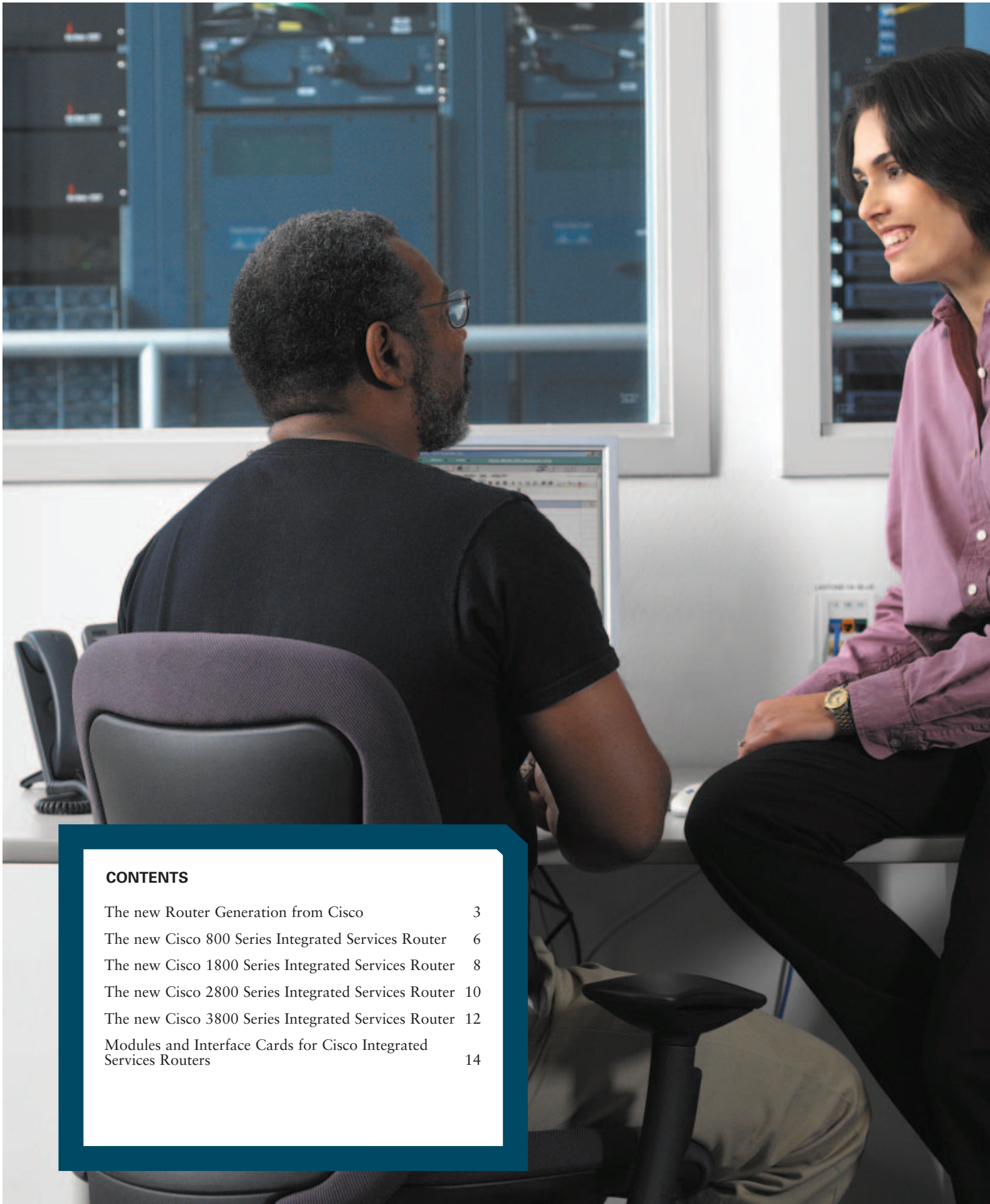


ALL SERVICES INCLUDED



An overview of Cisco Integrated Services Routers



CONTENTS

The new Router Generation from Cisco	3
The new Cisco 800 Series Integrated Services Router	6
The new Cisco 1800 Series Integrated Services Router	8
The new Cisco 2800 Series Integrated Services Router	10
The new Cisco 3800 Series Integrated Services Router	12
Modules and Interface Cards for Cisco Integrated Services Routers	14

THE NEW ROUTER GENERATION FROM CISCO

The new Cisco Integrated Services Routers offer much more than just the intelligent delivery of data packets to the right address. As their name suggests, these Integrated Services Routers comes with a range of integrated services covering data, security, voice and wireless technology. In particular, the ISR 2800 and 3800 Series enable you to set up a complete IP communication system without the need to buy or install additional devices within a remote Branch Office environment. Not only does this help to reduce procurement costs but it also simplifies the maintenance and operational life cycle management of the remote locations.

