and routers that host AON nodes, and upgrade any platforms as required.

Caution Data loss may occur if deployment requests are staged when you begin the upgrade. You must ensure that any existing deployment requests are in the open (unstaged) state before you shut down AMC for the upgrade.

This upgrade requires you to upgrade only AMC to version 2.1.1. You are not required to upgrade nodes unless you want the benefit of the software defects resolved since the previous release. Should you elect to upgrade only some nodes, your AON environment can operate with a mix of 2.1 and 2.1.1 nodes.

To complete the upgrade, perform the following steps:

Step 1 Ensure that all users of ADS have synchronized PEP and message type changes before you begin the upgrade. Deploy these changes to nodes if necessary.

Step 2 Use **tar** or a similar command to back up the directory in which AMC is installed.

c. For example: **tar cvzf amc1_1_backup.tar.gz /opt/amc**

d. Copy the backup file to an external device.

Step 3 On each node being upgraded, copy the system and start-up configurations to a TFTP server.

a. Use **copy running-config startup-config** to save the current system configuration.

b. Use **copy running-config tftp** to copy the configuration to a TFTP server.

Step 4 Use the following steps to upgrade AMC to version 2.1.1.53.

a. Deactivate any active nodes.

b. Log in to the server running AMC as root.

c. Run **aon-amc_2.1.1.53_k9_lnx.upgrade.bin**. Near the end of the upgrade, it prompts you to start AMC. You must enter **no** here.

Note Do not start AMC until instructed to do so in Step 6.

Step 5 Run the data upgrade script.

a. Change to the **/opt/amc/bin** directory.

b. Use **./upgradeData** to run the script

Step 6 Use **./amcd start** to launch AMC.

Note If you are upgrading only AMC, you have completed this procedure. If you are also upgrading nodes, proceed to Step 7.

Step 7 Establish a session to the node you are upgrading, then use the **software install** command to load the upgrade package.

```
aon-sm-1> $software install upgrade url ftp://server-address/aon-svc_2.1.1.53_k9_lnx.pkg
username user password password$
```

Note Only FTP is supported for online software upgrades.

```
WARNING:: This command will install the necessary software to
WARNING:: complete an upgrade.
Would you like to continue? [n] y
Downloading  aon-svc_2.1.1.53_k9_lnx.pkg
Bytes downloaded :  95927
Validating package signature ... done
Validating installed manifests .......complete.
Starting payload download
File :  aon-svc-full_2.1.1.53_k9_lnx.prt1  Bytes :  177750810
Validating payloads match registered checksums...
 - aon-svc-full_2.1.1.53_k9_lnx.prt1
..........................................................................................
................................................................................verified
```

Note The output produced during software installation and startup is extensive. It has been removed here for brevity.

Step 8 After waiting a few moments, session to the AON node and verify that it has successfully started. Use the **show version** command to verify that the node is running new software version.

```
aon-sm-1> show version
CPU Model:                    Pentium III (Coppermine)
CPU Speed (MHz):              996.909
CPU Cache (KByte):            256
Chassis Type:                 CAT6K
Module Type:                  Catalyst 6500 Series AON Module (WS-SVC-AON-1-K9)
Module Serial:                SAD092007UK
Global Software Version:      2.1.1.53
```

Step 9 Use AMC to activate the node, then go to **Network Node > Manage > Show** to confirm that AMC reflects the node’s new software version.

Upgrading from AON 2.1 to AON 2.1.2

The steps that follow cover the tasks required for upgrading AMC and AON nodes from version 2.1 to version 2.1.2.

Caution Data loss may occur if you attempt to upgrade from a 1.*x* release to AON version 2.1.2. You must first upgrade from 1.*x* to version 2.1.

Note This procedure refers to the default installation directory of **/opt/amc**. If your AMC is installed in a different directory, substitute that location when performing the steps below.

