ANEXOS

Direccionamiento para Sur Americana de espectáculos

Antiguo direccionamiento IP					
Sucursal	Network	Hosts		Broadcast Address	Subset Mask
		from	To		
Lido	172.20.0.0	172.20.0.1	172.20.0.30	172.20.4.31	255.255.255.224
Almacén	172.20.0.32	172.20.0.33	172.20.0.46	172.20.0.47	255.255.255.240
Santa Fe	172.20.0.96	172.20.0.97	172.20.0.126	172.20.0.127	255.255.255.224
Concreta	172.20.0.128	172.20.0.129	172.20.0.158	172.20.0.159	255.255.255.224
San Ignacio	172.20.0.160	172.20.0.161	172.20.0.190	172.20.0.191	255.255.255.224
Sambil	172.20.0.192	172.20.0.193	172.20.0.222	172.20.0.223	255.255.255.224
Hatillo	172.20.2.0	172.20.2.1	172.20.2.30	172.20.2.31	255.255.255.224
Buenaventura	172.20.2.192	172.20.2.193	172.20.2.222	172.20.2.223	255.255.255.224
Oficina Principal	172.20.4.0	172.20.4.1	172.20.4.256	172.20.4.255	255.255.255.0
Victoria Plaza	172.20.5.32	172.20.5.33	172.20.5.62	172.20.5.63	255.255.255.224
Recreo	172.20.5.64	172.20.5.65	172.20.5.94	172.20.5.95	255.255.255.224
Lagomall	172.20.5.96	172.20.5.97	172.20.5.126	172.20.5.127	255.255.255.224
Babilón	172.20.6.0	172.20.6.1	172.20.6.30	172.20.6.31	255.255.255.224
Metrópolis	Nueva				
Lagunita	Nueva				

Nuevo direccionamiento IP					
Sucursal	Network	Hosts		Broadcast Address	Subset Mask
		from	to		
Lido	172.20.11.0	172.20.11.1	172.20.11.254	172.20.11.255	255.255.255.0
Almacén	172.20.10.0	172.20.10.1	172.20.10.254	172.20.10.255	255.255.255.0
Santa Fe	172.20.17.0	172.20.17.1	172.20.17.254	172.20.17.255	255.255.255.0
Concreta	172.20.16.0	172.20.16.1	172.20.16.254	172.20.16.255	255.255.255.0
San Ignacio	172.20.12.0	172.20.12.1	172.20.12.254	172.20.12.255	255.255.255.0
Sambil	172.20.13.0	172.20.13.1	172.20.13.254	172.20.13.255	255.255.255.0
Hatillo	172.20.15.0	172.20.15.1	172.20.15.254	172.20.15.255	255.255.255.0
Buenaventura	172.20.18.0	172.20.18.1	172.20.18.254	172.20.18.255	255.255.255.0
Oficina Principal	172.20.4.0	172.20.4.1	172.20.4.254	172.20.4.255	255.255.255.0
Victoria Plaza	172.20.23.0	172.20.23.1	172.20.23.254	172.20.23.255	255.255.255.0
Recreo	172.20.14.0	172.20.14.1	172.20.14.254	172.20.14.255	255.255.255.0
Lagomall	172.20.21.0	172.20.21.1	172.20.21.254	172.20.21.255	255.255.255.0
Babilón	172.20.20.0	172.20.20.1	172.20.20.254	172.20.20.255	255.255.255.0
Metrópolis	172.20.22.0	172.20.22.1	172.20.22.254	172.20.22.255	255.255.255.0
Lagunita	172.20.19.0	172.20.19.1	172.20.19.254	172.20.19.255	255.255.255.0

Direccionamiento para Venefilms: ellos no disponían de interconexión por lo que todo el direccionamiento es nuevo.

Sucursal	Network	Hosts				Broadcast	Subset Mask
		from	to	Router	Server		
Virtudes, Pto. Fijo. Edo. Falcón	172.20.30.0	172.20.30.1	172.20.30.254	172.20.30.1	172.20.30.2	172.20.30.255	255.255.255.0
Alto Prado, Mérida	172.20.31.0	172.20.31.1	172.20.31.254	172.20.31.1	172.20.31.2	172.20.31.255	255.255.255.0
Doral Plaza, Maracaibo	172.20.32.0	172.20.32.1	172.20.32.254	172.20.32.1	172.20.32.2	172.20.32.255	255.255.255.0
Galerías Maracaibo	172.20.33.0	172.20.33.1	172.20.33.254	172.20.33.1	172.20.33.2	172.20.33.255	255.255.255.0
Marina Plaza, Cumana	172.20.34.0	172.20.34.1	172.20.34.254	172.20.34.1	172.20.34.2	172.20.34.255	255.255.255.0
Monagas Plaza, Maturín	172.20.35.0	172.20.35.1	172.20.35.254	172.20.35.1	172.20.35.2	172.20.35.255	255.255.255.0
Pirineos, San Cristóbal	172.20.36.0	172.20.36.1	172.20.36.254	172.20.36.1	172.20.36.2	172.20.36.255	255.255.255.0
Plaza Mayor, Lecherías	172.20.37.0	172.20.37.1	172.20.37.254	172.20.37.1	172.20.37.2	172.20.37.255	255.255.255.0
Valera, Edo. Trujillo	172.20.38.0	172.20.38.1	172.20.38.254	172.20.38.1	172.20.38.2	172.20.38.255	255.255.255.0

Direccionamiento para Blancica: ellos continuaran usando el direccionamiento que venían usando

Sucursal	Network	Hosts			Broadcast	Subset Mask
		from	to	Router		
Plaza Las Américas	10.0.3.0	10.0.3.1	10.0.3.254	10.0.3.1	10.0.3.255	255.255.255.0
Centro Plaza	192.168.2.0	192.168.2.1	192.168.2.254	192.168.2.1	192.168.2.255	255.255.255.0
Tolón	Datos no disponibles					

Data sheet´s:

Cisco ASA 5500 Series Adaptive Security Appliances

Cisco® ASA 5500 Series Adaptive Security Appliances are purpose-built solutions that combine best-in-class security and VPN services with an innovative, extensible services architecture. Designed as a core component of the Cisco Self-Defending Network, the

Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting home office, branch office, small and medium-sized business, enterprise, and data center networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

The Cisco ASA 5500 Series delivers a powerful combination of multiple market-proven technologies in a single platform, making it operationally and economically feasible for organizations to deploy comprehensive security services to more locations. The comprehensive portfolio of services within the Cisco ASA 5500 Series enables customization for location-specific needs through tailored product editions for small to medium-sized businesses and for enterprises.

These editions enable superior protection by providing the right services for the right location.

Each edition combines a focused set of Cisco ASA 5500 Series services (such as firewall, SSL and IPsec VPN, IPS, and content security services) to meet the needs of specific environments within the enterprise network. By ensuring the security needs of each location are met, the overall network security posture is raised.

Figure 1. Cisco ASA 5500 Series Adaptive Security Appliances

The Cisco ASA 5500 Series helps businesses more effectively and efficiently protect their networks while delivering exceptional investment protection through the following key elements:

● **Market-proven security and VPN capabilities**—Full-featured, high-performance firewall, intrusion prevention (IPS), content security, and Secure Sockets Layer/IP Security (SSL/IPsec) VPN technologies deliver robust application security, user- and applicationbased access control, worm and virus mitigation, malware protection, content filtering, and remote user/site connectivity.

● **Extensible services architecture**—Taking advantage of a modular services processing and policy framework offered by the Cisco ASA 5500 Series, businesses can apply specific security and network services on a per-traffic-flow basis, delivering highly granular policy controls and a wide range of protective services with streamlined traffic processing. The efficiencies of this policy framework, as well as software and hardware extensibility through user-installable security services modules (SSMs) and security services cards (SSCs), advance the evolution of existing services and the deployment of new services without requiring a platform replacement or performance compromise. With these capabilites, the Cisco ASA 5500 Series provides the foundation for highly customizable security policies and unprecedented services extensibility to help protect against the fast-evolving threat environment.

● **Reduced deployment and operations costs**—The multifunction Cisco ASA 5500 Series allows for platform, configuration, and management standardization, helping to decrease the costs of deployment and ongoing operations.

