To stay competitive in a challenging marketplace, small and medium-sized businesses (SMBs) must continually control costs, overcome competitive pressures, and manage resources while maintaining business integrity and network security. At the same time, they must improve their business efficiency and respond to customers more quickly. The Cisco® Secure Network Foundation helps businesses match technology and network solutions to meet these critical business challenges—both today and in the future.

The Cisco Secure Network Foundation provides a flexible communications platform that serves as the cornerstone to an organization's information needs and the foundation for other networking solutions as the business evolves. The Cisco Secure Network Foundation delivers performance, built-in security, and high reliability, to help ensure that data is protected and that applications function as promised.

Designed for today's increasingly mobile businesses, the Cisco Secure Network Foundation also helps enhance productivity by making information and business applications accessible anywhere, anytime.

**Business Benefits for Today and Tomorrow**

Because each business is unique, its evolution and use of technology will be as well. The Cisco Smart Business Roadmap provides a structured, planned evolution path to help businesses keep pace with change and make smart technology purchases. The roadmap is designed to enable SMBs to align a network technology plan with their business priorities. And it gives business and technical decision makers the confidence of knowing that their immediate technology investments will support their long-term goals.

The Cisco Secure Network Foundation is an integral part of the Cisco Smart Business Roadmap. With the Cisco Secure Network Foundation, SMBs can unlock a variety of benefits:

- **Provides a complete solution**—Cisco SMB solutions are easy-to-manage, end-to-end solutions, eliminating the trouble of trying to join together different devices from many manufacturers.
- **Helps keep costs affordable**—Cisco SMB networking products are tailored to meet the specific needs of small businesses. They will help you protect your network and make the most of the equipment you have already purchased—to meet your business needs now and tomorrow.
- **Helps you keep ahead of your competition**—Easy-to-use products let you quickly reach the network tools you use every day and respond to your customers' needs. Their flexible design lets you change or build on the network to meet new business demands.
- **Shields the network from attacks**—Cisco Self-Defending Network technologies help you protect your network from hackers, viruses, and other threats. They will help you keep your business operations up and running while you safeguard your most important business data.
- **Helps your employees accomplish more**—Giving your employees secure wired and wireless access to the Internet, e-mail, and other network tools can help them be more productive and respond to customers more quickly. They can even work from home or on the road, and enjoy better job satisfaction.
- **Provides smooth, reliable operation**—Reliable technical support resources like Cisco SMB Support Assistant are available when you need them. Trained Cisco support staff deliver the high level of customer service you expect, and answer your questions quickly and professionally. Cisco services and support are an affordable way to help businesses protect their networks and keep them running smoothly and reliably. Designed precisely for SMBs, the Cisco Secure Network Foundation meets all of your networking needs, so you can carry on with your business.

To help make the Cisco Secure Network Foundation a reality, Cisco provides easy-to-use blueprints for extending network capability to support advanced applications in businesses from fewer than 20 users up to 500 users. These blueprints are based on Cisco extensive experience in creating networks for successful SMBs.

Cisco Secure Network Foundation Blueprints for SMBs are formulated according to size:

- Security Blueprint: 20 to 100 user ports per site
- Security Blueprint: 100 to 250 user ports per site
- Security Blueprint: 250 to 500 user ports per site
Secure Network Foundation Blueprint: 20 to 100 Users

This reference blueprint provides a network diagram and product table for your main office, remote office, and teleworkers. This is only a suggested blueprint.

Security Blueprint for SMBs with 20 to 100 User Ports per Site

Main Business Location
20–100 Users

Remote Site

Teleworker

Product Table

This product table identifies Cisco solutions for SMBs with 20 to 100 user ports per site. It is intended to be a starting point in choosing Cisco products for your main business location, remote offices, and teleworker connectivity.

