NETWORK MANAGEMENT TOOLS

I. CiscoWorks LAN Management Solution

Product Overview

Simplify LAN Management

CiscoWorks LAN Management Solution (LMS) is a suite of powerful management tools that simplify the configuration, administration, monitoring, and troubleshooting of Cisco networks. It integrates these capabilities into a best-in-class solution for:

- Improving the accuracy and efficiency of the network operations staff
- Increasing the overall availability of the network by simplifying configuration and quickly identifying and fixing network problems
- Maximizing network security through integration with access control services and audit of network-level changes

CiscoWorks LMS provides:

- A centralized system for sharing device information across all LAN management applications, improving manageability, and increasing systemwide awareness of network changes
- Network discovery, topology views, end-station tracking, and VLAN management
- Real-time network fault analysis with easy-to-deploy, device-specific, best-practice templates
- Hardware and software inventory management, centralized configuration tools, and syslog monitoring
- Monitoring and tracking of network response time and availability
• Real-time device and link management, as well as port traffic management, analysis, and reporting

**Featured Products**

CiscoWorks Assistant — A web-based tool that provides workflows to help resolve network management and deployment issues.

LMS Portal — Displays all the important statistics and details of the CiscoWorks LMS applications installed on your CiscoWorks server, in a single page.

CiscoWorks Device Fault Manager — Provides real-time detailed detection, analysis, and reporting of device faults; often identifies problems before users realize they exist.

CiscoWorks Campus Manager — Configures, manages, and visualizes complex physical and logical Layer 2 infrastructures, user tracking, VLAN management and configuration, network discrepancies, best practices and topology mapping.

CiscoWorks Resource Manager Essentials — Provides network inventory, device configurations and changes, as well as software updates, along with syslog analysis.

CiscoWorks Internetwork Performance Monitor — Offers proactive measurement of network response time and availability as well as real-time and historical analysis of congestion and latency problems.

**II. Cisco Unified Operations Manager**

![Cisco Unified Operations Manager](image_url)

**Product Overview**
Cisco® Unified Operations Manager (UOM) is the cornerstone of the Cisco Unified Communications Management Suite, designed specifically for managing the Cisco Unified Communications 8.0 Solution. The Cisco Unified Communications Management Suite offers provisioning, monitoring, diagnostics, and extensive reporting capabilities to:

- Simplify the management of your Cisco Unified Communications environment
- Reduce the total cost of ownership
- Help ensure high-quality service and end-user satisfaction
- Optimize your Cisco Unified Communications resources

Cisco Unified Operations Manager provides comprehensive voice network monitoring with diagnostics for the entire Cisco Unified Communications system, including the underlying voice transport infrastructure.

Cisco Unified Operations Manager identifies the role of every device and application in the Cisco Unified Communications network and monitors them, detecting operational faults with voice-application-aware intelligence. The resulting alerts facilitate rapid troubleshooting of outages, with context-sensitive links to the appropriate services for that device. There are no workflow rules to write, no thresholds to define, and no time-consuming management setup to budget for.

Features and Benefits of Cisco Unified Operations Manager

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated discovery</td>
<td>• Automated discovery of Cisco Unified Communications Manager cluster elements and associated Cisco Unified Communications applications, phones, and gateways</td>
</tr>
</tbody>
</table>
| Service-level view | • Single view to visualize and monitor the entire Cisco Unified Communications system  
|                    | • Context-sensitive, right-click menus for diagnostics, Layer 2 physical connectivity, and status and performance monitoring |
| Alerts and events  | • Quick glance, real-time status of all the faults in the Unified Communications network  
|                    | • Customizable views for selective and focused monitoring |
| Performance        | • Visibility into critical performance metrics of each element, such as resource usage |
### III. Cisco Configuration Professional

**Product Overview**

Cisco Configuration Professional is a GUI based device management tool for Cisco access routers. It simplifies router, firewall, IPS, VPN, unified communications, WAN, LAN and basic wireless configuration through easy-to-use wizards.

Cisco Configuration Professional is a valuable productivity-enhancing tool for network administrators and channel partners for deploying routers in medium-sized businesses and enterprise branch offices with increased confidence and ease. Cisco Configuration Professional has configuration checks built into the application thereby reducing errors.

