Cisco Application Networking Manager 3.0

Product Overview

Cisco® Application Networking Manager (ANM) software is part of the Cisco ACE Application Control Engine product family and is a critical component of any data center or cloud computing architecture that requires centralized configuration, operation, and monitoring of Cisco data center networking equipment and services. Cisco ANM provides this management capability for the Cisco ACE devices, as well as operations management for the Cisco Content Services Switch (CSS), Cisco Content Switching Module (CSM), Cisco Content Switching Module with SSL (CSM-S), and Cisco ACE Global Site Selector (GSS).

Cisco ANM helps customers manage multidevice data center network services effectively. By using Cisco ANM, customers can streamline the deployment and ongoing maintenance of their Cisco ACE virtualized environment, providing a unified interface for Cisco ACE troubleshooting, maintenance, operations, and monitoring. It also unifies the operations management and monitoring of real and virtual servers spanning a load-balancing infrastructure of Cisco ACE, CSS, CSM, and CSM-S devices. Cisco ANM also centralizes operations management of virtual IP answers and Domain Name System (DNS) rules for Cisco ACE GSS devices.

Cisco ANM is ideal for enterprises and service providers that implement Cisco ACE and provides additional value to customers using Cisco CSS, CSM, CSM-S, and Cisco ACE GSS devices. These customers include data center infrastructure providers, application service providers, large enterprises, and e-business data centers. Even small and medium-sized enterprises with small deployments of Cisco ACE devices can take benefit from Cisco ANM through the entry-point offering.

Features and Benefits

Device and Service Configuration

Cisco ANM simplifies Cisco ACE provisioning through forms-based configuration management of Layer 4 through 7 virtualized network devices and services. With Cisco ANM, network managers can create, modify, and delete all virtual contexts of the Cisco ACE, control the allocation of resources among virtual contexts, and define and manage high availability. Within these virtual contexts, Cisco ANM enables configuration of load-balancing services, including application control lists (ACLs), real servers, server farms, sticky groups, SSL services and health monitoring, and the service bindings to the hosting Cisco Catalyst® 6500 Series Switch and Cisco 7600 Router VLAN interfaces for the Cisco ACE Module.

Cisco ANM enables rapid creation, modification, and prestaged or immediate deployment of common services by operators of all skill levels. It does this by including sets of provisioning forms and methods for basic, advanced, and expert users.

Cisco ANM 3.0 Guided Setup provides GUI guidance and networking diagrams to help simplify the configuration of Cisco ANM and its associated devices. Guided Setup presents a logical and comprehensive workflow, enabling the user to rapidly complete provisioning of new systems, contexts, and applications. To complete a deployment, the user simply follows the steps. The steps change depending on the options selected, guiding the user through the provisioning process. Cisco ANM guides the user through the configuration presenting only the appropriate configuration selections that may apply, offering default configuration choices as well as options for the user to customize the configuration. The user can use elements already deployed as necessary, and the user can revisit any part of Guided Setup to edit new or existing services without having to start from the beginning.

At each configuration step, Cisco ANM provides the user with critical, just-in-time guide text about the main concepts as well as advice. For more experienced users, this text can be hidden. A Learn More hyperlink helps the user understand the functions at an even deeper level.