Solution Features for Main Business Location and Remote Sites

<table>
<thead>
<tr>
<th>Main Business Location</th>
<th>20–100 Users (SMB Complete)</th>
<th>20–100 Users (SMB Enhanced)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>• Cisco 2801 Integrated Services Routers&lt;br&gt;• Cisco 2811 Integrated Services Routers&lt;br&gt;• Cisco 2851 Integrated Services Routers&lt;br&gt;• Cisco 2861 Integrated Services Routers&lt;br&gt;• Cisco 2861 Integrated Services Routers</td>
<td>• Cisco 2811 Integrated Services Routers&lt;br&gt;• Cisco 2851 Integrated Services Routers&lt;br&gt;• Cisco 2861 Integrated Services Routers&lt;br&gt;• Cisco 2861 Integrated Services Routers&lt;br&gt;• Cisco 2861 Integrated Services Routers</td>
</tr>
<tr>
<td>Integrated security</td>
<td>• Cisco Security Agent for corporate servers&lt;br&gt;• VPN, firewall, and intrusion prevention with Cisco IOS® Software Advanced Security image&lt;br&gt;• Cisco Security Agent for corporate servers&lt;br&gt;• VPN, firewall, and intrusion prevention with Cisco IOS® Software Advanced Security image</td>
<td>• Cisco Security Agent for corporate servers&lt;br&gt;• VPN, firewall, and intrusion prevention with Cisco IOS® Software Advanced Security image&lt;br&gt;• Cisco Security Agent for corporate servers&lt;br&gt;• VPN, firewall, and intrusion prevention with Cisco IOS® Software Advanced Security image</td>
</tr>
<tr>
<td>Integrated wireless LAN controller</td>
<td>Cisco Wireless LAN Controller Modules</td>
<td>Cisco Wireless LAN Controller Modules</td>
</tr>
<tr>
<td>External switch</td>
<td>• Cisco Catalyst® Express 500 Series Switches&lt;br&gt;• Cisco Catalyst 2960 Series Switches</td>
<td>• Cisco Catalyst 2960 Series Switches&lt;br&gt;• Cisco Catalyst 3960 Series Switches</td>
</tr>
<tr>
<td>WLAN access points (external)</td>
<td>• Cisco Aironet® 1000 Series Lightweight Access Points&lt;br&gt;• Cisco Aironet 1130 AG Series Access Points&lt;br&gt;• Cisco Aironet 1230 AG Series Access Points</td>
<td>• Cisco Aironet 1000 Series Lightweight Access Points&lt;br&gt;• Cisco Aironet 1130 AG Series Access Points&lt;br&gt;• Cisco Aironet 1230 AG Series Access Points</td>
</tr>
<tr>
<td>Management</td>
<td>• Cisco Router and Security Device Manager (SDM)&lt;br&gt;• Cisco Security Monitoring, Analysis and Response System (MARS) 20</td>
<td>• Cisco SDM&lt;br&gt;• Cisco Security MARS 20</td>
</tr>
</tbody>
</table>

Remote Sites
Fewer than 10 Users

<table>
<thead>
<tr>
<th>Router</th>
<th>• Cisco 850 Series Integrated Services Routers&lt;br&gt;• Cisco 870 Series Integrated Services Routers</th>
</tr>
</thead>
</table>

Fewer than 20 Users

<table>
<thead>
<tr>
<th>Router</th>
<th>• Cisco 870 Integrated Services Routers&lt;br&gt;• Cisco 1800 Series Fixed-Configuration and Modular Integrated Services Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Sites</td>
<td>Fewer than 10 Users</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Integrated security</strong></td>
<td>• Yes • Cisco IOS Firewall • Cisco IOS Software VPN (Advanced Encryption Standard/Triple Data Encryption Standard [AES/3DES]) • Cisco IOS IPS • Cisco Easy VPN, Dynamic Multipoint VPN (DMVPN)</td>
</tr>
<tr>
<td><strong>Integrated content</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>External switch</strong></td>
<td>• Cisco Catalyst Express 500 Series Switches • Cisco Catalyst 2960 Series Switches</td>
</tr>
<tr>
<td><strong>Teleworker Sites</strong></td>
<td><strong>Fewer than 10 Users</strong></td>
</tr>
<tr>
<td><strong>Integrated routing, security, and wireless</strong></td>
<td>Cisco 870W Series Integrated Services Routers</td>
</tr>
</tbody>
</table>
Secure Network Foundation Blueprint: 100 to 250 Users

This reference blueprint provides a network diagram and product table for your main office, remote office, and teleworkers. This is only a suggested blueprint.

Security Blueprint for SMBs with 100 to 250 Users

Product Table

This product table identifies Cisco solutions for SMBs with 100 to 250 user ports per site. It is intended to be a starting point in choosing Cisco products for your main business location, remote offices, and teleworker connectivity.