The new device manager for Cisco integrated services routers, Cisco Configuration Professional will replace Cisco Router and Security Device Manager (SDM) over time. Like SDM, Cisco Configuration Professional assumes a general understanding of networking technologies and terms but assists individuals unfamiliar with the Cisco CLI. To find out when a new version of Cisco Configuration Professional is available for download, visit [http://www.cisco.com/go/ciscocp](http://www.cisco.com/go/ciscocp) periodically.

| Monitoring | (CPU, memory, media digital signal processor [DSP] resources), active calls, trunk statistics (trunk usage, port usage, gateway statistics) and so on
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Graphic chart views for side-by-side comparison of selected metrics</td>
<td></td>
</tr>
<tr>
<td>Diagnostics tests</td>
<td>• Synthetic tests (call processor to phone) and phone-to-phone tests, helping to ensure end-to-end service connectivity</td>
</tr>
</tbody>
</table>
Cisco Configuration Professional Express, a light-weight version of Cisco Configuration Professional, is available on the router's flash and can be used to configure some of the router's LAN and WAN interfaces and minimal Cisco IOS Software security features

Ease of Use and Built-In Application Intelligence

With Cisco Configuration Professional you can remotely configure and monitor your Cisco routers without using the Cisco IOS Software CLI. If you are not an expert with Cisco IOS Software, the Cisco Configuration Professional GUI (Figure 1) can help you in your day-to-day operations; the application:

- Provides easy-to-use smart wizards
- Assists you through comprehensive online and video help

Cisco Configuration Professional smart wizards guide you step-by-step through router configuration workflow by systematically configuring LAN and WAN interfaces; firewalls; IPSs; and IPsec VPNs. These smart wizards can intelligently detect incorrect configurations and propose fixes, such as allowing Dynamic Host Configuration Protocol (DHCP) traffic through a firewall if the WAN interface is DHCP-addressed.

Online help embedded within Cisco Configuration Professional contains appropriate background information, in addition to step-by-step procedures to help you enter correct data into the application. Networking, security, and voice terms and definitions that you might encounter are included in an online glossary.

If you are a network professional familiar with Cisco IOS Software and security features, Cisco Configuration Professional offers advanced configuration tools to quickly configure and fine-tune router security features, allowing you to review the commands generated by the application before delivering the configuration changes to the router.
IV. Cisco Security Manager Suite

Product Overview

The Cisco® Security Management Suite is a framework of next-generation security management tools designed for the operational management and policy administration of the Cisco Self-Defending Network. This suite of integrated applications simplifies the management process by automating tasks associated with the functional areas of security management: configuration, monitoring, analysis, mitigation, identity, and auditing. The result is an increased level of security assurance, better organizational productivity, and lower overall TCO.

The primary components of the Cisco Security Management Suite include the Cisco Security Manager and the Cisco Security Monitoring, Analysis, and Response System (MARS).

Cisco Security Manager is a powerful but easy-to-use solution for configuring firewall, VPN, and intrusion prevention system (IPS) policies on Cisco security firewalls, routers, and appliances. To deal with the complexity of different security devices, operating systems, and configuration interfaces, Cisco Security Manager has been designed to act as a layer of abstraction. The result is an application with usability enhancements that deliver a superior look and feel to simplify the process of scalable policy definition and deployment. For example, if a network or security administrator wants to implement a policy of limited instant-messaging traffic during business hours, they can do so in a series of simple clicks. The user experience is the same regardless of the actual security device type that is enforcing the rule—whether it is a Cisco PIX® firewall, a Cisco IOS® Software-based integrated services router, a Cisco ASA adaptive security appliance, or a Cisco Catalyst® switch services module. Cisco Security Manager helps administrators reduce user error and maintain consistent policies across the secure network infrastructure.

The second component of the Cisco Security Management Suite is Cisco Security MARS, an appliance-based, all-inclusive solution that provides insight and control of the existing security deployment. This appliance allows network and security administrators to identify, manage, and counter security threats. By
using the existing network and security infrastructure, Cisco Security MARS can monitor security events and information from a wide variety of sources, including third-party devices and hosts. By using a best-of-breed correlation engine, Cisco Security MARS can not only identify anomalous behavior and security threats, but can also recommend precision removal of those elements, leading to rapid threat mitigation.