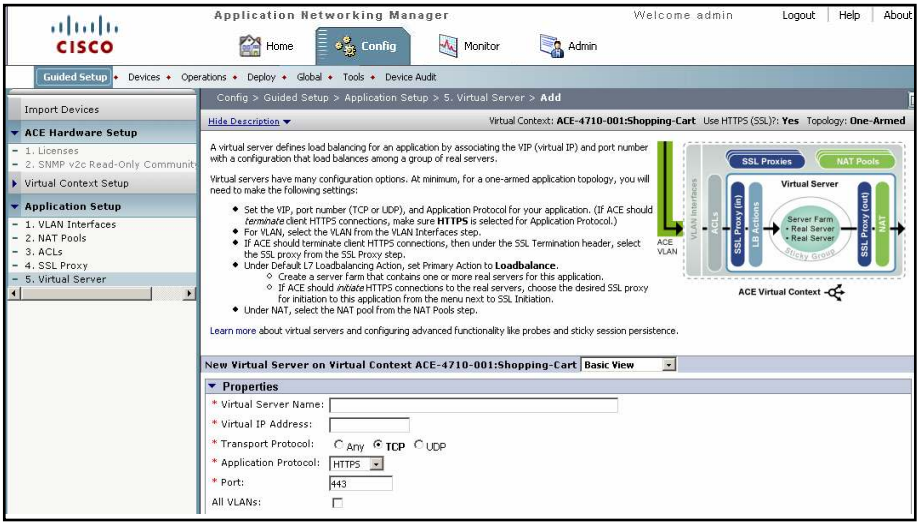
Cisco ANM 3.0 enhances this guidance with illustrations that reflect the specific selections made by the user. For example, the application setup steps show the three most popular configurations.

Cisco ANM 3.0 Guided Setup allows you to quickly perform the following tasks:

- Establish communication between Cisco ANM and Cisco ACE devices
- Configure Cisco ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability deployments.
- Create and connect to a Cisco ACE virtual context.
- Set up a load-balancing application from Cisco ACE to a group of back-end servers.

Using Cisco ANM 3.0 Guided Setup, even operators new to the system can immediately get value from their Cisco ACE systems by provisioning the most common services quickly and easily (Figure 1).

Figure 1. Cisco ANM 3.0 Guided Setup



Advanced users can go directly to the configuration forms without using Guided Setup. Expert users can go a step beyond to the Cisco ANM expert mode, where they can implement even the most intricate configurations of services while still gaining the security and error reduction afforded by performing these tasks through the Cisco ANM GUI and building block–based configuration management.

Additional device and service configuration features include:

- Cisco ANM global building blocks speed deployment of common configuration components and support the standardization of those configurations for devices, virtual contexts of devices, and services.
- Cisco ANM provides the capability to discover all chassis, modules, appliances, virtual contexts, and service definitions across a large number of systems for systems established prior to Cisco ANM deployment.
- All these configuration tasks can be performed using a secure web-based GUI, eliminating the need to use the Cisco ACE command-line interface (CLI).