Upgrade Prerequisites

Before beginning, be sure to complete the following steps:

- Download all of the files needed to upgrade your AON environment. If you are upgrading nodes, copy the appropriate files to an FTP server.
- Develop a backup and recovery strategy for the devices in your environment. At minimum you should have a TFTP server to store node configurations and external storage to back up your AMC installation.
- Verify that the Cisco IOS and CatOS versions for the switches and routers that host AON nodes, and upgrade any platforms as required.

Caution Data loss may occur if deployment requests are staged when you begin the upgrade. You must ensure that any existing deployment requests are in the open (unstaged) state before you shut down AMC for the upgrade.

This upgrade requires you to upgrade only AMC to version 2.1.2. You are not required to upgrade nodes unless you want the benefit of the software defects resolved since the previous release. Should you elect to upgrade only some nodes, your AON environment can operate with a mix of 2.1 and 2.1.2 nodes.

To complete the upgrade, perform the following steps:

Step 1 Ensure that all users of ADS have synchronized PEP and message type changes before you begin the upgrade. Deploy these changes to nodes if necessary.

Step 2 Use AMC to deactivate all active nodes.

Step 3 Use **tar** or a similar command to back up the directory in which AMC is installed.

c. For example: **tar cvzf amc1_1_backup.tar.gz /opt/amc**

d. Copy the backup file to an external device.

Step 4 On each node being upgraded, copy the system and start-up configurations to a TFTP server.

a. Use **copy running-config startup-config** to save the current system configuration.

b. Use **copy running-config tftp** to copy the configuration to a TFTP server.

Step 5 Use the following steps to upgrade AMC to version 2.1.2.29.

a. Deactivate any active nodes.

b. Log in to the server running AMC as root.

c. Run **aon-amc_2.1.2.29_k9_lnx.upgrade.bin**. Near the end of the upgrade, it prompts you to start AMC. You must enter **no** here.

Note Do not start AMC until instructed to do so in Step 7.

Step 6 Run the data upgrade script.

a. Change to the **/opt/amc/bin** directory.

b. Use **./upgradeData** to run the script

Step 7 Use **./amcd start** to launch AMC.

Note If you are upgrading only AMC, you have completed this procedure. If you are also upgrading nodes, proceed to Step 8.

Step 8 Establish a session to the node you are upgrading, then use the **software install** command to load the upgrade package.

```
aon-sm-1> $software install upgrade url ftp://server-address/aon-svc_2.1.2.29_k9_lnx.pkg
username user password password$
```

Note Only FTP is supported for online software upgrades.

```
WARNING:: This command will install the necessary software to
WARNING:: complete an upgrade.
Would you like to continue? [n] y
Downloading  aon-svc_2.1.2.29_k9_lnx.pkg
Bytes downloaded :  95927
Validating package signature ... done
Validating installed manifests .......complete.
Starting payload download
File :  aon-svc-full_2.1.2.29_k9_lnx.prt1  Bytes : 177744975
Validating payloads match registered checksums...
 - aon-svc-full_2.1.2.29_k9_lnx.prt1
..........................................................................................
................................................................................verified
Calculating delta.... complete.
Retrieving calculated file change sets:
 - Installed file sets...complete.
 - Target file change sets...complete.
Comparing changed source and target files...complete.
Calculating upgrade work order ... complete.
Creating uninstall change sets:
 complete. No added files found.
 - logging added components ... complete.  No removed files found.
Clearing previous downgrade files ... complete.
Uninstall change set processing complete.
Writing upgrade work order to disk ... complete.
[17813 refs]
.
Disabling disk spindown on /dev/hdc

/dev/hdc:
 setting standby to 0 (off)
SHUTDOWN: cli_state.sh shutdown Success
SHUTDOWN: AONSShutdown Success
SHUTDOWN: procMgr -p ntp stop Success
SHUTDOWN: procMgr -p stunnel_client stop Success
SHUTDOWN: procMgr -p stunnel_server stop Success
install-files.sh /dwnld/.work_order
Remove  ///sw/installed/manifest/global_manifest.sig
add_file /dwnld/pkgdata/aon-svc_2.1.2.29_k9_lnx.pkg 1 /
sw/installed/manifest/global_manifest.sig none
Remove  //dwnld/pkgdata/aon-svc_2.1.2.29_k9_lnx.pkg
Remove  //dwnld/pkgdata/aon-svc-full_2.1.2.29_k9_lnx.prt1
Console> (enable)
```

The AON node reboots and returns you to the command line of the host router or switch.