Introducing the Cisco ASA 5500 Series

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5520, 5540, 5550, and 5580

Adaptive Security Appliances-purpose-built, high-performance security solutions that take advantage of Cisco expertise in developing industry-leading, award-winning security and VPN solutions. The series builds upon proven technologies from Cisco PIX® 500 Series Security Appliances, Cisco IPS 4200 Series Sensors, and Cisco VPN 3000 Series Concentrators. Designed as a key component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting small and medium-sized business (SMB), enterprise, and service provider networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

Through its unique Modular Policy Framework (MPF), the Cisco ASA 5500 Series brings a new level of security and policy control to applications and networks. MPF allows businesses to adapt and extend the profile of the Cisco ASA 5500 Series through highly customizable, flow-specific security policies tailored to application requirements while providing performance and extensibility through user-installable SSMs. This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSM. Furthermore, the modular hardware architecture of the Cisco ASA 5500 Series along with flexible MPF enables the integration of future network and security, extending the outstanding investment protection provided by the Cisco ASA 5500 Series, and allowing businesses to adapt their network defenses to new threats as they arise.

All Cisco ASA 5500 Series appliances include maximum IPsec VPN users on the base system; SSL VPN is licensed and purchased separately. By converging SSL and IPsec VPN services with comprehensive threat defense technologies, the Cisco ASA

5500 Series provides highly customizable network access tailored to meet the requirements of diverse deployment environments while providing advanced endpoint and network-level security.

Cisco ASA 5505 Adaptive Security Appliance

The Cisco ASA 5505 Adaptive Security Appliance is a next-generation, full-featured security appliance for small business, branch office, and enterprise teleworker environments. The Cisco ASA 5505 delivers high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, "plug-and-play" appliance. Using the integrated Cisco Adaptive Security Device Manager, the Cisco ASA 5505 can be rapidly deployed and easily managed, enabling businesses to minimize operations costs. The Cisco ASA 5505 features a flexible 8-port 10/100 Fast Ethernet switch, whose ports can be dynamically grouped to create up to three separate VLANs for home, business, and Internet traffic for improved network segmentation and security. The Cisco ASA 5505 provides two Power over Ethernet (PoE) ports, enabling simplified deployment of Cisco IP phones with zero-touch secure voice over IP (VoIP) capabilities, and deployment of external wireless access points for extended network mobility. The Cisco ASA 5505 also provides significant expandability and investment protection through its modular design, similar to the rest of the Cisco ASA 5500 Series, offering both an external expansion slot and multiple USB ports that enable the addition of services in the future.

As business needs grow, customers can install a Security Plus upgrade license, enabling the Cisco ASA 5505 Adaptive Security Appliance to scale to support a higher connection capacity and a higher number of IPsec VPN users, add full DMZ support, and integrate into switched network environments through VLAN trunking support. Furthermore, this upgrade license maximizes business continuity by enabling support for redundant ISP connections and stateless Active/Standby high-availability services. This combination of market-leading security and VPN services, advanced networking features, flexible remote management capabilities, and future extensibility makes the Cisco ASA 5505 an excellent choice for businesses requiring a best-inclass small business, branch office, or enterprise teleworker security solution.

Cisco ASA 5510 Adaptive Security Appliance

The Cisco ASA 5510 Adaptive Security Appliance delivers advanced security and networking services for small and medium-sized businesses and enterprise remote/branch offices in an easyto- deploy, cost-effective appliance. These services can be easily managed and monitored by the integrated, Cisco Adaptive Security Device Manager application, thus reducing the overall deployment and operations costs associated with providing this high level of security. The Cisco ASA 5510 Adaptive Security Appliance provides high-performance firewall and VPN services and five integrated 10/100 Fast Ethernet interfaces. It optionally provides high-performance intrusion prevention and worm mitigation services through the AIP SSM, or comprehensive malware protection services through the CSC SSM. This unique combination of services on a single platform makes the Cisco ASA 5510 an excellent choice for businesses requiring a cost-effective, extensible, DMZ-enabled security solution.

As business needs grow, customers can install a Security Plus license, upgrading two of the Cisco ASA 5510 Adaptive Security Appliance interfaces to Gigabit Ethernet and enabling integration into switched network environments through VLAN support. This upgrade license maximizes business continuity by enabling Active/Active and Active/Standby high-availability services. Using the optional security context capabilities of the Cisco ASA 5510 Adaptive Security Appliance, businesses can deploy up to five virtual firewalls within an appliance to enable compartmentalized control of security policies on a departmental level. This virtualization strengthens security and reduces overall management and support costs while consolidating multiple security devices into a single appliance.

Businesses can extend their SSL and IPsec VPN capacity to support a larger number of mobile workers, remote sites, and business partners. Businesses can scale up to 250 SSL VPN peers on each Cisco ASA 5510 by installing an SSL VPN upgrade license; 250 IPsec VPN peers are supported on the base platform. VPN capacity and resiliency can also be increased by taking advantage of the Cisco ASA 5510's integrated VPN clustering and load-balancing capabilities (available if a Security Plus license is installed). The Cisco ASA 5510 supports up to 10 appliances in a cluster, supporting a maximum of 2500 SSL VPN peers or 2500 IPsec VPN peers per cluster.

Table 1. Cisco ASA 5510 Adaptive Security Appliance Platform Capabilities and Capacities

Feature	Description
Firewall Throughput	Up to 300 Mbps
Maximum Firewall and IPS Throughput	● Up to 150 Mbps with AIP SSM-10 ● Up to 300 Mbps with AIP SSM-20
VPN Throughput	Up to 170 Mbps
Concurrent Sessions	50,000; 130,000***
IPsec VPN Peers	250
SSL VPN Peer License Levels*	10, 25, 50, 100, or 250
Security Contexts	Up to 5**
Interfaces*	Five Fast Ethernet ports; 2 Gigabit Ethernet + 3 Fast Ethernet***
Virtual Interfaces (VLANs)	50; 100***
Scalability*	VPN clustering and load balancing
High Availability	Not supported; Active/Active, Active/Standby***

* Separately licensed feature; includes two with the base system

** Separately licensed feature; includes two with the Cisco ASA 5510 Security Plus license

*** Upgrade available with Cisco ASA 5510 Security Plus license

Cisco 1800 Series Integrated Services Routers: Cisco 1841 Router (Modular)

Cisco Systems® is redefining best-in-class enterprise and small- to-medium-sized business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, and video services. Founded on 20 years of leadership and innovation, the modular Cisco® 1800 Series of integrated services routers (refer to Figure 1) intelligently embed data and security into a single, resilient system for fast, scalable delivery of mission-critical business applications. The best-in-class Cisco 1800 Series architecture has been specifically designed to meet requirements of small-to-medium-sized businesses, small enterprise branch offices, and service provider-managed services applications for delivery of concurrent services at wire-speed performance. The integrated secure systems architecture of the Cisco 1800 Series delivers maximum business agility and investment protection.

Product Overview

Cisco 1800 Series integrated services routers are the next evolution of the award-winning Cisco 1700 Series modular access routers. The Cisco 1841 router (Figure 1) is designed for secure data connectivity and provides significant additional value compared to prior generations of Cisco 1700 Series routers by offering more than a fivefold performance increase and integrated hardware-based encryption enabled by an optional Cisco IOS® Software security image. The Cisco 1841 dramatically increase interface card slot performance and density over the Cisco 1700 Series while maintaining support for more than 30 existing WAN interface cards (WICs) and multiflex trunk cards (voice/WICs [VWICs]-for data only on the Cisco 1841 router). The Cisco 1841 router features secure, fast, and high-quality delivery of multiple, concurrent services for small-to-medium-sized businesses and small enterprise branch offices. The Cisco 1841 router offers embedded hardware-based encryption enabled by an optional Cisco IOS Software security image; further enhancement of VPN performance with an optional VPN acceleration module; an intrusion prevention system (IPS) and firewall functions; interfaces for a wide range of connectivity requirements, including support for optional integrated switch ports; plus sufficient performance and slot density for future network expansion and advanced applications as well as an integrated real-time clock.
Support of high-density WICs (HWICs) is optional.