Monitoring Dashboards with Real-Time and Historic Graphing

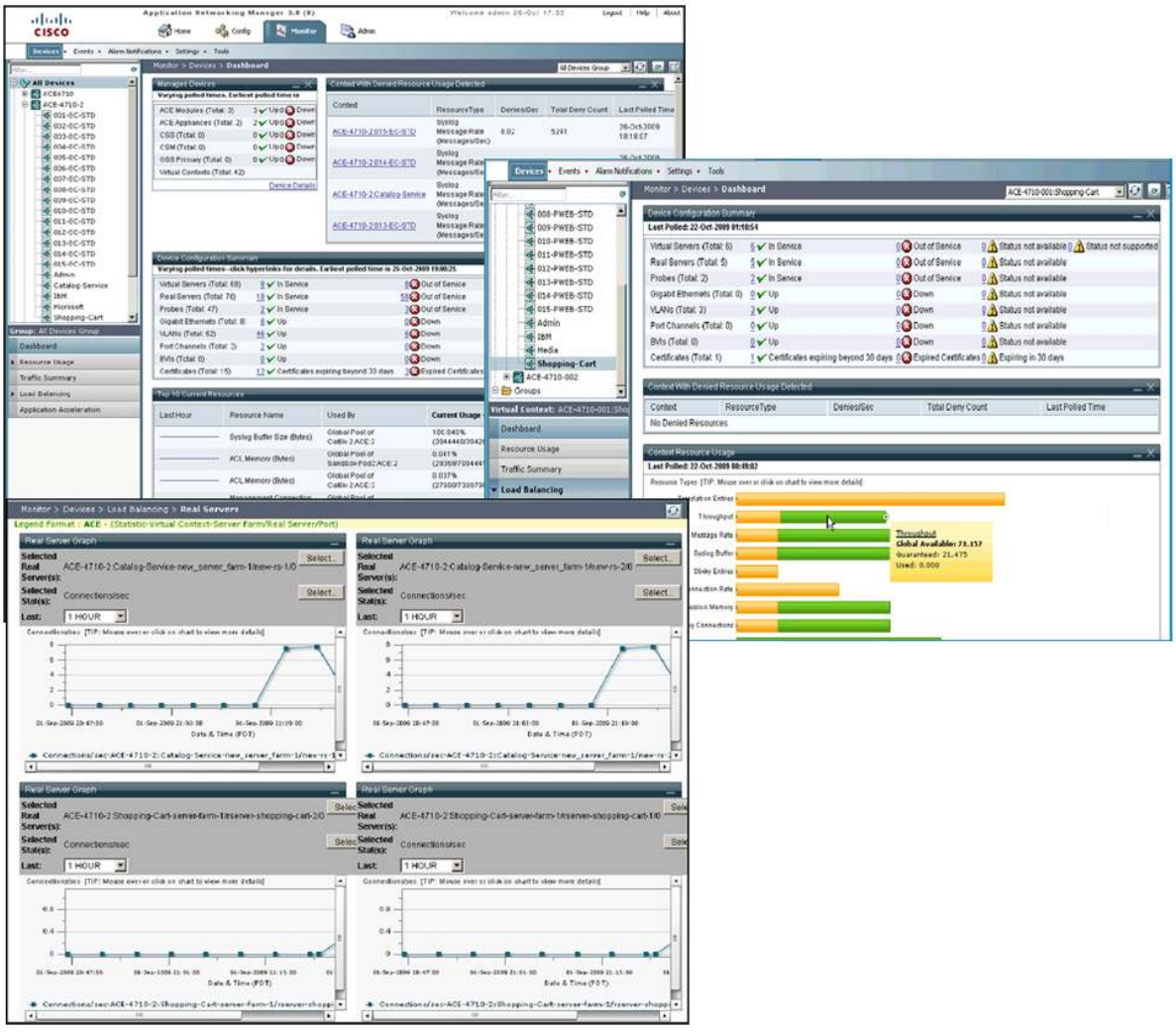
Cisco ANM provides up-to-date information about the health and state of all devices, virtual contexts, and applications managed by Cisco ANM. It provides this information through real-time monitoring dashboards. These dashboards enable operations staff to see the most useful information at a glance, to quickly and easily perform more in-depth analysis and speed troubleshooting and problem resolution.

Cisco ANM 3.0 monitoring includes dashboards at the systemwide top level for all managed devices, and for Cisco ACE Modules and Cisco ACE appliances it provides dashboards at the device and virtual context levels.

These dashboards display health, utilization and performance data for such elements as device-wide traffic, context resource allocation and use, load-balancing statistics, and real server utilization. For instance, the Cisco ACE device-level dashboard includes the Context with Denied Resource Usage Detected table, which lists all contexts for which a resource request was denied after reaching the maximum limit, enabling the operator to track virtual contexts that may need additional resources allocated.

Cisco ANM 3.0 stores historical data for a selected list of statistics calculated over the last 1-hour, 2-hour, 4-hour, 8-hour, 24-hour, or month interval. Operators can view this historical data as a statistical graph. Up to four objects can be overlaid on a single graph for comparison.. Figure 2 shows an example of historic graphing, as well as portions of a top-level dashboard and a context-level dashboard.

