Q&A

CISCO ROUTER AND SECURITY DEVICE MANAGER VERSION 2.2

GENERAL QUESTIONS

Q. What is the Cisco Router and Security Device Manager (SDM)?

A. Cisco SDM is an intuitive, Web-based device-management tool for Cisco IOS® Software-based routers. Cisco SDM simplifies router and security configuration through smart wizards, which help customers quickly and easily deploy, configure, and monitor Cisco Systems® router without requiring knowledge of the Cisco IOS Software command-line interface (CLI).

Q. How do I order Cisco SDM?

A. Cisco SDM is factory installed on all Cisco 1800, 2800 and 3800 series routers both non-bundle and bundle SKUs.

On Cisco 1700 Series, Cisco 2600XM, Cisco 2691, Cisco 3700 Series, Cisco 7204VXR, 7206XVR, and Cisco 7301 Cisco SDM is factory installed on the security bundles (K9) and optionally orderable on all other SKUs.

On Cisco 831-SDM, Cisco 836-SDM, Cisco 837-SDM, Cisco Small Business 100 Series, Cisco 850 Series, and Cisco 870 Series Cisco SDM Express is factory installed on the router flash, and a Cisco SDM CD is bundled with the router.

For routers that did not ship with Cisco SDM preinstalled, Cisco SDM can be downloaded free of charge from the Software Center on Cisco.com.

Q. How many devices can Cisco SDM administer?

A. One. Cisco SDM is a tool for configuring, managing, and monitoring a single Cisco router. Each Cisco router is accessible with its own copy of Cisco SDM.

Q. What primary features are supported in Cisco SDM Version 2.2?

A. The primary features of Cisco SDM are listed in Table 1:

Table 1.

Feature	Benefit
New Hardware Support	
• NME-16ES-1G-P, NME-X-23ES-1G-1P, NME-XD-24ES-1S-P, and NME-XD-48ES-2S-P • USB Flash keys and USB eTokens • ADSL 2/2+ and ISDN HWICs • NM-1FE-FX-V2 and NM-1FE2W-V2	• Automatically recognize, configure, and monitors the new hardwares • IOS image management, digital certificate storage and secure credentials with USB tokens • VLAN trunking and Ethernet sub-interface configuration support
Application Firewall	
• Advanced firewall wizards, policy views, inspection rule editors and log views • P2P applications: BitTorrent, Kazaa, Gnutella, eDonkey • Instant Messaging: Yahoo, MSN, AOL • Protocol Conformance: HTTP & Email (SMTP/POP/IMAP)	• Delivers application level control and unified threat management for accelerated security solutions deployment • Protocol anomaly detection services • High, Medium, Low firewall policy settings for accelerated and easy deployment

Feature	Benefit
Granular Protocol Inspection	
• User customizable application to port (or port range) mapping	• More granular application inspection and control over TCP and UDP ports
Incident Control Services (ICS) Support	
• Trend Micro signatures	• Rapid deployment and customization of signatures for day-zero protection against new attacks
Network Admission Control (NAC)	
• Configuration wizard and client security posture management on routers	• Simple and fast integration of NAC into existing network infrastructure
Threat-Based Intrusion Protection	
• Threat based signature categories to ease IPS deployments • Signature creation wizards, event viewer	• Easier and more intelligent signature selection based on available resources, real time reporting of signature engine status
Dynamic DNS	
• HTTP and IETF based updates • Integration with existing WAN interface configuration wizard	• Scalable, remote management of dynamically addressed routers
Easy VPN Server and Remote Enhancement	
• Advanced wizards, remote config update, web intercept, dial backup and QoS support	• Scalable, easy to manage, secure remote access for teleworkers or small offices on hub routers or branch office access routers
Usability Improvements	• Ability to view in real-time SDEE alarms from IPS signature engines • Layer 3 and above Firewall Policy templates • Application Firewall Alarm log • NAT wizards to simplify IP Address management • Search toolbar for SDM UI pages, features and wizards

