CHAPTER 9

IOS® Software and Network Management

Cisco IOS® Software and Network Management at a Glance

Product	Features	Page
Cisco IOS Software	Feature-rich network operating system supported on wide range of Cisco products • Provides a common IP fabric, functionality, and command-line interface (CLI) across network infrastructures • Enables a vast array of key routing, multiservice, traffic shaping, security/firewall, and traffic monitoring applications, and a broad variety of network connections	9-3
CiscoWorks Small Network Management Solution	Web-based network management solution designed for small to medium businesses (SMB) • Device auto-discovery using SNMP simplifies setup and reduces startup time • Standards-based, multi-vendor management • Event management and topology mapping application • Includes Cisco's popular CiscoView Element Management Tool	9-9
CiscoWorks LAN Management Solution	Provides key applications needed to manage Cisco switch-based Enterprise campus networks. This bundle includes: • Campus Manager • Device Fault Manager • Resource Manager Essentials • CiscoView	9-11
CiscoWorks VPN/Security Management Solution	Combines general device management tools for configuring, monitoring, and troubleshooting enterprise networks with powerful security solutions for managing virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). CiscoWorks VMS is organized into several functional areas: • Firewall Management • IDS Management, network and host-based • Host Intrusion Prevention System Management • VPN Router Management • Security Monitoring • VPN Monitoring • Operational Management	9-12
CiscoWorks Security Information Management Solution and CiscoWorks Security Information Management Solution Engine	A solution that collects, analyzes, and correlates security event data from across the enterprise-letting you detect and respond to security events as they occur. The hardware-based solution engine option provides the same features and functions as the CiscoWorks SIMS software on a dedicated appliance. The Solution Engine requires minimal setup and installation. • Event monitoring of multivendor security environments • Extensive reporting for operators and high-level administrators • Risk assessment information to understand overall vulnerability of critical network assets within the enterprise • Forensics tools to investigate attacks	9-14
CiscoWorks Network Connectivity Center	• A suite of network and service management software that manages increasingly complex and distributed networks and IT environments in alignment with business priorities. Leveraging sophisticated modeling, analysis, and automation technologies, itprovides end-to-end insight into how the intelligent network health relates to key business services. It automatically pinpoints service-affecting faults and calculates their business impacts, therefore minimizing service downtime while lowering operating cost and reducing business risk. The suite includes: Cisco NCC Network Connectivity Monitor (NCM); NCM Global Console; Cisco NCC Application Services Manager (ASM); Cisco NCC Application Connectivity Monitor (ACM); Cisco NCC Business Impact Manager (BIM); Cisco NCC ATM/Frame Relay Availability Manager; Cisco NCC MPLS VPN Manager; Cisco NCC Routing Protocol Services Manager (RPSM); Cisco NCC Report Manager; Cisco NCC Adapters; Cisco NCC Business Dashboard	9-15

Product	Features	Page
CiscoWorks Manager IP Telephony Environment Monitor	A suite of telephony management applications that ensures the readiness and manageability of converged networks supporting VoIP and IP telephony traffic and applications. It enables operations and administrative personnel to check the state and operational health of key resources in their converged networks that support IP telephony implementations. The bundle includes: • Voice Health Monitor • Default Fault Manager • CiscoView and Downloadable Modules: • IP Phone Information Utility • IP Phone Help Desk Utility • Gateway Statistics Utility • WAN Performance Utility • Tactical Graphics Utility	9-17
CiscoWorks Voice Manager for Voice Gateways	Enables the management and monitoring of devices used as gateways between analog voice equipment and the data network. • Enhanced capabilities to configure and provision voice ports • Create and modify dial plans on voice-enabled Cisco routers for voice over IP (VoIP), voice over Frame Relay (VoFR), and voice over ATM (VoATM) network deployments	9-19
CiscoWorks QoS Policy Manager (QPM)	Enables centralized administration and automated deployment of bandwidth reservation and prioritization policies for network applications across converged voice, video and data networks. • Differentiates services of Web applications, voice traffic, and business-critical applications • Validate QoS settings and results with traffic analysis • Real time and historical reports for QoS troubleshooting • Control roles and privileges for policy view, modification and deployment	9-20
CiscoWorks Wireless LAN Solution Engine	A hardware based wireless LAN management solution that provides template-based configuration with user-defined groups to effectively manage a large number of access points and bridges • Monitors LEAP authentication servers • Enhances security management through mis-configuration detection on access points and bridges	9-22
CiscoWorks Hosting Solution Engine	A hardware-based content management solution for e-business operations in Cisco-powered data Centers. This product provides network infrastructure monitoring and Layer 4-7 hosted services configuration and activation. • Flexible security model offers tiered user access to server management	9-23
Cisco Catalyst 6500 Series Network Analysis Modules 1 and 2	NAM is an integrated, network monitoring instrumentation and Web-browser based traffic analysis solution for the Catalyst 6500 based environments. It enables greater visibility into traffic at all layers of the network by providing real time traffic analysis and troubleshooting capabilities.	9-24
Cisco Network Analysis Module for Branch Routers - Cisco 2600/3660/3700 Series Network Analysis Module	The Cisco 2600/3660/3700 Series NAM is an integrated traffic-monitoring network module that enables network managers to gain application-level visibility into network traffic with the ultimate goal of improving performance, reducing failures, and maximizing return on network investments.	1-1
Cisco Secure User Registration Tool (URT)	Provides organizations with increased LAN security by actively identifies users within the network and creates user registration policy bindings that help support mobility and tracking: • Ensures that users are associated with their authorized subnet/VLAN • Addresses the challenges associated with campus user mobility • Supports Web-based authentication for Windows, Macintosh, and Linux client platforms • Secure user access to the VLAN with MAC address-based security option to allow multiple users connected to a hub access to a VLAN served by single switch port	5-13
Cisco Secure Access Control Server (ACS) for Windows and Cisco Secure Access Control Server Solution Engine	Cisco® Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. An important component of the Cisco Identity-Based Networking Services (IBNS) architecture. It supports several access connection types, including wired and wireless LANs, dialup, broadband, content, storage, voice over IP (VoIP), firewalls, and VPNs. It helps ensure enforcement of assigned policies by allowing network administrators to control: • Who can log in to the network • Privileges each user has in the network • Security audit or account billing information that is recorded	5-10
Cisco IOS Tools	List of essential IOS web-based tools available on Cisco.com	9-9

Cisco IOS® Software

The family of Cisco IOS Software products (T, S and XR) enables Cisco to meet the network infrastructure requirements of Large and Small Enterprises, as well as Service Providers, because each software product is architected to meet the needs of a given customer type. Customers benefit from shared intellectual property and technologies between family members and all Cisco IOS products deliver the consistent look and feel.

Key Features

- Availability—Automatically recover from errors; adapt to network infrastructure changes
- Security—Protects network devices allowing them to remain operative, and thereby controllable, even during an attack
- Manageability—Instrumentation required to manage devices, technologies and network
- Flexibility—Adapts to evolving requirements
- Scalability—Allows networks to expand in size and capability

Security

Cisco IOS network security is integrated into Cisco switches, routers, and wireless access devices to protect the network and secure information. It delivers a sophisticated set of security capabilities such as Encrypted IPSEC VPNs , Firewall , Intrusion Detection Systems , Trust & Identity, 802.1x Wireless LAN Security, some of which may be hardware-assisted. Cisco IOS security technologies work with Cisco security appliances to provide the right type of security, where customers need it most.