Step 9 After waiting a few moments, session to the AON node and verify that it has successfully started. Use the **show version** command to verify that the node is running new software version.

```
aon-sm-1> show version
CPU Model:                    Pentium III (Coppermine)
CPU Speed (MHz):              996.909
CPU Cache (KByte):            256
Chassis Type:                 CAT6K
Module Type:                  Catalyst 6500 Series AON Module (WS-SVC-AON-1-K9)
Module Serial:                SAD092007UK
Global Software Version:      2.1.2.29
```

Step 10 Use AMC to activate the node, then go to **Network Node > Manage > Show** to confirm that AMC reflects the node's new software version.

Upgrading from AON 2.1.1 to AON 2.1.2

To upgrade from AON 2.1.1 to AON 2.1.2 run the AON upgrade installer—aon-amc_2.1.2.29_k9_lnx.upgrade.bin—and upgrade the firmware for Cisco 8300 AON Appliance series.

Upgrading Firmware on the AON Appliance

If you are upgrading software on an existing Cisco 8300 AON Appliance, the firmware upgrade must be completed before installing AON 2.1.2 or later software images.

Note The Cisco Application-Oriented Networking version 2.1.2 images already contain the updated device drivers needed for the new firmware.

Note Once you upgrade to AON version 2.1.2, you cannot downgrade to an earlier AON software version. This new firmware set works on the older version of Cisco 8300 AON Appliance hardware.

Warning **Once you start the upgrade process, do not remove the CD from the system until you complete Step 23.**

Warning **Do not remove power or reboot the system while one of the updates are running. Removal of power in the middle of a firmware update can damage components.**

For more detailed instructions on the individual tasks that comprise this upgrade, see the following sections in this document:

- Upgrade Prerequisites, page 2-19
- Upgrading Firmware and BIOS, page 2-20

Upgrade Prerequisites

- You must be physically present wherever the hardware is installed to manually insert the CD containing the software.

- Access the Cisco 8300 AON Appliance hardware through a Remote Console Terminal or directly via keyboard and monitor or a direct serial cable connection. You can use a good telnet client (CRT, secure CRT, HyperTerminal) to connect to the Appliance hardware.

Note Do not use an SSH client because it does not work correctly.

- All the firmware upgrades must be done with a device that is physically connected to the hardware and contains all the necessary software. We suggest that you burn the firmware upgrade software file onto a single CD after downloading the file from Cisco.com. The file **apl-aon-8342-biosfwupdate.iso** contains all of the necessary firmware upgrades.

Upgrading Firmware and BIOS

Step 1 Use AMC to deactivate the node, then insert the CD into the CD drive.

Warning **Do not eject the CD until you have completed the entire procedure.**

Step 2 From the CLI, properly restart your machine. The system automatically recognizes the CD and boots into DOS, and displays boot information as follows:

```
ISOLINUX 3.11 2005-09-02 Copyright (C) 1994-2--5 H. Peter Anvin
Cisco AON 8300 Series Appliance BIOS and Firmware Update for AON 2.1.2, 2.2

Defaults to "disk" if press <Enter> or after 5 minute timeout
    disk)BOOT to Cisco Bootloader or hard disk drive
    bios)INSTALL interactive System BIOS 1.09, ZUEC54BUS 2006/06/15
    diag)INSTALL unattended Diagnostic 1.05, ZUYT27A
    bmc)INSTALL BMC firmware 2.07, Z2BT05E 2006/05/10, IPMI 2.0
    cpld) INSTALL CPLD firmware 1.06, HEUD18A
raidbios) INSTALL ServeRAID 8i BIOS 5.1-0 Build 9234 2006/6/14
    getver)LOAD SPint v3.02 to get version of BIOS, BMC; get ringdumps
Type choice at boot: prompt
boot:
```

Step 3 At the prompt, type **BMC**, then press **Enter**.