Q. What primary features are supported in Cisco SDM Version 2.1.1?

A. The primary features of Cisco SDM are listed in Table 2:

Table 2. Primary Features of Cisco SDM

Feature	Description
Interface Configuration (LAN and WAN)	• Ethernet, Fast Ethernet, Gigabit Ethernet • PPP over Ethernet (PPPoE): Autodetect PPPoE encapsulation • Asymmetric DSL (ADSL) and G.SHDSL, PPPoE and RFC 1483 Routing: Autodetect and autoconfigure xDSL • PPP over ATM (PPPoE) on xDSL interfaces • T1/E1 (serial: High-Level Data Link Control [HDLC], Point-to-Point Protocol [PPP], and Frame Relay) • ISDN Basic Rate Interface (BRI)

Feature	Description
Security Configuration	• Network Address Translation (NAT) • Access control list (ACL) • Firewall (Context-Based Access Control [CBAC]), policy-based configuration • IPSec VPNs: site-to-site VPN, Easy VPN Server, Easy VPN Remote Client v3, generic routing encapsulation [GRE] over IP Security [IPSec], Dynamic Multipoint VPN [DMVPN] hub and spoke • Digital Certificates (PKI) • Dial backup
System Configuration	• Host name, domain name, enabled secret password • Date and time • Hardware clock on Cisco 1800, 2800 and 3800 series routers • Dynamic Host Configuration Protocol (DHCP) (server, client, and relay) • Domain Name System (DNS) • IP services • Simple Network Management Protocol (SNMP) • User accounts with Role-Based access. Default access profiles – Administrator, Monitor (read-only), Firewall Administrator, Easy VPN Remote • vty (Telnet), SSHv1, SSHv2
Routing Configuration	• Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP) • Static routes
Security Audit	• Router security configuration checkup • Router security configuration recommendation • One-step router security lock-down
Monitoring	• System overview • Interface status • Firewall status • VPN status • Logging
Ease of Use (Wizards)	• Startup wizard, LAN wizard, WAN wizard, firewall wizard (with or without DMZ), VPN wizards (Easy VPN remote client, Easy VPN Server, site-to-site VPNs , GRE over IPSec, DMVPN hub, DMVPN spoke), QoS Policy, security audit, and one-step router lock-down
Online Help	• Help page for each window and dialog box • “How do I” tutorials for tasks not supported by wizard mode • Example scenarios and topologies on each wizard page • Background educational material on relevant security technology
Cisco SDM Upgrade	• Easy upgrade of Cisco SDM on router Flash memory from Cisco.com
Router Date and Time Setup	• Ability to automatically synchronize router clock with Network Time Protocol (NTP) servers or Cisco SDM management station
Router Management Access Policy	• Secure policy for remote router management across WAN interface
Xauth Login Prompt for IPSec Tunnels	• Ability to bring up IPSec tunnels waiting for Xauth authentication by giving authentication information through Cisco SDM

Feature	Description
Intrusion Prevention and Detection	• Ability to create Cisco IOS Software Intrusion Prevention System (IPS) rules, apply Cisco recommended pre-configured signatures, import latest signature package downloaded from Cisco.com, customize and deploy signatures, check SDEE log • Ability to provision and manage the Cisco Intrusion Detection System Network Module (part number NM-CIDS)
Logical Interface Support for VPN and Firewall	• Support for logical interfaces such as loopback for IPSec tunnels and firewall rules
VLAN Interface Support	• Support for VLAN interface configuration for Cisco EtherSwitch® ports
Cisco CNS Configuration Engine Integration	• Feature whereby Cisco SDM Startup wizard prompts the user to enter Cisco CNS 2100 Series Intelligence Engine) address to receive the final Cisco IOS Software configuration from a centralized provisioning system; this feature helps enable easy and highly scalable deployment of Cisco router customer premises equipment (CPE) without requiring costly staging or preinstalled custom configuration
New Router Home Page	• Improved design of the router home page for quick and easy retrieval of essential information about Cisco IOS Software configuration
Router Security Audit Improvement	• Ability to export Security Audit Report for printing or archiving purposes • Ability to unfix security configuration changes made by Security Audit. This allows the user to fine-tune the router security policy if it breaks some applications in the network.
Cisco SDM Express	• Offers quick and easy router deployment for basic WAN access configurations • Ideal router deployment tool for non-expert users
PC-Based SDM	• No extra Flash memory space required on router for SDM • Great tool to manage the installed base of Cisco routers
Integrated Wireless Management	• Reduce time and skill set required to bring up wireless interfaces • Offers flexibility to customize wireless configuration and security based on site-specific needs