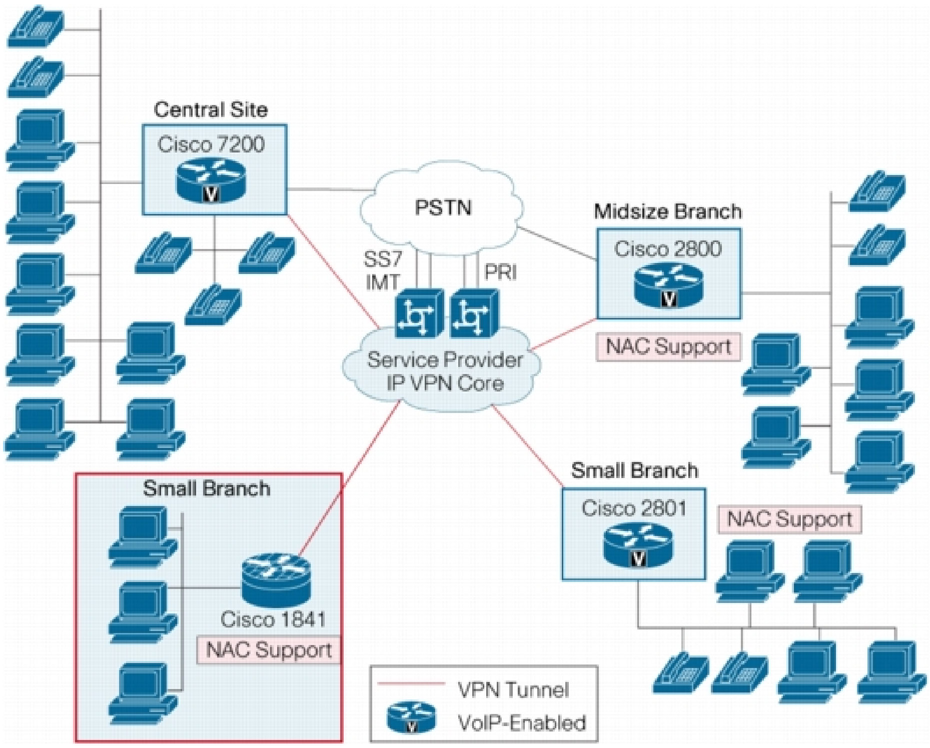
Figure 1. Cisco 1800 Series Integrated Services Routers

Applications

Secure Network Connectivity for Data

Security has become a fundamental building block of any network, and Cisco routers play an important role in embedding security at the customer's access edge. The Cisco IOS Software security feature sets for the Cisco 1841 router that enable the hardware-based encryption on the motherboard provide a robust array of features such as Cisco IOS Firewall, IPS support, IP Security (IPSec) VPNs (Digital Encryption Standard [DES], Triple DES [3DES], and Advanced Encryption Standard [AES]), SSL Web VPN, Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport (GET) VPN, and Easy VPN , Network Admissions Control (NAC) for antivirus defense, Secure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMP) in one solution set. In addition, the Cisco 1841 router offers bundled network security solutions with IPSEC and SSL VPN encryption-acceleration modules, making it the industry's most robust and adaptable security solution available for small-to-medium-sized businesses and small enterprise branch offices. As Figure 2 demonstrates, the Cisco 1800 Series routers help enable customers to deliver high-performance, concurrent, mission-critical data applications with integrated, end-to-end security.

Figure 2. Secure Network Connectivity with Cisco 1841 Router



Integrated Services

The new, high-performance and secure integrated services architecture of the Cisco 1841 router (as shown in Figure 2) enables customers to deploy simultaneous services such as secured data communications with traditional IP routing at wire-speed performance. By offering a hardware-based encryption on the motherboard that can be enabled with an optional Cisco IOS Software security image and the flexibility to integrate a wide array of services, modules, and interface cards, the Cisco 1841 router helps enable businesses to incorporate the functions of a standalone secure data solution.

Primary Features and Benefits

Architecture Features and Benefits

The Cisco 1841 modular architecture has been specifically designed to meet requirements of small to medium-sized businesses and small enterprise branch offices as well as service provider-managed applications for concurrent services at wire-speed performance. The Cisco 1841 router, together with other Cisco integrated services routers such as the Cisco 2800 Series, provide the broadest range of secure connectivity options in the industry combined with availability and reliability features. In addition, Cisco IOS Software provides support for a complete suite of transport protocols, quality of service (QoS), and security. Table 1 gives the architecture features and benefits of the Cisco 1841 router.

Table 1. Architecture Features and Benefits of Cisco 1841 Router

Feature	Benefit
High-Performance Processor	• Supports concurrent deployment of high-performance, secure data services with headroom for future applications
Modular Architecture	• Offers wide variety of LAN and WAN options; network interfaces are field-upgradable to accommodate future technologies • Provides many types of slots to add connectivity and services in the future on an "integrate-as-you-grow" basis • Supports more than 30 modules and interface cards, including existing WAN (WIC) and multiflex (VWIC) interface cards (for data support only on the Cisco 1841 router) and advanced integration modules (AIMs)
Integrated Hardware-Based Encryption Acceleration	• Offers cryptography accelerator as standard integrated hardware that can be enabled with an optional Cisco IOS Software for 3DES and AES encryption support • Provides enhanced feature set of security performance through support of optional VPN acceleration card for

	VPN 3DES or AES encryption
Ample Default Memory	• Provides 32 MB of Flash and 128 MB of synchronous dynamic RAM (SDRAM) memory to support deployment of concurrent services
Integrated Dual High-Speed Ethernet LAN Ports	• Helps enable connectivity speeds up to 100BASE-T Ethernet technology without the need for cards and modules • Allows segmentation of the LAN
Support for Cisco IOS 12.3T, 12.4, 12.4T Feature Sets and Beyond	• Supports the Cisco 1841 router starting with Cisco IOS Software Release 12.3T • Helps enable end-to-end solutions with support for latest Cisco IOS Software-based QoS, bandwidth management, and security features
Integrated Standard Power Supply	• Provides for easier installation and management of the router platform

Modularity Features and Benefits

The Cisco 1841 router provides enhanced modular capabilities while protecting customer investments. The modular architecture has been designed to provide the increased bandwidth and performance required to support concurrent, secure applications. Most existing WICs, multi-flex trunk interface cards (for data only), and Advanced Integration Modules (AIMs) are supported in the Cisco 1841. Table 2 lists the modularity features and benefits of the Cisco 1841 router.

Table 2. Modularity Features and Benefits of Cisco 1841 Router

Feature	Benefit
HWIC Slots	• The modular architecture on the Cisco 1841 router supports HWIC slots. The newly designed high-speed WAN interface slots significantly increase the data-throughput capability (up to 800-Mbps aggregate). Table 6 lists the High Speed WAN Interface cards supported on the Cisco 1841. • Both slots on the Cisco 1841 router are HWIC slots and provide compatibility with WICs and multiflex trunk (VWICs) interface cards (for data only).
AIM Slots (internal)	• The Cisco 1841 router supports hardware-accelerated encryption through AIM modules (AIM-VPN/BPII-PLUS, AIM-VPN/SSL-1). • The Cisco 1841 router has one internal AIM slot.

Secure Networking Features and Benefits

The Cisco 1800 Series features a built-in hardware-accelerated encryption on the motherboard that can be enabled with an optional Cisco IOS Software security image. The onboard hardware-based encryption acceleration offloads the encryption processes to provide greater IPSec 3DES and AES throughput. With the integration of optional VPN AIMs, NAC for antivirus defense, and Cisco IOS Software-based firewall and IPS support, Cisco offers the industry's leading robust and adaptable security solution for small to medium-sized businesses and small enterprise branch offices. Table 3 outlines router-integrated security features and benefits.

Table 3. Features and Benefits of Secure Networking

Feature	**Benefit**
Hardware-Based Encryption on Motherboard	• Support for hardware-based encryption on the Cisco 1841 can be enabled through an optional Cisco IOS Software security image.
AIM-Based VPN Acceleration	• Support for an optional dedicated VPN AIM can deliver two to three times the performance of embedded encryption capabilities.
SSL Web VPN	• Allows businesses to securely and transparently extend their networks to any Internet-enabled location using SSL VPN; the Cisco IOS WebVPN supports clientless access to applications such as HTML-based intranet content, e-mail, network file shares, and Citrix and to the Cisco SSL VPN Client, enabling full network access remotely to virtually any application
AIM-Based SSL VPN	• An optional dedicated SSL VPN AIM module provides SSL VPN acceleration and supports two times the number of tunnels when compared to embedded IOS based SSL VPN capabilities. The SSL VPN AIM module also supports IPSEC VPN and IP Payload Compression Protocol in hardware.
NAC	• NAC allows network access only to compliant and trusted endpoint devices for antivirus defense.
IPS Support	• Flexible support is provided with Cisco IOS Software. • New intrusion-detection-system (IDS) signatures can be dynamically loaded independent of the Cisco IOS Software release.
Cisco Easy VPN Remote and Server Support	• This feature eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.

