Cisco Application Networking Manager Version 2.0

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

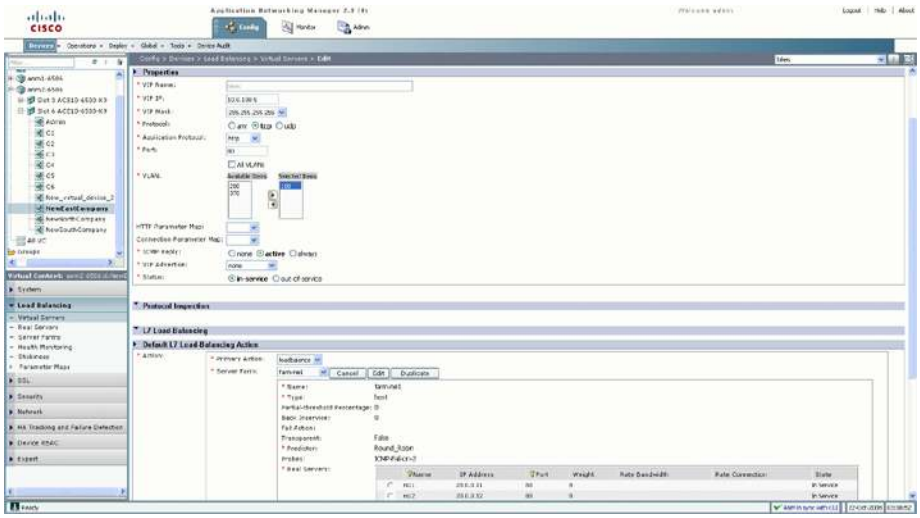
Product Overview

Cisco ANM helps to manage multidevice data center network services effectively. Version 2.0 simplifies management of the 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 ACE, CSS, CSM, and CSM-S devices. ANM also centralizes operation management of virtual IP (VIP) answers and DNS rules for GSS devices.

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 are able to create, modify, and delete all virtual contexts of the Cisco ACE, as well as control the allocation of resources among the virtual contexts. Within these virtual contexts, Cisco ANM enables 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. It does this by including a varying set of provisioning forms for the basic, advanced, and expert user. Using 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).

Figure 1. Cisco ANM Virtual Server Configuration



Using the advanced forms, a knowledgeable user can easily exercise the more powerful features of Cisco ACE without having to master the Cisco ACE system itself. Advanced 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 graphical user interface or building block–based configuration management.

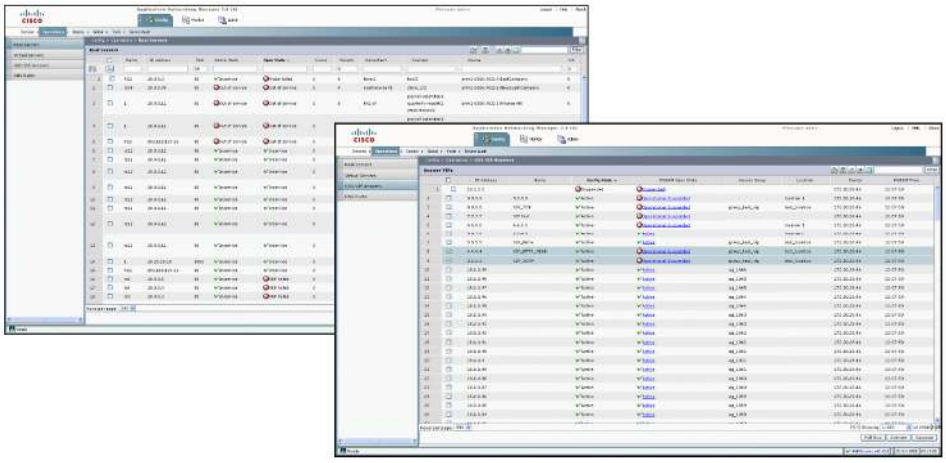
Cisco ANM provides up-to-date information on the health and state of all ANM-managed devices, virtual contexts, and services through real-time device and service monitoring, allowing operations staff to use this monitoring to pinpoint the source of a potential problem.

Throughout all functions, Cisco ANM uses an administrator-defined role-based access control (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.

