



# Cisco Router and Security Device Manager

The screenshot displays the Cisco Router and Security Device Manager (SDM) interface for a Cisco 2801 router. The window title is "Cisco Router and Security Device Manager (SDM): 10.70.237.68". The interface includes a menu bar (File, Edit, View, Tools, Help) and a toolbar with icons for Home, Configure, Monitor, Refresh, Save, Search, and Help. The main content area is divided into several sections:

- About Your Router:** Host Name: 2801. Hardware: Model Type: Cisco 2801, Available / Total Memory(MB): 182/256 MB, Total Flash Capacity: 61 MB. Software: IOS Version: 12.4(11)T, SDM Version: 2.4. Feature Availability: IPv4, IPv6, NAT, etc.
- Configuration Overview:** Includes sections for Interfaces and Connections, Firewall Policies, VPN, Routing, and Intrusion Prevention.

Interfaces and Connections	
Total Supported LAN:	2
Configured LAN Interface:	2
DHCP Server:	Not Configured
Total Supported WAN:	0
Total WAN Connections:	0

VPN	
IPSec (Site-to-Site):	1
Xauth Login Required:	0
No. of DMVPN Clients:	0
GRE over IPSec:	0
Easy VPN Remote:	0
No. of Active VPN Clients:	0

Routing	
No. of Static Route:	1
Dynamic Routing Protocols:	None

Intrusion Prevention: IPS not supported

10:10:57 PCTime Mon Apr 02 2007

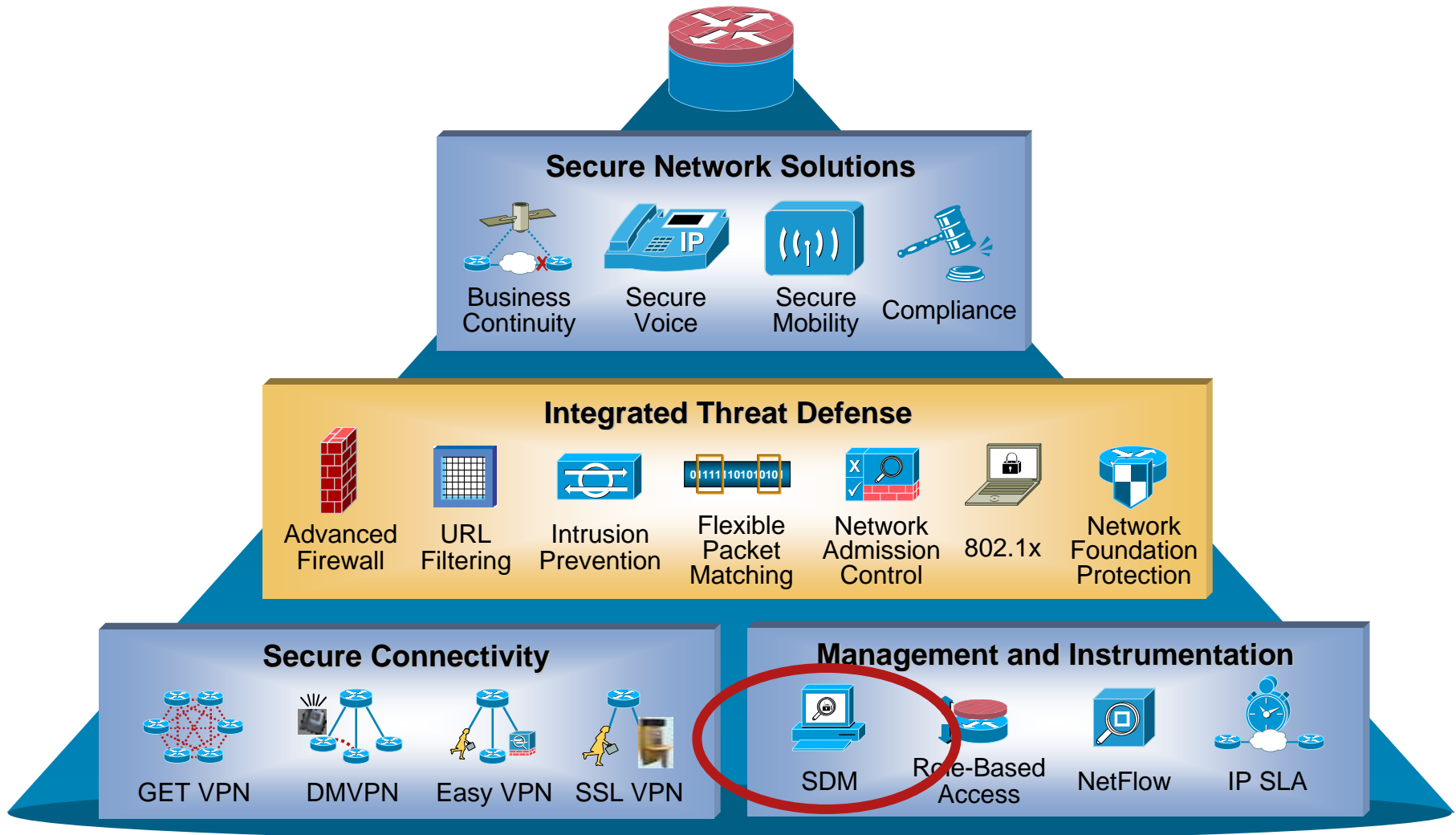


# Agenda

- Cisco Security Technology and Management
- SDM v2.5 Features and Benefits
- SDM Availability and Ordering

# Cisco Security Technologies

## Cisco Integrated Service Routers



# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>Cisco Easy VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures password expiry via AAA—12.4(6)T and onwards feature</li></ul>	<ul style="list-style-type: none"><li>▪ Cisco Routers running Cisco IOS® VPN Server today support password aging where the user is prompted to change his password if it has expired rather than receive an authentication failure with no clear reason code as before</li></ul>