High Availability

Cisco offers a comprehensive solution to High Availability Networking (HAN) that minimizes network outages and ensures non-stop access to the most business critical applications. Cisco HAN takes a network-wide approach, delivering the most cohesive and collaborative solution to maintain high network availability. Cisco's software using various technologies targets potential causes of downtime allowing customers to build networks with a high Mean Time Between Failure and a low Mean Time To Recovery

Management Instrumentation

Cisco IOS Software provides a rich set of embedded features that enable customers to efficiently measure and manage network and application bandwidth to set and meet performance expectations. Whether using Cisco IOS SNMP MIBs with centralized network management software, purposed appliances, or making changes to configurations with Cisco IOS CLI, the management instrumentation benefits operators in all areas of the network. It rapidly incorporates new network services and devices; Reduces downtime with adaptive fault management; and, enables SPs to manage the performance of differentiated services, while Enterprises can verify the SLAs they purchase.

Routing

Cisco IOS Software offers the industry's widest variety of enterprise and service provider-class routing protocols. Protocols that provide for integration, and are integrated with each other, enable the convergence of data, voice and video networking. Routing Technology's adaptive behavior enables customer networks to evolve with user needs. It is critical to scalability and allows networks to expand in size and capability, while preserving hardware and network investments. The technology includes Optimized Edge Routing (OER), On Demand Routing (ODR), Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), IP Multicast, Integrated IS-IS, Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP).

Multicast

Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast technologies include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

Key Features

- Efficiently deploys and scales distributed group applications across the Internet
- Creates a ubiquitous, enterprise-wide content distribution model
- Solves traffic congestion problems
- Allows service providers to deploy value-added streaming services that leverage their existing infrastructure.

Multiprotocol Label Switching (MPLS)

Cisco pioneered Multi protocol Label Switching (MPLS) and has made it available in Cisco IOS Software for significant advantages in applications like virtual private networks (VPNs) and traffic engineering. It enables service providers to offer many new services to customers at lower costs, replaced some Frame Relay, leased line and Asynchronous Transfer Mode (ATM) services that were not cost-effective, and converged services onto one network. It fuses intelligent routing capabilities with the performance of switching. It provides significant benefits to networks with pure IP architectures and those with IP and ATM or a mix of other Layer 2 technologies.

MPLS technology is key to implementing scalable Virtual Private Networks (VPNs) and end-to-end QoS, enabling efficient utilization of existing networks to meet growth needs and to rapidly correct link fault and node failure. This technology also helps deliver highly scalable, differentiated IP services with simpler configuration, management, and provisioning for both Internet service providers and end-user customers.

For More Information

See the Cisco IOS MPLS Web site: **http://www.cisco.com/go/mpls**

Quality of Service (QoS)

QoS is the set of techniques to manage network resources. Achieving the required QoS by managing delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. QoS is the set of techniques to manage network resources. IOS does this through following features:

- Differentiated Services—Performs Packet classification based on IP precedence and QoS group setting and Bandwidth management through various rate limiting features
- Integrated Services—IOS does through RSVP typically perform admission control, Classification, policing, and scheduling of data packets on a per-flow basis and keeps a database of information for each flow
- Network-Based Application Recognition—IOS does this in two steps Intelligent classification engine used with class-based features and Protocol Discovery and analysis

IPv6

IPv6—Internet Protocol version 6—is the next generation of the protocol that runs the Internet. IPv6 is currently a set of draft standards in the Internet Engineering Task Force (IETF). IPv6 is designed to improve upon IPv4's scalability, ease-of-configuration, and re-introduce the original TCP/IP benefits for global networking. Fundamentally, IPv6 expands network addressing from the current 32-bit address length to 128-bit, accommodating future growth in IP devices and users. The 128 bits provide approximately 3.4 x 1038 addressable nodes, enough to allocate over a million addresses per person on the planet.

For More Information

See the Cisco IOS IPv6 Web site: **http://www.cisco.com/go/ipv6**

IOS Packaging and Licensing

Cisco IOS Software code is continuously refreshed and maintained to adapt to the changing needs of customers, and the evolution of markets. Software refresh occurs to ensure new features work with existing ones, make existing features work better together, improve platform performance, and optimize for device memory. As of Cisco IOS 12.3, customer needs are better suited with updated framework for feature sets, reduced in number from forty-four to eight, Refined and simplified as of 12.3, subsequent releases will improve the release selection experience due to fewer feature sets, and the consistency of feature set naming and feature inheritance.

The new features set framework is available on Cisco 1700, 2600XM, 2691, and 3700 Series Routers as of Cisco IOS Software 12.3.

The Principle of Feature Inheritance

Cisco IOS Packaging inherits all of the Cisco IOS Software features and services available in the packages below it, offering customers a clear migration and upgrade path.

Feature Set Naming Conventions

The new package names emphasize the inheritance characteristics of Cisco IOS Packaging. They also provide a high-level feature content description of the new packages, which further simplifies the image selection process. The new packages are introduced as upgrade and migration opportunities in Cisco IOS Software Release 12.3[1].

1. Cisco 1720, Cisco 2600 non-XM, and the Cisco 3600 Router Series do not support Cisco IOS Packaging in Release 12.3

New Naming Convention Categories

Category	Naming Convention
Base	Entry level image, (i.e., IP Base)
Services	Addition of IP Telephony Service, MPLS, Net Flow, Voice over IP (VoIP), Voice over Frame Relay (VoFR), and ATM (i.e., SP Services, Enterprise Services)
Advanced	Addition of VPN, Cisco IOS Firewall, 3DES encryption, SSH, Cisco IOS IPSEC and Intrusion Detection Systems (IDS) (i.e., Advanced Security, Advanced IP Services)
Enterprise	Additional of multi-protocols, including IBM, IPX, AppleTalk (i.e., Enterprise Base, Enterprise Services)

Cisco IOS Packaging Platform Support

Platforms that migrate to the new packaging framework with target packages

	IP Base	IP Voice	Advanced Security	Advanced IP Services	SP Services	Enterprise Base	Enterprise Services	Advanced Enterprise Services
Cisco 3745	X	X	X	X	X	X	X	X
Cisco 3725	X	X	X	X	X	X	X	X
Cisco 2691	X	X	X	X	X	X	X	X
Cisco 2600 XM Series	X	X	X	X	X	X	X	X
Cisco 1751-V, 1760	X	X	X	X	X	X	X	X
Cisco 1721, 1751	X		X			X		

Cisco IOS Trains

A Cisco IOS train is a vehicle for delivering releases that evolve from a common code base. In recent years, with the addition of thousands of new features, hundreds of new applications, and a wide array of platforms, Cisco IOS Software diversified from one train of releases to multiple trains supporting different feature sets for different customer needs.

Types of Trains

Cisco IOS releases are delivered on the following types of trains

Train	Description	Examples
mainline	Consolidates releases and fixes defects. Inherits features from the parent T train, and does not add additional features.	12.2, 12.3
T	Introduces new features and fixes defects.	12.3T
S	Consolidates 12.1E, 12.2 mainline, and 12.0S, which supports high-end backbone routing, and fixes defects.	12.0S, 12.2S
E	Targets enterprise core and SP edge, supports advanced QoS, voice, security, and firewall, and fixes defects.	12.1E
B	Supports broadband features and fixes defects.	12.2B, 12.3B

Bug Synchronizing and Feature Integration

Bug fixes to maintenance releases on a mainline train are synchronized with subsequent maintenance releases on the child T train. New features are integrated into the T train only-the mainline train receives bug fixes only.

Train Lifecycle Milestones

At some point in the life of a train, Cisco stops selling, maintaining, and supporting it. Cisco informs customers that a train has reached one of these milestones by issuing product bulletins and other communications. First Customer Shipment (FCS), End of Sale (EoS), End of Engineering (EoE), and End of Life (EoL) are associated with lifecycle milestones.

Milestones in the Life of a Train

The following table briefly describes the train lifecycle milestones

Milestone	Available through Sales Channels	Bug Fixes	TAC Support	Download from Cisco.com
FCS	Yes	Yes[1]	Yes	Yes
EoS	No	Yes	Yes	Yes
EoE	No	No	Yes	Yes
EoL	No	No	No	No

1. FCS corresponds to the first maintenance release on the train. Each new release receives regular maintenance during the early part of the life cycle.