The following information displays during the BMC upgrade:

```
Decompressing BMC firmware
reading fullfw.cmt...wrote 15357 SRECa to fullfw.mot
Acquiring BMC attributes
Updating BMC Firmware

BMC's IPMI level migration starting (step 1 of 4).
Config Loader Version 1.0, OSA Technologies, INC. (c) 2005

Upload configurations from BMC
Processing......Success!

Flash Loader v1.29.0.45, OSA Technologies, Inc. (c)2005

                          firmware       image
    IPMI Version=             1.5        2.0
    major revision=            1          2
    minor revision=           18          7
    manufacturer ID=           2          2
    product ID=                7          7
```

```
Start programming...
Writing to Address: 0x0007F280.......OK
Download to Flash OK.

BMC initilaization...OK
BMC Firmware and SDRs updated successfully!!!

BMC's IPMI level migration still in progress (step 2 of 4).
BMC's IPMI level migration still in progress (step 3 of 4).
BMC's IPMI level migration still in progress (step 4 of 4).
Config Loader Version 1.0 . OSA Technologies, Inc. (c)2005

Download configurations to BMC
Processing......Success!

Any user passwords on the BMC will need to be redefined after
IPMI level migration.
BMC's IPMI level migration completed.

Updating BMC's Boot Block.
Please remove the disk from the drive and restart the system.
C:\>
```

Note The BMC upgrade takes about 3 minutes.

Step 4 At the prompt, type **Reboot**, then press **Enter**.

Step 5 After the machine reboots, type **cpld** and press **Enter**. Then you follow the following:

```
==============================================================
       Spint/x460/x260 CPLD UPDATE DISKETTE
==============================================================
Current time is xxxxx, 2006 at 16:36:51

Current level of CPLD code - 1.03

Code level after flash - 1.06

**************DO NOT POWER OFF THE SYSTEM OR REMOVE AC POWER DURING PLD FLASH

[A] - Flash CPLD code
[B} - Exit Utility

Please enter choice and then press enter
```

Step 6 Enter **A** and press **Enter**.

This starts the CPLD upgrade. When it has completed, that screen displays the following:

```
You have successfully flashed the CPLDs for this system.
*****************REMOVE AC POWER CORD AND REBOOT SYSTEM*******************
*****************REMOVE AC POWER CORD AND REBOOT SYSTEM*******************
*****************REMOVE AC POWER CORD AND REBOOT SYSTEM*******************
```

Step 7 Type **Reboot** and then press **Enter**.

Step 8 After the machine reboots, type **raidbios** and press **Enter**.

Note If asked for a second diskette, just ignore the request and press **Enter**.

Step 9 When asked for a confirmation to upgrade to RAID BIOS, type **Y**.

The screen displays the following:

```
Adaptec Flash Utility V5.1-0 B9234
(c) Adaptec Inc. 1999-2006. All Rights Reserved.
Updating Controller 0 (IBM ServRAID 8i)
Please insert disk labeled "IBM ServRAID 8i Firmware Disk 1"
and press ENTER or press ESC to cancel
Reading flash image file (Build 9234) ...
Please insert disk labeled "IBM ServRAID 8i Firmware Disk 2"
amd press ENTER or press ESC to cancel
Reading flash image file (Build 9234) ...
AFU is about to update firmware on controller(s) IBM ServRAID 8i
*** PLEASE DO NOT REBOOT THE SYTEM DURING THE UPDATE ***
This might take a few minutes.
Writing IBM ServRAID 8i flash image to controller 0...OK. Verifying...OK.
Please restart the computer to allow firmware changes to take effect.
A:\>_
```

Step 10 Type **Reboot** and then press **Enter**.