<p><b>Cisco Easy VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures split DNS—12.4(9)T and onwards feature</li></ul>	<ul style="list-style-type: none"><li>▪ Split-DNS enables the Cisco Easy VPN Client to act as a “DNS proxy,” directing Internet queries to the DNS server of the ISP and directing corporate DNS requests to the corporate DNS servers</li></ul>

# SDM v2.5 Features and Benefits

**Available  
December 2007**

Feature	Benefits
<p><b>Cisco Easy VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures Cisco Tunneling Control Protocol (cTCP)—12.4(9)T and onwards feature</li></ul>	<ul style="list-style-type: none"><li>▪ When Cisco Tunneling Control Protocol is enabled on client and head end devices, IKE and Encapsulating Security Payload (ESP) traffic will be encapsulated in the TCP header, so that the firewalls in between the client and the head end device would simply permit this traffic, perceiving it as TCP traffic</li></ul>
<p><b>Cisco Easy VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures per-user AAA policy download with PKI—12.4(4)T and onwards feature</li><li>▪ The username to get the attributes from AAA server will be obtained from digital certificate of the client. The attributes can be ACLs, QoS policies, etc. These attributes are configured on the RADIUS servers</li></ul>	<ul style="list-style-type: none"><li>▪ The Easy VPN server can download user specific attributes for a remote client from the AAA server and push them to the client during mode configuration</li></ul>

# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>Cisco Easy VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures identical addressing—12.4(11)T and onwards feature</li><li>▪ Identical IP feature works only with EasyVPN Remote configured in 'Network-Extension' mode</li><li>▪ This feature is an EasyVPN Remote side functionality enhancement. Its implementation involves no change on the existing EasyVPN Server configuration</li><li>▪ EasyVPN Remote is configured with Virtual Tunnel Interface</li></ul>	<ul style="list-style-type: none"><li>▪ 'EasyVPN Remote Identical Addressing' feature combines NAT with EasyVPN in order to allow remotes with overlapping internal IP Addressing to connect to the Server</li></ul>

# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>Cisco SSL VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures port forwarding (Thin-Client)—Auto applet download functionality and Port-Forward Enhancements</li><li>▪ Port forwarding requires a very small application that runs on the end user's system, often in the form of Java or ActiveX</li><li>▪ The client application is a port forwarder that listens for connections on a port that are defined for each application. When packets come in on that port, they are tunneled inside of an SSL connection to the SSL VPN device, which unpacks them and forwards them to the real application server</li></ul>	<ul style="list-style-type: none"><li>▪ To use the port forwarder, the end user simply points the application he wants to run at his own system rather than the real application server</li></ul>

# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>Cisco SSL VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures RADIUS accounting</li></ul>	<ul style="list-style-type: none"><li>▪ RADIUS accounting allows for a session to be accounted for by indicating when the session starts, and when it stops</li><li>▪ Additionally, session identifying information and session usage information will be passed to the RADIUS server via RADIUS attributes and VSA (Vendor Specific Attributes)</li><li>▪ Integrate RADIUS accounting for SSLVPN sessions</li></ul>
<p><b>Cisco SSL VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures application ACL support</li></ul>	<ul style="list-style-type: none"><li>▪ Provides greater granularity of control than traditional network layer ACLs</li></ul>

# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>Cisco SSL VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures RADIUS accounting</li></ul>	<ul style="list-style-type: none"><li>▪ RADIUS accounting allows for a session to be accounted for by indicating when the session starts, and when it stops</li><li>▪ Additionally, session identifying information and session usage information will be passed to the RADIUS server via RADIUS attributes and VSA (Vendor Specific Attributes)</li><li>▪ Integrate RADIUS accounting for SSLVPN sessions</li></ul>
<p><b>Cisco SSL VPN</b></p> <ul style="list-style-type: none"><li>▪ Configures application ACL support</li></ul>	<ul style="list-style-type: none"><li>▪ Provides greater granularity of control than traditional network layer ACLs</li></ul>

# SDM v2.5 Features and Benefits



Feature	Benefits
<p>Cisco SSL VPN</p> <ul style="list-style-type: none"><li>▪ URL Obfuscation (Clientless mode)</li></ul>	<ul style="list-style-type: none"><li>▪ A user can connect in with little requirements beyond a basic web browser. The user would have the ability to reach web servers or webified resources like file shares</li></ul>

# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>Cisco SSL VPN</b></p> <ul style="list-style-type: none"><li>▪ Transcend Client Support—Phase 1</li></ul>	<ul style="list-style-type: none"><li>▪ Support for additional client-side platforms such as Apple-Mac, Linux and PDAs</li><li>▪ The VPN client could also use additional transport mechanism such as DTLS which is more suitable for real time traffic as well as the cases when the underlying network is jittery (due to TCP over TCP issues)</li><li>▪ The transcend client can also be installed in a standalone mode instead of being GW-downloadable. In this mode, transcend client will work like a browser for authentication with the GW; saving the download time/bandwidth</li></ul>

# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>WAAS Hardware Supported</b></p> <ul style="list-style-type: none"><li>▪ NME-WAE-502-K9</li><li>▪ NME-WAE-522-K9</li><li>▪ NME-WAE-302-K9</li><li>▪ Configures WCCP and an IP address on the WAE module. Registers the WAE module with the WAAS central manager</li></ul>	<ul style="list-style-type: none"><li>▪ A single user interface to configure the router and also provide for initial configuration and monitoring of the WAAS network module</li></ul>

# SDM v2.5 Features and Benefits



**Available  
December 2007**

Feature	Benefits
<p><b>Cable Hardware Supported</b></p> <ul style="list-style-type: none"><li>▪ Cisco c815 router</li><li>▪ HWIC-CABLE-D-2</li><li>▪ HWIC-CABLE-E/J-2</li></ul>	<ul style="list-style-type: none"><li>▪ Allows easy configuration of the cable interface including setting IP address on the cable interface</li><li>▪ Allows monitoring of key statistics like bandwidth on upstream and downstream traffic</li></ul>
<p><b>Wireless Hardware Support</b></p> <ul style="list-style-type: none"><li>▪ Airlink Phase II</li></ul>	<ul style="list-style-type: none"><li>▪ Allows configuration of a rich set of features in a single UI</li><li>▪ Advanced Encryption Service (AES), IEEE 802.1x Local authentication service for EAP-FAST, SSID globalization, Multiple Basic Service Set ID (BSSID), wireless root, non-root bridge and universal client mode, multiple encrypted VLANs, VLAN assignment by name, Wi-Fi multimedia required elements</li></ul>