Figure 2. Cisco ANM Monitoring Dashboards and Graphs



Additional monitoring features include:

- Export of graphed data in JPEG picture file or Microsoft Excel file format for archival or other purposes
- Health and performance dashboards that include top-N and alarm and event graphs and tables
- Support for various levels of monitoring views for Cisco ACE, CSS, CSM, and CSM-S devices

Event Logging and Threshold Crossing Alerts

Cisco ANM provides a dedicated event view of syslog and Simple Network Management Protocol (SNMP) trap events collected from Cisco ACE Modules and Cisco ACE appliances. Cisco ANM monitoring dashboards display the latest five critical events with an option to open an event view to display all events.

Within Cisco ANM, user-definable threshold-crossing alerts can be defined that span multiple devices and virtual services, so that health, availability, fault-tolerant status, utilization, and resource capacity can be monitored with both crossing and clearing notifications generated through an SNMP trap or an email message, or both. For example, an SNMP trap notification can be generated to inform an enterprise event management system of abnormal utilization rates for a particular application, while both an SNMP trap and alarm email (configured to a pager) can be generated whenever a critical application server fails to respond to the Cisco ACE.

SSL Certificates Monitoring

A global list of all certificates used by the managed Cisco ACE is available in the monitoring dashboards. The dashboards show the total count of SSL certificates and the count of SSL certificates that are valid, expired, or expiring within 30 days. At each dashboard level, a hyperlink leads to a view of the SSL certificates list based on the selection, displaying the certificate name, device name, days until expiration, expiration date, and date the certificate was evaluated to determine the days until expiration. As with all elements, the user's display is limited to those elements that the user has rights to view.

In addition to health and utilization threshold crossing alerts, Cisco ANM can be configured to monitor the certificate expiration status and to generate warning alerts (using SNMP traps and email) prior to the SSL certificate's expiration date (usually annually).

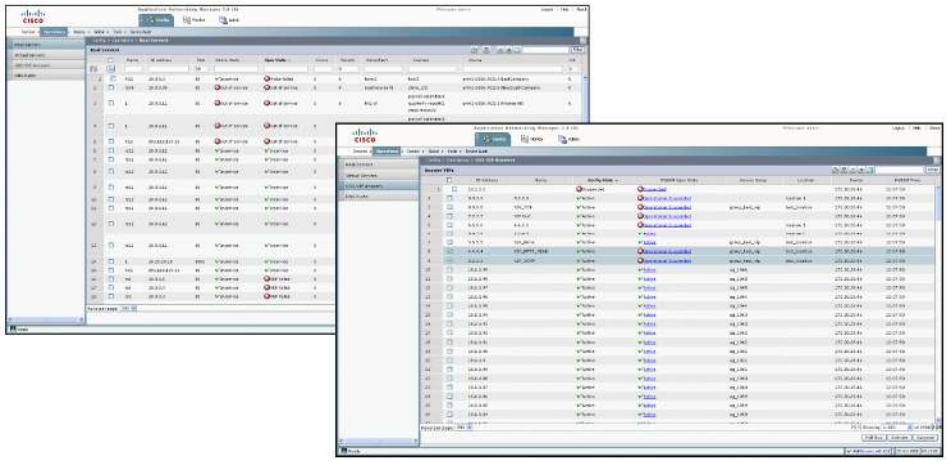
With these two features, the staff responsible for renewal of the certificates and related keys can acquire and put in place the necessary updates in a timely manner, thus avoiding service interruption due to expired certificate and key pairs.

Securely Delegated Operations Management

Cisco ANM enables productivity gains for service and server managers by offering four operation-specific displays through which managers can monitor their assigned virtual and real servers as well as global load-balancing virtual IP answers and DNS rules.

By taking advantage of Cisco ANM secure delegation capabilities, application and server managers can perform their daily management tasks, such as taking one or more real servers in or out of service, with options for graceful shutdown and cleared connections. They can do this without needing to know the type of network device that is supporting their servers (Cisco ACE, CSS, CSM, or CSM-S), the network topology, or other network operations. For clusters of Cisco ACE GSS devices, Cisco ANM enables centralized operations to activate and suspend virtual IP answers and DNS answer groups for global load balancing across one or more clusters of Cisco ACE GSS devices (Figure 3).

