Cisco Application Networking Manager Version 1.1

Cisco® Application Networking Manager (ANM) software enables centralized configuration, operations, monitoring, and reporting of Cisco data center networking equipment and services. Version 1.1 of Cisco ANM focuses on providing this management capability for the Cisco Application Control Engine.

Product Overview

Cisco ANM helps to manage multidevice data center network services effectively. Version 1.1 simplifies management of the Cisco Application Control Engine (ACE) virtualized environment, providing a unified interface for Cisco ACE troubleshooting, maintenance, operations, and performance monitoring.

Cisco ANM simplifies Cisco ACE provisioning through forms-based configuration management of Layer 4–7 virtualized network devices and services. With Cisco ANM, network managers are able to create, modify, and delete all of the virtual partitions of the Cisco ACE module, as well as control the allocation of resources among the virtual partitions. Within these virtual partitions, Cisco ANM enables complete configuration of the content networking and Secure Sockets Layer (SSL) services.

Cisco ANM enables rapid creation, modification, and prestaged or immediate deployment of common services by operators of all skill levels. Cisco ANM does this by including a varying set of provisioning forms for the basic, advanced, and expert user. Utilizing the basic forms, even operators new to the system can get value from their Cisco ACE systems “right out of the box” by provisioning the most common services quickly and easily (Figure 1).

Utilizing the advanced forms, a more knowledgeable user can just as easily exercise the more powerful features of Cisco ACE without having to master the Cisco ACE system itself. Even more advanced users can go a step beyond to the Cisco ANM expert mode to implement even the most intricate configurations of services while still gaining the security, audit ability, and error-reduction afforded by performing these tasks though the Cisco ANM graphical user interface or template-based configuration management.

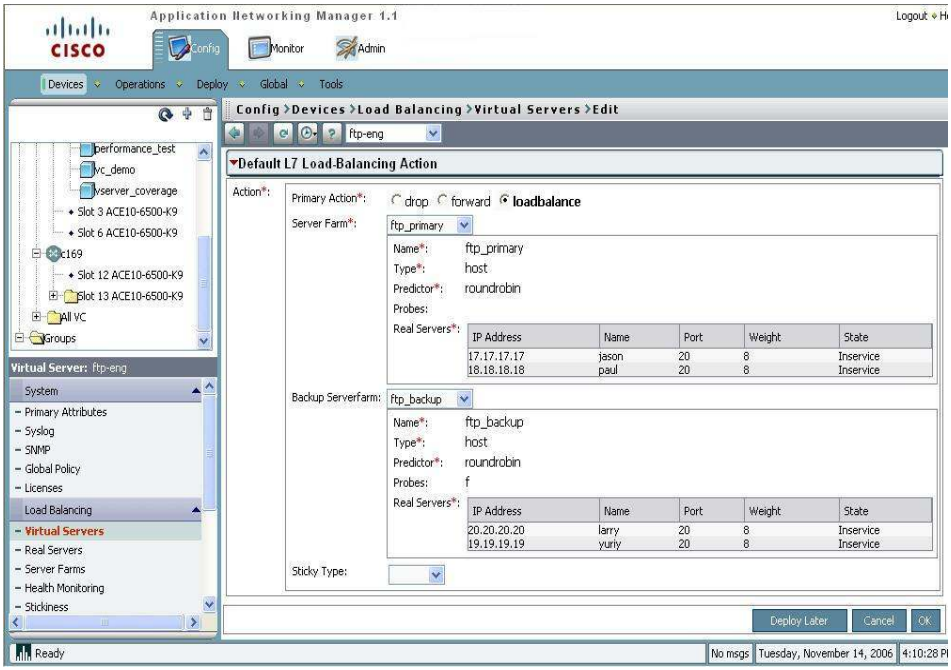
To help ensure compliance and synchronization and avoid “configuration drift,” Cisco ANM users can audit deployed configurations against the expected configurations.