Solution Features for Main Business Location and Remote Sites

<table>
<thead>
<tr>
<th>Main Business Location</th>
<th>100–250 Users (SMB Complete)</th>
<th>100–250 Users (SMB Enhanced)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Cisco 2811 Integrated Services Routers</td>
<td>Cisco 2821 Integrated Services Routers</td>
</tr>
<tr>
<td></td>
<td>Cisco 2821 Integrated Services Routers</td>
<td>Cisco 2851 Integrated Services Routers</td>
</tr>
<tr>
<td>Integrated security</td>
<td>Cisco Security Agent for corporate servers</td>
<td>Cisco Security Agent for corporate servers</td>
</tr>
<tr>
<td>Integrated content</td>
<td>Yes/Network module</td>
<td>Yes/Network module</td>
</tr>
<tr>
<td>External switch</td>
<td>Cisco Catalyst Express 500 Series Switches</td>
<td>Cisco Catalyst 2960 Series Switches</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 2960 Series Switches</td>
<td>Cisco Catalyst 3560 Series Switches</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3560 Series Switches</td>
<td>Cisco Catalyst 3750 Series Switches</td>
</tr>
<tr>
<td>WLAN access points (external)</td>
<td>Cisco Aironet 1000 Series Lightweight Access Points</td>
<td>Cisco Aironet 1000 Series Lightweight Access Points</td>
</tr>
<tr>
<td></td>
<td>Cisco Aironet 1130 AG Series Access Points</td>
<td>Cisco Aironet 1130 AG Series Access Points</td>
</tr>
<tr>
<td></td>
<td>Cisco Aironet 1230 AG Series Access Points</td>
<td>Cisco Aironet 1230 AG Series Access Points</td>
</tr>
<tr>
<td></td>
<td>Cisco 4000 Series Wireless LAN Controllers</td>
<td>Cisco 4000 Series Wireless LAN Controllers</td>
</tr>
<tr>
<td><strong>Main Business Location</strong></td>
<td>100–250 Users (SMB Complete)</td>
<td>100–250 Users (SMB Enhanced)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Management</td>
<td>• Cisco SDM</td>
<td>• Cisco SDM</td>
</tr>
<tr>
<td></td>
<td>• Cisco Security Mars 20</td>
<td>• Cisco Security MARS 20</td>
</tr>
<tr>
<td></td>
<td>• Cisco Security Mars 50</td>
<td>• Cisco Security MARS 50</td>
</tr>
<tr>
<td>Remote Sites</td>
<td>Fewer than 20 Users</td>
<td>Fewer than 50 Users</td>
</tr>
<tr>
<td>Router</td>
<td>• Cisco 870 Series Integrated Services Routers</td>
<td>• Cisco 1800 Series Fixed-Configuration and Modular Integrated Services Routers</td>
</tr>
<tr>
<td></td>
<td>• Cisco 1800 Series Fixed-Configuration and Modular Integrated Services Routers</td>
<td>• Cisco 2811 Integrated Services Routers</td>
</tr>
<tr>
<td>Integrated security</td>
<td>• Yes</td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Firewall</td>
<td>• Cisco IOS Firewall</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Software VPN (AES/3DES)</td>
<td>• Hardware VPN accelerator (AES/3DES)</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS IPS</td>
<td>• Cisco IOS IPS</td>
</tr>
<tr>
<td></td>
<td>• Cisco Easy VPN, DMVPN</td>
<td>• Cisco Easy VPN, DMVPN, NAC</td>
</tr>
<tr>
<td>Integrated content</td>
<td>No</td>
<td>Yes/Network module</td>
</tr>
<tr>
<td>External switch</td>
<td>• Cisco Catalyst Express 500 Series Switches</td>
<td>• Cisco Catalyst Express 500 Series Switches</td>
</tr>
<tr>
<td></td>
<td>• Cisco Catalyst 2960 Series Switches</td>
<td>• Cisco Catalyst 2960 Series Switches</td>
</tr>
<tr>
<td>Telesworker Sites</td>
<td>Fewer than 20 Users</td>
<td>Fewer than 50 Users</td>
</tr>
<tr>
<td>Integrated routing, security, and wireless</td>
<td>Cisco 870W Series Integrated Services Routers</td>
<td>Cisco 870W Series Integrated Services Routers</td>
</tr>
</tbody>
</table>
This reference blueprint provides a network diagram and product table for your main office, remote office, and teleworkers. This is only a suggested blueprint.

Security Blueprint for SMBs with 250 to 500 User Ports per Site

Main Business Location
250–500 Users

Remote Site

Teleworker

Product Table

This product table identifies Cisco solutions for SMBs with 250 to 500 user ports per site. It is intended to be a starting point in choosing Cisco products for your main business location, remote offices, and teleworker connectivity.

Cisco offers a choice of integrated, all-in-one products and dedicated appliances. This gives you the flexibility to create a “right-sized” infrastructure that meets your specific business and budget needs.