Cisco IOS Releases

A release is a snapshot in time of the code base of a train. Types of Releases include Maintenance releases, Rebuild releases, General Deployment (GD) releases, and Special releases.

Release	Description
Maintenance Releases	A maintenance release is a scheduled revision of Cisco IOS Software that introduces new features or bug fixes, or both. Maintenance releases typically occur every eight to thirteen weeks, depending on the train.
Rebuild Releases	Circumstances and business demands may require that a number of images from a Cisco IOS train be rebuilt and posted prior to the next planned maintenance release. Rebuilds are a Cisco IOS vehicle that delivers fixes on an accelerated schedule.
General Deployment (GD) Releases	A Cisco IOS Software release reaches GD certification when its quality has been demonstrated by extensive deployment in diverse networks over extended periods of time; Cisco IOS releases achieve GD status after meeting strict standards
General Deployment (GD) Release Criteria	A GD release must meet the following criteria: • Improving Trend in Defect Backlog – Customer Advocacy (CA) evaluation of known defects – No new features or platforms, defect resolution commits only – No open Critical Account Program (CAP) issues – Defect density measurements – Software Reliability Engineering (SRE) projected defects – Minimal code changes No serious defects in previous maintenance releases • Customer Success – Extensive customer exposure – High level of customer satisfaction • Cisco Deployment – Comprehensive system test and deployment in Cisco's internal network • Documentation – Release Notes Enclosures (RNEs) complete
General Deployment (GD) Lifecycle	After a release attains GD status, every subsequent revision of the release is also GD. Consequently, when a release is declared GD, it enters a restricted maintenance phase. While in this phase, modification of the code, including bug fixes, is strictly limited and controlled by a program manager to prevent bugs from being introduced into the release.
Special Releases	A special release is a branch from a train code base that is introduced to quickly meet market demands for new features or additional platform support. The early field adoption of new features and platforms that Cisco introduces in special releases benefits customers who need to run new network equipment or services. The following table lists technology identifiers used in the names of special releases.

Special Release Technology Identifiers

Identifier	Target Technology or Platform
X	Varies, one time release
Y	
Z	
A	Aggregation/Access Server/Dial
D	xDSL
H	SDH/SONET
J	Aironet Wireless Networking
M	Mobile Wireless
W	ATM/LAN Switching/Layer 3 Switching

Lifecycle of Special Releases

Cisco’s end of life (EoL) policy is not applicable to special releases

Interim Builds

An interim build is software from an internal Cisco engineering build process that the Cisco Technical Assistance Center (TAC) gives customers to use on a temporary basis to address a specific issue. Customers who have an interim build installed on their network should contact TAC for assistance in replacing the interim build.

Important Communications about Releases

Cisco issues many software advisories to customers for informational purposes only. Often, software advisories describe problems with Cisco IOS Software that are platform specific or occur under unusual circumstances, and therefore, do not affect most customers. Often, no action is required by the customer.

Critical Release Communication Types

Security Advisory	Product Security Incident Response Team (PSIRT) issues a security advisory to alert customers to security issues that directly impact Cisco products and to help customers repair the Cisco product.
Security Notices	Cisco issues Security Notices about issues that require a response to information posted to a public forum, or to make recommendations to mitigate general problems affecting network stability.
Deferral Advisory	Cisco issues a deferral advisory to announce the removal of a Cisco IOS image from Cisco's offerings and to introduce a replacement image. A deferral advisory is most often issued to correct a defect. At the time that the deferral of a Cisco IOS image is advised, customers are strongly urged to migrate from the affected image to the replacement image.

Cisco IOS Software Licenses

A Cisco IOS Software License includes the right to use a particular software release and feature set on one router. In some cases, additional value-added functionality is provided in software images but not covered by the "base" Cisco IOS Software License. The right to use these features is offered through a feature license.

A feature license conveys the right to use a feature, but cannot add a feature to a software release that does not support it. For example, purchasing a WAN Packet Protocols/Net flow license for software Release 11.0 will not upgrade the software to support Net flow. Choose a software release that supports all required features, then choose any necessary feature licenses.

Cisco IOS Software Upgrade Licenses

Customers who purchase “base” software licenses may wish to increase their software functionality or feature set at some point. The following illustrates the benefits of software feature licenses as well as how they are used to provide increased software functionality.

Example	Description
Upgrade A Feature Set (Single)	If a customer purchased a Router with Enterprise software, earlier and now wants to upgrade to Enterprise with Firewall/IDS, the customer has one of two options • With a valid maintenance contract, the customer may purchase the software feature license, Firewall/IDS Upgrade, to upgrade from Enterprise to Enterprise with Firewall/IDS. • Without maintenance, the customer will need to purchase a new software license Enterprise/FW/IDS, in order to upgrade from Enterprise to Enterprise with Firewall/IDS.
Upgrade Feature Sets (Multiple)	If a customer purchased a router with IP software, product code and now wants to upgrade to Enterprise with IPSEC 56, the customer has one of two options • With a valid maintenance contract, the customer will need to purchase two software feature license: IP to Enterprise and IPSEC 56 Upgrade. The first license upgrades from IP to Enterprise, and the second upgrades from Enterprise to Enterprise/IPSEC 56. • Without maintenance, the customer will need to purchase a new software license, Enterprise/IPSEC 56, in order to upgrade from IP to Enterprise with IPSEC 56.

Key Cisco IOS Tools

Tool	Description
Software Selector	**Finds required features for a given technology.** http://tools.cisco.com/ITDIT/ISTMAIN/servlet/index
Feature Navigator	**Finds releases that support a set of software features and platforms, and compares releases.** http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp
Software Advisor	**Compares IOS releases, matches IOS and CatOS features to releases, and finds out which software release supports a given hardware device.** http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi
Cisco IOS Upgrade Planner	**Finds releases by platform, release, and feature set, and downloads images of Cisco IOS Software.** http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?
Bug Toolkit	**Searches for known bugs based on software version, feature set, and keywords.** http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

For More Information on Cisco IOS Software

See the Cisco IOS Software Web site: **http://www.cisco.com/go/ios**
See the Cisco IOS Reference Web Site: **http://www.cisco.com/warp/customer/620/1.html**

Cisco Network Management Overview

Cisco is transforming traditional network management by focusing on the strengths of Internet-based architectures for greater accessibility and simplification of network management tools, tasks, and processes. Cisco's network management strategy calls for a Web-based model with the following characteristics:

- Simplification of tools, tasks, and processes
- Web-level integration with NMS platforms and general management products
- Capable of providing end-to-end solutions for managing routers, switches, and access servers
- Creation of a management intranet by integrating discovered device knowledge with CCO and third-party application knowledge

CiscoWorks Small Network Management Solution

CiscoWorks Small Network Management Solution (SNMS) is an end-to-end network management solution ideal for small networks which might include two or three branch offices. CiscoWorks SNMS is a comprehensive, cost-effective, and user-friendly solution that provides advanced monitoring, and configuration capabilities. It also provides management capabilities that simplify network administration. CiscoWorks SNMS enables network operators to more efficiently and effectively manage the network through a simplified browser-based interface that can be accessed anytime from anywhere within the network. CiscoWorks SNMS provides tools that make the job of configuring, monitoring, and troubleshooting routers, switches, firewalls, and other business applications, quicker and helps reduce the likelihood of human errors. Businesses that use CiscoWorks SNMS can enjoy the twin advantages of decreasing downtime and the ability to easily roll out changes in the network.