Dynamic Multipoint VPN (DMVPN)	• DMVPN is a Cisco IOS Software solution for building IPSec + generic routing encapsulation (GRE) VPNs in an easy and scalable manner.
Group Encrypted Transport (GET) VPN	• GET VPN is a Cisco IOS Software solution that simplifies securing large Layer 2 or MPLS networks requiring partial or full-mesh connectivity by providing tunnel-less VPN connectivity
Cisco IOS Firewall, Including URL Filtering	• URL filtering support is available with optional Cisco IOS Security Software.
Real-Time Clock Support	• Real-time clock support keeps an accurate value of date and time for applications that require an accurate time stamp-such as logging, debugging, and digital certificates.
Cisco Router and Security Device Manager (SDM)	• An intuitive, easy-to-use, Web-based device management tool embedded within the Cisco IOS Software access routers can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features. • Cisco SDM helps resellers and customers to quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of the Cisco IOS Software command-line interface. **NOTE:** All 1841 Routers with 32MB Flash will ship with SDM Express and Router-SDM CD. Those with 64MB Flash and above will ship with Full SDM.
USB Port (1.1)	• The integrated USB port is configurable with an optional USB token for secure configuration distribution and off-platform storage of VPN credentials.

Cost of Ownership and Ease of Use

The Cisco 1841 router continues the heritage of offering versatility, integration, and power to small-to-medium-sized businesses and small enterprise branch offices. It offers many enhancements to support the deployment of multiple integrated services in the branch office. Key features and benefits that lower the cost of ownership and improve ease of use are outlined in Table 4.

Table 4. Cost of Ownership and Ease of Use-Features and Benefits

Feature	Benefit
Integrated Channel Service Unit (CSU)/Data Service Unit (DSU)	This feature consolidates typical communications equipment found in branch-office wiring closets into a single, compact unit. This space-saving solution provides better manageability.
USB Port (1.1)	The integrated USB peripheral port is provided to allow support for enhanced provisioning and simplified image distribution as well as other functions. These enhancements aid in reducing support costs and downtime.
Enhanced Setup Feature	An optional setup wizard with context-sensitive questions guides the user through the router configuration process, allowing faster deployment.
CiscoWorks, CiscoWorks VPN/Security Management Solution (VMS) and Cisco IP Solution Center (ISC) Support	Advanced management and configuration capabilities are offered through a Web-based GUI.
Cisco AutoInstall	This feature configures remote routers automatically across a WAN connection to save the cost of sending technical staff to the remote site.

Summary and Conclusion

As companies increase their security requirements and their need for integrated services, more intelligent office solutions are required. The best-in-class Cisco 1800 Series architecture has been specifically designed to meet these requirements for secure concurrent services at wire-speed performance. The Cisco 1841 Router offers the opportunity to consolidate the functions of separate devices into a single, compact solution that can be remotely managed. By providing integrated services, as well as great modular density and high performance, the Cisco 1841 router provides security, versatility, scalability, and flexibility for multiple applications to the small-to-medium-sized office and small enterprise branch office, and the service provider customer edge. The Cisco 1841 router easily accommodates a wide variety of network applications, such as secure branch-office data access including NAC for antivirus defense, VPN access and firewall protection, business-class DSL, IPS support, inter-VLAN routing, and serial device concentration. The Cisco 1841 router provides customers with the industry's most flexible, secure, and adaptable infrastructure to meet both today's and tomorrow's business requirements for maximum investment protection.

Specifications

Table 5 gives product specifications of the Cisco 1841 Router.

Table 5. Product Specifications of Cisco 1841 Router

Cisco 1800 Series	**Cisco 1841**
Target Applications	Secure data
Chassis	
Form factor	Desktop, 1-rack-unit (1RU) height (4.75 cm high with rubber feet)
Chassis	Metal
Wall-mountable	Yes
Rack-mountable	Yes (Optional Rackmount kit: ACS-1841-RM-19=)
Dimensions (W x D)	• 13.5 x 10.8 in. (34.3 x 27.4 cm) • Height without rubber feet: 1.73 in. (4.39 cm) • Height with rubber feet: 1.87 in. (4.75 cm)
Weight	• Maximum: 6.2 lb (2.8 kg); with interface cards and modules • Minimum: 6.0 lb (2.7 kg) (no interface cards and modules)
Architecture	
DRAM	Synchronous dual in-line memory module (DIMM) DRAM
DRAM capacity	• Default: 128 MB • Maximum: 384 MB
Flash memory	External compact Flash
Flash memory capacity	• Default: 32 MB • Maximum: 128 MB
Modular slots-total	Two
Modular slots for WAN access	Two

Modular slots for HWICs	Two
Modular slots for voice support	None-The Cisco 1841 does not support voice
Analog and digital voice support	No
VoIP support	Voice-over-IP (VoIP) pass-through only
Onboard Ethernet ports	Two 10/100
Onboard USB ports	One (1.1)
Console port	One-up to 115.2 kbps
Auxiliary port	One-up to 115.2 kbps
Onboard AIM slots	One (internal)
Packet-voice-DSP-module (PVDM) slots on motherboard	None-The Cisco 1841 does not support voice
Integrated hardware-based encryption on motherboard	Yes
Encryption support in software and hardware by default	DES, 3DES, AES 128, AES 192, AES 256
Power Supply Specifications	
Internal power supply	Yes
Redundant power supply	No
DC power support	No
AC input voltage	100 to 240 VAC
Frequency	50 to 60 Hz

AC input current	1.5A maximum
Output power	50W (maximum)
System Power Dissipation	
	153 BTU/hr
Software Support	
First Cisco IOS Software release	12.3(8)T
Cisco IOS Software default image, release	IP BASE, 12.4(1)
Environmental	
Operating temperature	32 to 104°F (0 to 40°C)
Operating humidity	10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating
Nonoperating Temperature	-4 to 149°F (-25 to 65°C)
Operating altitude	10,000 feet (3000 meters) @ 77°F (25°C)
Noise level	Normal operating temperature: • <78° F/26°C: 34 dBA • >78°F/26°C through <104°F/40°C: 37 dBA • >104°F/40°C: 42 dBA
Regulatory Compliance	
Safety	• UL60950-1 • CAN/CSA 60950-1 • AS 3260 • EN60950-1
EMI	• EN 55022, 1998, class A • CISPR22, 1997, class A • CFR47, Part 15, Subpart B, 1995, class A • EN61000-3-2 Harmonic Current Emission (only for equipment >75W but <16A) • EN61000-3-3 Voltage Fluctuation and Flicker (only for

	equipment ≤16A)
Immunity	• CISPR24, 1997 ITE-Immunity characteristics, Limits and methods of measurement • EN 55024,1998 ITE-Immunity characteristics, Limits and methods of measurement • EN50082-1, 1997 Electromagnetic compatibility-Generic immunity standard, Part 1 • EN 300 386, 1997 Telecommunications network equipment EMC requirements • The requirements are covered by the following standards: • IEC 61000-4-2:1995 Immunity to Electrostatic Discharges • IEC 61000-4-3:1995 Immunity to Radio Frequency Electromagnetic Fields • IEC 61000-4-4:1995 Immunity to Electrical Fast Transients • IEC 61000-4-5:1995 Immunity to Power Line Transients (Surges) • IEC 61000-4-6:1996 Immunity to Radio Frequency Induced Conducted Disturbances • IEC 61000-4-11:1995 Immunity to Voltage Dips, Voltage Variations, and Short Voltage Interruptions
Network homologation	• USA-TIA-968-A, T1.TRQ.6-2001 • Canada-CS-03 • European Union-RTTE Directive 5/99 • Argentina-CTR 21 • Australia-AS/ACIF S002, S003, S016 , S031, 3043 • Brazil-225-540-788, CTR3, 225-100-717 Edition 3, NET 001/92 1990 • China-ITU-G.992.1, ITU-G.992.1, ITU-G.991.2, CTR3, ITU I.431 1993 • Hong Kong-HKTA 2033, HKTA 2033, HKTA 2014, HKTA 2017 Issue 3 2003, HKTA 2011 Issue 1, HKTA 2011 Issue 2, HKTA 2013 Issue 1 • India-I_DCA_18_02_Jun_99-199, S/ISN-01/02 Issue 1999 S/ISN-02 1 1998, IR/PRI-01/02 Issue 1 1998, S/INT-2W/02 MAY 2001, S/INT-2W/02 MAY 2001 • Israel-U.S. approval accepted • Japan-Technical condition (DoC acceptance in process) • Korea-U.S. approval accepted • Mexico-U.S. approval accepted • New Zealand-PTC 270/272, CTR 3, ACA 016 Revision 4 1997, PTC 200 • Singapore-IDA TS ADSL1 Issue 1, IDA TS ADSL 2, IDA

	TS HDSL, IDA TS ISDN 1 Issue 1 1999, IDA TS ISDN 3 Issue 1 1999, IDA TS PSTN 1 Issue 4, IDA TS PSTN 1 Issue 4, IDA TS PSTN 1 Issue 4 • South Africa-U.S. approval accepted • Taiwan-U.S. approval accepted

Modular Support

Table 6 gives the modules and interface cards that the Cisco 1841 router supports.