**BUSINESS BENEFITS**

With a powerful set of applications, an integrated architecture, and a comprehensive partnering strategy, the Cisco Security Management Suite is positioned to provide organizations with a best-of-breed management solution for their security networks. With tools that automate and simplify operational tasks, administrators can derive value from:

- **Policy consistency and security assurance**-Cisco Security Manager allows you to deploy consistent security policies across thousands of security devices in a short span of time.

- **Rapid threat mitigation for improved company network uptime**-Cisco Security MARS allows organizations to quickly identify and respond to network and security threats such as worms and viruses, preventing widespread outbreaks and significant downtime.

**V. CiscoWorks Network Compliance Manager**

**Product Overview**

Enterprises seeking to facilitate high performance business applications increasingly rely on sophisticated networking infrastructure and the power of new technologies. Network operations and security managers rely on systems that can automate network deployments, handle large and complex topologies, and track and audit how actual network deployments comply with design requirements and best practices. Enterprise networks must comply with regulatory policies, corporate IT methodologies, and technology best practices—individually of scale, networking technologies deployed, and the combination of vendors providing networking equipment.

**Network Lifecycle Automation**

NCM automates the complete operational lifecycle of network devices, which includes:

- **Discover and track**: Includes discovering and cataloging the network, visualizing the Layer 2 and
Layer 3 network topology, initial device turn-up, and creating initial snapshots of device configurations

- Change and configure: Includes creating and deploying configuration changes in a structured manner, such as using configuration templates or scripts, peer reviewing and approving proposed changes, and maintaining an archive of previous configurations.
- Audit and enforce: Includes defining compliance policies for your network devices, detecting violations in real time, and autoremediating problems.
- Maintain and support: Includes providing reports on device inventory, change activity, and compliance.

**Enforce Policies, Standardize Operations, and Meet Compliance**

Bringing networks into compliance with corporate or regulatory standards is a nontrivial, labor-intensive, error-prone, and difficult task. NCM helps you meet compliance standards through a network compliance model that maps device information, including configurations and run-time diagnostics, as well as policies and user roles, into a normalized structure to prevent compliance violations before they occur.

Built-in best practices immediately measure network compliance against industry-accepted best practices. NCM incorporates policies such as the National Security Agency (NSA) router configuration guidelines.

Predefined reports for Information Technology Infrastructure Library (ITIL), the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI) standard, and other regulations offer immediate insight into network compliance. These reports provide the metrics that each of these regulations or processes requires, increasing visibility and saving auditors and network engineers time.

**New Features in CiscoWorks NCM 1.5**

- Virtual device and virtual context support: NCM now provides support for virtual devices, including VMware's Virtual Switch (vSwitch) technology available through VMware's Infrastructure (ESX) and the Cisco® Nexus 1000v Series switches. These new virtual devices can be managed alongside legacy devices, providing centralized support.

- Enhanced relationship modeling: Devices may have relationships with other devices or contained modules.
that run an independent operating system-complete with a full configuration and interfaces. NCM 1.5 distinguishes relationship types including both user-defined and system-defined relationships.

- Enhanced task scheduling: Two key task management features, task prioritization and round-robin execution of group tasks, have been implemented to improve the execution order of tasks.

- Enhanced Device Selector and Device Group Explorer: With the enhanced Device Selector and Device Group Explorer you can easily navigate group trees to select devices and device groups for a variety of use cases.

VI. Cisco Active Network Abstraction

Product Overview

Cisco® Active Network Abstraction (ANA) is a network management foundation for Cisco-based service provider IP networks.

ANA addresses the challenge of managing converged, multiservice, and multivendor IP networks through its unique model-based virtual network abstraction. Its service-aware design supports Multiprotocol Label Switching (MPLS), Carrier Ethernet, and IP Radio Access Network (RAN)/Mobile Transport over Packet (MToP) and extends to emerging technologies.

Cisco ANA offers service providers the following functional tiers:
Cisco ANA is designed to be extended and integrated into customers' network management systems. It operates between the network and the operations support systems.