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 or cleared connections. They can do this without needing to know the type of network device that is supporting their servers (ACE, CSS, CSM, or CSM-S), the network topology, or other network operations.

ANM version 2.0 expands this centralized operations support to include the ability to activate and suspend VIP answers and DNS answer groups for global load balancing across one or more clusters of GSS devices (Figure 2).

Figure 2. Cisco ANM Securely Delegated Operations



Cisco ANM is ideal for enterprises and service providers that implement Cisco ACE, as well as providing additional value to customers utilizing Cisco CSS, CSM, CSM-S, or GSS devices. 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.

Key Features and Benefits

Device and Service Configuration

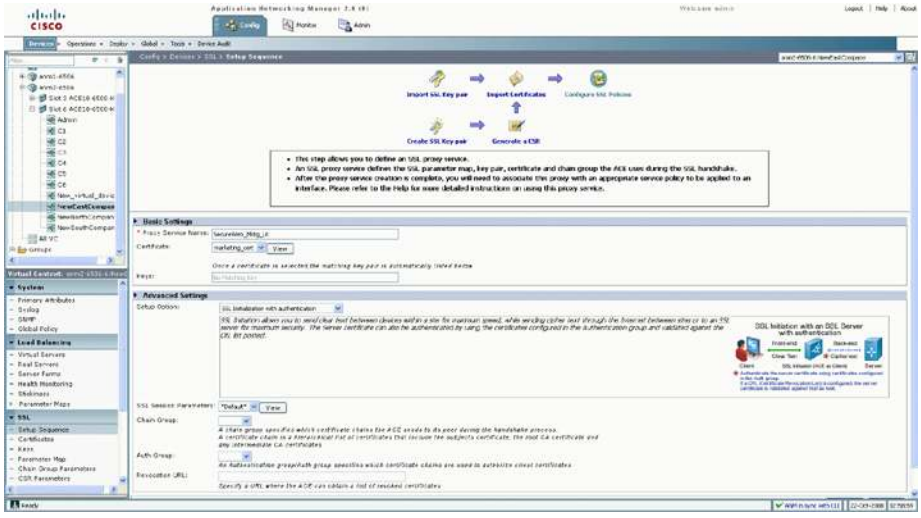
The introduction of virtual contexts, up to 250 per Cisco ACE, allows exceptional control of the application-delivery infrastructure. For each virtual context, administrators can tune the processing resources—such as bandwidth, connection setup rate, SSL transaction rate, and syslog rate—as well as many memory resources, such as the number of concurrent connections and access control lists (ACLs). Thus, business organizations, customers, subscribers, and applications can all share a physical Cisco ACE while being completely isolated from one another.

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

Cisco ANM supports robust Layer 4 through 7 configuration of Cisco ACE devices. To accomplish this, it 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 customize 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 and Cisco 7600 Router VLAN interfaces for the Cisco ACE. Cisco ANM extends these capabilities to the configuration of redundant Cisco ACE devices. For SSL services, including key management, chain groups, certificate signing requests, and proxy services, a wizard-based interface guides the user through the configuration tasks (see Figure 3).

Figure 3. Cisco ANM SSL Configuration Wizard



Cisco ANM's global "building-blocks" feature speeds deployment of common configuration components and supports 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 Cisco ANM deployment.

All of these configuration tasks can be performed using a secure web-based GUI, eliminating the need to use the Cisco ACE command-line interface (CLI).

Operations—Delegated Server Management

Cisco ANM provides productivity gains for services and server managers by offering four operations-specific displays where they can monitor their assigned virtual and real servers, as well as global load-balancing VIP answers and DNS rules.

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

For administrators who manage large numbers of devices, these displays include the ability to toggle filters on and off 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 the need for server managers to know the network topology or operations. In addition to ACE devices, this capability spans CSS, CSM, and CSM-S devices, enabling operators to use ANM exclusively to perform this common task.

A significant advantage of 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 and Secure Access

A granular user access model, 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 removes 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 creation, editing and modification, or 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, 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 and take specific virtual servers in or 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.

Monitoring

Cisco ANM provides a series of up-to-date, at-a-glance health and performance monitoring displays of the managed device infrastructure, saving time and resources in daily operations while also aiding in troubleshooting and problem resolution.