Table 6. Modules and Interface Cards the Cisco 1841 Router Supports

Items	**Description**	**Cisco 1841**
Ethernet Switching HWICs		
HWIC-4ESW	4-port 10/100 BaseT Ethernet switch HWIC	√
Cable HWICs		
HWIC-CABLE-D-2	1 port DOCSIS 2.0 Cable HWIC	√
HWIC-CABLE-E/J-2	1 port Euro/J DOCSIS 2.0 Cable HWIC	√
Wireless Access Point HWICs		
HWIC-AP-AG-A	AP HWIC, 2 radios (2.4/5Ghz Radios 802.11 a/b/g) Americas	√
HWIC-AP-AG-E	AP HWIC, 2 radios (2.4/5Ghz Radios 802.11 a/b/g) Europe	√
HWIC-AP-AG-J	AP HWIC, 2 radios (2.4/5Ghz Radios for 802.11 a/b/g) Japan	√
HWIC-AP-G-A	AP HWIC, w 2.4 Ghz Radio for 802.11 b/g Americas	√
HWIC-AP-G-E	AP HWIC w 2.4 Ghz Radio for 802.11 b/g Europe	√
HWIC-AP-G-J	AP HWIC w 2.4 Ghz Radio for 802.11 b/g Japan	√

Serial HWICs/WICs		
HWIC-4A/S	4-Port Async/Sync Serial HWIC	√
HWIC-8A/S-232	8-Port Async/Sync Serial HWIC EIA-232	√
HWIC-8A	8-port Async HWIC	√
WIC-1T	1-port serial WIC	√
WIC-2T	2-port serial WIC	√
WIC-2A/S	2-port asynchronous or synchronous serial WIC	√
CSU/DSU WICs		
WIC-1DSU-T1-V2	1-port T1/Fractional-T1 CSU/DSU WIC	√
WIC-1DSU-56K4	1-port 4-wire 56-/64-kbps CSU/DSU WIC	√
ISDN BRI WICs		
WIC-1B-U-V2	1-port ISDN Basic Rate Interface (BRI) with integrated NT1 (U interface)	√
WIC-1B-S/T-V3	1-port ISDN BRI with S/T interface	√
DSL HWICs/WICs		
HWIC-1ADSL	1-port ADSLoPOTS HWIC	√
HWIC-1ADSLI	1-port ADSLoISDN HWIC	√
HWIC-ADSL-B/ST	2-port HWIC w/ 1-port ADSLoPOTS and 1-port ISDN BRI-S/T	√
HWIC-ADSLI-B/ST	2-port HWIC w/ 1-port ADSLoISDN and 1-port ISDN BRI-S/T	√
WIC-1ADSL	1-port asymmetric DSL (ADSL) over basic-telephone-service WIC	√

WIC-1ADSL-DG	1-port ADSL over basic telephone service with dying-gasp[1] WIC	√
WIC-1ADSL-I-DG	1-port ADSL over ISDN with dying-gasp1 WIC	√
WIC-1SHDSL-V3	1-port G.shdsl WIC with 4-wire support	√
HWIC-2SHDSL	2-Pair G.SHDSL HWIC with 2-wire and 4-wire support	√
HWIC-4SHDSL	4-Pair G.SHDSL HWIC with 2-wire, 4-wire, and 8-wire support	√
Wireless WAN 3G HWIC		
HWIC-3G-CDMA	3G WWAN HWIC-EVDO Rev A/Rel 0/1xRTT-800/1900MHz	√
HWIC-3G-GSM	3G WWAN HWIC-EVDO Rev A/Rel 0/1xRTT-800/1900MHz	√
Analog Modem WICs		
WIC-1AM	1-port analog modem WIC	√
WIC-2AM	2-port analog modem WIC	√
WIC-1AM-V2	1-port analog modem WIC (updated version)	√
WIC-2AM-V2	2-port analog modem WIC (updated version)	√
T1, E1, and G.703 VWICs		
VWIC-1MFT-T1	1-port RJ-48 multiflex trunk-T1	√ (data only)
VWIC-2MFT-T1	2-port RJ-48 multiflex trunk-T1	√ (data only)
VWIC-2MFT-T1-DI	2-port RJ-48 multiflex trunk-T1 with drop and insert	√ (data only)
VWIC-1MFT-E1	1-port RJ-48 multiflex trunk-E1	√ (data only)

VWIC-1MFT-G703	1-port RJ-48 multiflex trunk-G.703	√ (data only)
VWIC-2MFT-E1	2-port RJ-48 multiflex trunk-E1	√ (data only)
VWIC-2MFT-E1-DI	2-port RJ-48 multiflex trunk-E1 with drop and insert	√ (data only)
VWIC-2MFT-G703	2-port RJ-48 multiflex trunk-G.703	√ (data only)
VWIC2-1MFT-T1/E1	1-port 2nd generation multiflex trunk-T1/E1	√ (data only)
VWIC2-2MFT-T1/E1	2-port 2nd generation multiflex trunk-T1/E1	√ (data only)
VWIC2-1MFT-G703	1-port 2nd generation multiflex trunk-G.703	√ (data only)
VWIC2-2MFT-G703	2-port 2nd generation multiflex trunk-G703	√ (data only)
AIMs		
AIM-VPN/BPII-PLUS	Enhanced-performance DES, 3DES, AES, and compression VPN encryption AIM	√
AIM-VPN/SSL-1	DES/3DES/AES/SSL VPN Encryption/Compression	√

Cisco 2800 Series Integrated Services Routers

Cisco Systems®, Inc. is redefining best-in-class enterprise and small- to- midsize business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, video, and wireless services. Founded on 20 years of leadership and innovation, the Cisco® 2800 Series of integrated services routers (refer to Figure 1) intelligently embed data, security, voice, and wireless services into a single, resilient system for fast, scalable delivery of mission-critical business applications. The unique integrated systems architecture of the Cisco 2800 Series delivers maximum business agility and investment protection.

Figure 1. Cisco 2800 Series

Product Overview

The Cisco 2800 Series comprises four platforms (refer to Figure 1): the Cisco 2801, the Cisco 2811, the Cisco 2821, and the Cisco 2851. The Cisco 2800 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold performance improvement, up to a tenfold increase in security and voice performance, embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, Cisco 2600, and Cisco 3700 Series.

The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services
at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide range of wired and wireless connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

Secure Network Connectivity for Data, Voice, and Video

Security has become a fundamental building block of any network. Routers play an important role in any network defense strategy because security needs to be embedded throughout the network. The Cisco 2800 Series features advanced, integrated, end-to-end security for the delivery of converged services and applications. With the Cisco IOS® Software Advanced Security feature set, the Cisco 2800 provides a robust array of common security features such as a Cisco IOS Software Firewall, intrusion prevention, IPSec VPN, Secure Socket Layer (SSL) VPN, advanced application inspection and control, Secure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMPv3) in one secure solution set. Additionally, by integrating security functions directly into the router itself, Cisco can provide unique intelligent security solutions other security devices cannot, such as network admissions control (NAC) for antivirus defense; Voice and Video Enabled VPN (V3PN) for quality-of-service (QoS) enforcement when combining voice, video, and VPN; and Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport (GET) VPN, and Easy VPN for enabling more scalable and manageable VPN networks. In addition, Cisco offers a range of security acceleration hardware such as the intrusion-prevention network modules and advanced integration modules (AIM) for encryption, making the Cisco 2800 Series the industry's most robust and adaptable security solution available for branch offices. As Figure 2 demonstrates, using a Cisco 2800 Series uniquely enables customers to deliver concurrent, mission-critical data, voice, and video applications with integrated, end-to-end security at wire-speed performance.