Q. Which Cisco routers and Cisco IOS Software releases does Cisco SDM Version 2.2 support?

A. The supported routers and Cisco IOS Software releases are listed in Table 3.

Table 3. Supported Routers and Cisco IOS Software Releases

Router	Cisco IOS Software Version
Cisco Small Business 101, 106, and 107	• 12.3(8)YG or later
Cisco 831 and 837	• 12.2(13)ZH or later • 12.3(2)T or later
Cisco 836	• 12.2(13)ZH or later • 12.3(2)XA or later • 12.3(4)T or later
Cisco 851, 856, 871, 876, 877, and 878	• 12.3(8)YI or later
Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, 1760 and 1870V	• 12.2(13)ZH or later • 12.3(13)T3 or later • 12.3(1)M or later
Cisco 1801, 1802, 1803, 1811, and 1812	• 12.3(8)YI or later
Cisco 1841	• 12.3(8)T4

Router	Cisco IOS Software Version
Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, and 2651XM Multiservice Routers, and Cisco 2691 Multiservice Routers	• 12.2(15)ZJ3 or later • 12.2(11)T6 or later • 12.3(1)M or later
Cisco 2801, 2811, 2821, and 2851	• 12.3(8)T4 or later
Cisco 3620, 3640, 3661, and 3662	• 12.2(15)ZJ3 or later • 12.211)T6 or later • 12.3(1)M or later
Cisco 3725 and 3745	• 12.2(15)ZJ3 or later • 12.2(11)T6 or later • 12.3(1)M or later
Cisco 3825 and 3845	• 12.3(11)T or later
Cisco 7204VXR, 7206VXR and 7301	• 12.3(2)T or later • 12.3(1)M or later • No support for B, E, or S train releases on Cisco 7000 routers

Q. Does Cisco SDM reflect the changes made by the CLI or other Cisco SDM sessions?

A. Cisco SDM is designed to allow users to configure the router with both Cisco SDM and the CLI.

When Cisco SDM is launched, it reads the existing configuration and presents the features that it supports as available for configuration changes through the UI. Other aspects of the configuration that Cisco SDM does not understand are preserved but are not configurable through the UI.

Q. Can Cisco SDM be used by multiple users on the same router at the same time?

A. A common scenario for Cisco SDM is to have one or more users who are monitoring the router concurrently and at the same time another user may use Cisco SDM to modify the router configuration router.

It is **not** recommended that multiple users use Cisco SDM to modify the configuration at the same time. Although Cisco SDM permits this scenario, it does not assure consistent or predictable results.

Q. How am I ensured that Cisco SDM is a secure management tool?

A. Several safeguards are used to help ensure that access to a Cisco router with Cisco SDM is secure:

- Restricted Cisco SDM clients—The hosts that are allowed to access Cisco SDM (and the router HTTP server) can be configured through the UI page Additional Tasks -> Remote Access -> Management Access
- Signed applets—Cisco SDM is a Cisco signed applet; users must explicitly permit the download of the applet to their workstation.
- SSHv2 or SSHv1—Cisco routers can be configured through Cisco SDM for SSHv1 or SSHv2. If SSH is enabled on the router, Cisco SDM uses SSH to communicate Cisco IOS CLI with the router.
- HTTPS (Secure Sockets Layer [SSL])—Cisco SDM detects the presence of the SSL support in the HTTP server and recommends to users that they use the HTTPS protocol. With this choice the communication between your workstation and the Cisco router is secured with the SSL. Supported in most browsers, SSL enables information to be encrypted through the 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES).