Step 11 After the machine reboots, type **BIOS** and press **Enter**.

The update utility displays the following:

```
0 - Exit
1 - Update POST/BIOS
2 - Update Diagnostic
3 - Backup Current POST/BIOS
4 - Restore POST/BIOS from the backup version on a drive
5 - Restore POST/BIOS from the ROM backup version

    Select an option _
```

Step 12 Select Option **1** and press **Enter**.

Step 13 When prompted for the serial number, type **Y** for yes and enter the serail number found on the faceplate of the Appliance.

Step 14 When prompted for the machine type, type **Y** for yes and enter **8863PDH**.

Step 15 When prompted for a value for the asset tag, type **N** for no.

Step 16 When prompted for saving the current Flash code to disk, type **N** for no.

Step 17 When prompted for a confirmation of BIOS upgrade, select option **1** again.

After the BIOS upgrade completes, the machine should automatically reboot.

Step 18 After the machine reboots, type **diag** and press **Enter**.

The update utility displays the following:

```
Flash Update Utility
Version 1.02

The system Diagnostic is being updated.
This may take upto 5 minutes.
Do not power off or restart the system during this procedure.
```

When the System Diagnostic upgrade is complete, the screen displays the following:

```
Thanks for using the POST/BIOS Utility
```

Step 19 Type **reboot** and press **Enter** to restart the system.

Step 20 After the machine reboots, type **getver** at the command prompt and press **Enter**.

Step 21 Type **x366** and press **Enter**.

Note The information scrolls by fast.

Step 22 You can use **cntrl-s** to pause and review the output. Following is a typical example:

```
This nodes BMC address = 0CA8
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
³     Spint Dump Tool Ver 3.02      ³
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Current time is Thursday Jul 6, 2006 at 18:58:42
Current BMC Time is: 7/6/2006 19:1:0
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
³        System Information         ³
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Model number = 8863PDH
S/N          = KQD2960
POST/BIOS Build ID      = ZUEC54BUS
          Build Date    = 06/15/06
BMC Build ID            = Z2BT05E
    Build Date          = 04-24-06
    Build Time          = 11:16:44
    Major Revision      = 02
    Minor Revision      = 05
    IPMI Revision       = 2.0
CPU Card CPLD Revision = 0D
PCI Card CPLD Revision = 19
I/O Card CPLD Revision = 12
Model number = 8863PDH
S/N          = KQD2960
-- More --
```

Step 23 Remove the CD from the DVD-CD drive.

Step 24 Type **reboot** and press **Enter**.

Step 25 After the machine reboots, the sceen displays the following:

```
Symmetric Multiprocessing System
Intel Xeon MP ~3.1 GHz

04096 MB Memory: Installed
4 Processor Packages Installed


Press F1 for Setup
Press F2 for Diagnostics
Press F12 to select boot device
```

Enter **F1**.

Step 26 Ignore the interim screen that displays “Configuration Error” and press **Enter**.

Step 27 In the following screen displaying “Configuration/Setup Utility,” select **Load Default Settings**.

Step 28 Press **Enter**.

Step 29 Next select **Exit Setup** and confirm to save changes.

The system reboots and returns you to the Cisco Boot Loader.

Upgrading to AON 2.4

You can upgrade to AON 2.4 from any of the following releases:

- AON version 2.1.0
- AON version 2.1.1
- AON version 2.1.2
- AON version 2.1.5
- AON version 2.2

Unlike earlier releases, the AMC installer upgrades both the code and the data from the previous AMC installation. There is no need to run a separate process to upgrade PEPs, message types, and attribute domains.