Cisco ANA offers partners and integrators a rich northbound API and flexible query language to its standards-compliant network information model as well as comprehensive developer support services. Extremely customizable, Cisco ANA can be deployed along service provisioning systems, inventory and performance management systems, assurance systems, and more.

Installed on carrier-class servers, Cisco ANA is highly distributed, providing resiliency, high availability, and scalable deployments that support thousands of network elements.

Features and Benefits

ANA provides a suite of GUI applications and tools that offer a simple, intuitive interface to visualize the managed network and services, navigate the network, navigate to details of network element inventory and fault status, and launch other tools.

Network Discovery and Visualization

Fundamental to Cisco ANA is its ability to discover and identify dynamically and automatically basic network components, adjacencies, and connectivity. Cisco ANA obtains end-to-end visibility of network resources and builds up a virtual network abstraction by means of device-specific virtual network elements (VNEs). Cisco ANA maintains a detailed physical inventory model, including fans, slots, cards, and ports, and a comprehensive logical networking model and configuration by polling of routing, bridging, and Label Switch Entity (LSE) tables, as well as hundreds of other device properties. Network changes are detected and reflected in the virtual network layer and reported in the form of alarms and northbound interface notifications. The network operator sees an accurate, detailed, end-to-end topological view of the layered multidomain IP network.

VII.   Cisco IP Solution Center

Product Overview
Cisco® IP Solution Center (ISC) is a family of intelligent network management applications that help reduce overall administration and management costs by providing automated resource management and rapid profile-based planning and provisioning capabilities that accelerate deployment of Multiprotocol Label Switching (MPLS) and Carrier Ethernet technologies. Cisco IP Solution Center also helps reduce operational costs by providing automated workflow-based troubleshooting and diagnostic capabilities for MPLS VPNs. The applications can operate as standalone applications or as a suite. Functions include provisioning and automated diagnostics for MPLS VPNs; ATM, Frame Relay, and Ethernet over MPLS VPNs; ATM and Frame Relay transport over Carrier Ethernet VPNs; and planning and configuration of MPLS traffic engineering.

Cisco IP Solution Center delivers complete lifecycle management, from creating the IP service to real-time VPN and MPLS traffic engineering tunnel provisioning, activation, troubleshooting, and diagnostics. Cisco IP Solution Center provides the provisioning, planning, and automatic diagnostics tools that accelerate deployment and time to market of IP services. Simultaneously, it simplifies management of multiple technologies by providing an integrated management product.

### Features and Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tracking of Layer 3 and Layer 2 resources</strong></td>
<td>Manages resources such as Border Gateway Protocol (BGP) autonomous system, regions, customers, customer sites, access domains, service provider administrative domains, virtual routing and forwarding (VRF) names, IP addresses, VLAN IDs, pseudowire virtual circuit IDs, route distinguishers, and route targets.</td>
<td>Automation of resource management reduces cost of previously manual and time-consuming tasks and helps ensure accuracy.</td>
</tr>
<tr>
<td><strong>Rapid profile-based provisioning</strong></td>
<td>Allows service operators to define Layer 3 and Layer 2 VPN provisioning parameters in a service policy; uploads the network-element configuration to calculate the change in configuration needed for successful service activation.</td>
<td>Helps control operational costs by accelerating service deployments. The use of service policies for service activation greatly reduces the service operator's tasks—the only parameters required for service activation have already been captured in the service policy. By uploading the configuration prior to applying it, Cisco IP Solution Center helps ensure that the service activation configuration will be successfully and rapidly applied and will not collide with the existing configuration.</td>
</tr>
<tr>
<td><strong>Recognition of incorrect service configuration</strong></td>
<td>Provides postprovisioning validation of the service design in order to determine if the Layer 3 and Layer 2 VPNs are active and functional.</td>
<td>Reduces the time it takes to troubleshoot network outages due to incorrect service configuration by verifying that the commands for a service are present on the network elements and the links involved or VPN is working correctly.</td>
</tr>
<tr>
<td><strong>Investment protection for Cisco IOS Software and line cards</strong></td>
<td>Provides comprehensive platform and Cisco IOS Software support.</td>
<td>Reduces time to market of new services and lowers the cost of upgrading customer OSSs due to upgrades in platforms, software versions, and line cards by providing extensive support of the latest Cisco hardware and Cisco IOS Software versions.</td>
</tr>
</tbody>
</table>