Figure 3. Cisco ANM Securely Delegated Operations



On a single screen, operators can monitor the administrative and operational state all their servers (server health) and the number of connections active on the servers (server utilization). For administrators and applications managers using the Cisco ACE GSS, Cisco ANM operations support for Cisco ACE GSS virtual IP answer and DNS answer groups enables many more simultaneous users to perform activation and suspension tasks than would be possible using the Cisco ACE GSS embedded manager.

For administrators who manage large numbers of devices, these displays include the capability to toggle filters on and off for any displayed data elements and custom configuration options, with a customization feature common to almost all Cisco ANM displays.

From the virtual server and real server displays, server managers can perform their daily management tasks, such as taking one or more servers in or out of service, with options for graceful shutdown and cleared connections. This delegated activation and suspension of servers eliminates the need for server managers to know the network topology or operations. In addition to Cisco ACE devices, this capability extends to Cisco CSS, CSM, and CSM-S devices, enabling operators to use Cisco ANM exclusively to perform these common tasks.

A significant advantage of the Cisco ANM virtual server and real server displays, as with all features in Cisco ANM, is that role-based access control (RBAC) can be used to securely delegate access to view or modify operations of any virtual or real servers.

Granular RBAC and Secure Access

Throughout all functions, Cisco ANM uses an administrator-defined RBAC security model that facilitates delegation of authority and responsibility for operations, administration, and monitoring of the managed devices, including activation and suspension of selected load-balanced servers. The Cisco ANM administrator can define with high granularity the tasks and options that are made available to individual users or user groups.

RBAC is used to administratively grant user authorization to access network resources, such as virtual contexts of Cisco ACE devices, content networking and load balancing, and SSL services, as well as individual application services. This feature eliminates unnecessary overhead between network administrators, network operations center (NOC) staff, systems operators, and server managers, enabling faster service deployment, simplifying the workflow within IT, and reducing configuration errors.

RBAC allows each virtual context in Cisco ACE to be managed by the appropriate business or IT team. Using Cisco ANM, an unlimited number of administratively defined domains can be created within each virtual context, providing further granularity for controlling resources within that virtual context or spanning multiple virtual contexts. Similarly,

Cisco ANM administrators can define and assign user roles that specify which of 34 defined actions a user can take against the network resources they can reach, such as configuration, editing and modification, and device and service monitoring. A set of predefined roles is provided with the product to speed implementation and provide examples that administrators can tailor to their specific needs.

Used in combination, domains and roles make it possible to control access and allow tasks based on the application, business department, or user. For example, network managers can be allowed to configure all operation variables, while the application and server owners can be allowed only to monitor and take specific virtual servers in and out of service for maintenance without risk to other IT configurations.

All user access to Cisco ANM is secured. Between the user's web browser and the Cisco ANM server, 128-bit full encryption SSL2 is used, so that authorized users can monitor, activate, and configure Layer 4 through 7 services remotely, even through firewalls. During login to Cisco ANM, users are authenticated either by local accounts created on Cisco ANM or (preferably) by TACACS+ or RADIUS remote authentication.

Cisco ACE Checkpoint Management and Centralized Backup and Restore

The Cisco ACE includes a checkpoint configuration feature at the context level to create configuration snapshots. The Cisco ACE stores the checkpoint for each context in a hidden directory in flash memory. These saved checkpoints can be applied to the Cisco ACE context to cause the running configuration to revert to the configuration in effect at the time the checkpoint was created.

For all Cisco ACE devices, Cisco ANM provides checkpoint management as a means to create configuration snapshots and subsequently apply that snapshot to quickly roll back the configuration to that held in a selected snapshot. Users can also use Cisco ANM to view the configuration stored in each saved checkpoint.