Converged IP Communications

As shown in Figure 2, the Cisco 2800 Series can meet the IP Communications needs of small-to-medium sized business and enterprise branch offices while concurrently delivering an industry-leading level of security within a single routing platform. Cisco CallManager Express (CME) is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones, including wired and cordless WLAN phones. This solution is for customers with data-connectivity requirements interested in deploying a converged IP telephony solution for up to 96 IP phones. With the Cisco 2800 Series, customers can securely deploy data, voice, and IP telephony on a single platform for their small-to-medium sized branch offices, helping them to streamline their operations and lower their network costs. The Cisco 2800 Series with optional Cisco CME support offers a core set of phone features that customers require for their everyday business needs and takes advantage of the wide array of voice capabilities that are embedded in the Cisco 2800 Series (as shown in Table 1) together with optional features available in Cisco IOS Software to provide a robust IP telephony offering for the small to medium-sized branch-office environment.

Wireless Services

The Cisco 2800 Series can provide a complete wireless solution for branch offices, small/medium sized businesses, and Wi-Fi hotspots. Wireless services enable greater mobility for employees, partners, and customers, resulting in increased productivity. The Cisco 2800 Series supports an integrated access point for wireless LAN connectivity, Wi-Fi Hotspot services for public access, wireless infrastructure services for cordless WLAN telephony and for larger sites, and land mobile radio over IP for radio users.

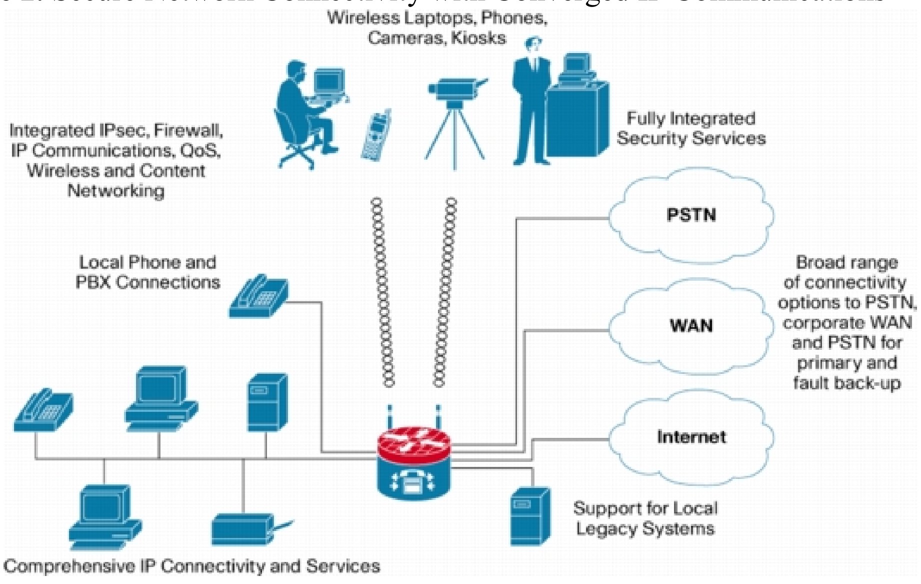
Integrated Services

Figure 2 also highlights the fact that with the unique integrated services architecture of the Cisco 2800 Series, customers can now securely deploy IP Communications with traditional IP routing while leaving interface and module slots available for additional advanced services. With the optional integration of a wide array of services modules, the Cisco 2800 Series offers the ability to easily integrate the functions of standalone network appliances and components into the Cisco 2800 Series chassis itself. Many of these modules, such as the Cisco Network Analysis Module, Cisco Voice Mail Module, Cisco Intrusion Detection Module, Wide Area Application Services Module, and Cisco Content Engine Module, have embedded processors and hard drives that allow them to run largely independently of the router while allowing management from a single management interface. This flexibility greatly expands the potential applications of the Cisco 2800 Series beyond traditional routing while still maintaining the benefits of integration. These benefits include ease of management, lower solution costs (CAPEX and OPEX), and increased speed of deployment.

Applications

Secure Network Connectivity with Converged IP Communications

Figure 2. Secure Network Connectivity with Converged IP Communications



Wireless Laptops, Phones, Cameras, Kiosks
Integrated IPsec, Firewall, IP Communications, QoS, Wireless and Content Networking
Fully Integrated Security Services
PSTN
Local Phone and PBX Connections
Broad range of connectivity options to PSTN, corporate WAN and PSTN for primary and fault back-up
WAN
Internet
Support for Local Legacy Systems
Comprehensive IP Connectivity and Services

Architecture-Features and Benefits

The Cisco 2800 Series architecture has been designed specifically to meet the expanding requirements of enterprise branch offices and small-to-medium-sized businesses for today's and future applications. The Cisco 2800 Series provides the broadest range of connectivity options in the industry combined with leading-edge availability and reliability features. In addition, Cisco IOS Software provides support for a complete suite of transport protocols, Quality-of-Service (QoS) tools, and advanced security and voice applications for wired and wireless deployments.

Table 1. Architecture-Features and Benefits

Feature	**Benefit**
Modular Architecture	• A wide variety of LAN and WAN options are available. Network interfaces can be upgraded in the field to accommodate future technologies. • Several types of slots are available to add connectivity and services in the future on an "integrate-as-you-grow" basis. • The Cisco 2800 supports more than 90 modules, including WICs, VICs, network modules, PVDMs, and AIMs (Note: the Cisco 2801 router does not support network modules).
Embedded Security Hardware Acceleration	• Each of the Cisco 2800 Series routers comes standard with embedded hardware cryptography accelerators, which when combined with an optional Cisco IOS Software upgrade help enable WAN link security and VPN services.
Integrated Dual Fast Ethernet or Gigabit Ethernet Ports	• The Cisco 2800 Series provide two 10/100 on the Cisco 2801 and Cisco 2811 and two 10/100/1000 on the Cisco 2821 and Cisco 2851
Support for Cisco IOS Software	• The Cisco 2800 helps enable end-to-end solutions with full support for the latest Cisco IOS Software-based QoS, bandwidth management, and security features. • Common feature and command set structure across the Cisco 1700, 1800, 2600, 2800, 3700 and 3800 series routers simplifies feature set selection, deployment, management, and training.
Optional Integrated Power Supply for Distribution of Power Over Ethernet (PoE)	• An optional upgrade to the internal power supply provides in-line power (802.3af-compliant Power-over-Ethernet [PoE] and Cisco standard inline power) to optional integrated switch modules.
Optional Integrated Universal DC Power	• On the Cisco 2811, 2821, and 2851 routers an optional DC power supply is available that extends possible

Supply	deployments environments such as central offices and industrial environments (Note: not available on the Cisco 2801).
Integrated Redundant-Power-Supply (RPS) Connector	• On the Cisco 2811, 2821, and 2851 there is a built in external power-supply connector that eases the addition of external redundant power supply that can be shared with other Cisco products to decrease network downtime by protecting the network components from downtime due to power failures.

Modularity-Features and Benefits

The Cisco 2800 Series provides significantly enhanced modular capabilities (refer to Table 2) while maintaining investment protection for customers. The modular architecture has been redesigned to support increasing bandwidth requirements, time-division multiplexing (TDM) interconnections, and fully integrated power distribution to modules supporting 802.3af PoE or Cisco in-line power, while still supporting most existing modules. With more than 90 modules shared with other Cisco routers such as the Cisco 1700, 1800, 2600, 3700, and 3800 series, interfaces for the Cisco 2800 Series can easily be interchanged with other Cisco routers to provide maximum investment protection in the case of network upgrades. In addition, taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

Table 2. Modularity-Features and Benefits

Feature	**Benefit**
Enhanced Network-Module (NME) Slots	• The NME slots support existing network modules (Note: NM and NME support on Cisco 2811, 2821, and 2851 only) • NME Slots offer high data throughput capability (up to 1.6Gbps) and support for Power over Ethernet (POE). • NME slots are highly flexible with support for extended NMEs (NME-X on Cisco 2821 and 2851 only) and enhanced double-wide NMEs (NME-XDs) (Note: Cisco 2851 only).
High-Performance WIC (HWIC) Slots with Enhanced Functionality	• Four integrated HWIC slots on Cisco 2811, 2821, and 2851 and two integrated HWIC slots on Cisco 2801 allow for more flexible and dense configurations. • HWICs slots can also support WICs, VICs, and VWICs • HWIC slots offer high data throughput capability (up to 400 Mbps half duplex or 800 Mbps aggregate throughput)

	and Power over Ethernet (POE) support. • A flexible form factor supports up to two double-wide HWIC (HWIC-D) modules.
Dual AIM Slots	Dual AIM slots support concurrent services such as hardware-accelerated security, ATM segmentation and reassembly (SAR), compression, and voice mail (Refer to Table 7 for more details on specific platform support).
Packet Voice DSP Module (PVDM) Slots on Motherboard	Slots for Cisco PVDM2 Modules (DSP Modules) are integrated on the motherboard, freeing slots on the router for other services.
Extension-Voice-Module (EVM) Slot	The EVM supports additional voice services and density without consuming the network-module slot (Note: available only on Cisco 2821 and 2851).
USB Support	Up to two USB ports are available per Cisco 2800 series router. The routers' Universal Serial Bus (USB) ports enable important security and storage capabilities.