### VIII. Cisco Network Registrar

#### Product Overview

Cisco® Network Registrar® is an IP address management application that delivers IP address management (IPAM) features to ease the task of administering Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services. For enterprise customers, Cisco Network Registrar offers a user-friendly GUI coupled with a built-in, granular administrative role capability to help users focus on running their business rather than dedicating the time to managing their DNS and DHCP services. For cable providers, Cisco Network Registrar provides scalable DNS and DHCP services for millions of devices and forms the basis of a DOCSIS® cable modem provisioning system. For telecom service providers, Cisco Network Registrar is an integral part of service networks such as DSL and WiMAX as well as voice over l(VoIP) and business services infrastructures.

Cisco Network Registrar includes a standards-compliant DNS server that offers an advanced feature set, with support for incremental zone transfers, dynamic updates, and notifications. To secure DNS services, Cisco Network Registrar supports transactional signature (TSIG) to authenticate DNS zone transfer and update requests. Cisco Network Registrar DHCP server offers DHCP safe failover with redundant DHCP servers, dynamic DNS updates, and DOCSIS cable modems and integration with directory services using Lightweight Directory Access Protocol Version 3 (LDAPv3).

#### Features and Benefits
<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usability</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration wizard</td>
<td>A configuration wizard helps users navigate through different Cisco Network Registrar configuration steps. With the wizard, users can easily perform DHCP and DNS configuration by entering the parameters that are essential for the configuration. This is the basic configuration mode. The advanced configuration mode is still available for users with more in-depth experience of DNS and DHCP configuration.</td>
</tr>
<tr>
<td>Real-time server status dashboard</td>
<td>The dashboard provides an at-a-glance, real-time indicator of the server health, system metrics, alarms and alerts, and inventories of the Cisco Network Registrar server. The dashboard displays graphs for monitoring DHCP and DNS general information, throughput, and error data that can affect network operations. To measure address usage over time, the dashboard can collect DHCP utilization information for a time period and present graphs showing trends that are useful for capacity planning.</td>
</tr>
<tr>
<td>Improved search capability</td>
<td>Users can search for an IP address and retrieve the relevant information associated with the address. Users can find out the current state of the address, the scope to which it belongs, and the date and time the lease was granted. Users can start the search by entering the IP address or a MAC address that is associated with the IP address.</td>
</tr>
<tr>
<td>Carrier-class lease reservation performance</td>
<td>For users with needs for static IP address assignment, Cisco Network Registrar can handle up to 500,000 lease reservations. Because Cisco Network Registrar supports failover deployment, the enhanced lease reservation synchronizes the lease reservation between the main and the backup server to make sure that any update to the configuration will be populated between these servers. Modification to the reserved lease configuration can be done through the web UI, a command-line interface (CLI), and the Java Software Development Kit (SDK).</td>
</tr>
</tbody>
</table>

**IX. Cisco Configuration Assistant**

**Product Overview**

Cisco® Configuration Assistant simplifies the task of configuring, deploying, and administering Cisco small business network solutions. Designed specifically for small business networks serving up to 100 users, this PC-based application with a simple graphical user interface (GUI) that allows you to discover and configure Cisco Smart Business Communications System (SBCS) platforms.
After the network is deployed, Cisco Configuration Assistant can synchronize network configuration settings, provide troubleshooting tools, and present the real-time status of all of the Cisco small business devices in the network. Together, these capabilities substantially reduce the time the system administrator must devote to deploying and configuring the network.

Features and Benefits

Cisco Configuration Assistant provides comprehensive configuration, deployment, and ongoing network management support by the system administrator for the entire line of products in the Cisco SBCS. For a full list of supported features.

Setup wizards: Cisco Configuration Assistant 2.2 includes an easy-to-use telephony setup wizard that allows users to configure IP addressing functions such as the WAN IP address and the voice and data VLAN IP address. The wizard also adds configuration options for automated attendant, business schedules, localization, inbound and outbound dial plans, users and phones, and call blast and hunt groups.