Note Due to architectural improvements, you must upgrade all nodes to version 2.4. A 2.4 AMC cannot manage nodes running previous software releases.

Note If you are upgrading an AON Appliance from version 2.1.1 or earlier, you must first upgrade firmware and BIOS on the appliance. See the "Upgrading Firmware on the AON Appliance" section on page 2-19.

Projects

AON 2.4 introduces the concept of projects to partition the work performed by different development teams. A project contains all of the resources, created by a team. Resources created using previous AON releases are distributed among two projects during the upgrade. All PEP and message type resources are placed in a user project, while all other resources (property sets, extensions, etc.) are placed in the predefined "System" project.

Prefixes are used to identify resources created by individual projects. Each project has a unique prefix which is prepended to the name of each resource belonging to the project. By convention, the predefined "System" project has no prefix. During the installation, you will be asked to specify a name and prefix for the user project, and the prefix will be added to the names of all PEPs and message types. After the upgrade, you can find these resources in the project you specified

Note Due to a defect in AON Release 2.4, you cannot use a number as the first character of a prefix. Use only a letter.

For more details about projects, see the Enterprise Lifecycle Management chapter of the *AON Administration Guide*

Users

AON 2.4 includes two new user roles, application developer and system administrator. The system administrator is a super user. Users with the following roles in previous AON releases now have this role:

- network administrator
- security administrator
- application administrator

For more information on user roles, see the AMC Administration chapter of the *AON Administration Guide*.

Upgrading the AON Management Console to Version 2.4

Note This procedure refers to the default installation directory of **/opt/amc**. If your AMC is installed in a different directory, substitute that location when performing the steps below.

Upgrade Prerequisites

Before beginning, be sure to complete the following steps:

- Download all of the files needed to upgrade your AON environment.
- Develop a backup and recovery strategy for the devices in your environment. At minimum you should have a TFTP server to store node configurations. The AMC installer will give you the opportunity to backup your database before proceeding with the upgrade. If you elect to perform this backup, you must specify a location for which AMC has write permissions.
- Ensure that there are no open deployment requests (DRs) within AMC. The installer exits if it finds open DRs.
- Verify that the Cisco IOS and CatOS versions for the switches and routers that host AON nodes, and upgrade any platforms as required. See the appropriate Release Notes for Cisco Application-Oriented Networking for requirements that apply to your AON release.

To upgrade AMC, perform the following steps.

Step 1 Ensure that ADS users have synchronized PEPs, message types, and other data with AMC.

Step 2 Use AMC to deactivate any active nodes.

Step 3 Copy the AMC upgrade file to the local machine and make it executable.

```
[root@localhost root]# chmod +x aon-amc_2.4.0.58_k9_lnx.upgrade.bin
```