# SDM v2.5 Features and Benefits



Feature	Benefits
<p><b>Additional Hardware Supported</b></p> <ul style="list-style-type: none"> <li>18xx SKUs supported</li> </ul>	<ul style="list-style-type: none"> <li>CISCO1801-M/K9, CISCO1801W-AG-E/K9, CISCO1801W-AG-C/K9, CISCO1801WM-AGE/K9, CISCO1801W-AG-A/K9, CISCO1801W-AG-N/K9, CISCO1802W-AG-E/K9, CISCO1803W-AG-A/K9, CISCO1803W-AG-E/K9, CISCO1811W-AG-A/K9, CISCO1811W-AG-C/K9, CISCO1811W-AG-N/K9, CISCO1812/K9, CISCO1812-J/K9, CISCO1812W-AG-P/K9, CISCO1812W-AG-C/K9, CISCO1812W-AG-E/K9, CISCO1812W-AG-J/K9, CISCO1801, CISCO1801/K9, CISCO1801W-AG-B/K9, CISCO1802, CISCO1802/K9, CISCO1802, CISCO1903/K9, CISCO1803G-B/K9, CISCO1811/K9, CISCO1811W-AG-B/K9</li> </ul>

# SDM Supported VPN Technologies

## Industry-Leading VPN Solutions

Solution	Key Technologies
Standard IPSec	<ul style="list-style-type: none"><li>▪ Full standards compliance for interoperability with other vendors</li></ul>
Advanced Site-to-Site VPN	<ul style="list-style-type: none"><li>▪ Hub-and-Spoke VPN<ul style="list-style-type: none"><li>Enhanced Easy VPN—Dynamic Virtual Tunnel Interfaces, Reverse Route Injection, dynamic policy push and high scalability</li><li>Routed IPSec + GRE or DMVPN with dynamic routing</li></ul></li><li>▪ Spoke-to-Spoke VPN: Dynamic Multipoint VPN (DMVPN)—On-demand VPNs (partial mesh)</li></ul>
Advanced Remote Access VPN	<ul style="list-style-type: none"><li>▪ Easy VPN (IPSec): Cisco dynamic policy push and FREE VPN Clients for Windows, Linux, Solaris and Mac platforms</li><li>▪ SSL VPN: No client pre-installation required and provides end-point security through Cisco Secure Desktop</li></ul>

# Cisco Routers and Cisco IOS Release Support

SDM-Supported Platforms	Minimum Supported Cisco IOS Versions
SB 101, SB 106, SB 107	12.3(8)YG
831, 836, 837	12.2(13)ZH, 12.3.2XA, 12.3(2)T
851, 857, 871, 876, 877, 878	12.3(8)YI
1701, 1711, 1712	12.2(15)ZL, 12.3.2XA
1710, 1721, 1751, 1751-v, 1760, 1760-v	12.2(13)ZH, 12.2(13)T3
1801, 1802, 1803, 1811, 1812	12.3(8)YI
1841	12.3(8)T4
2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691	12.2(11)T6, 12.3(1)M, 12.3(2)T
2801, 2811, 2821, 2851	12.3(8)T4
3620, 3640, 3640A, 3661, 3662	12.2(11)T6, 12.3(1)M, 12.3(2)T
3725, 3745	12.2(11)T6, 12.3(1)M, 12.3(2)T
3825, 3845	12.3(11)T
7204VXR, 7206VXR, 7301	12.3(2)T, 12.3(3)M