Cisco ANM provides up-to-date information on the health, state, and utilization of the managed Cisco ACE modules, virtual partitions, and services through both real-time, current, and past device and service monitoring. Operations staff can use this monitoring to pinpoint the source of a potential problem. Systems and application managers can use these monitoring and reporting capabilities for performance management and resource planning.

Throughout all functions, Cisco ANM uses an administratively defined role-based access control (RBAC) security model that facilitates delegation of authority and responsibility for operations, administration, and monitoring of Cisco ACE, including activation and suspension of selected load-balanced servers. The Cisco ANM administrator can define which tasks and options are made available to individual users or user groups. Cisco ANM user auditing helps ensure that all activities by all users are securely logged and that this information is made available only to authorized users for audit purposes.

Cisco ANM is ideal for enterprises and service providers that implement Cisco ACE modules. These customers range from data center infrastructure providers, application service providers, and large enterprises to e-business data centers. Even small and medium-sized enterprises with small deployments of Cisco ACE can take advantage of the benefits of Cisco ANM through the entry-point offering.

Figure 1. Cisco ANM Virtual Server Configuration



Key Features and Benefits

Device and Service Configuration

With the introduction of virtual partitions, up to 250 per module, the Cisco ACE module allows exceptional control of the application-delivery infrastructure. For each virtual partition, administrators can tune the processing resources—such as bandwidth, connection setup rate, SSL transaction rate, and syslog rate—as well as many memory resources, such as the number of concurrent connections and access control lists (ACLs) and so on. Thus, business organizations, customers and subscribers, and applications can all share a physical Cisco ACE module with complete isolation among them.

Cisco ANM empowers multiple concurrent operators and administrators with the ability to turn on a new application or service within these virtual partitions, or modify an existing one, with a few clicks rather than going through tedious, time-consuming processes of selecting, qualifying, deploying, and troubleshooting a new device.

Cisco ANM supports robust Layer 4–7 configuration of Cisco ACE modules. To accomplish this, Cisco ANM employs forms from which users can select which features and functions to invoke for any particular service being implemented. For each of the features and functions selected, Cisco ANM guides the user through the configuration by presenting only the appropriate configuration selections that may apply, offering default configuration choices as well as options for the user to specialize the configuration.

These forms support configuration of virtual contexts, resource class management, and load-balancing services including ACLs, real servers, server farms, sticky groups, and health monitoring along with the service bindings to the hosting Cisco Catalyst® 6500 Series Switch VLAN interfaces. The forms also support configuration of SSL services including certificate and key management, chain groups, certificate signing requests, and proxy services. Cisco ANM extends these configuration capabilities to the configuration of redundant Cisco ACE modules themselves.

For expert users seeking to implement the more powerful functionality possible in Cisco ACE without using the command-line interface (CLI) or utilizing programmatic methods, Cisco ANM template-based provisioning speeds deployment of configurations that are more complex and supports the standardization of those configurations for devices, virtual partitions of devices, and services. Because templates can be created through the expert mode interface or by “cloning” existing configurations, even configurations created by the basic or advanced forms-based provisioning can become templates and then expanded upon to support more intricate, specialized service implementations.

Once created, the configuration within a template can be protected from further editing by the use of version “tagging.” This helps ensure that what was put in a template and used for service creation or auditing will not change in the future without clear traceability. This enables the proper audit control and, when necessary, rapid rollback of erroneous or problematic configuration deployment. By using this capability, it is also possible for organizations to work step by step toward eliminating variation in their operations, an important factor in increasing network and service reliability while also reducing overall operational expenses.

For systems established prior to the deployment of Cisco ANM, it provides the capability to discover all chassis, modules, virtual partitions, and service definitions across a large number of systems.

All of these configuration tasks can be performed using a secure Web-based GUI, eliminating the need to use the Cisco ACE module’s CLI.

Operations—Delegated Server Management

Cisco ANM provides productivity gains for services and server managers by offering two operations-specific displays where they can monitor their assigned virtual and real servers. On a single screen, operators can monitor the administrative and operational state of all their servers (that is, the servers’ health), as well as the number of connections active on their servers (that is, the servers’ utilization).