Positioned between CiscoWorks for Windows (CWW) and the CiscoWorks LAN Management Solution (LMS), SNMS introduces network administrators to the functionality of Resource Manager Essentials along with the multi-vendor device monitoring and SNMP management features of WhatsUp Gold. SNMS provides a cost effective solution that can be easily installed and used today while providing a transition path to CiscoWorks LAN Management Solution.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Small Network Management Solution	• Simple integrated installation, autodiscovery and automated import of devices using SNMP • Standards-based multi vendor management • Reduce the time and complexity of keeping the networks' configuration, software version and connectivity optimized

Key Features

- Aids in avoiding configuration mismatches via templates for Simple Network Management Protocol (SNMP) community, Terminal Access Controller Access Control System (TACACS), enable, syslog, SNMP trap destinations, Cisco Discovery Protocol (CDP) and Domain Name System (DNS) to prevent CLI command errors
- Provides a snapshot of the current state of a specific device with detailed graphical back and front views
- Provides a single window to monitor and manage Cisco network devices and non-network devices such as PCs, servers, and applications
- Monitors and reports on hardware, configuration, and inventory changes
- Provides reports that analyze prerequisites and impacts of proposed software updates
- Simplifies remote access to SNMS applications through a secure web browser while providing tiered user access based upon role permission

CiscoWorks Small Network Management Solution Components

CiscoWorks Small Network Management Solution includes the following tools:

- CiscoView—Provides graphical back and front panel views of Cisco devices; dynamic, color-coded graphical displays to simplify device-status monitoring, device-specific component diagnostics, device configuration, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol
- WhatsUp Gold from Ipswitch, Inc.—Provides network discovery, mapping, monitoring, and alarm tracking
- Resource Manager Essentials—Resource Manager Essentials (RME) provides tools for building and managing network inventory, deploying configuration and software image changes, archiving configurations, and providing an audit trail of network changes

Important: RME has a device limit of 40 or fewer Cisco devices.

Specifications

Feature	CiscoWorks Small Network Management Solution
Server	Hardware: PC-compatible computer with 1 GHz or faster Pentium processor; CD-ROM drive; 100Base-T or faster connection; 512 MB RAM; 9 GB available disk drive space; 1 GB virtual memory
	Software: Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)
Client	Hardware: PC-compatible computer with 1 GHz or faster Pentium processor
	Operating System: Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM
	Browser: Internet Explorer 6.0 Service Pack 1, on Windows operating systems

Selected Part Numbers and Ordering Information

CiscoWorks Small Network Management Solution	
CWSNM-1.5-K9	CiscoWorks Small Network Management Solution 1.5 for Windows; includes WhatsUp Gold 8.0, Common Services 2.2 with CiscoView 6.0, Resource Manager Essentials 3.5 (40 Cisco device restriction)
CWSNM-1.5-WINMR-K9	Maintenance kit for customers that purchased SNMS 1.0 X and now want new device support and code upgrades; kit includes support for Windows and updates to all components - September 2003

For More Information

See the CiscoWorks Small Network Management Solution Web Site:
http://www.cisco.com/go/wrsnms

CiscoWorks LAN Management Solution

The CiscoWorks LAN Management Solution consists of operationally focused tools. These tools include fault management, scalable topology views, sophisticated configuration, Layer 2/3 path analysis, voice-supported path trace, traffic monitoring, end-station tracking, workflow application server management, and device troubleshooting capabilities. CiscoWorks LMS combines applications and tools for configuring, monitoring, and troubleshooting the campus network.

When to Sell

Sell This Product	When a Customer Needs These Features
LAN Management Solution	• A set of tools for managing Cisco's award winning Catalyst switches • Time saving user tracking and path trace analysis tools with support of IP phones • Automated process of inventorying network devices, updating device software, and managing configuration to reduce the time and errors involved in network updates • Browser-accessible, graphical tool for configuring and monitoring Cisco device components and operational status • VLAN, ATM, or LANE service management tools • Active fault monitoring of Cisco devices

Key Features

- Campus Manager—Web-based applications designed for managing Layer 2 device and connectivity discovery, workflow application server discovery and management, detailed topology views, virtual LAN/LAN Emulation (VLAN/LANE) and ATM configuration, end-station tracking, Layer2/3 path analysis tools, and IP phone user and path information
- Device Fault Manager—Provides real-time fault analysis for Cisco devices, automatically includes Cisco devices into its monitoring environment and applies a Cisco "Best Practices" fault rule to each device
- Resource Manager Essentials—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	Description
Server	Hardware: Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) or IBM PC compatible with 550-MHz or higher Pentium III processor running; (Dual processor system required for hosting multiple management solutions) Software: Solaris 2.8; Microsoft Windows 2000 Advanced Server (with Terminal Services turned off), Server or Professional Edition with Service Pack 3
Client	Hardware: IBM PC-compatible computer with 300-MHz or higher Pentium processor; Sun Ultra 10, HP9000 Series; IBM RS/6000 running Software: Windows XP Professional with Service Pack 1, Windows 2000 Professional with Service Pack 2 or 3, Windows Server with Server Pack 2 or 3; Solaris 2.7, 2.8; HP-UX 11.0; AIX 4.3.3 Web Browser support for Windows 2000/XP: Netscape 4.78 or 4.79 or Internet Explorer 6.0 with Service Pack 1; Solaris support for Netscape 4.76 only
Supported Cisco Devices	Most Cisco IOS Software routers, access servers, hubs, and switches
Supported Cisco IOS Software Versions[1]	Generally supports: Cisco IOS Software Versions 10.3 and higher; Catalyst Supervisor code 2.1 through 4.1

1. Some CiscoWorks applications require certain versions of IOS and CAT these releases in order to operate, please see the specific application documentation and release notes for more information

Selected Part Numbers and Ordering Information[1]

LAN Management Solution	
CWLMS-2.2-K9	LAN Management Solution 2.2 for Windows and Solaris; includes Campus Manager 3.3, Device Fault Manager 1.2, Resource Manager Essentials 3.5, Common Services 2.2 with CiscoView 5.5
CWLMS-2.2-P1-K9	Cross Bundle Discount LMS 2.2 for Windows and Solaris platforms; available to customers who have previously purchased RWAN 1.X and want to add LMS
LAN Management Solution Upgrades	
CWLMS-2.2-UP-K9	Upgrade kit for LMS 1.X customers wanting to upgrade to LMS 2.2; kit includes support for both Windows and Solaris platforms; primary value of this kit is to provide DFM to LMS 1.X customers
CWLMS-MAY03-MR-K9	Maintenance kit for customers that purchased LMS 2.X and want new device support and code updates; kit includes support for both Windows and Solaris platforms; includes updates to all LMS 2.X components. Customers with LMS 1.X will not be able to install DFM 1.2 (use PN# CWLMS-2.2-UP-K9 to purchase the LMS 2.2 upgrade with DFM)

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the LAN Management Solution Web site: **http://www.cisco.com/go/lms**

CiscoWorks VPN/Security Management Solution

CiscoWorks VPN/Security Management Solution (VMS), an integral part of the SAFE Blueprint for network security, combines Web-based tools for configuring, monitoring, and troubleshooting enterprise virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). It offers the ability to monitor remote access links, and IPSec based site to site VPN links. VMS is a Web-based solution that provides a "dashboard" view of critical VPN resources and their performance, VPN hardware and configuration and troubleshooting reports.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks VPN/Security Management Solution	• Complete management of a SAFE infrastructure environment • Configuring and monitoring VPN, PIX, IOS routers, and IDS devices. • Monitoring large remote access, and site-to-site hub and spoke VPNs from a single management console and focus on problem areas and performance.