<table>
<thead>
<tr>
<th>Solution Features for Main Business Location and Remote Sites</th>
<th>250–500 Users (SMB Complete; Integrated)</th>
<th>250–500 Users (SMB Enhanced; Integrated Security Appliance Recommended)</th>
</tr>
</thead>
</table>
| Router | • Cisco 2851 Integrated Services Routers  
• Cisco 3825 or 3845 Integrated Services Routers | • Cisco 3825 or 3845 Integrated Services Routers |
| WAN services | Yes | Yes |
| Integrated content | Yes/Network module | Yes/Network module |
| Switching | • Cisco Catalyst 2960 Series Switches  
• Cisco Catalyst 3560 Series Switches  
Core + Distribution 3560 and Access 3560 PWR  
or Core + Distribution 3560 and Access 2960 | • Cisco Catalyst 3560 Series Switches  
• Cisco Catalyst 3750 Series Switches  
Core + Distribution 4500 (Layer 3) and Access 4500 PWR  
or Core + Distribution 3750 (Layer 3) and Access 3750 PWR |
| Wireless access points (external) | • Cisco Aironet 1000 Series Lightweight Access Points  
• Cisco Aironet 1130 AG Series Access Points  
• Cisco Aironet 1230 AG Series Access Points | • Cisco Aironet 1000 Series Lightweight Access Points  
• Cisco Aironet 1130 AG Series Access Points  
• Cisco Aironet 1230 AG Series Access Points |
| Wireless LAN controller | • Cisco 2000 Series Wireless LAN Controllers  
• Cisco 4000 Series Wireless LAN Controllers | • Cisco 2000 Series Wireless LAN Controllers  
• Cisco 4000 Series Wireless LAN Controllers |
<p>| Management | Cisco Security MARS 50 | Cisco Security MARS 50 |</p>
<table>
<thead>
<tr>
<th>Remote Sites</th>
<th>Fewer than 50 Users</th>
<th>Fewer than 100 Users</th>
</tr>
</thead>
</table>
| Router       | • Cisco 870 Series Integrated Services Routers  
               • Cisco 1800 Series Fix-Configuration and Modular Integrated Services Routers  
               • Cisco 2801 Integrated Services Routers  
               • Cisco 2811 Integrated Services Routers    | • Cisco 2801 Series Integrated Services Routers  
               • Cisco 2811 Series Integrated Services Routers  
               • Cisco 2851 Series Integrated Services Routers |
| WAN services | Yes                 | Yes                 |
| Integrated Wireless LAN Controller | Cisco Wireless LAN Controller Module | Cisco Wireless LAN Controller Module |
| Integrated LAN security | Yes | Yes |
| Integrated security | • Yes  
                        • Cisco IOS Firewall  
                        • Cisco IOS Software VPN (AES/3DES)  
                        • Cisco IOS IPS  
                        • Cisco Easy VPN, DMVPN | • Yes  
                        • Cisco IOS Firewall  
                        • Hardware VPN accelerator (AES/3DES)  
                        • Cisco IOS IPS  
                        • Cisco Easy VPN, DMVPN, NAC |
| Integrated content | No | Yes/Network module |
| External switch | • Cisco Catalyst 2960 Series Switches  
                    • Cisco Catalyst 3560 Series Switches | • Cisco Catalyst 2960 Series Switches  
                    • Cisco Catalyst 3560 Series Switches |
| Teleworker Sites | Fewer than 50 Users | Fewer than 100 Users |
| Integrated routing, security, and wireless | Cisco 870W Series Integrated Services Routers | Cisco 870W Series Integrated Services Routers |
### Secure Network Foundation Blueprint: Product Information

#### Routing

<table>
<thead>
<tr>
<th>Cisco 850/870 Series Integrated Services Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased performance to run concurrent integrated services (data, QoS for voice and video, security, and wireless)</td>
</tr>
<tr>
<td><strong>Security</strong> Security with integrated firewall and VPN, or advanced security with integrated firewall, firewall, IPS, and VLAN</td>
</tr>
<tr>
<td><strong>Wireless 802.11</strong> Secure wireless 802.11b/g</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco 1800 Series Fixed and Modular Integrated Services Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased performance for broadband delivery of concurrent, secure data services, including data, QoS for voice and video, security, and wireless</td>
</tr>
<tr>
<td>Consolidated additional LAN/WAN features in a single box (optional backup, 8-port managed switch, and Power over Ethernet [PoE])</td>
</tr>
<tr>
<td><strong>Security</strong> Advanced security with integrated firewall, VPN, IPS, and VLAN</td>
</tr>
<tr>
<td><strong>Wireless 802.11</strong> Optional integrated 802.11a/b/g secure WLAN (multiple options for antennas)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco 1800 Series Modular Integrated Services Routers, featuring:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Integrated 8-port switch</td>
</tr>
<tr>
<td>• Integrated v92 modem or ISDN Basic Rate Interface (BRI) port</td>
</tr>
<tr>
<td>• DSL support</td>
</tr>
<tr>
<td>• Optional 802.11a/b/g support</td>
</tr>
<tr>
<td>• Optional PoE</td>
</tr>
<tr>
<td>• Cisco IOS Software Advanced Security feature set (firewall, intrusion prevention, and VPN)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco 1800 Series Modular Integrated Services Routers, featuring:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 2 modular data slots</td>
</tr>
<tr>
<td>• Support for T1/E1, DSL modem, and serial high-speed WAN interface cards (HWICs)</td>
</tr>
<tr>
<td>• 2 standard 10/100BASE-T ports</td>
</tr>
<tr>
<td><strong>Default hardware encryption (enabled using Cisco IOS Advanced Security feature set)</strong></td>
</tr>
</tbody>
</table>

#### Cisco 2801 Integrated Services Routers

This entry-level rack-mount router, powered by Cisco IOS Software, supports multservice data, voice, video, and fax integration, and features VLAN and VPN support, multiple WAN access options, and more. The Cisco 2801 Integrated Services Router is an economical and highly flexible solution for a small business needing secure Internet and intranet access for its main business location.