Q. Does Cisco SDM support configuration over a WAN link after the router has been configured locally?

A. Yes. Cisco SDM can be used to configure the WAN link. 64kbps or above is recommended for better performance.

Q. Why is Cisco SDM implemented in Java?

A. Cisco SDM was developed as a client-heavy application in order to minimize the impact of Cisco SDM on router performance. Java is the industry standard for cross-platform applications. Its rich feature set and user-interface libraries allow Cisco SDM to provide a highly professional and esthetically appealing user interface.

Q. How many languages does SDM support?

A. Seven, English, Japanese, Simplifed Chinese, French, German, Spanish and Italian

SYSTEM REQUIREMENTS

Q. What are the minimum requirements of the browser client workstation to support Cisco SDM?

A. Cisco SDM is supported on Windows-based PC platforms and industry-standard browsers only:

- Windows 2003 Server (Standard Edition), Windows XP Professional, Windows 2000 Professional, Windows NT 4.0 Workstation (Service Pack 4), and Windows ME.
- Japanese, Simplified Chinese, French, German, Spanish and Italian language OS Support: Windows XP Professional, Windows 2000 Professional and installation of the respective language pack.

Note: Windows 2000 Advanced Server is **not** supported by Cisco SDM.

- Internet Explorer 5.5 or later or Netscape 7.1 and 7.2
- Java Virtual Machine (JVM) built-in browsers required, Java plug-in (Java Runtime Environment Version 1.4.2_05 or later)

Q. Is Java Plug-in Java Runtime Environment (JRE) supported, if yes which JRE version is supported?

A. Yes, Cisco SDM supports JRE version 1.4.2 or later. JRE is required to enable IPS feature in Cisco SDM. All other features in Cisco SDM (except IPS) are supported with built-in JVM in the browser.

Q. How much space will SDM take on router's flash?

A. Cisco SDM 2.1.1 requires minimum of 6 MB of free Flash memory (in the first partition, if the Flash memory is partitioned) on the router. Cisco SDM Express requires minimum of 2 MB of free Flash memory on the router. Cisco Wireless Management file requires additional 1.9 MB. Rest of the SDM files can be installed on PC hard disk.

Q. Does SDM use router’s CPU and DRAM when launched from the router?

A. Cisco SDM by itself has negligible impact on router CPU and DRAM since it utilizes PC’s CPU and DRAM during it’s execution. Every instance of Cisco SDM launched from the router opens one HTTP(s) and Telnet/SSH session to the router.

DOWNLOADING, UPGRADING, AND INSTALLING CISCO SDM

Q. How do I know if I have Cisco SDM Express or Cisco SDM loaded on router flash?

A. The quickest test is to connect your PC to the lowest-numbered Ethernet port with a cross-over cable and browse to http://<*router ip-adress*> and see if SDM Express or Cisco SDM launch point is present on the resulting web page. Please refer to Cisco Router and Security Device manager (SDM) quick Start Guide for PC configuration. Alternatively, you can use the CLI to check that the Cisco SDM files are present in the router Flash memory: enter **show flash** and look for the Cisco SDM file set: es.tar (for Cisco SDM Express), sdm.tar (for Cisco SDM), ips.tar (for IPS), wlanui.tar (for Cisco WLAN Application), home.tar, home.shtml, common.tar, and sdmconfig-xyz.cfg.

Q. How do I upgrade my router in order to run Cisco SDM?

A. Reference the detailed documentation for this process at http://www.cisco.com/go/sdm. Refer to the document *Downloading and Installing SDM*.