Networks are increasingly evolving from closed to more open systems by interconnecting business partners, suppliers, and customers. These open networks are becoming more reliant on un-trusted and sometimes public networks, such as the Internet, to carry converging voice, video, and data. At the same time, security threats have grown exponentially both from within the network as well as at the network perimeter. Without the appropriate security policies, processes, and products, Internet connectivity can compromise the very gains in productivity that companies are working so hard to achieve.

As a result, an enterprise must defend all parts of the network against external and internal threats, while maintaining a careful balance between the need for access and the need for protection. The use of an open network environment increases the need for robust and comprehensive security, as network topologies now have additional areas to protect.

Integrating products from different manufacturers can be a complex task, with the administration and management of disparate products often taking up considerable time.

When the integration effort is a multiplication factor of both the number of products being integrated and the number of locations at which the effort has to take place, it is easy to see why reducing the overall complexity of this effort through the introduction of embedded, integrated security can provide tangible operational efficiencies whilst reducing the costs associated with supply chain management.

Cisco Integrated Services Routers have been engineered to deliver secure, concurrent support for voice, data and video. They therefore form the foundation for Cisco's vision of the Intelligent Information Network; a whole system approach to intelligence in and between devices, services and applications. New applications can be implemented faster, running more smoothly and efficiently in day-to-day operation. The services integrated into the new Cisco Integrated Services Routers are:

- comprehensive security functions
- setting up of VPN connections
- voice over IP communication (from Series 2800 upwards)
- connectivity with wireless devices
- integrated management through Cisco SDM

Keep out – integrated security

There are lots of products on the market that promise you security. However, when you install products from multiple manufacturers in head office, on other sites or in the home offices of your employees, whilst you may gain security, you can lose an overall view of the network. Where is the attack coming from? Which ones should the administrator be worried about? What measures need to be put in place immediately?

For this reason, it makes sense to source as many security functions as possible from a single supplier, perhaps even integrated into products. Consistent security guidelines are then easier to define and the day-to-day work of the system administrator is made much easier; whether when installing, maintaining, identifying errors or adding new applications. Cisco Integrated Services Routers combine secure internet access, firewalls, intrusion detection, intrusion prevention encryption, dynamic routing functions, comprehensive QoS and the secure transmission of voice and video.

The Cisco IOS® Firewall: With this software, a Stateful Inspection Firewall is integrated into the router to provide internal users with secure, per-application-based access control for all traffic across perimeters, such as perimeters between private enterprise networks and the Internet. Also known as Context-Based Access Control (CBAC).

The applications monitored by Context Based Access Control (CBAC) include TCP and UDP internet applications, HTTP (Java blocking), SMTP, FTP, TFTP and multi-media applications such as SIP, SCCP (Skinny), H.323, RTSP, RealAudio and other voice/video applications.

Intrusion Detection: Cisco IDS can help to identify over one hundred of the most familiar forms of attack¹ by way of signatures that sample across the data stream, thus recognising potential security compromises early. Cisco IDS also helps to identify and protect against suspicious activity before it affects the network and can send an alarm message to a network or security management console.

Data encoding: Either by way of software or using dedicated hardware modules, Cisco's routers encode the VPN communications using a 56-bit Data Encryption Standard (DES), 128-bit Triple DES (3DES) or 256-bit Advanced Encryption Standard (AES). Encoding can also be performed over a X.509 Public Key Infrastructure (PKI).

Network Admission Control (NAC): Using the Cisco Trust Agent software (CTA) installed on desktop computers and terminal servers, information on the security status can be gathered from across the system. This information is supplied by the products of other manufacturers, e.g. by anti-virus programmes, and transmitted to Cisco network components. These decide in turn whether the network request of an end station is permissible or not. CTA also works with the Cisco Security Agent (CSA), a security solution for end stations that protects against Day-Zero and similar attacks.