<table>
<thead>
<tr>
<th>Cisco 2811 Integrated Services Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2800 Series Integrated Services Routers bring big-company capabilities to small businesses with an award-winning combination of multiservice integration (data, voice, video, and fax), flexible LAN and WAN configurations, security options, high-performance processors, a router-integrated content delivery system (requires optional module), and investment protection in a compact solution.</td>
</tr>
<tr>
<td>The modularity of the Cisco 2800 Series enables small businesses to update their networks as budget and business application needs dictate.</td>
</tr>
<tr>
<td><strong>Security</strong> Onboard encryption, NAC, inline IPS, dynamically loaded signatures, more VPN tunnels, and high-performance firewalls</td>
</tr>
<tr>
<td><strong>Voice</strong> Designed for medium density, IP telephony, voicemail, auto attendant, and conferencing needs</td>
</tr>
<tr>
<td><strong>Wireless</strong> Wireless LAN Controller Module supports up to 6 Cisco lightweight access points</td>
</tr>
<tr>
<td><strong>Comprehensive Layer 2 and Layer 3 Services</strong> Fast Ethernet and Gigabit Ethernet switch ports, VLANs, application optimization, and PoE, as well as wire-speed concurrent services and headroom for growth</td>
</tr>
<tr>
<td><strong>Modularity and Investment Protection</strong> More slots for advanced services via support for network modules (NM, NME, NME-X, and NME-XD) with packet voice DSP modules (PVDMs) and Advanced Integration Modules (AIMs); works with previous Cisco 1700, 2600, and 3700 Series interfaces, and adds new services</td>
</tr>
<tr>
<td><strong>Scalability, Density, and Resiliency</strong> Inline IP phone power for enhanced, scalable, and intelligent services and interface options for growth</td>
</tr>
</tbody>
</table>

Cisco 2811 Integrated Services Routers support a wide range of security features, including:

- **Onboard encryption accelerator process:** With support for IP Security (IPsec) DES, 3DES, and 128-, 192-, and 256-bit AES.
- **Optional high-performance AIM-VPN:** Dedicated encryption processor card supporting IPsec DES; 3DES; 128-, 192-, and 256-bit AES; and hardware compression with IP Payload Compression Protocol (IPPCP).
- **Cisco IOS Software-based firewall enhancement:** Sophisticated security and policy enforcement with transparent firewall, IPv6 firewall, voice over IP (VoIP), and authentication, authorization, and accounting (AAA) support.
- **DMVPN support:** Cisco IOS Software-based solution for building IPsec + generic routing encapsulation (GRE) VPNs in an easy and scalable manner.
- **Dynamic inline intrusion detection system (IDS) support:** A dynamic load of the latest IDS signature files to any targeted router using CiscoWorks VPN and Security Monitoring Solution (VMS) or Cisco IPS Center (ISC) software.
- **Cisco EasyVPN server and client support:** The ability to receive and send IPsec configurations from server to clients for easy deployment of VPNs.
- **SSL server support:** SSL support for remote VPN users.
- **Real-time clock:** Mechanism to keep public key infrastructure (PKI) VPN certificates up to date in case of router downtime or reboot.
- **Standards-based secure voice support:** Secured Routing Update Protocol (SRTP) to protect VoIP media and voicemail media, and signaling encryption to provide call privacy and security for IP Communications deployments.
- **Optional USB secure token support:** Optional USB for secure configurations, distributions, and off-platform storage of VPN credentials.
Cisco 2800 Series Integrated Services Routers
Cisco 2800 Series Integrated Services Routers bring big-company capabilities to small businesses with an award-winning combination of multiservice integration (data, voice, video, and fax), flexible LAN and WAN configurations, security options, high-performance processors, a router-integrated content-delivery system (requires optional module), and investment protection in a compact solution.

The modularity of the Cisco 2800 Series enables small businesses to update their networks as budget and business application needs dictate.

Security
Onboard encryption, NAC, inline IPS, dynamically loaded signatures, more VPN tunnels, and high-performance firewalls

Voice
Designed for medium-density, IP telephony, voicemail, auto attendant, and conferencing needs

Wireless
Wireless LAN Controller Module supports up to 6 Cisco lightweight access points

Comprehensive Layer 2 and Layer 3 Services
Fast Ethernet and Gigabit Ethernet switch ports, VLANs, application optimization, and PoE, as well as wire-speed concurrent services and headroom for growth

Modularity and Investment Protection
More slots for advanced services via NM, NME, NME-X, and NME-XD support with PVDMs and AILMs; works with previous Cisco 1700, 2600, and 3700 Series interfaces, and adds new services

Scalability, Density, and Resiliency
Inline IP phone power, online insertion, and scalable services and interface options for growth
Cisco 2851 Integrated Services Routers support a wide range of security features, including:
• Onboard encryption accelerator process: With support for IPSec DES, 3DES, and 128-, 192-, and 256-bit AES.
• Optional high-performance AIM-VPN: Dedicated encryption processor card supporting IPSec DES; 3DES; 128-, 192-, and 256-bit AES; and hardware compression with IPPCP.
• Cisco IOS Software-based firewall enhancement: Sophisticated security and policy enforcement with transparent firewall, IPv6 firewall, VoIP, and AAA support.
• DMVPN support: Cisco IOS Software-based solution for building IPSec + GRE VPNs in an easy and scalable manner.
• Dynamic inline IDS support: A dynamic load of the latest IDS signature files to any targeted router using CiscoWorks VMS or Cisco ISC software.
• Cisco Easy VPN server and client support: The ability to receive and send IPSec configurations from server to clients for easy deployment of VPNs.
• SSL server support: SSL support for remote VPN users.
• Real-time clock: Mechanism to keep PKI VPN certificates up to date in case of router downtime or reboot.
• Standards-based secure voice support: SRTP to protect VoIP media and voicemail media, and signaling encryption to provide call privacy and security for IP Communications deployments.
• Optional USB secure token support: Optional USB for secure configurations, distributions, and off-platform storage of VPN credentials.
• URL filtering support: To manage employee Internet access.