Q. How do I upgrade Cisco SDM files on the router?

A. Cisco SDM supports two upgrading methods, from Cisco.com or from a local PC. Launch the upgrade feature from “Tools” menu in Cisco SDM.

- **From Cisco.com**: Cisco SDM files are downloaded from Cisco.com to the local Cisco SDM management station, and then the Cisco SDM files are uploaded to routers.
- **From a local PC**: If you have the latest Cisco SDM files on the local Cisco SDM management station, you can upload Cisco SDM files to routers from the station.

You must ensure that the HTTP ACLs allow backing up Cisco SDM files from routers to a local Cisco SDM management station, and that the Remote Copy Protocol (RCP) ACLs allow copying new Cisco SDM files from a local Cisco SDM management station to routers.

Q. How do I install Cisco SDM files on my PC?

A. Please refer to Downloading and Installing Cisco Router and Security Device Manager.

Q. Does Cisco SDM installed on PC offers same features as Cisco SDM installed on the router flash?

A. Yes, Cisco SDM on PC also allows you to use SDM to manage other routers running proper IOS image on the network

Q. How do I link Cisco SDM Express with Cisco SDM installed on my PC?

A. Cisco SDM Express provide *Cisco SDM* launch tool.

Q. How do I launch Cisco SDM WLAN Application?

A. Cisco SDM WLAN Application can be launched from Cisco SDM/Configuration -> Interfaces and Connections

Q. What is SDM WLAN Application?

A. Please refer to Cisco Router and Security Device Manager: WLAN.

HOW DOES CISCO SDM WORK?

Q. What is the communication mechanism between Cisco SDM and the Cisco router?

A. Cisco SDM communicates with routers for two purposes: to access the Cisco SDM application files for download to the PC and to read and write the router configuration and status. Cisco SDM uses HTTP(s) to download the application files (sdm.tar, home.tar) to the PC. A combination of HTTP(s), Telnet/SSH is used to read and write the router configuration.

Q. How does Cisco SDM deliver configuration changes to the Cisco router?

A. For Cisco IOS Software Releases 12.3M and 12.3T, Cisco SDM uses a method that batches Cisco IOS configuration commands together and delivers by HTTP(s) to the router. For earlier Cisco IOS Software releases, Cisco SDM uses RCP as the transport. In both cases Cisco SDM relies on Telnet/SSH access for communication to the router for interactive Cisco IOS commands.

Q. How do I access Cisco SDM from the browser client workstation?

A. Cisco SDM prefers to communicate over SSL (HTTPS) to the router for both local and secure remote management; you have the choice to use the less secure HTTP.

Q. How does Cisco SDM support the advanced users who wish to validate the Cisco IOS Software configuration generated by Cisco SDM?

A. Cisco SDM allows advanced users to pre-review the CLI configurations that Cisco SDM is about to deliver to the router. SDM users can enable the “Preview CLI” option under the Edit -> Preference Menu item in Cisco SDM. Additionally, SDM users can export the running configuration as a text file through File -> Save Running Config to PC menu option.

Q. How do I update IPS signatures using Cisco SDM?

A. Please refer to Cisco Router and Security Device Manager: Intrusion Prevention System.

Q. How can I backup the router configuration using Cisco SDM?

A. Cisco SDM File Menu provides *Save Running Config to PC* function to backup the router configuration.

Q. How can I use Cisco IOS AutoInstall feature and with Cisco SDM installed on router?

A. Cisco SDM can now be ordered with a no factory default configuration option. Use ROUTER-SDM-NOCF or ROUTER –SDM-CD-NOCF part numbers to let manufacturing install Cisco SDM without a factory default Cisco IOS configuration. When the Cisco router starts up for the first time (without a factory default configuration) it will initiate the standard AutoInstall sequence. To use Cisco SDM on such a router make sure the IOS configuration contains the following lines

```
ip http server
ip http secure-server
ip http authentication local
ip http timeout-policy idle 600 life 86400 requests 10000
username username privilege 15 secret 0 password
line vty 0 4
privilege level 15
login local
transport input telnet ssh
logging buffered 51200 warning
```