Checkpoints can protect the Cisco ACE system in cases in which a problem arises after configuration modification, especially when a complex set of configuration changes have been made in a short period of time. To prevent the need to reboot and reconstruct a good working configuration on a Cisco ACE after unsuccessfully modifying the running configuration, operators can more rapidly recover using a Cisco ACE checkpoint. Using the Cisco ANM checkpoint feature, operators can create a copy of a known stable running configuration before making modifications. Thereafter, if the modifications to the running configuration result in problems, the operator can use the checkpoint to roll back the configuration to the previous stable configuration in just moments.

For Cisco ACE Module A2.3(0) or higher, Cisco ANM 3.0 provides centralized backup and restore features that can create a backup of the running configurations for one or more entire Cisco ACE devices, including the running configuration, licenses, scripts, checkpoints, certificates, and keys (if they are exportable). Backup can be performed for one, many, or all contexts on one, many, or all Cisco ACE Modules running the required software release or higher. This global backup and copy function allows operators to back up the configuration and dependencies of multiple Cisco ACE devices simultaneously or copy existing backup configuration files from disk0 of multiple Cisco ACE devices to a remote server.

Additional Features

Discovery and Device Management

- IP and network discovery (using ping sweep, IP range, and Cisco Discovery Protocol)
- Credential discovery (using Secure Shell [SSH] Protocol, TACACS, and SNMP)
- Layer 2 and 3 connectivity
- Chassis, module, and appliance discovery (physical inventory and logical)
- Device import through add and delete operations
- Management of device access credentials

Global

- Configurable homepage for quick access to or saved direct login to commonly used task pages
- Logging of user activity for actions taken in Cisco ANM by users (who did what, when, and from where)
- RBAC role and domain support
- Debugging tool: snapshot of running Cisco ANM system and Cisco ACE configurations
- Support for system failover and high availability

Product Specifications

Table 1 lists the product specifications for Cisco ANM 3.0.

Table 1. Product Specifications

Product Parameter	Specification
Product Compatibility	Cisco ACE Module (both ACE10-6500-K9 and ACE20-MOD-K9) installed in Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Cisco ACE 4710 appliance, Cisco CSS, Cisco CSM, Cisco CSM-S, and Cisco ACE GSS as specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html.
Protocols	**For web client:** • Use HTTP or HTTPS. • For additional information, refer to the "Supported Web Browser" section of the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html. **For communication with managed devices:** See the specifications in the "Cisco ANM Ports Reference" section of the Installation Guide for Cisco Application Networking Manager 3.0 available at http://www.cisco.com/en/US/products/ps6904/prod_installation_guides_list.html.
Reliability and Availability	Cisco ANM High Availability (HA) is a configuration option for implementing Cisco ANM servers in a highly available active and standby mode. In this configuration, the active Cisco ANM server maintains a stateful synchronization with the standby Cisco ANM server so that if the active server fails, or if an administrative action failover occurs, the standby server can transparently take over operations.

System Capacity

Cisco ANM 3.0 is designed to support up to 50 Cisco ACE devices for full management, up to 40 Cisco CSS, CSM, and CSM-S devices for delegated activation and suspension of real and virtual servers with monitoring, and up to 3 clusters of Cisco ACE GSS. The exact number of devices supported depends upon the scale of operations on each device. For Cisco ACE devices, this value is weighted by the number of virtual contexts per Cisco ACE and the number of configured components and services within each virtual context (servers, server farms, health monitoring probes, and complexity of service configurations). For other devices, the value is weighted by the number of real and virtual servers (Cisco CSS, CSM, and CSM-S) and by the number of virtual IP answers, DNS rules, and cluster sizes (Cisco ACE GSS).

System Requirements

Table 2 lists the system requirements for Cisco ANM.