# Cisco SDM Availability and Ordering

830-SDM; Cisco SB 100, 850, and 870 Series 1700 and 2600XM Security Bundles  Cisco 1800 Series Routers (except Cisco 1841 Router model with more than 64 MB flash memory)	SDM Express on Flash, SDM CD bundled
Cisco 1841 Router Model (flash memory greater than 64 MB)	SDM factory-installed (no SDM CD)
Cisco 2800 and 3800 Series Routers (all SKUs including Bundles)	SDM factory-installed (no SDM CD)
2691, 3700, 7204VXR, 7206VXR, 7301 Security Bundles	SDM factory-installed (no SDM CD)

**SDM Can Be Downloaded from CCO for Existing Routers:**

<http://www.cisco.com/cgi-bin/tablebuild.pl/sdm>

# SDM Localization

## Six languages to be supported

- German, French, Spanish, Italian, Japanese and Simplified Chinese
- Applicable to all user interface, screens, wizards, online help, tutorials and marketing material translated
- Image upgrade will automatically pick the installed language version



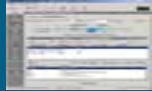


# Backup Slides



# Cisco Security Management Suite

## Cisco Security Device Manager



Quickest way to setup a device

Wizards to configure firewall, IPS, VPN, QoS, and wireless

Ships with device

## Cisco Security Manager

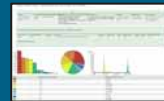


New solution for configuring routers, appliances, switches

New user-centered design

New levels of scalability

## Cisco Security MARS



Solution for monitoring and mitigation

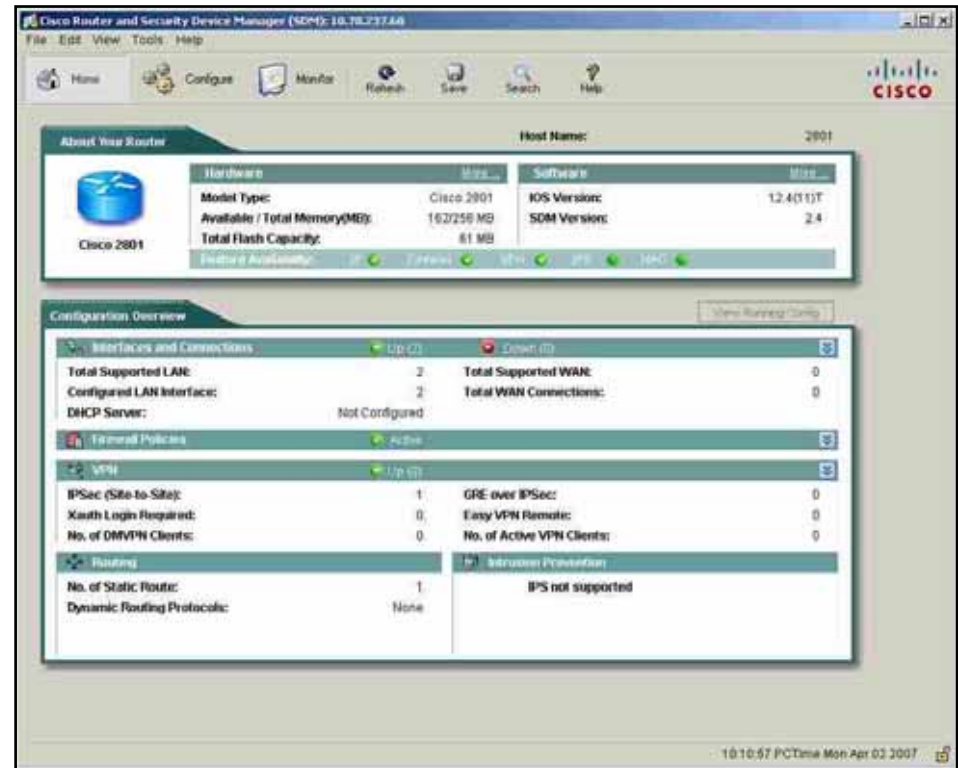
Uses control capabilities within infrastructure to eliminate attacks

Visualizes attack paths

# Ease of Use and Application Intelligence

Cisco Security Device Manager (SDM) Is an Intuitive, Web-Based Tool

- Ease of Use: Smart wizards, built-in tutorials
- Application Intelligence: Knowledge base of TAC-approved Cisco IOS configurations
- Integrated Services Management: Routing, switching, security, wireless, QoS