Monitoring provides system view, traffic summary, resource usage view, VIP service path, load-balancing statistics, and application acceleration views. These views are available on a per-context basis (for ACE) as well as at the device group level. Monitoring views are supported for ACE, CSS, CSM, and CSM-S devices. 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 and Cisco 7600 chassis.

User-definable threshold crossing alerts can be set 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 via Simple Network Management Protocol (SNMP) trap, email, or both.

Product Specifications

Table 1 lists the product specifications for Cisco Application Networking Manager 2.0.

Table 1. Product Specifications

Product Parameter	Specification
Product compatibility	Cisco ACE Service 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 Content Services Switch, Cisco Content Switching Module, Cisco Content Switching Module with SSL, and Cisco ACE Global Site Selector as specified in the *Supported Devices Table for the Cisco Application Networking Manager 2.0*
Protocols	**For web client:** • HTTP or HTTPS **For communication with Cisco ACE devices:** • HTTPS/Secure Shell (SSH) version 2/XML (read and write) • SNMP version 2c (read-only) • Syslog over User Datagram Protocol (UDP) or TCP (inbound notifications only) For details, refer to the *Supported Devices Table for the Cisco Application Networking Manager 2.0*
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 that if the active server fails, or an administrative action "failover" occurs, the standby server can seamlessly take over operations.

System Capacity

Cisco ANM 2.0 is designed to support up to 50 Cisco ACE devices for full management, up to 40 CSS, CSM, and/or CSM-S devices for delegated activation/suspension of real and virtual servers with monitoring, and up to 3 clusters of GSS. The exact number of devices supported depends upon the scale of operations on each device. For ACE devices, this is weighted by the number of virtual contexts per 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, it is weighted by the number of real and virtual servers (CSS, CSM, and/or CSM-S) and by the number of VIP answers, DNS rules, and cluster sizes (GSS).

Features

Discovery and Device Management

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

Provisioning

- Virtual context administration and resource assignment
- Forms and/or wizard-based configuration (server load balancing, application acceleration, SSL, security, and connectivity to Cisco Catalyst 6500 Series Switch and Cisco 7600 connectivity)
- Logging of all configuration and operations actions

Operations

- Securely delegated service and global load balancing activation and suspension

Monitoring and Logging

- Monitoring of health and utilization of virtual contexts and services
- Monitoring through syslog, SNMP, and CLI polling
- Threshold-crossing alerts (to alerts page and external notification via trap, email, or both)
- Monitoring of faults and events (to monitoring and notifications pages)
- Logging of all user activity for all actions taken in ANM by all users (who did what, when, from where)

Global

- RBAC role and domain support
- Debugging tool: Snapshot of running Cisco ANM system and ACE configurations
- Support for system failover 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 RAM • 60-GB minimum, 80-GB+ recommended hard drive/fixed storage • CD-ROM drive • One 100-Mbps Ethernet interface for single Cisco ANM configuration, 2 full-duplex interfaces for Cisco ANM high-availability configuration
Server software requirements	• Red Hat Enterprise Linux AS 5 Update 2 (5.2) 32-bit Server Edition is required for all new Cisco Application Networking Manager installation. • Cisco Application Networking Manager upgrade from ANM 1.2 to ANM 2.0 will continue to support servers running Red Hat Enterprise Linux 4.2/4.5 as supported by ANM 1.2. Migration to Red Hat Enterprise Linux AS 5 Update 2 is highly recommended.
Client hardware requirements	As specified in the *Supported Devices Table for the Cisco Application Networking Manager 2.0*
Client software requirements	As specified in the *Supported Devices Table for the Cisco Application Networking Manager 2.0*

Ordering Information

The ANM server software (ANM-SERVER-20-K9) includes support for up to two ACE devices, each with up to five partitions (Virtual Contexts) each. Operations support for the GSS is included within the base ANM server software license. Additional licensing is available to expand the use of ANM up to system capacity or to add operations support for CSS, CSM and CSM/S. ANM “HA” licensing should be used for installation on a hot stand-by ANM server for high availability.

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-20-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-20-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	Product 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 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.
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 C78-507112-00 11/08