A computer which has not been patched using the latest anti-virus updates could infect another computer on the network. However, that computer will only be allowed access to resources by the Cisco Integrated Services Router when it has received the latest anti-virus updates and these have been installed on its system.

URL filtering: Allows a network administrator to easily apply Internet use policies to permit access only to company-approved URLs or categories of sites

A good connection – telephony using Cisco routers

A converged network can play a critical part in helping a company to identify new ways to generate revenue, reduce operational costs, increase organisational flexibility, and generate a sustainable competitive advantage. Cisco IP Communications deliver increased productivity and greater mobility for employees who can access information anywhere on the corporate network as and when they need it.

Innovative applications and services are enabling companies to transform their businesses by simplifying and enhancing their business processes. Organisations can deliver improved customer care and responsiveness.

In addition, the total cost of network ownership is reduced in several ways. Investments in existing network infrastructure are protected by ensuring that migration is a key consideration in the design of the converged network. Administration and

¹ For a current list of which forms of attack can be identified by Cisco IDS, refer to www.cisco.com

maintenance are simplified. Moves, adds and changes are much easier and quicker and centralised call processing means that remote offices can enjoy the same applications as the main office.

Fast provision: This complete solution helps voice and data connections with branch offices and other sites to be standardised, more simple and faster. The opportunity to write scripts in Cisco CallManager Express allows the simultaneous administration of a number of external contact points and facilitates installation.

Virtual Private Networks with Cisco Routers

The advantages of a VPN, compared to other connections are:

- Potentially lowering operating costs and better use of bandwidth
- Improved geographical coverage and availability
- Simpler connection of individual workstations, e.g. of teleworkers
- Secure data transfer with automatic encoding
- Easy scalability
- Simplified outsourcing via managed services of an internet service provider

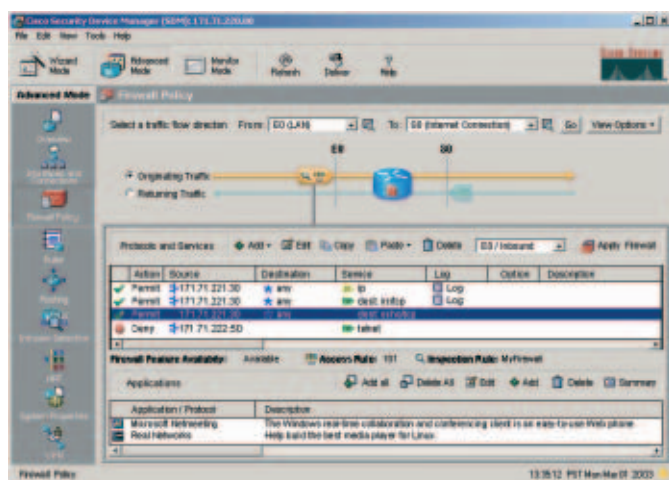
Cisco offers a range of options for putting together VPNs. For example, for mobile employees there is a purely software-based solution. For smaller installations, such as branch offices, there are VPN-ready routers equipped not only with dynamic routing but also with QoS and support for IP-multicast data traffic. For larger installations, special VPN equipment is employed, such as VPN Concentrators. New from Cisco are the VPN functions Easy VPN and Dynamic Multipoint VPN. With Easy VPN, Cisco Unity Client Protocols are used to help lower the configuration costs of VPN connections. Remotely-installed routers take their configuration from a central VPN 3000 Concentrator operating as an IPSec server. Dynamic Multipoint VPN (DMVPN) allows for the configuration of multiple VPN connections, without the central router having to record individual configuration data for connected routers.

The recently released version of the Cisco Router and Security Device Manager (SDM), Version 2.1, allows for convenient administration of routing and security services, includes intelligent assistants and enables you to run detailed error searches and correction. The new version supports additional Cisco devices and interface cards; furthermore it is available in six languages.

Download the latest Cisco SDM version for free at: www.cisco.com/cgi-bin/tablebuild.pl/sdm

Integrated administration of the Cisco Integrated Services Router

Cisco Security Device Manager (SDM) for graphical configuration – The SDM is available for all Cisco Access Routers from the 800 Series to the 3800 Series. Using a browser and particularly suited to small and medium-sized businesses, it offers a graphical tool for determining the security configuration of a router. SDM makes possible the configuration of LAN-/WAN, firewall and all VPN connections. In addition, SDM contains security audit functions with which router configuration can be checked and recommendations for the improvement of protection levels, based on the advice of the renowned ICSA Labs, can be provided. With SDM, small and medium-sized companies can use all the security functions of the Cisco Access Router easily with limited administrative effort and configure the router without the need for extensive support.