Step 4 Execute the upgrade package and enter the information requested by the application.

```
[root@cisco opt]# ./aon-amc_2.4.0.58_k9_lnx.upgrade.bin
Preparing to install...
Enter the directory to install the AMC to [/opt/amc]:
Directory "/opt/amc" exists.
Upgrade existing installation? [y|n]:y
Attempting to stop any AMC processes in /opt/amc
Stopping AMC...Waiting for services to complete...Done.
Stopping AMC Database...Done.
Starting AMC Database...Done.
sleeping for 15 seconds ...
Getting AMC Version as:2.1.2.29
Checking the database for active Global Deployment Requests...
Checking the database for active Node Deployment Requests...
Done checking database for active Global and Node Deployment Requests
Stopping AMC Database...Done.
Would you like to back up the AMC directory? [y|n]:y
The estimated backup file size is: 252.0M
Please specify the backup location: [/tmp]:
Backing up existing AMC directory - /opt/amc - Please wait !!!
Extracting archive.
Configuring paths.
Configuring the ports that the AMC will listen on.
If you are installing more than one AMC, these values
must be unique to each installation.
Enter a port for https [7010]:
Enter a port for communication with AONS nodes [7011]:
Enter a port for server shutdown signals [7025]:
Enter a port for the database [2638]:
Enter AMC logging level (DEBUG|INFO|NOTICE|WARN|ERROR|FATAL) [INFO]:
Enter log file rollover threshold size (KB) [1024]:
Enter number of backup logs to keep [5]:
The AMC requires a keystore file and password
to communicate with the AONS node.
Enter the path to the keystore file [/root/amcKeystore.cisco.com.jks]:
You may optionally enter a keyname within the keystore.
Enter a keyname, otherwise enter none [none]:
Enter a password for this keystore:
about to load the root certs
Loading /opt/amc/admin/security/keystores/ciscocerts/cap-rtp-003.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-root.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-manu-ca.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-manu-ca-dev.cer
Loading /opt/amc/admin/security/keystores/ciscocerts/cisco-test-ca-2048.cer
Setting permissions for AMC installation...
Finalizing installation...
Done.
Enter a Project Name (up to 256 characters) [USER_PROJECT]:Resources_2_1
Enter a Project Prefix (up to 50 characters) [PREFIX]:Res_2_1
Starting AMC Database...Done.
sleeping for 15 seconds ...
Database Upgrade Begins...
Output of the upgrade process can be found in /opt/amc/log/upgradeData.log
AMC is not running
Stopping AMC Database...Done.
The backup file can be located at /tmp/20061115162508.AMCbackup.tar.gz
The upgrade process may have generated Global and Node DRs, please log onto the AMC and
deploy all staged DRs to complete the AMC upgrade process.
Would you like to run the AMC now? [y|n]:y
Starting AMC Database...Done.
Starting AMC...Done.
AMC logfile is /opt/amc/log/amc.log
Upgrade successful.
To uninstall, run '/opt/amc/bin/amcSetup uninstall'.
[root@cisco opt]#
```

Step 5 Ensure that ADS users uninstall any previous versions of the application, then they must install version 2.4. Previous versions of ADS will not connect to AMC version 2.4.

Upgrading Nodes to Version 2.4

Due to architectural improvements, you must upgrade all nodes to version 2.4. AMC version 2.4 cannot manage nodes running releases before AON 2.4.

To upgrade a node, perform the following steps:

Step 1 Use AMC to deactivate the node. Establish a session to each node and use the **software install** command to load the upgrade package.

```
aon-sm-1> $software install clean url ftp://server-address/aon-svc_2.4.0.58_k9_lnx.pkg
username user password password$
```

Note Only FTP is supported for online software upgrades.

```
WARNING:: This command will install the necessary software to
WARNING:: complete an upgrade.
Would you like to continue? [n] y
Downloading  aon-svc_2.4.0.58_k9_lnx.pkg
Bytes downloaded :  95927
Validating package signature ... done
Validating installed manifests .......complete.
Starting payload download
File :  aon-svc-full_2.4.0.58_k9_lnx.prt1  Bytes :  177750810
Validating payloads match registered checksums...
 - aon-svc-full_2.4.0.xx_k9_lnx.prt1
...........................................................................................
.................................................................................verified
```

Note The output generated during an upgrade is extensive. It has been removed for brevity.

After completing the upgrade, the AON node reboots.

Step 2 After waiting a few moments, session to the AON node and verify that it has successfully started. Use the **show version** command to verify that the node is running new software version.

```
aon-sm-1> show version
CPU Model:                    Pentium III (Coppermine)
CPU Speed (MHz):              996.909
CPU Cache (KByte):            256
Chassis Type:                 CAT6K
Module Type:                  Catalyst 6500 Series AON Module (WS-SVC-AON-1-K9)
Module Serial:                SAD092007UK
Global Software Version:      2.4.0.58
```

Step 3 Using AMC, wait for the node to register, then go to **Network Node > Manage > Show** to confirm that AMC reflects the node's new software version.

Step 4 Use AMC to activate the node. AMC will then deploy upgraded configuration data to the node.