Secure Networking-Feature and Benefits

The Cisco 2800 Series features enhanced security functionality as shown in Table 3. Integrated on the motherboard of every Cisco 2800 Series router is hardware-based encryption acceleration that offloads the encryption processes to provide greater IPSec throughput with less overhead for the router CPU when compared with software-based solutions. With the integration of optional VPN modules (for enhanced VPN tunnel count), Cisco IOS Software-based firewall, network access control, or content-engine network modules, Cisco offers the industry's most robust and adaptable security solution for branch-office routers.

Table 3. Secure Networking-Feature and Benefits

Feature	**Benefit**
Cisco IOS Software Firewall	• Sophisticated security and policy enforcement provides features such as stateful, application-based filtering (context-based access control), per-user authentication and authorization, real-time alerts, transparent firewall, and IPv6 firewall.
Secure Sockets Layer (SSL)	• SSL provides security for web transactions by handling authentication, data enryption and digital signatures. The 2800 Series supports SSL VPNs and SSL acceleration via the AIM-VPN/SSL-3.

Onboard VPN Encryption Acceleration	• The Cisco 2800 Series supports IPSec Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192, and AES 256 cryptology without consuming an AIM slot.
Network Admissions Control (NAC)	• A Cisco Self-Defending Network initiative, NAC seeks to dramatically improve the ability of networks to identify, prevent, and adapt to threats by allowing network access only to compliant and trusted endpoint devices.
Multiprotocol Label Switching (MPLS) VPN Support	• The Cisco 2800 Series supports specific provider edge functions plus a mechanism to extend customers' MPLS VPN networks out to the customer edge with virtual routing and forwarding (VRF) firewall and VRF IPSec. For details on the MPLS VPN support on the different versions of the Cisco 2800 Series, please check the feature navigator tool on http://www.cisco.com.
USB eToken Support	• USB eTokens from Aladdin Knowledge Systems (available at http://www.aladdin.com/etoken/cisco/) provides secure configuration distribution and allows users to store VPN credentials for deployment
AIM-Based Security Acceleration	• Support for an optional dedicated security AIM can deliver 2 to 3 times the performance of embedded encryption capabilities with Layer 3 compression.
Intrusion Prevention System (IPS)	• Flexible and high performance support is offered through Cisco IOS® Software or an intrusion-detection-system (IDS) network module. • The ability to load and enable selected IDS signatures in the same manner as Cisco IDS Sensor Appliances
Advanced Application Inspection and Control	• Cisco IOS Firewall includes HTTP and several email inspection engines that can be used to detect misuse of port 80 and email connectivity.
Cisco Easy VPN Remote and Server Support	• The Cisco 2800 Series eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.
Dynamic Multipoint VPN (DMVPN)	• DMVPN is a Cisco IOS Software solution for building IPSec + generic routing encapsulation (GRE) VPNs in an easy and scalable manner.
Group Encrypted Transport (GET)	• GET VPN is a Cisco IOS Software solution that simplifies securing large Layer 2 or MPLS networks requiring partial or

VPN	full-mesh connectivity by providing tunnel-less VPN connectivity.
URL Filtering	• URL filtering is available onboard with an optional content-engine network module or external with a PC server running the URL filtering software.
Cisco Router and Security Device Manager (SDM)	• This intuitive, easy-to-use, Web-based device-management tool is embedded within the Cisco IOS Software access routers; it can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features.

IP Telephony Support-Features and Benefits

The Cisco 2800 Series allows network managers to provide scalable analog and digital telephony without investing in a one-time solution (refer to Table 4 for more detail), allowing enterprises greater control of their converged telephony needs. Using the voice and fax modules, the Cisco 2800 Series can be deployed for applications ranging from voice-over-IP (VoIP) and voice-over-Frame Relay (VoFR) transport to robust, centralized solutions using the Cisco Survivable Remote Site Telephony (SRST) solution or distributed call processing using Cisco Call Manager Express (CME). The architecture is highly scalable with the ability to connect up to 12 T1/E1s trunks, 52 foreign-exchange-station (FXS) ports, or 36 foreign-exchange-office (FXO) ports.

Table 4. IP Telephony Support-Features and Benefits

Feature	**Benefit**
IP Phone Support	• Optional support for Cisco in-line power distribution to Ethernet switch network modules and HWICs can be used to power Cisco IP phones.
EVM Module Slots	• Extension Voice Module Slots, available only on the Cisco 2821 and Cisco 2851, provide support for the Cisco High-Density Analog and Digital Extension Module for Voice and Fax, providing support for up to 24 total voice and fax sessions without consuming a Network Module Slot.
PVDM (DSP) Slots on Motherboard	• DSP (PVDM2) modules deliver support for analog and digital voice, conferencing, transcoding, and secure Real-Time Transport Protocol (RTP) applications.
Integrated Call Processing	• Cisco CME is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones. Cisco CME delivers telephony features similar to those that are commonly used by business users to meet the requirements of the

	small to medium-sized offices.
Integrated Voice Mail	• Support for up to a 250 mailboxes using the Cisco Unity® Express voice messaging system is possible with the integration of an optional voice-mail AIM or network module.
Broad Range of Voice Interfaces	• Interfaces for public switched telephone network (PSTN), private branch exchange (PBX), and key system connections include FXS; FXO; analog direct inward dialing (DID); ear and mouth (E&M); Centralized Automated Message Accounting (CAMA); ISDN Basic Rate Interface (BRI); and T1, E1, and J1 with ISDN Primary Rate Interface (PRI); QSIG; E1 R2; and several additional channel-associated-signaling (CAS) signaling schemes.
Survivable Remote Site Telephony (SRST)	• Branch offices can take advantage of centralized call control while cost-effectively providing local branch backup using SRST redundancy for IP telephony.

Wireless Support-Features and Benefits

The Cisco 2800 Series can provide a complete wireless solution for branch offices, small/medium sized businesses, and Wi-Fi hotspots. Wireless services enable greater mobility for employees, partners, and customers, resulting in increased productivity.

Table 5. Wireless Support-Features and Benefits

Feature	**Benefit**
WLAN Connectivity	• The 802.11b/g or 802.11a/b/g HWIC access point interface card can be used to provide integrated WLAN connectivity to mobile clients at sites requiring a single access point, resulting in mobility and enhanced productivity for users. • Dual RP-TNC connectors enable diversity and allow for optimum coverage through the use of external antennas.
Wireless Infrastructure Services	• Telephony support for wired and WLAN IP phones is delivered by Cisco CallManager Express (CCME) or by Survivable Remote Site Telephony (SRST) with Cisco CallManager. Cordless WLAN IP phones allow users to be mobile and more productive. • Integrated switch modules with Power over Ethernet (POE) enable support for Cisco Aironet access points (for larger sites) as well as wired IP phones. • Mobility for clients from WLAN to cellular networks is enabled by Mobile IP home agent support.

	• IEEE 802.1x local authentication using LEAP provides enhanced reliability through survivable authentication for WLAN clients during WAN failures. • Customizable guest access is enabled with the service selection gateway features, along with the Subscriber Edge Services Manager.
Land Mobile Radio Over IP	• LMR over IP support allows radio users (e.g., security personnel, maintenance personnel, police officers, etc.) to communicate via IP with phone and PC users, delivering improved communications and productivity.
Wi-Fi Hotspot Services	• The access zone router and service selection gateway services features can be used to deploy secure public WLAN access services with an integrated HWIC-AP for small sites or with Cisco Aironet access points for larger sites. Wi-Fi hotspot services can be offered for additional revenue for public locations (e.g., restaurants, hotels, airports, etc.) or a value-added service for customer satisfaction.