Key Features

- Management and Monitoring Centers—Supplies the latest in management functionality and multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control. The management and monitoring centers include Management Center for Firewalls, Management Center for IDS Sensors, Management Center for Cisco Security Agents, Management Center for VPN Routers, and Monitoring Center for Security
- VPN Monitor—Allows network administrators to collect, store, and view information on IPSec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser
- Cisco IDS Host Sensor Console—Provides real-time analysis and reaction to network hacking attempts by identifying an attack and preventing access to critical server resources before any unauthorized transactions occur
- Resource Manager Essentials (RME)—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	CiscoWorks VPN/Security Management Solution
Server	Hardware: IBM PC-compatible computer with 1-GHz or faster Pentium processor; Sun UltraSPARC 60 MP with 440-MHz or faster processor; Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server)
	Software: Windows 2000 Professional, Server, and Advanced Server (Service Pack 3); Sun Solaris 2.8
Server	Hardware: IBM PC-compatible computer with 300-MHz or faster Pentium; Solaris SPARCstation or Sun Ultra 10
	Software: Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM; Solaris 2.8
	Browser: Internet Explorer 6.0 Service Pack 1, on Windows operating systems; Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

Selected Part Numbers and Ordering Information

CiscoWorks VPN/Security Management Solution	
CWVMS-2.2-UR-K9	CiscoWorks VMS 2.2 Windows (unrestricted device usage; 1 server installation license); Includes: Management Center for Firewalls 1.1, for IDS Sensors 1.2, for Cisco Security Agents 4.0, and for VPN Routers 1.1, CiscoWorks Auto Update Server 1.1, CiscoWorks Monitoring Center for Security 1.2, CiscoWorks VPN Monitor 1.2, RME 3.5, and Common Services 2.2[1]
CWVMS-2.2-WINR-K9	CiscoWorks VMS 2.2 Windows (20-device restricted usage; 1 server installation license); Includes: Management Center for Firewalls 1.1, for IDS Sensors 1.2, for Cisco Security Agents 4.0, and for VPN Routers 1.1, CiscoWorks Auto Update Server 1.1, CiscoWorks Monitoring Center for Security 1.2, CiscoWorks VPN Monitor 1.2, RME 3.5, and Common Services 2.2
CWVMS-2.2-WUPGR-K9	Upgrade from CSPM 2.x (unrestricted license), CiscoWorks VMS 1.X or 2.X (restricted licenses) to CiscoWorks VMS 2.2 for Windows and Solaris (unrestricted license)[1]
CWVMS-2.2-UPGUR-K9	Upgrade from CSPM 2.X (restricted license) or CiscoWorks VMS 1.X (restricted license) to CiscoWorks VMS 2.2 for (20-device restricted license)[1]
CWVMS-DEC03URMR-K9	Minor update kit for existing VMS 2.X Windows and Solaris (unrestricted license)[1]
CWVMS-DEC03RMR-K9	Minor update kit for existing VMS 2.X Windows Only (20-device restricted license)[1]

1. Contains Windows-only versions of Management Center for Firewalls 1.1, for IDS Sensors 1.2, for Cisco Security Agents 4.0 and for VPN Routers 1.1, CiscoWorks Auto Update Server 1.1, and CiscoWorks Monitoring Center for Security 1.2

For More Information

See the CiscoWorks VPN/Security Management Solution Web site:
http://www.cisco.com/go/vms

CiscoWorks Security Information Management Solution and CiscoWorks Security Information Management Solution Engine

The CiscoWorks Security Information Management Solution (SIMS) is a solution for effectively gathering and analyzing the overwhelming amount of security event data that companies receive through growing numbers of multi-vendor security devices and systems installed throughout their network. SIMS is based on technology from netForensics and incorporates powerful features to help companies better manage their growing security infrastructure and effectively monitor millions of event messages, without additional staff.

CiscoWorks SIMS 3.1 also introduces a new, hardware-based solution engine option that provides the same features and functions as the CiscoWorks SIMS 3.1 software on a dedicated appliance. The CiscoWorks SIMS 3.1 Solution Engine requires minimal setup and installation.

The hardware based solution engine provides regional scalability for customers with small to medium deployments and the software only solution provides global scalability for larger deployments.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Security Information Management Solution	• Security monitor with advanced visualization for quickly detecting known and unknown threats • Perform risk assessments and analysis to determine overall vulnerability of enterprise network assets • Manage and correlate events from SAFE and multi-vendor security environments

Key Features

- Complete event monitoring for SAFE and all multivendor security environments
- Advanced visualization for fast and intuitive security monitoring
- Integrated risk assessment to understand the overall vulnerability of any particular asset within the enterprise
- Comprehensive reporting and forensics for all levels of security operations
- Productivity gains and cost reduction
- Flexible deployment options of either software only or network appliance with SIMS pre-installed on a Cisco 1160 Solutions Engine

Specifications

Feature[1]	CiscoWorks Security Information Management Solution (Open Server)
Server	Hardware: Linux: Dual Intel Pentium IV with 1.5 GHz (Server Class) with 4 GB RAM and 18 GB available disk space for full install; Solaris: Dual UltraSPARC-Iii with 444 MHz (Server Class) with 4 GB RAM and 18 GB available disk space for full install Software: Linux: Red Hat Linux, Solaris: 2.8
Client	Hardware: IBM PC-compatible computer with 300-MHz or faster Pentium; Solaris SPARCstation or Sun Ultra 10 Software: Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM; Solaris 2.8 Browser: Internet Explorer 6.0 Service Pack 1, on Windows operating systems; Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

1. For complete Server and Client Hardware and Software requirements, please refer to the Product Literature or Installation documentation for specific details and requirements; Information on the CiscoWorks Security Information Management Solution Engine can be found in the Product Literature

Selected Part Numbers and Ordering Information[1]

CiscoWorks Security Information Management Solution (Open Server)	
CWSIME-1160-K9	Security Information Management Solution Engine 3.1; includes the Cisco 1160 hardware platform and Security Information Management Solution software version 3.1
CWSIM-3.1-SS-K9	Security Information Management Solution 3.1 Starter Kit for Solaris; restricted license for monitoring 30 devices; License covers installation of 1 master engine, 1 distributed engine server and 1 database server. Includes release CDs for all software and documentation. Web enabled license activation required upon receipt
CWSIM-3.1-SL-K9	Security Information Management Solution 3.1 Starter Kit for Linux; restricted license for monitoring 30 devices; License covers installation of 1 master engine, 1 distributed engine server and 1 database server. Includes release CDs for all software and documentation. Web enabled license activation required upon receipt
CWSIM-3.1-DS-K9	Additional database server license for existing SIM 3.1 installations running Solaris. Web enabled license activation required upon receipt
CWSIM-3.1-DL-K9	Additional database server license for existing SIM 3.1 installations running Linux. Web enabled license activation required upon receipt
CWSIM-3.1-EN-K9	Distributed Engine add-on license for SIM 3.1 installations running Solaris or Linux. Web enabled license activation required upon receipt

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the CiscoWorks Security Information Management Solution Web site:
http://www.cisco.com/go/sims

CiscoWorks Network Connectivity Center Products

The Cisco® Network Connectivity Center (NCC) delivers end-to-end management across multiple tools, technologies, and silos. From networks and applications to business impact and dashboard views, Cisco NCC manages the entire IT environment in alignment with an organization's business objectives.

Organizations continue to measure IT investments against how they contribute to business objectives. Primary organizational goals include improving service levels and reducing operating costs by optimizing the performance of the infrastructure and the applications that deliver critical business services.

Cisco NCC is a suite of network and service management software that manage increasingly complex and distributed IT environments in alignment with business priorities. Using sophisticated modeling, analysis, and automation technologies, Cisco NCC provides end-to-end insight into how IT health relates to business services. It automatically pinpoints service-affecting faults and calculates their business impact, giving you the information you need to maximize service delivery while lowering operating costs and reducing business risk.