Table 2. System Requirements

Description	Specification
Server Hardware Requirements	• Generic PC • Equivalent of 3-GHz Pentium III CPU performance (dual processors and dual-core CPUs are supported) • 2 GB RAM • 60-GB minimum hard drive or fixed storage (80 GB or more recommended) • CD-ROM drive • One 100-Mbps Ethernet interface for single Cisco ANM configuration; two full-duplex interfaces for Cisco ANM high-availability configuration
Server Software Requirements	• Red Hat Enterprise Linux 5 (base server) Update 2 (5.2) or Update 3 (5.3) 32-bit Server Edition (Linux 2.6 kernel) is required for Cisco ANM 3.0 installation. • Cisco ANM upgrade from Cisco ANM 2.0 to Cisco ANM 3.0, but those operating on Red Hat Enterprise Linux 4.0 must upgrade to Red Hat Enterprise Linux 5 (base server) Update 2 (5.2) or Update 3 (5.3) 32-bit Server Edition (Linux 2.6 kernel), following the instructions provided in the Installation Guide for Cisco Application Networking Manager 3.0 available at http://www.cisco.com/en/US/products/ps6904/prod_installation_guides_list.html.
Client Hardware Requirements	As specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html.
Client Software Requirements	As specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html.

Ordering Information

The Cisco ANM server software (Cisco ANM-SERVER-30-K9) includes support for up to two Cisco ACE devices, each with up to five partitions (virtual contexts). Operations support for Cisco ACE GSS is included in the base Cisco ANM server software license. Additional licensing is available to expand the use of Cisco ANM up to system capacity or to add operations support for Cisco CSS, CSM, and CSM-S. Cisco ANM high-availability licensing should be used for installation on a hot standby Cisco ANM server for high availability.

To place an order, visit the Cisco Ordering homepage. Table 3 provides ordering information.

Table 3. Ordering Information

Part Number	Description
ANM-SERVER-30-K9	ANM Server Software
ANM-AD-005	ANM License For 5 ACE Devices
ANM-AD-010	ANM License For 10 ACE Devices
ANM-AD-020	ANM License For 20 ACE Devices
ANM-AD-050	ANM License For 50 ACE Devices
ANM-AV-020	ANM License For 20 VC On One ACE Device
ANM-AV-050	ANM License For 50 VC On One ACE Device
ANM-AV-100	ANM License For 100 VC On One ACE Device
ANM-AV-250	ANM License For 250 VC On One ACE Device
ANM-CD-010	ANM License For 10 CSS, CSM, or CSM-S Devices
ANM-CD-040	ANM License For 40 CSS, CSM, or CSM-S Devices
ANM-AV-UP1=	Upgrade ANM License—AV-020 To AV-050
ANM-AV-UP2=	Upgrade ANM License—AV-050 To AV-100
ANM-AV-UP3=	Upgrade ANM License—AV-100 To AV-250
ANM-SERVER-30-H-K9	ANM HA Server Software
ANM-AD-005-H	ANM HA License For 5 ACE Devices
ANM-AD-010-H	ANM HA License For 10 ACE Devices

Part Number	Description
ANM-AD-020-H	ANM HA License For 20 ACE Devices
ANM-AD-050-H	ANM HA License For 50 ACE Devices
ANM-AV-020-H	ANM HA License For 20 VC On One ACE Device
ANM-AV-050-H	ANM HA License For 50 VC On One ACE Device
ANM-AV-100-H	ANM HA License For 100 VC On One ACE Device
ANM-AV-250-H	ANM HA License For 250 VC On One ACE Device
ANM-CD-010-H	ANM HA License For 10 CSS, CSM, or CSM-S Devices
ANM-CD-040-H	ANM HA License For 40 CSS, CSM, or CSM-S Devices
ANM-AV-UP1-H=	Upgrade ANM HA License—AV-020 To AV-050
ANM-AV-UP2-H=	Upgrade ANM HA License—AV-050 To AV-100
ANM-AV-UP3-H=	Upgrade ANM HA License—AV-100 To AV-250

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services programs help you protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services and Cisco Advanced Services.

For More Information

For more information about Cisco ANM, visit http://www.cisco.com/go/anm or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-572610-00 12/09