Cisco 3845 Integrated Services Routers
The Cisco 3845 Integrated Services Router is the flagship of the Cisco access router portfolio, providing high-performance routing, low-density switching, security, voice, IP telephony, voicemail, video, and content networking in a single, integrated solution. This design helps SMBs adapt incrementally to evolving business needs.

By transparently integrating advanced technologies, adaptive services, and secure communications into a single, resilient system, Cisco 3845 Integrated Services Routers help to ease deployment and management, lower network cost and complexity, and provide unmatched investment protection.

Security
Onboard encryption, NAC, optional inline IPS, dynamically loaded signatures, greater VPN tunnels, and high-performance firewalls

Voice
Optimized for large enterprise branch IP telephony, voicemail, auto attendant, and conferencing needs; features highest density levels for analog-to-digital voice and legacy-to-dial aggregation

Wireless
Wireless LAN Controller Module supports up to 6 Cisco lightweight access points

Comprehensive Layer 2 and Layer 3 Services
Fast Ethernet and Gigabit Ethernet switch ports, VLANs, wireless, application optimization, and PoE; wire-speed for up to T3/E3 throughput

Maximum Modularity and Investment Protection
Cisco 3845 Integrated Services Routers provide four slots for network modules, and can support up to four NM, NME, or NME-X modules, or two NMD or NME-XD modules. Provides four single-width or two double-width HWIC slots, two AIM slots, four PVDM slots, two USB ports, and optional support of up to 48 ports of IP phone power output. Works with Cisco 1700, 2600, and 3700 Series network modules, voice interface cards (VICs), and WAN interface cards (WICs).

Scalability, Density, and Resiliency
Highest levels of resiliency with redundant power supply options, optional inline power, and hot-swappable network modules. Scalable services and interfaces for future requirements.
Cisco 3845 Integrated Services Routers support a wide range of security features, including:
• Onboard encryption accelerator process: With support for IPSec DES, 3DES, and 128-, 192-, and 256-bit AES.
• Optional high-performance AIM-VPN: Dedicated encryption processor card supporting IPSec DES; 3DES; 128-, 192-, and 256-bit AES; and hardware compression with IPPCP.
• Cisco IOS Software-based firewall enhancement: Sophisticated security and policy enforcement with transparent firewall, IPv6 firewall, VoIP, and AAA support.
• DMVPN support: Cisco IOS Software-based solution for building IPSec + GRE VPNs in an easy and scalable manner.
• Dynamic inline IDS support: A dynamic load of the latest IDS signature files to any targeted router using CiscoWorks VMS or Cisco ISC software.
• Cisco Easy VPN server and client support: The ability to receive and send IPSec configurations from server to clients for easy deployment of VPNs.
• SSL server support: SSL support for remote VPN users.
• Real-time clock: Mechanism to keep PKI VPN certificates up to date in case of router downtime or reboot.
• Standards-based secure voice support: SRTP to protect VoIP media and voicemail media, and signaling encryption to provide call privacy and security for IP Communications deployments.
• Optional USB secure token support: Optional USB for secure configurations, distributions, and off-platform storage of VPN credentials.
• Network Analysis Module (NAM) support: Integrated traffic-monitoring helps enable application-level visibility into the network for remote troubleshooting and traffic analysis.
Cisco Catalyst Express 500 Series Switches
Cisco Catalyst Express 500 Series Switches deliver world-class networking to businesses with up to 250 employees. Powered by Cisco technology and managed with a GUI, this family of Layer-2-managed Fast Ethernet and Gigabit Ethernet switches offers nonblocking, wire-speed performance that provides a secure network foundation optimized for data, wireless, and voice. Built-in advanced encryption and security features help ensure that your devices and network are protected.

Cisco Catalyst 2960 Series Switches
The new Cisco Catalyst 2960 Series offers fixed-configuration, standalone switches that provide desktop 10/100 Fast Ethernet and 10/100/1000 Gigabit Ethernet connectivity for entry-level enterprise, midmarket, and branch office networks, enabling enhanced LAN services. Cisco Catalyst 2960 Series Switches offer integrated security, including NAC, advanced QoS, and resiliency, to deliver intelligent services for the network edge.

The Cisco Catalyst 2960 Series Switch offers:
- Intelligent features at the network edge, sophisticated access control lists (ACLs), and enhanced security
- Dual-purpose (alternative wired) uplinks for Gigabit Ethernet uplink flexibility, allowing the network manager to use either a copper or a fiber uplink
- Network control and bandwidth optimization via advanced QoS, granular rate-limiting, ACLs, and multicast services
- Network security through a wide range of authentication methods and data encryption technologies, and NAC based on users, ports, and MAC addresses
- Easy-to-network configuration, upgrades, and troubleshooting as part of the midmarket or branch solution using Cisco Network Assistant
- Autoconfiguration for specialized applications using Cisco Smartports

Cisco Catalyst 3560 Series Switches
The 24- and 48-port fixed-configuration switches include IEEE 802.3af and Cisco prestandard PoE in Fast Ethernet and Gigabit Ethernet configurations. The Cisco Catalyst 3560 Series is an ideal access-layer switch for LAN access or branch-office environments, combining 10/100/1000 and PoE configurations for maximum productivity, advanced integrated security, QoS, availability, and investment protection. Cisco Catalyst 3560 Series Switches also enable the deployment of new applications such as IP telephony, wireless access, video surveillance, building management systems, and remote video kiosks.