Q. How does Cisco SDM handle unsupported interfaces?

A. For unsupported interfaces such as ATM, Cisco SDM automatically detects if the interface supports security features, CBAC, cryptography, access group, and NAT. If the security features are supported, you can use Cisco SDM to configure the security features to the unsupported interfaces.

You need to configure the unsupported interface parameters directly through the CLI.

Q. Can Cisco SDM be used to configure a router with an IP basic Cisco IOS image, e.g. without Firewall or VPN feature set?

A. Yes, you can use Cisco SDM to configure other available features such as LAN and WAN interfaces, routing protocols, access lists, and QoS Policies. However, if a certain feature is not available, such as a firewall or VPN, Cisco SDM disables the UI pages for that feature.

Q. What is a management policy?

A. The management policy feature allows the router administrator to easily create a rule to block management access (Web- and SNMP-based management applications) to the router except for specific remote management hosts or networks. Such a management policy is inherently more secure than opening the router to be remotely manageable by any external network or host.

To create a management policy launch Additional Tasks -> Router Access -> Management Access.

Q. Where are the configuration changes made by Cisco SDM stored?

A. Configuration changes are delivered to the router automatically when a wizard is successfully finished or changes are applied in Cisco SDM configuration pages. The router's running configuration (in DRAM) is modified, and optionally the router's startup configuration (in NVRAM) is modified. You can also choose to save the configuration file to your PC using the *Save Running Config to PC* option.

Q. What files are required for Cisco SDM's *Reset to Factory Default* feature to work?

A. Cisco SDM replaces the current startup configuration with a factory or default configuration and then reloads the router. The default configuration files are contained in the Cisco SDM image in Flash memory with the names, sdmconfig-xxxx.cfg, where the *xxxx* string denotes the relevant router platform.

After a *Reset to Factory Default*, the next invocation of Cisco SDM begins with the Startup Wizard.

Q. How do I know if the configuration on my router conforms to Cisco network security recommendations?

A. Cisco SDM provides a security audit feature. When invoked, Cisco SDM Security Audit checks your router configuration against a list of Cisco recommended settings, and presents you with a report card. This report card informs you about potential security problems identified. You can then instruct Cisco SDM which problem(s) to fix, and Cisco SDM then corrects the problems for you.

Q. Will I be blocked from accessing Cisco SDM by applying a security audit or one-step lock-down?

A. The Cisco SDM Security Audit feature by default limits access to the HTTP service by configuring an access class that permits access from only directly connected network nodes. This setting allows subnets of all inside interfaces to access the router with HTTP. Similarly, applying a default firewall policy through the firewall wizards or Firewall Policy page will block the user from accessing Cisco SDM from an outside interface. A warning dialog box is shown to the user before such an access list or firewall policy is applied to the router. It is recommended that Cisco SDM should be launched from an inside interface before applying a default firewall policy on the router.

Q. What features are enabled or disabled by the one-step lock-down function?

A. Table 4 lists all the actions that one-step lock-down performs: (any new additions/deletions in SDMv2.0)

Table 4. Actions Performed by One-Step Lock-Down

One-Step Lock-Down Action Items	Cisco IOS Software Equivalent
Disable Finger Service	`no service finger`
Disable Packet Assembler/Disassembler (PAD)	`no service pad`
Disable Small Servers (TCP and User Datagram Protocol [UDP])	`no service tcp-small-servers` `no service udp-small-servers`
Disable BOOTP	`no ip bootp server`
Disable Identification Service	`no ip identd`
Disable Cisco Discovery Protocol	`no cdp run`
Disable Source Routing	`no ip source-route`
Enable Password Encryption	`service password-encryption`
Enable TCP Keepalives for Inbound and Outbound Telnet Sessions	`service tcp-keepalives-in` `service tcp-keepalives-out`