Cisco NCC builds on industry-leading, ready-to-use root cause and impact analysis technology that pinpoints connectivity problems in real time and identifies their impact. Cisco NCC extends that analysis from end to end across the IT environment, including multitechnology, multivendor networks; operations support system (OSS), packaged, and proprietary applications; and business services and processes.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Network Connectivity Center Products	• Eliminate time-consuming manual event analysis and ensure corrective action can begin early before significant network service problems arise • Faster problem isolation to prevent downtime and provide continuous availability of networked business applications • Easy to install right out-of-the-box with embedded knowledge of Cisco devices integrated into the tool so the need for costly and time-consuming development of custom rules and their implementation is not needed and saves valuable time

Key Features

- Fast, accurate discovery of the entire environment
- Built-in information model that maps components and their relationships across layers
- Automated root cause analysis-no rules writing required.
- Business impact analysis that aligns IT with business objectives
- Advanced automation, including analysis, escalation, and updates
- Scalable architecture to manage the world's largest infrastructures
- Flexible, Web-based dashboard views

Specifications

Feature[1]	CiscoWorks Network Connectivity Center Products
Software	Solaris 2.8 or 2.9, Windows 2000 Server, Windows XP (console only)

1. For complete Server and Client Hardware and Software requirements, please refer to the Product Literature or Installation documentation for specific details and requirements

Selected Part Numbers and Ordering Information[1]

CiscoWorks Network Connectivity Center Products	
CNCC-NCMP1.1-50K9	Cisco NCC NCM production server;includes software and 50 devices and 1 console
CNCC-NCMP1.1-100K9	Cisco NCC NCM production server;includes software and 100 devices and 1 console
CNCC-ASMP-1.0-50	Cisco NCC Application Services Manager-includes 1 ASM RTU Production server license with 50 ASM Managed Hosts device licenses.
CNCC-ACMP-1.0-20	Cisco NCC Application Connectivity Monitor - includes 1 ACM RTU Production server License 20 device license.
CNCC-BIMP-1.0-K9	Cisco NCC Business Impact Manager - includes 1 BIM RTU Production server License.
CNCC-ATFP-1.0	Cisco NCC ATM/Frame Relay Manager ñ Includes 1 ATM/FR RTU Production server License and 20 ATM/FR Managed Devices licenses.
CNCC-MPVP-1.0-100	Cisco NCC MPLS VPN Manager - Includes 1 MPLS VPN RTU Production server License and 100 Managed CE Devices.
CNCC-RPP-1.0-50	Cisco NCC RPSM - Includes 1 NCM/ RPSM Manager Production RTU server License and 50 Managed RPSM Devices licenses.
CNCC-BDP-1.0-K9	Cisco NCC Business Dashboard - Includes 1 Business Dashboard RTU Production server License and 1 Business Dashboard Concurrent User License.
CNCC-RMP-1.0-K9	Cisco NCC Report Manager - Includes 1 Report Manager RTU Production server License and 1 Report Manager Named User License.

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the CiscoWorks Network Connectivity Center Products Web site:
http://www.cisco.com/en/US/products/ps5934/index.html

CiscoWorks Manager IP Telephony Environment Monitor

CiscoWorks IP Telephony Monitor (ITEM) is a suite of applications and tools that facilitate effective management of Cisco-based IP telephony implementations. ITEM is designed to manage AVVID and IOS-based telephony environments with specialized tools and processes appropriate to both large and small installations. ITEM consists of a product bundle as well as several optional components that can be downloaded from the Cisco Systems, Inc. website. CiscoWorks ITEM provides information and tools in three areas to instill high confidence that Cisco-based IP telephony environments are performing as expected.

CiscoWorks ITEM provides several tools that enable Operations and Help-desk personnel respond to customer issues and to maintain surveillance on the introduction and movement of IP telephones in their environment. These optional tools increase the awareness and accountability for telephony resources and can play an important role in enterprise security programs yet are simple to install and use.

CiscoWorks ITEM also provides tools for Operations and Administrative personnel to monitor and manage telephony resources requiring financial expenditures. These tools, part of an ongoing program to capture and record capacity management data, can be used in conjunction with HP OpenView Performance Insight: Cisco IP Telephony Statistics Report Pack to produce meaningful utilization and capacity reports.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks IP Telephony Environment Monitor	• Network managers who need to effectively manage their converged networks while maintaining high confidence that their IP telephony environments are performing as expected • Network Managers who need to use synthetic traffic (replicating key forms of network activity associated with VoIP and IP telephony) to enable around-the-clock monitoring of key voice elements in the network

Key Features

The IP Telephony Monitor (ITM) is the primary application of the ITEM bundle. ITM tracks the health of IP telephony environments by proactively monitoring Cisco voice elements in the network to alert operations personnel to potential problems and to help minimize IP telephony service downtime. It supports the health monitoring of AVVID Cisco CallManager, Cisco AVVID IP telephony applications and platforms, IOS Telephony-based hardware, the gateways and gatekeepers, and in-line power switches. Main features of ITM are:

- Problem-focused fault analysis
- Synthetic traffic generation and monitoring
- Real-time Alerts and Activities Display
- Integration with CiscoWorks desktop
- Integration with enterprise management systems
- Support for Layer 2 and Layer 3 network devices
- Support of AVVID and IOS-based IP telephony applications and services
- Incremental device support

Optional Drop-In Modules

Fault History Manager

Fault History is an optional drop-in module (downloadable from Cisco.com Software Center) that provides a web-based tool to access historical fault and alert data from a database. The user has several filtering options that can facilitate the search for specific information.

IP Phone Information Utility

The IP Phone Information Utility is an optional drop-in module (downloadable from Cisco.com Software Center) that provides a web-based tool to show detailed information about individual IP telephone. The operator can access the IP phone information by using its extension number, IP address, and/or MAC address. This utility bases its information on the devices created in VHM.

IP Phone Help Desk Utility

The IP Phone Help Desk Utility is an optional applet (downloadable from Cisco.com Software Center) that provides a MS Windows 2000 desktop tool to show summary information about individual IP telephone. The help desk operator can access the IP phone information by using its extension number (or can configure the application to search by IP or MAC addresses). This utility requires a connection to an ITEM server running VHM with the IP Phone Information Utility installed.

Gateway Statistics Utility

When available, the Gateway Statistics Utility is an optional drop-in module (downloadable from Cisco.com Software Center) that provides a web-based tool to collect performance and behavior statistics about CCM-controlled IP telephony gateways. This statistical information can be subsequently exported for processing by reporting packages for capacity planning and trending information.

Specifications

Feature	CiscoWorks IP Telephony Environment Manager
Server	Hardware: IBM PC-compatible with 1 GHz or higher Pentium IV processor; UNIX (If DFM is on Unix platform; Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server); (Dual processor system required for hosting multiple management solutions) Software: Windows 2000 Server or Professional Edition with Service Pack 2; Solaris 2.8
Client	Hardware: IBM PC-compatible computer with 300 MHz or higher Pentium processor; Windows NT 4 (Workstation & Server) with Service Pack 6a, Win 98 or Windows 2000 Professional & Server with Service Pack 2 Browser: Windows 98/NT/2000: Netscape v4.77, 4.78, 4.79; Windows 98/NT/2000: Internet Explorer v5.5 with Service Pack 2, 6.0

Selected Part Numbers and Ordering Information

CiscoWorks IP Telephony Environment Monitor	
CWITEM-2.0-WIN-K9	CiscoWorks IP Telephony Environment Monitor 2.0 (Windows) for new customer installations; includes IP Telephony Monitor (ITM); this suite is intended for enterprise customers
CWITEM-2.0-ADD-K9	CiscoWorks IP Telephony Environment Monitor 2.0 (Windows) Add-On Kit for existing LMS 2.X customers; includes IP Telephony Monitor (ITM); this suite is intended for enterprise customers
CWITEM-2.0-UP-K9	Upgrade kit for existing IP Telephony Environment Monitor customers; includes IP Telephony Monitor (ITM). This suite is intended for the Enterprise customers
CWITEM-2.0-MV-K9	CiscoWorks IP Telephony Environment Monitor Multi-View 2.0 (Windows) for new customer installations; includes IP Telephony Monitor (ITM) Multi-View; this suite is intended for service provider customers

For More Information

See the CiscoWorks IP Telephony Environment Monitor Web site at:
http://www.cisco.com/go/cwvoip

CiscoWorks Voice Manager for Voice Gateways

CiscoWorks Voice Manager (CVM) 2.3 is a Web-based voice management and reporting solution. The application provides enhanced capabilities to configure and provision voice ports, and to create and modify dial plans on voice-enabled Cisco routers for voice-over-IP (VoIP), voice-over-Frame Relay (VoFR), and voice-over-ATM (VoATM) network deployments.