Cisco Catalyst 3750 Series Switches
Cisco Catalyst 3750 Series Switches are innovative products for medium-sized organizations and enterprise branch offices. Featuring Cisco StackWise™ technology, the switches improve LAN operating efficiency by combining ease of use and the highest resiliency available for stackable switches. The revolutionary Cisco StackWise stacking architecture brings high levels of resiliency, automation, advanced integrated security, QoS, availability, and performance to stackable switches. With Cisco StackWise technology, customers can create a single 32-Gbps switching unit with up to nine Cisco Catalyst 3750 Series Switches. The 24- and 48-port 10/100/1000 Mbps switches with PoE are supported for maximum productivity and investment protection, while enabling the deployment of new applications such as IP telephony, wireless access, video surveillance, building management systems, and remote video kiosks.

Cisco Catalyst 4500 Series Switches
The Cisco Catalyst 4500 Series is a midrange modular switch series that offers nonblocking Layer 2 through Layer 4 switching capabilities. The Cisco Catalyst 4500 Series features a centralized modular architecture that provides operational simplicity, media flexibility, and expandability, extending deployment life while reducing the cost of ownership by minimizing recurring operational expenses and improving return on investment (ROI).

The Cisco Catalyst 4500 Series also delivers:
- Investment protection: An evolutionary centralized architecture allows for the easy upgrade of all system ports to higher-level functions with simple supervisor upgrades
- High availability: Hardware- and software-based resiliency is designed into the architecture to help minimize network downtime
- Ease of use and manageability: Web-based management offers centralized configuration and control of all ports for operational simplicity
- Comprehensive security: Advanced security capabilities mitigate information theft and limit damage from worms and viruses
- Power over Ethernet: PoE enables the deployment of new applications such as IP telephony, wireless access, video surveillance, building management systems, and remote video kiosks
- Scalability: This high-density solution offers up to 102-Mbps nonblocking performance, independent of the number of security policies or Layer 3 services enabled
- Deployment flexibility: This series offers a broad selection of chassis, high-performance supervisors, line cards, and power supplies

Cisco Catalyst 6500 Series Switches
Cisco Catalyst 6500 Series Switches offer the highest levels of availability and integrated security, strongest support for converged applications, superior operational efficiency, leading scalability and flexibility, and unmatched, long-term investment protection.

The Cisco Catalyst 6500 Series continues to set the standard for high-end LAN switching with industry-leading innovations, such as:

**Highest Availability**
- Cisco IOS Software modularity
- In-Service Software Upgrades (ISSU) and stateful process restarts
- Generic Online Diagnostics (GOLD)
- Nonstop Forwarding and Stateful Switchover (NSF/SSO) delivers application and service continuity
- Redundant system components provide hardware-level resiliency

**Highest Level of Integrated Security**
- Multiple denial-of-service (DoS) attack mitigation mechanisms
- Integrated security service modules (VPN, SSL VPN, firewall, IPS, and anomaly detection)

**Strongest Support for Converged Applications**
- Embedded real-time monitoring of VoIP call quality
- Cisco Communication Media Module
- Wireless LAN Controller Module
- Application-Oriented Networking (AON) Module
The Cisco Aironet 1130 AG Access Point delivers the versatility, high capacity, security, and enterprise-class features required in more challenging RF environments. It is designed for wireless LANs in rugged environments or installations that require specialized antennas, and features dual antenna connectors for extended range, coverage versatility, and more flexible installation options. The Cisco Aironet 1230 AG Series combines antenna versatility with industry-leading transmit power, receive sensitivity, and delay spread for high multipath and indoor environments, providing reliable performance and throughput for the most demanding requirements. The Cisco Aironet 1230 AG access point is available in either a lightweight version or as an autonomous version that may be field-upgraded to lightweight operation.

Cisco Aironet 1230 AG Series Access Points

Cisco PIX 501 Security Appliances (for Teleworkers and Small Remote Offices)
Cisco PIX® 501 Security Appliances offer increased performance to run concurrent integrated services, including data, voice and video, and security.

Cisco PIX 506E Security Appliances (for Teleworkers and Small Remote Offices)
Cisco PIX 506E Security Appliances offer increased performance to run concurrent integrated services, including data, voice and video, and security.