Sequence Number and Time Stamps of All Debug and Log Messages	`service timestamps debug datetime localtime show-timezone msec`
	`service timestamps log datetime localtime show-timeout msec`
	`service sequence-numbers`

Enable Cisco Express Forwarding or Distributed Cisco Express Forwarding	`ip cef`
Cisco IOS Software Autosecure Residues	`no ip gratuitous-arps`
Minimum Password Length	`security passwords min-length 6`
Lock Access to Console or vty Line after Unsuccessful Attempts	`security authentication failure rate 3 log`

One-Step Lock-Down Action Items	Cisco IOS Software Equivalent
Tune Scheduler Interval or Allocation	**scheduler interval 500** **scheduler allocate 4000 1000**
Set tcp synwait Time to 10 Seconds	**ip tcp synwait-time 10**
Text Banner	**banner ~** Authorized access only! Disconnect IMMEDIATELY if you are not an authorized user! ~
Enable Logging for Security and Sequence Numbers with Input for Logging Server	**logging on** **logging console critical** **logging trap debugging** **logging buffered 51200**
For Cryptographic Cisco IOS Software Images, Enable Secure Shell (SSH) Protocol and Serial Control Protocol (SCP) for Access and File Transfer **Set SSH Timeouts and Retries to the Minimum Possible**	**!** **ip ssh time-out 60** **ip ssh authentication-retries 2** **!** **line vty 0 4** **transport input ssh telnet** *(def: Telnet)* **!**
Disable SNMP if Not Being Used	Only Disable SNMP: **no snmp-server**
Enable NetFlow on Software Forwarding Platforms	**int** *<all-interfaces>* **ip route-cache flow**
Disable Internet Control Message Protocol (ICMP) Redirects	**int** *<all-interfaces>* **no ip redirects**
Disable Proxy-arp	**int** *<all-interfaces>* **no ip proxy-arp**
Disable Directed Broadcast	**int** *<all-interfaces>* **no ip directed-broadcast**
Disable MOP Service on Ethernet Interfaces	**int** *<all-Ethernet&FastEthernet_interfaces>* **no mop enabled**
Disable ICMP Unreachables on All Interfaces	**int** *<all-interfaces>* **no ip unreachables**
Disable Mask Reply Messages	**int** *<all-interfaces>* **no ip mask-reply**
Disable Sending Unreachable Messages to the Source for the Packets that are Discarded or Routed to NULL	**int null 0** **no ip unreachables**

INTEROPERABILITY AND RELATIONSHIP TO OTHER CISCO APPLICATIONS

Q. How do Cisco SDM and the Cisco Router Web Setup (CRWS) tool relate to each other on my Cisco 830 Series routers?

A. For Cisco 830 Series routers, either the Cisco Router Web Setup tool or Cisco SDM can be used for configuration. CRWS is ideally suited for simple WAN access configuration of Cisco 830 Series routers. Cisco SDM should be used when security configurations (firewall, site-to-site VPNs, NAT, ACLs, etc.) are required or the Cisco 830 users want a more secure method of managing their routers (for example, SSL- or SSH-based management). Here's the link to the document for switching a router from CRWS to SDM:
http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a0080404969.html

Q. How do Cisco SDM and Cisco IP Solution Center (ISC) relate to each other?

A. The Cisco ISC offers a highly scalable security management solution for Cisco IOS Software routers and Cisco security appliances. The Cisco ISC can cost-effectively scale to 10,000 or more devices. Cisco SDM complements network operations center (NOC)-based centralized management tools such as the Cisco ISC by aiding the deployment of LAN, WAN, and security features at the device level.