Cost of Ownership and Ease of Use-Features and Benefits

The Cisco 2800 Series continues the heritage of offering versatility, integration, and power to branch offices. The Cisco 2800 Series offers many enhancements to help enable the support of multiple services in the branch office as shown in the table below.

Table 6. Cost of Ownership and Ease of Use-Feature and Benefits

Feature	Benefit
Integrated Channel Service Unit/Data Service Unit (CSU/DSU), Add/Drop Multiplexers, Firewall, Modem, Compression, and Encryption	• Consolidates typical communications equipment found in branch-office wiring closets into a single, compact unit; this space-saving solution provides better manageability
Optional Network Analysis Module	• Provides application-level visibility into network traffic for troubleshooting, performance monitoring, capacity planning, and managing network-based services (Note: Cisco 2811, 2821, and 2851 only)
Cisco IOS IP Service Level Agreements (IP SLAs)	• With Cisco IOS IP SLAs, users can verify service guarantees, increase network reliability by

	validating network performance, proactively identify network issues, and increase Return on Investment (ROI) by easing the deployment of new IP services
Cisco IOS Software Warm Reboot	• Reduces system boot time, and decreases downtime caused by Cisco IOS Software reboots (Cisco 2811, 2821 and 2851)
Enhanced Setup Feature	• Optional setup wizard with context-sensitive questions guides the user through the router configuration process, allowing faster deployment
CiscoWorks Support	• Offers advanced management and configuration capabilities through a Web-based GUI
Cisco AutoInstall	• Configures remote routers automatically across a WAN connection to save cost of sending technical staff to the remote site
Cisco IOS Embedded Event Manager (EEM)	• Enables automation of many network management tasks and directs the operation of Cisco IOS to increase availability, collect information, and notify external systems or personnel about critical events

Summary and Conclusion

As companies strive to lower the cost of running their network and increase the productivity of their end users with network applications, more intelligent branch-office solutions are required. The Cisco 2800 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services at wire speed. The Cisco 2800 Series is designed to consolidate the functions of many separate devices into a single, compact package that can be managed remotely. Because the Cisco 2800 Series routers are modular devices, interface configurations are easily customized to accommodate a wide variety of network applications, such as branch-office data access, integrated switching, voice and data integration, wireless LAN services, dial access services, VPN access and firewall protection, business-class DSL, content networking, intrusion prevention, inter-VLAN routing, and serial device concentration. The Cisco 2800 Series provides customers with the industry's most flexible, adaptable infrastructure to meet both today's and tomorrow's business requirements for maximum investment protection.

Product Specifications

Table 7. Chassis Specifications

Cisco 2800 Series	**Cisco 2801**	**Cisco 2811**	**Cisco 2821**	**Cisco 2851**
Product Architecture				
DRAM	• Default: 128 MB • Maximum: 384 MB	• Default: 256 MB • Maximum: 768 MB	• Default: 256 MB • Maximum: 1 GB	
Compact Flash	• Default: 64 MB • Maximum: 128MB	• Default: 64 MB • Maximum: 256 MB		
Fixed USB 1.1 Ports	1	2		
Onboard LAN Ports	2-10/100		2-10/100/1000	
Onboard AIM (Internal) Slot	2			
Interface Card Slots	• 4 slots; 2 slots support HWIC, WIC, VIC, or VWIC type modules • 1 slot supports WIC, VIC, or VWIC type modules • 1 slot supports VIC or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules		
Network-Module Slot	No	1 slot, supports NM and NME type modules	1 slot, supports NM, NME and NME-X type modules	1 slot, supports NM, NME, NME-X, NMD and NME-XD type modules

Extension Voice Module Slot	0	1
PVDM (DSP) Slots on Motherboard	2	3
Integrated Hardware-Based Encryption	Yes	
VPN Hardware Acceleration (on Motherboard)	DES, 3DES, AES 128, AES 192, and AES 256	
Optional Integrated In-Line Power (PoE)	Yes, requires AC-IP power supply	
Console Port (up to 115.2 kbps)	1	
Auxiliary Port (up to 115.2 kbps)	1	
Minimum Cisco IOS Software Release	12.3(8)T	
Rack	Yes, 19-inch	Yes, 19- and 23-in. options

Mounting				
Wall Mounting	No	Yes	No	No
Power Requirements				
AC Input Voltage	100 to 240 VAC, autoranging			
AC Input Frequency	47-63 Hz			
AC Input Current	2A (110V) 1A (230V)		3A (110V) 2A (230V)	
AC Input Surge Current	50A maximum, one cycle (-48V power included)			
AC-IP Maximum In-Line Power Distribution	120W	160W	240W	360W
AC-IP Input Current	4A (110V) 2A (230V)		8A (110V) 4A (230V)	
AC-IP Input Surge Current	50A maximum, one cycle (-48V power included)			
DC Input Voltage	No DC Power Option available	24 to 60 VDC, autoranging positive or negative		
DC Input Current	• No DC Power Option available	• 8A (24V) • 3A (60V) • Startup current 50A<10 ms	• 12A (24V) • 5A (60V) • Startup current 50A<10 ms	
Power	150W (511	170W (580	280W (955	280W (955

Dissipation-AC without IP Phone Support	BTU/hr)	BTU/hr)	BTU/hr)	BTU/hr)
Power Dissipation-AC with IP Phone Support-System Only	150W (511 BTU/hr)	210W (717 BTU/hr)	310W (1058 BTU/hr)	370W (1262 BTU/hr)
Power Dissipation-AC with IP Phone Support-IP Phones	180W (612 BTU/hr)	160W (546 BTU/hr)	240W (819 BTU/hr)	360W (1128 BTU/hr)
Power Dissipation-DC	Not applicable	180W (614 BTU/hr)	300W (1024 BTU/hr)	300W (1024 BTU/hr)
RPS	No	External only, connector for RPS provided by default		
Recommended RPS Unit	No RPS option	Cisco RPS-2300 Redundant Power System		
Environmental Specifications				
Operating Temperature	32° to 104°F (0° to 40°C)			
Non-Operating Temperature	-4° to 149°F (-20° to 65°C)	-40° to 158°F (-40° to 70°C)		
Maximum Operating	• 40°C @ sea level • 31°C @ 6,000 ft	• 40°C @ sea level • 40°C @ 6,000 ft (1800 m)		

Temperature at Altitude	(1800 m) • 25°C @ 10,000 ft (3000 m) Note: Derate 1.5°C per 1000 ft	• 30°C @ 13,000 ft (4000 m) • 27.2°C @ 15,000 ft (4600 m) Note: Derate 1.4°C per 1,000 ft above 6,000 ft	
Operating Humidity	10 to 85% non-condensing	5 to 95%, non-condensing	
Dimensions (H x W x D)	• 1.72 x 17.5 x 16.5 in. • (43.7 x 445 x 419 mm)	• 1.75 x 17.25 x 16.4 in. • (44.5 x 438.2 x 416.6 mm)	• 3.5 x 17.25 x 16.4 in. • (88.9 x 438.2 x 416.6 mm)
Rack Height	1 rack unit (1RU)		2RU
Weight (Fully Configured)	13.7 lb (6.2 kg)	14 lb (6.4 kg)	25 lb (11.4 kg)
Noise Level (Min/Max)	• 39 dBA for normal operating temperature (<90°F/32.2°C) • 53.5 dBA (@ maximum fan speed)	• 47 dBA for normal operating temperature (<90°F/32.2°C) • 57 dBA (@ maximum fan speed)	• 44 dBA for normal operating temperature (<90°F/32.2°C) • 53 dBA (@ maximum fan speed)
Regulatory Compliance			
NEBS	No	Yes	Yes
Safety	• UL 60950 • CAN/CSA C22.2 No. 60950 • IEC 60950 • EN 60950-1 • AS/NZS 60950		
Immunity	• EN300386 • EN55024/CISPR24 • EN50082-1 • EN61000-6-2		

EMC	• FCC Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI Class A • EN 300386 • EN61000-3-3 • EN61000-3-2
FIPS-2	FIPS 140-2 Certification for 2801, 2811, 2821, 2851
TELCOM **	• For all four platforms, Telecom compliance standards depend upon country and interface type. Interfaces comply with FCC Part 68, CS-03, JATE Technical Conditions, European Directive 99/5/EC and relevant TBR's. For specific information see the datasheet for the specific interface card. • Homologation requirements vary by country and interface type. For specific country information, see the on-line approvals data base: http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH&module=EXTERNAL_SEARCH