Cisco ASA 5500 Series Adaptive Security Appliances
The Cisco ASA 5500 Series of high-performance, multifunction security appliances delivers converged firewall, IPS, network antivirus, and VPN services, including:
- Market-proven security and VPN capabilities: Full-featured, high-performance firewall, IPS, network antivirus, and IPSec/SSL. VPN technologies deliver robust application security, user- and application-based access control, worm and virus mitigation, malware protection, and remote user and site connectivity.
- Unique Adaptive Identification and Mitigation services architecture: Allows businesses to adapt and extend the security services profile of the Cisco ASA 5500 Series through highly customizable flow-specific security policies that tailor security needs to application requirements while providing performance and security service extensibility via user-installable security services modules (SSMs).
- Reduced deployment and operations costs: Multifunction appliance allows for platform, configuration, and management standardization, decreasing the cost of deployment and ongoing operations.

Cisco Security Agent for Corporate Servers
- Dramatically reduces downtime, widespread attack propagation, and cleanup costs
- Complements Cisco portfolio and the SAFE blueprint for true defense-in-depth security
- Zero-update architecture eliminates signatures and reduces the cost of hot-fix management
- Common, consolidated agent reduces deployment and management costs
- Offers host-based protection for servers and desktops
- Prevents attacks, especially “day-zero” viruses and worms

Cisco Aironet 1000 Series Lightweight Access Points
Cisco Aironet 1000 Series Lightweight Access Points deliver an affordable and upgradable WLAN solution, setting the standard for high-performance secure, manageable, and flexible WLANs. The Cisco Aironet 1000 Series supports a single radio and is available in an IEEE 802.11a/g version or IEEE 802.11b version that is field-upgradable to 54-Mbps 802.11g.

Cisco Aironet 1130 AG Series Access Points
The Cisco Aironet 1130 AG Series Access Point packages high capacity, high security, and enterprise-class features delivering wireless LAN access for a low total cost of ownership. Designed for wireless LAN coverage in offices and similar RF environments, this unobtrusive access point features integrated antennas and dual IEEE 802.11a/g radios for robust and predictable coverage, delivering a combined capacity of 108 Mbps. The competitively priced Cisco Aironet 1130 AG Series is ready to install and easy to manage, reducing the cost of deployment and ongoing maintenance. The Cisco Aironet 1130 AG Access Point is available in either a lightweight version or as an autonomous version that may be field-upgraded to lightweight operation.

Cisco Wireless LAN Controllers
Cisco wireless LAN controllers are responsible for systemwide wireless LAN functions, such as security policies, intrusion prevention, RF management, QoS, and mobility. They work in conjunction with Cisco 1000 Series Lightweight Access Points to support business-critical wireless applications. From voice and data services to location tracking, Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build secure wireless networks—from branch offices to main offices.

Cisco 2000 Series Wireless LAN Controllers
- Supports up to 6 Cisco lightweight access points
- Cisco 4000 Series Wireless LAN Controllers
- Specific models support 12, 25, 50, and 100 Cisco lightweight access points

Management
Cisco SDM
Cisco SDM is a productivity-enhancing tool for network and security administrators. Cisco channel partners can use Cisco SDM for faster and easier deployment of Cisco routers for integrated services like dynamic routing, WAN access, wireless, firewall, VPN, IPS, and QoS.

Cisco Security MARS 20
This appliance-based, all-inclusive solution provides control of your existing security deployment. A core component of the Cisco security-management lifecycle, Cisco Security MARS empowers your security and network organizations to identify, manage, and counter security threats. It uses your existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of the overall regulatory compliance solution kit.

Cisco Security MARS 50
This appliance-based, all-inclusive solution provides control of your existing security deployment. A core component of the Cisco security-management lifecycle, Cisco Security MARS empowers your security and network organizations to identify, manage, and counter security threats. It uses your existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of the overall regulatory compliance solution kit.

Cisco Wireless LAN Controllers
Cisco wireless LAN controllers are responsible for systemwide wireless LAN functions, such as security policies, intrusion prevention, RF management, QoS, and mobility. They work in conjunction with Cisco 1000 Series Lightweight Access Points to support business-critical wireless applications. From voice and data services to location tracking, Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build secure wireless networks—from branch offices to main offices.

Cisco 2000 Series Wireless LAN Controllers
- Supports up to 6 Cisco lightweight access points
- Cisco 4000 Series Wireless LAN Controllers
- Specific models support 12, 25, 50, and 100 Cisco lightweight access points

Management
Cisco SDM
Cisco SDM is a productivity-enhancing tool for network and security administrators. Cisco channel partners can use Cisco SDM for faster and easier deployment of Cisco routers for integrated services like dynamic routing, WAN access, wireless, firewall, VPN, IPS, and QoS.

Cisco Security MARS 20
This appliance-based, all-inclusive solution provides control of your existing security deployment. A core component of the Cisco security-management lifecycle, Cisco Security MARS empowers your security and network organizations to identify, manage, and counter security threats. It uses your existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of the overall regulatory compliance solution kit.

Cisco Security MARS 50
This appliance-based, all-inclusive solution provides control of your existing security deployment. A core component of the Cisco security-management lifecycle, Cisco Security MARS empowers your security and network organizations to identify, manage, and counter security threats. It uses your existing network and security investments to identify, isolate, and recommend precise removal of offending elements. It also helps maintain internal policy compliance and can be an integral part of the overall regulatory compliance solution kit.

The Cisco Security MARS 50 appliance is ideal for handling event volumes of up to 1000 events per second.