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

From the virtual server and real server operations displays, server managers can also perform their daily management tasks, such as taking one or more servers in and out of service, with options for graceful shutdown or cleared connections. This delegated activation and suspension of servers eliminates any need for server managers to have knowledge of the network topology or operations.

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

Granular RBAC, Secure Access, and User Auditing

A granular user access model, RBAC, is used to administratively segment authorized user-group access to network resources such as virtual partitions of Cisco ACE modules, content networking and load balancing, and SSL services, as well as to individual application services. This removes unnecessary overhead between network administrators, network operations center (NOC) staff, systems operators, and server managers, which enables faster service deployment, simplifies workflow within IT, and reduces configuration errors.

RBAC allows each virtual partition 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 partition, providing further granularity for controlling resources within that virtual partition or spanning multiple virtual partitions. Similarly, Cisco ANM administrators can define and assign user roles that specify which actions a user can take against the network resources they can reach, such as configuration creation, editing and modification, deleting, monitoring, and reporting.

Used in combination, these domains and roles make it possible to control access and allow tasks based on application, business organization, or user. For example, network managers can be allowed to configure all operations variables while the application and server owners can be allowed only to monitor, report on, and take specific virtual servers in or out of rotations 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 Secure Sockets Layer 2 (SSL2) is used so that authorized users can monitor, activate, and configure Layer 4–7 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.

To complete the security environment, Cisco ANM also records the configuration changes that users make to devices into an audit log file. This helps ensure that a clear record of who changed what and when is maintained. This log is stored in a secure file not accessible by nonauditor user roles. User auditing enables secure tracking of who did what, when, and to which devices and services.

Monitoring and Reporting

Cisco ANM provides a series of up-to-date, at-a-glance health and performance monitoring displays of the Cisco ACE infrastructure, which saves time and resources in daily operations while also aiding in troubleshooting and problem resolution. Customizable monitoring and reporting displays include a variety of monitoring data including event notifications for user-defined threshold-crossing alerts.

A Virtual Context Management display provides real-time data showing the status of the virtual partitions across all managed Cisco ACE modules. In the same manner, the Chassis Management display shows the device status along with model and Cisco IOS® Software version data for the hosting Cisco Catalyst 6500 Series chassis.

The monitoring and reporting displays (which can also be exported or printed) give the operators the basic information necessary to perform Cisco ACE infrastructure performance and utilization analysis, enable service usage reporting, as well as forecast and plan for resource demand.

Product Specifications

Table 1 lists the product specifications for Cisco Application Networking Manager 1.1.

Table 1. Product Specifications

Product Parameter	Specification
Product Compatibility	Cisco ACE Service Module (ACE10-6500-K9) installed in Cisco Catalyst 6500 series switches as specified in the Supported Devices Table for the Cisco Application Networking Manager 1.1
Software Compatibility	Cisco ANM 1.1 supports Cisco ACE modules running software version 3.0(0)A1(3)
Protocols	**For Web client:** • HTTPS/SSHv2 **For communication to Cisco ACE module:** • HTTPS/SSHv2/XML (read and write) • SNMPv2c, SNMPv3/MD5-DES (read-only) • Syslog over User Datagram Protocol (UDP) or TCP (inbound notifications only)
Reliability and Availability	ANM-HA is a configuration option for implementing Cisco ANM servers in a highly available active/standby mode. In this configuration, the active Cisco ANM server maintains a stateful synchronization with the standby Cisco ANM server so if the active server fails, or an administrative action “failover” occurs, the standby server will take over operations.
Programming Interfaces	A Web Service Description Language (WSDL)–based API is not generally available with Cisco ANM 1.1 and is available only through special accommodation. If you are interested in such an API, ask your Cisco account manager for further information.