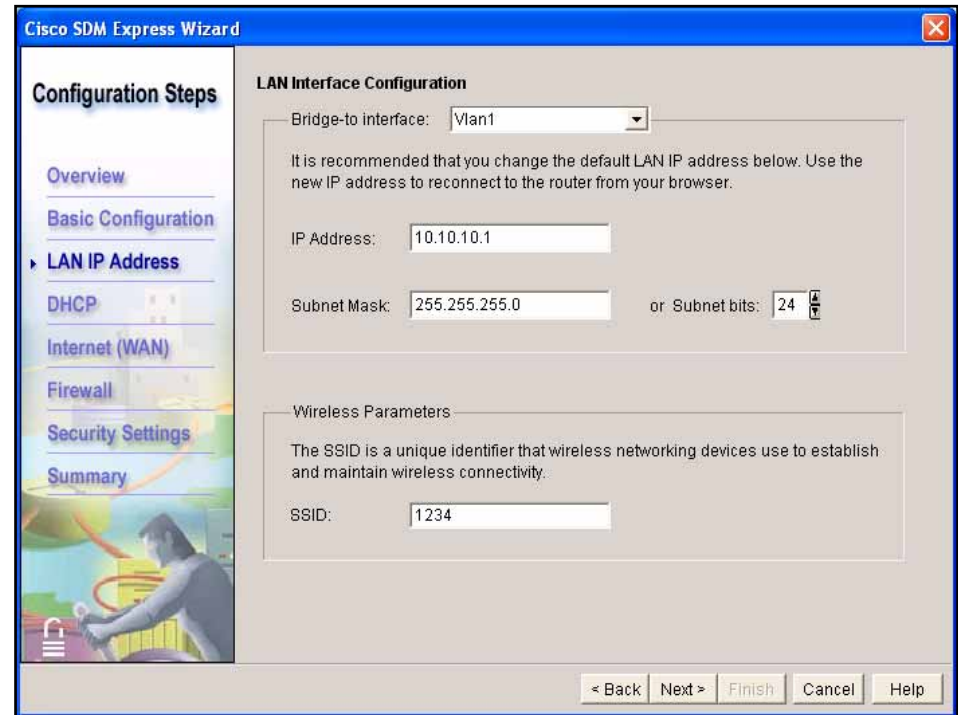


# Ease of Initial Configuration

- Less than 30 minutes to deploy

WAN and LAN ports,  
DHCP server, WLAN,  
Firewall, Auto-security

- SDM Express designed for novice users



The screenshot displays the Cisco SDM Express Wizard interface. On the left, a vertical sidebar titled "Configuration Steps" lists various configuration options: Overview, Basic Configuration, LAN IP Address (which is currently selected and expanded), DHCP, Internet (WAN), Firewall, Security Settings, and Summary. The main window is titled "LAN Interface Configuration" and contains the following fields and text:

- Bridge-to interface:** A dropdown menu showing "Vlan1".
- IP Address:** A text input field containing "10.10.10.1".
- Subnet Mask:** A text input field containing "255.255.255.0".
- or Subnet bits:** A text input field containing "24".
- Wireless Parameters:** A section with a text input field for "SSID" containing "1234".

Below the configuration fields, there is a note: "It is recommended that you change the default LAN IP address below. Use the new IP address to reconnect to the router from your browser." and another note: "The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity." At the bottom right of the window, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

# Customer and Partner Benefits

	Features	Benefits
Ease of Use	Graphical user interface	Reduce TCO/enhanced productivity
Application Intelligence	Built-in knowledge of interactions between different Cisco IOS features, industry best practices, and TAC-recommended configurations	Improve network uptime through reduced instances of configuration errors
Real-Time Graphical Monitoring and Role-Based Access	Easy-to-comprehend charts of router and network resource usage; read-only user profile	<p>Make effective use of IT staff and remote branch administrators with limited technical expertise</p> <p>Service providers can reduce OpEx by offering a graphical read-only view of the CPE services to end customers</p>
WAN and VPN Troubleshooting	Troubleshooting integrated with Cisco TAC knowledge base of recovery actions	Reduce mean time to repair (MTTR) by leveraging integration of routing, LAN, WAN, and security features on the router for detailed troubleshooting