The Video Monitoring wizard provides trouble-free setup for streaming Video from a Cisco Small Business Video Surveillance Camera WVC2300 or PVC2300 to a Cisco SPA525G wireless IP phone.

The Phone VPN wizard configures the SSL-VPN client on the Cisco SPA525G wireless IP phone, enabling voice connectivity to and from any remote location with internet access.


Voice configuration: Cisco Configuration Assistant can interact with and configure key voice applications and devices. Simply access the telephony services through the phone icon on the Cisco Configuration Assistant dashboard to easily set up and configure the phone system's users and phones. Cisco Configuration Assistant supports multisite configuration, allowing a maximum of five Cisco Unified Communications 500 sites to be networked together in a full-mesh data and voice virtual private network (VPN).

Security configuration: Cisco Configuration Assistant allows users to activate the most commonly used Cisco software security features, including Network Address Translation (NAT) and firewalls. The tool can also configure the Cisco Unified Communications 500 Series as a VPN server or the Cisco 500 Series Secure Router as a VPN client.
Switch configuration: Cisco Configuration Assistant provides a quick and easy way to configure LAN ports on the Cisco Unified Communications 500 Series and the Cisco Catalyst® Express and ESW 500 Series Switches. The tool enables dynamic VLAN assignment of voice and data traffic and simplifies activation of QoS, security, and Power over Ethernet (PoE) features. The Smartports feature in Cisco Configuration Assistant allows each switch port to be customized to match the device that is connected, whether it is an IP phone, PC, access point, router, or LAN switch.

X. Cisco netManager IP Infrastructure

Product Overview

Cisco netManager IP Infrastructure 1.0 is part of the Cisco netManager family of products, built to manage small and medium-sized data networks of up to 100 devices and 100 wireless access points. It provides easy-to-use monitoring and diagnostics for small and medium-sized networks of Cisco network devices, non-Cisco network devices, and office devices like servers and printers.

Cisco netManager IP Infrastructure 1.0 monitors all components of small and medium-sized IP networks built by Cisco as well as third-party network devices to provide current operational status of all the elements in the network. It features built-in rules and thresholds as well as automatic device identification and data collection to help enable easy setup and immediate monitoring of the managed network. It continuously monitors the different elements of the system including routers, switches, PIX® firewalls, intrusion detection systems (IDSs), Adaptive Security Algorithm (ASA), and wireless access points. Cisco netManager IP Infrastructure also monitors any third-party devices that may exist in the network such as servers, workstations, printers, and other networking devices and provides basic availability monitoring for each of these devices. It also features an extensible monitoring framework in which coverage may be extended by adding different active monitors based on supported protocols like HTTP, Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), and so on that help enable custom monitoring for both Cisco and third-party devices.

Typical Applications
Cisco netManager IP Infrastructure 1.0 is recommended for monitoring small and medium-sized networks with Cisco network devices, non Cisco network devices, and office desktop devices. A single Windows-based server/workstation running Cisco netManager IP Infrastructure 1.0 software can monitor the entire network with up to 100 network and office desktop devices and 100 wireless access points distributed across 10 remote sites.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network-level monitoring support</td>
<td>Monitors and evaluates the current operational status of all the supported network and office desktop devices. Monitored components include routers, switches, PIX firewalls, ASA, IDS, wireless access points, servers, printers, workstations and applications.</td>
</tr>
<tr>
<td>Autodiscovery</td>
<td>Provides console-based autodiscovery of the network. Autodiscovery of the network can be performed using SNMP smart scan, IP range scan, and network neighborhood scan.</td>
</tr>
<tr>
<td>Device import</td>
<td>Provides the capability to import devices statically into the system through bulk import of devices using a host import file and individual addition of devices</td>
</tr>
<tr>
<td>Real-time actionable network level topology</td>
<td>Provides visibility into network connectivity and related information by means of an autogenerated real-time physical connectivity view that not only shows interconnections between different devices but also presents the current operational status of each of the devices and applications in the network.</td>
</tr>
<tr>
<td>Contextual menus and diagnostic tools</td>
<td>Increases productivity of network managers and facilitates faster trouble isolation by providing contextual diagnostic tools and easy one-click access to embedded device management systems</td>
</tr>
</tbody>
</table>