System Capacity

Cisco ANM 1.1 is designed to support between 4 and 40 Cisco ACE modules, deployed across as many as 20 Cisco Catalyst 6500 Series chassis. The exact number of modules supported depends upon the scale of operations on each module as weighted by the number of virtual partitions per module and the number of configured components and services within each virtual partition (servers, server farms, health monitoring probes, and complexity of service configurations).

Features

Discovery and Device Management

- IP/network discovery (ping sweep, IP range, Cisco Discovery Protocol)
- Credential discovery (Secure Shell [SSH] Protocol, TACACS, Simple Network Management Protocol [SNMP])
- Layer 2 and 3 connectivity
- Chassis and module discovery (physical/inventory, logical)
- Device import through seed file, add/delete operation
- Managing device access credentials

Provisioning

- Virtual context administration and resource assignment
- Forms-based configuration (server load balancing, SSL, security, Cisco Catalyst 6500 Series Switch connectivity)
- Templates: context creation, versioning and upgrade support
- Auditing out-of-band changes, comparing template and device configuration
- Service activation and suspension

Monitoring and Reporting

- Monitoring and reporting of health, utilization, and performance of virtual partitions and services
- Monitoring through syslog, trap, SNMP polling
- Threshold-crossing alerts (to alerts page)
- Monitoring of faults and events (to alerts page)

Global

- RBAC, domain support, user activity audit
- Debugging tool: snapshot of running Cisco ANM system and devices
- System failover support and high availability
- System backup and restore

System Requirements

Table 2 lists the system requirements for Cisco Application Networking Manager.

Table 2. System Requirements

Description	Specification
Server Hardware Requirements	• Generic PC • Equivalent of 3 GHz Pentium III CPU performance (dual processors or dual-core CPUs are supported) • 2 GB of RAM • 30 GB minimum, 80 GB+ recommended hard drive/fixed storage • 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	• Server OS: Red Hat Enterprise Linux v.4 Enterprise Server (ES) 4 Update 2 or later or Advanced Server (AS) V4 Update 2 or later. (Linux 2.6 kernel) • Additional server software requirements: Sun Java 2 Platform Standard Edition (J2SE) 5.0
Client Hardware Requirements	• IBM PC-compatible computer with 300 MHz or faster Pentium • Solaris SPARCstation or Sun Ultra 10 with 333 MHz processor • 256 MB of RAM (minimum)
Client Software Requirements	**Client OS requirements:** • Windows 2000 Server or Professional Edition with Service Pack 4 • Windows XP Professional with Service Pack 1 with Microsoft Virtual Machine • Solaris 8 and Solaris 10 OS **Client browser requirements:** • Microsoft Internet Explorer 6.0, Service Pack 1 on Windows 2000 Server, Professional, or Advanced Server with Service Pack 4 • Firefox 1.5 on Windows, Linux, Solaris 8 and Solaris 10 • All browsers require cookies enabled and DHTML enabled

Ordering Information

To place an order, visit the Cisco Ordering Home Page. Table 3 lists ordering information.

Table 3. Ordering Information

Part Number	Product Description
ANM-SERVER-11-K9	ANM Server Software
ANM-AD-005-11	ANM License For Up To 5 ACE Devices
ANM-AD-010-11	ANM License For Up To 10 ACE Devices
ANM-AD-020-11	ANM License For Up To 20 ACE Devices
ANM-AD-050-11	ANM License For Up To 50 ACE Devices
ANM-AV-020	ANM License For 20 VC On One ACE
ANM-AV-050	ANM License For 50 VC On One ACE
ANM-AV-100	ANM License For 100 VC On One ACE
ANM-AV-250	ANM License For 250 VC On One ACE
ANM-AD-UP1=	Upgrade ANM License - AD-005 To AD-010
ANM-AD-UP2=	Upgrade ANM License - AD-010 To AD-020
ANM-AD-UP3=	Upgrade ANM License - AD-020 To AD-050
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

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 help you to 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 or Cisco Advanced Services.

For More Information

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

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

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C78-384173-02 01/08