# SDM Usage Scenarios

- Cisco router initial deployment

  - SDM Express wizard for quick LAN, WLAN, WAN, and security setup

  - Integration with IE2100/CNS for mass deployments

  - Reduced skill set, faster deployment time

- Cisco IOS security management

  - Integrated routing and security configuration, monitoring, and troubleshooting

  - Graphical firewall and ACL policy view (traffic flows)

  - IPSec VPNs (configuration and monitoring) with QoS

  - NAT wizards

# SDM Usage Scenarios— Value-Added Services

- Security solutions deployment

IPSec VPN (site-to-site, RA) configuration and monitoring

NAT, firewall, IPS, access control policies, security audit

**Application-level security** with granular protocol inspection and application firewall support (P2P, IM, HTTP, SMTP/POP/IMAP)

**Collaborative security solutions** support with NAC configuration wizards and Cisco Incident Control Services (ICS) management

- Day-to-day router operations

Performance monitoring, interface status, hardware and software inventory, WAN/VPN troubleshooting

Syslog/firewall log, VPN tunnel monitoring, security audits

Search bar for easy navigation between SDM user interface and wizards

# SDM Usage in Managed CPE and MSSP

Usage Scenario	Business Benefit
Pilots and Proof of Concept	<ul style="list-style-type: none"><li>▪ Accelerates new feature acceptance (e.g., IPS, EzVPN Server, firewall)</li><li>▪ Quickly generate standard configurations for cookie-cutter deployments</li></ul>
Cisco Router Initial Deployment	<ul style="list-style-type: none"><li>▪ Minimal-touch mass deployment of CPE</li><li>▪ End-user self-installation or installation by less-skilled technician</li></ul>
Partial CPE Control to End User	<ul style="list-style-type: none"><li>▪ Firewall policies managed by end user, other services managed by service provider</li><li>▪ Read-only access to end user to check firewall logs</li><li>▪ Quicker bring-up of downed VPN tunnels</li></ul>
Day-to-Day Router Operations (Monitoring and Troubleshooting)	<ul style="list-style-type: none"><li>▪ Device/service-specific troubleshooting and recovery by NOC staff</li><li>▪ End-user self-help tool for troubleshooting</li></ul>

# Comprehensive Cisco IOS Feature Support

UI Features	SDM Express, performance monitor, syslog viewer, reset to factory, security audit, one-stop router lockdown and search toolbar
VPN	Easy VPN Server, Easy VPN Remote, Enhanced Easy VPN (DVTI), IPsec, SSL VPN, GRE over IPsec, DMVPN (full-mesh or hub-spoke), V3PN, digital certificates, VPN monitor, and troubleshooting
Firewall	Zone-based firewall, stateful inspection, application firewall, granular protocol inspection, DMZ, firewall log and policy table
Intrusion Prevention (IPS)	SDM v2.4 is compatible with Cisco IOS IPS feature in 12.4(11)T2 release in addition to 12.4(9)T or earlier T-Train and Cisco IOS 12.4 Mainline releases (automatic signature provisioning, dynamic signature update and signature customization, event viewer, signature creation wizards, threat-based signature categories)
Routing	OSPF, EIGRP, RIPv2 and static
Interfaces	10/100/1000 Ethernet, Dot11a/b/g, xDSL, Serial T1/E1, ISDN BRI, AM, 802.1x L2 port, 802.1x L3 spouse and kids feature and wireless
WAN	FR, PPPoA, PPPoE, PPP, HDLC, RFC 1483, dial-backup, ADSL autodetect, QoS, NBAR and troubleshooting
Advanced Configuration	Cisco IOS CA server, AutoQoS phase II, NAT wizards, ACL, VLAN, CLI preview mode, DHCP server, WLAN, date/time, NTP, DNS, SSHv2, management access policy and dynamic DNS