Q. How do Cisco SDM and CiscoWorks VPN/Security Management Solution (VMS) relate to each other?

A. CiscoWorks VMS offers an enterprise-class, centralized management solution for Cisco IOS Software routers and Cisco security appliances. Cisco SDM complements NOC-based centralized management tools such as the Cisco ISC by aiding the deployment of LAN, WAN, and security features at the device level.

Q. How do Cisco SDM and Cisco PIX® Device Manager relate to each other?

A. Cisco PIX Device Manager is a secure, Web-based device management tool for Cisco PIX security appliances. Cisco SDM is an intuitive, secure, Web-based device management tool embedded within the Cisco IOS Software-based routers. Both tools, Cisco PIX Device Manager and Cisco SDM, can be launched from a common Windows workstation to manage Cisco PIX Firewall or Cisco IOS Software routers, respectively.

Q. How do Cisco SDM and Cisco QoS Device Manager (QDM) relate to each other?

A. Cisco QoS Device Manager was a web-based application for configuring QoS Policies on some select models of Cisco Routers. Cisco QDM has now been End of Life and is not longer available. Cisco SDM now supports configuration of QoS policies on router interfaces and VPN tunnels (except EzVPN Remote). Additionally Cisco SDMv2.0 supports monitoring of QoS policies using NBAR based application traffic analysis and protocol discovery.

Q. How do Cisco SDM and Cisco Auto-QoS Enterprise feature relate to each other?

A. Cisco Auto-QoS Enterprise is a feature in Cisco IOS to automatically create QoS policies on WAN interfaces based on the real-time traffic analysis. Cisco SDM allows the user to view Auto-QoS generated QoS policies.

Cisco SDM does not use Auto-QoS commands for QoS policy configuration on the router but relies on modular QoS CLI (MQC) and NBAR protocol discovery engine. Please also refer to Cisco Router and Security Device Manager: Quality of Service.

Q. How do Cisco SDM Role-based Access and Cisco IOS Roles-based CLI access feature relate to each other?

A. Role-based CLI access or CLI Views feature was initially introduced in the 12.3(7)T release of Cisco routers. In 12.3(8)T several critical enhancements to this feature were committed to make it compatible with Cisco SDM.

Cisco SDM leverages the role-based CLI access feature to provide 4 factory default access profiles: Administrator, Firewall-Admin, Monitor, and EasyVPN Remote. All manually created access profiles (or views) are treated as Monitor (or Read-only) view by SDM.

To add users with specific access profiles launch Configure -> Additional Tasks -> Router Access -> User Account/CLI Views. Please refer to Cisco Router and Security Device Manager Role-Based Access.

LIMITATIONS AND WORKAROUNDS

Q. Is there a limitation on the size of the configuration that Cisco SDM can handle?

A. No, there is no inherent limitation on the size of the configuration file, but very large files that are more than **250 KB** can lead to slower performance of the user interface.

Q. Can NTP time be overridden by manual settings on the router?

A. No, if the router has already synchronized with the NTP server, manual settings will not change the router clock.

Q. Is Channelized T1/E1 supported by Cisco SDM?

A. No.

Q. Does Cisco SDM reflect the changes made by the Cisco SDM WLAN GUI?

A. Cisco SDM does not load the changes made on non-wireless specific parameters, such as interfaces and AAA servers through the Cisco WLAN Application automatically. Use Cisco SDM *Refresh* feature to reload the changes made by Cisco WLAN Application.

Q. Can I use Cisco SDM WLAN Application to configure a local authenticator (AAA) to serve as a stand-alone authenticator for a small wireless LAN?

A. Yes, please refer to Cisco Router and Security Device Manager: WLAN.

Note: You must enter 1812 as the authentication port and 1813 as the accounting port.

FOR MORE INFORMATION

For more information about Cisco Router and Security Device Manager, visit http://www.cisco.com/go/sdm or contact your local Cisco account representative.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205404.BE_ETMG_KL_9.05

Printed in the USA