When to Sell

Sell This Product	When a Customer Needs These Features
Voice Manager for Voice Gateways	• Network managers who need to maintain a distributed network architecture for increased scalability • Network Managers who need to manage multiple customer networks from one common server

Key Features

- Integration with CiscoWorks—Manage a wide variety of router and switch functions through the CVM integration with CiscoWorks, which provides a common platform for running different applications
- Multiple platform support—Supported Platforms: Cisco 1700, 2600, and 3600 series, Cisco MC3810 Multiservice Access Concentrator, Cisco AS5300, AS5350, AS5400, and AS5800 series universal access servers, and Cisco 7200 and 7500 series routers
- GUI-based voice ports, dial-plan generation management—Create and manage local dial plans and VoIP, VoFR, and VoATM network dial plans

Specifications

Feature	CiscoWorks Voice Manager for Voice Gateways
Server Hardware Requirements	Windows: 512 MB, Twice as much swap space as memory, 2 GB of disk space, 500 MHz, 10 MB in temporary directory, NTFS file system required for security option Solaris: Sparc Ultra 10, 256 MB, Same amount of swap space as memory, 2GB of disk space
Server Software Requirements	Windows: Windows 2000 Professional and Server, SP 3 and SP 4 (Solaris: Solaris 2.7 or 2.8
Client Hardware Requirements	Windows: 128 MB, IBM PC-compatible 300-MHz Pentium processor Solaris: Sparc Ultra 10, 128 MB
Client Software Requirements	Windows: Windows 2000 or Windows XP Solaris: Solaris 2.7 or 2.8 Display Setting: 1024 x 768 resolution, 16-bit color palette

Selected Part Numbers and Ordering Information[1]

CiscoWorks Voice Manager for Voice Gateways	
CWVM-2.3-K9	CiscoWorks Voice Manager 2.2 for Windows and Solaris; includes Voice Manager 2.2, and Common Services 2.2 with CiscoView (CV) 5.5
CWVM-2.3-UP-K9	Upgrade to CVM 2.3 for Windows and Solaris from CVM 1.X.
CWVM-2.3-MR-K9	Minor updates to CVM 2.3 for Windows and Solaris for customers currently using CVM 2.X.

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Voice Manager for Voice Gateways Web site at:
http://www.cisco.com/en/US/products/sw/cscowork/ps2432/index.html

CiscoWorks QoS Policy Manager

QoS Policy Manager allows you to centrally define and administer IOS and CAT parameters needed for differentiating network traffic. This ensures high availability and predictable performance for business-critical which rely on advanced voice and video services. Cisco QoS Policy Manager (QPM) 3.2 is a key enabler of end-to-end QoS for converged networks. It delivers differentiated services across network infrastructures with converged voice, video, and data applications, simply by taking advantage of Cisco IOS and Catalyst OS Software with built-in QoS mechanisms in LAN and WAN switching and routing equipment.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco QoS Policy Manager	• End-to-end QoS configuration and automated, reliable policy deployment, while eliminating device-by-device command streams • Rules-based policies that combine static and dynamic port applications and host system traffic filters • QoS Policy Manager's services, including congestion management & avoidance, and traffic-shaping • Efficiently translate policies to specific QoS config commands, ensuring consistency across domains • Validate policies prior to deploying them quickly and reliably to LAN and WAN policy domains • Generate Web-based reports on QoS policies deployed in the network

Key Features

- Measure traffic throughput for top applications and service classes plus troubleshoot problems with real-time and historical QoS feedback
- Centrally define roles and permissions and take advantage of Cisco Secure Access Control Server (ACS) to control privileges for policy view, modification and deployment for different device groups
- Partition network into administrative and deployment domains and use policy libraries for global QoS configuration. Modify, scale and monitor IOS AutoQoS voice policies on routers
- Use the secure, Web-based graphical user interface (GUI) for accurate end-to-end QoS configuration and automated, reliable policy deployment, while eliminating device-by-device command streams
- Setup wizard intelligently determines QoS policies and properties at each network point that requires IP telephony QoS configuration based on Cisco AVVID design recommendations
- Achieve business-driven service levels across the enterprise network by configuring traffic classification and allowing QoS policy enforcement through Cisco devices
- An integral part of Cisco content networking, QPM 3.1 delivers the appropriate service levels to business-critical applications by supporting the extension of IP packet classification to include application signature, Web URLs, and negotiated ports
- Enables congestion management, congestion avoidance, and bandwidth control by selectively activating QoS mechanisms on intelligently grouped LAN and WAN interfaces and providing support for external application programming interfaces (APIs) to trigger event-based policy distribution
- Extend security by defining access control policies to permit or deny transport of packets into or out of device interfaces

- Expose QoS policy conflicts, uploads existing device configurations, presents command-line interface (CLI) syntax that corresponds to policies, allows previewing configuration changes before deployment, supports incremental access control list (ACL) updates, defines ACL ranges, and restores or applys a previous version of a policy database and backup to a remote server
- Supports device inventory import from CiscoWorks Resource Manager Essentials shortens configuration time for devices targeted for policy enforcement and QoS monitoring
- Web-based reporting enables a user to quickly view and analyze QoS policy management

Specifications

Feature	Cisco QoS Policy Manager
Server	Server Hardware: PC-compatible computer with 1-GHz or faster Pentium processor, CD-ROM drive, 10BASE-T or faster connection, 1-GB RAM, 9-GB available disk drive space, 2-GB virtual memory, Server Operating System CiscoWorks QPM requires the following operating systems: Windows 2000 Professional, Server, and Advanced Server (Service Pack 3 or 4). Support for Advanced Server requires that Terminal Services be turned off. Ports Used by QPM—CiscoWorks QPM on Windows uses the following ports, in addition to the ports used by CiscoWorks Common Services: 51099 Java Naming and Directory Interface (JNDI) lookup port, 51199 JRMP lookup port, 51299 Admin page port, 10033 (Windows) Database port, 51899 Protocol Data Packet (PDP) port
Client	Hardware—PC-compatible computer with 300-MHz or faster Pentium processor Client Operating System— Windows 2000 (Server or Professional Edition) with Service Pack 3 or 4, or Windows XP SP1 (Server or Professional) Client Browser—Windows with SP 3 and Windows XP clients: Microsoft Internet Explorer 6.0 or Internet Explorer 6.0 with Service Pack 1, Netscape Navigator 7.1; Windows clients with SP 4: Microsoft Internet Explorer 6.0 with Service Pack 1, Netscape Navigator 7.1

Selected Part Numbers and Ordering Information[1]

Cisco QoS Policy Manager	
CWQPM-3.1-WINUR-K9	QoS Policy Mgr 3.1 for Windows (unrestricted device usage; 1 server installation license)
CWQPM-3.1-WINR-K9	QoS Policy Mgr 3.1 for Windows (20-device restricted usage; 1 server installation license)
CWQPM-3.1-URUP-K9	Upgrade to QPM 3.1 for Windows from QPM 1.x, 2.x or 3.0 to QPM 3.1 (unrestricted device usage; 1 server installation license)
CWQPM-3.1-URC-K9	Conversion of a QPM 3.1 20-device restricted usage license to unrestricted device usage license

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco QoS Policy Manager Web site: **http://www.cisco.com/go/qpm**

CiscoWorks Wireless LAN Solution Engine

CiscoWorks WLSE is a centralized systems-level solution for managing the entire Cisco Aironet® WLAN infrastructure. Advanced air/radio frequency (RF) and device management tools eliminate complexity and give administrators visibility into the WLAN. By quickly and easily detecting, locating, and disabling unauthorized (rogue) access points, CiscoWorks WLSE helps ensure security, while ensuring that policies are consistently applied throughout the network. This advanced capability can benefit any organization, including those that have not deployed WLANs but still want to guard against intruders.

New in 2.7 is self-healing WLANs, an advanced radio management feature that enables a Cisco Aironet Series access point to adjust its cell coverage area automatically to compensate for an adjacent disabled or failed access point. CiscoWorks WLSE further optimizes performance by detecting and locating RF interference, while proactively monitoring utilization and faults.

CiscoWorks WLSE automates a range of previously time-consuming and repetitive tasks, such as bulk firmware updates and mass configuration of access points and bridges. CiscoWorks WLSE may be transparently integrated with other network management systems (NMSs), operations support systems, and CiscoWorks applications. CiscoWorks WLSE runs on the CiscoWorks 1130 for Wireless LAN Solution Engine hardware platform, which is one rack unit high.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Wireless LAN Solution Engine	The CiscoWorks WLSE is ideal for enterprise customers: • Implementing large-scale Cisco Aironet WLAN infrastructures • Template-based configuration tool which can include a large number of uniform policies for Cisco access points and bridges • Access point and bridge mis-configuration alerts to minimize security vulnerabilities • Proactive fault and performance monitoring of Cisco access points, bridges, LEAP authentication server, and switches connected to the access points

Key Features

- Self-healing WLANs—If it detects that an access point has failed, it compensates by automatically increasing the power and cell coverage of nearby access points
- Additional device support—RF management support has been added for Cisco Aironet 1200 Series and Cisco Aironet 1100 Series access points with IEEE 802.11a and 802.11g radios, including Cisco Aironet 1200 Series dual mode radios (802.11a/802.11b and 802.11a/802.11g), and Cisco Aironet 1400 Series Wireless Bridge.
- Security and Wireless LAN Intrusion Detection System (IDS)—Protects organizations' RF environments and WLAN networks from unauthorized access
  - Integrated IDS—Standard Cisco Aironet access points are deployed with the radio (802.11a, b, or g) placed in multifunction mode to service client devices and to provide WLAN intrusion monitoring
  - Dedicated IDS—A dedicated access-point-only WLAN is deployed with the access point radio (802.11a, b, or g) placed in radio scan mode to support only WLAN intrusion monitoring
- Assisted site surveys and automated resite surveys—Automates the process of determining optimal access point radio transmit power and channel selection.
- Open Extensible Markup Language (XML) API—RF management data, in addition to network management data, may be accessed by third-party management systems using XML
- Real-time client tracking and reporting—A variety of reports, including real-time client tracking, present a powerful set of tools for troubleshooting and capacity planning

Selected Part Numbers and Ordering Information[1]

CiscoWorks Wireless LAN Solution Engine

CWWLSE-1130-19-K9	Wireless LAN Solution Engine 2.7; includes the Cisco 1130 hardware platform and wireless LAN management software version 2.7
CWWLSE-2.7-SWUP-K9	Software only upgrade kit for Wireless LAN Solution Engine 1.x customers wanting to upgrade their Cisco 1130 hardware to Wireless LAN management software version 2.7

For More Information

See the CiscoWorks Wireless LAN Solution Engine Web site:
http://www.cisco.com/go/wlse

CiscoWorks Hosting Solution Engine (HSE)

HSE is a turnkey network management appliance that monitors, activates, and configures a variety of e-business services in Cisco powered data centers. It provides up-to-date fault and performance information about network infrastructure and Layer 4-7 network services. The hardware running HSE is the Cisco 1140, which is a one rack unit (1RU) that enables convenient deployment on the same rack as the rest of other Cisco e-business networking devices.

HSE automatically discovers the entire data center infrastructure and instantly begins collecting statistics and management information, providing a current snapshot of the managed environment. It provides up-to-date information for operational staff to easily pinpoint the source of a problem and, itself, is a manageable Cisco device with a full Cisco Discovery Protocol implementation and supports Cisco MIB II.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Hosting Solution Engine	• Ideal for enterprise and service providers with e-business data center facilities • Granular user access model to partition network resources for Layer 4-7 services and switch ports, and authorize user group access to individual application services • Robust Layer 4-7 service configuration and service activation of server load balancing devices, including virtual servers, real servers, and content owners and rules

Key Features

- Granular user access model to partition network resources for Layer 4-7 services as well as for switch ports, and authorized user group access to individual application services
- Robust Layer 4-7 service configuration and service activation of content switches, including virtual servers, real servers, and content owners and rules
- Monitoring and reporting of SSL Proxy services on Cisco Catalyst 6000 Series with SSL Service Modules and Cisco Content Services Switch
- HTML-based, secure graphic user interface with easy customer view/report personalization and historical data reporting
- Upper layer NMS/OSS integration with SYSLOG, trap, email notifications and historical data XML export

Selected Part Numbers and Ordering Information[1]

Cisco 1105 Hosting Solution Engine

CWHSE1105-1.5-K9	CWHSE-1140-19-K9CiscoWorks Hosting Solution Engine; includes 1105 hardware platform with software version 1.7; can be configured for international power cords
CWHSE-1.8-SWMR-K9	Minor update kit for customers on HSE 1.x that do not have SAS support contracts; Includes minor update release for HSE 1.8

1. Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the 1105 Hosting Solution Engine Web site: **http://www.cisco.com/go/hse**

Cisco Catalyst 6500 Series Network Analysis Module 1 and 2(with NAM software version 3.3)

The Cisco Network Analysis Module (NAM) 1 and 2, second generation high performance network analysis modules for the Cisco Catalyst 6500 Series provides network monitoring instrumentation and web-browser based traffic analysis for Catalyst based AVVID environments. The NAM enables network managers to gain application-level visibility into network traffic with the ultimate goal of improving performance, reducing failures, and maximizing returns on network investment. The new NAMs are available in two hardware versions, NAM-1 and NAM-2, to meet diverse network analysis needs in a scalable switching environment running up to gigabit speeds. The NAMs come with an embedded, Web-based traffic analyzer, which provides full scale remote monitoring and troubleshooting capabilities that are accessible through a Web browser.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 6500 Series Network Analysis Module 1 and 2 (with NAM software version 3.3)	• Needs Application-Level visibility built into the network • Provides network managers visibility into all layers of network traffic • Monitoring in a scalable switching environment that supports traffic monitoring in a scalable switching environment • Offers investment protection by interfacing with both the bus and the crossbar switching fabric-based architectures in the Cisco Catalyst 6500 Series

Key Features

- Provides application-level Remote Monitoring (RMON) functions based on RMON2 and other advanced Management Information Bases (MIBs)
- Collects statistics on both data and VoIP streams flowing through the host switch using the Switch Port Analyzer (SPAN) and NetFlow Data Export features of the Cisco Catalyst 6500 Series
- Collects data from remote switches using the remote SPAN (RSPAN) feature of the Cisco Catalyst 6500 and 4000 Series switches
- Easy to deploy and use at LAN aggregation where they can see most of the traffic, at service points where performance is critical and at important access points where quick troubleshooting is required
- Application monitoring can be done using RMON, RMON2, and several extended RMON MIBs, which can detect the applications on the network and provide detailed information about how these applications utilize the bandwidth, which hosts access those applications, and which client/server pairs generate the most traffic
- Performance management provides valuable information about the delays in server responses to client requests

Selected Part Numbers and Ordering Information[1]

Cisco Catalyst 6500 Series Network Analysis Module 1 and 2(with NAM software version 3.3)	
WS-SVC-NAM-1	Catalyst 6500 Series Network Analysis Module 1. To order the NAM individually, please use the spare part number of WS-SVC-NAM-1=
WS-SVC-NAM-2	Catalyst 6500 Series Network Analysis Module 2. To order the NAM individually, please use the spare part number of WS-SVC-NAM-2=

1. Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco NAM Web site:
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html