THE NEW CISCO 800 SERIES INTEGRATED SERVICES ROUTER

The new Cisco 850 and 870 Series Integrated Services Routers offer secure WAN access, plus the optional ability to connect wireless components, in a single device. Quick installation and the opportunity to configure and administer the router remotely make it an ideal router for small firms and field workers.

The Cisco 850 Series Integrated Services Router

The Cisco 850 Series is a family of routers with fixed configurations and DSL and cable connectivity for WAN and internet. They come with the necessary levels of performance to be able to simultaneously operate services such as firewalls, VPN encoding and wireless data transfer for up to five users. The Cisco Router and Security Device Manager (SDM) is supplied as part of the package, to aid configuration and making possible remote router administration by IT staff or the service provider (within its managed services offering). The Cisco 850 Series Integrated Services Router offers:



Cisco 851 Ethernet Router

- Secure internet connections with a Stateful Inspection Firewall
- IPSec VPN support for small offices
- One 4-port LAN switch
- Secure, wireless connection over WLAN 802.11b/g option
- Simple, quick installation and maintenance. Remote administration using the Cisco Security Device Manager

	Cisco 851	Cisco 857
WAN Interface	10/100 Mbps	ADSL/POTS
Optional Wireless 802.11b/g	Yes	Yes
ISDN S/T (ISDN BackUp)	No	No
Dial BackUp with External Modem	No	No
VPN Hardware Assist	Yes	Yes
4-Port Switch	Yes	Yes
802.1af Standard (Power over Ethernet)	No	No
Console Port	Yes	Yes

Cisco 871 Ethernet Router,
Cisco 877 DSL Router



The Cisco Integrated Services Router 870 Series

The Cisco 870 Series is a family of routers with fixed configurations and fast broadband access over DSL, cable or metro Ethernet for WAN and internet. They have the necessary power to help simultaneously deliver services such as firewalls, VPN encoding and wireless data transfer for up to twenty users. On top of this there are Quality of Service functions designed to help optimise speech and video applications. The Cisco Router and Security Device Manager (SDM) is supplied as part of the package, aiding configuration and making possible remote router administration by IT staff or the service provider (within its managed services offering). The Cisco 870 Series Integrated Services Router offers:

- Secure internet connections with a Stateful Inspection Firewall
- IPSec VPN support for small offices
- Intrusion Prevention System and anti-virus support via Network Admission Control (NAC)
- One 4-port LAN switch with optional Power over Ethernet (802.3af)
- Ipv6 support
- VLAN support (setting up of virtual LANs)
- Secure, wireless connection over WLAN 802.11b/g option
- Simple, quick installation and maintenance. Remote administration using the Cisco Security Device Manager

	Cisco 871	Cisco 877	Cisco 876	Cisco 878
WAN Interface	10/100 Mbps	ADSL/POTS	ADSL/ISDN	G.SHDSL-4W
Optional Wireless 802.11b/g	Yes	Yes	Yes	Yes
ISDN S/T (ISDN BackUp)	No	No	Yes	No
Dial BackUp with External Modem	Yes	Yes	No	Yes
VPN Hardware Assist	Yes	Yes	Yes	Yes
USB 2.0 Ports (Security Tokens)	2	No	No	No
4-Port Switch, 802.1q	Yes	Yes	Yes	Yes
DMZ Ports	Yes	Yes	Yes	Yes
802.1af Standard (Power over Ethernet)	Yes	Yes	Yes	Yes
AUX & Console Ports	Yes	Yes	Yes	Yes

THE NEW CISCO 1800 SERIES INTEGRATED SERVICES ROUTER

The Cisco 1800 family of Integrated Services Routers is designed for small and medium-sized companies and establishments. It is made up of a range of fixed configuration routers and the modular Cisco 1841 router. The Cisco 1800 range is the successor to the successful 1700 Series, offering greater performance, more services and more functionality, e.g. wireless laptop connection.



Cisco 1841 Router

The Cisco Integrated Services Router models 1801, 1802, 1803, 1811 and 1812

These routers are delivered with a fixed configuration and offer a high-speed broadband internet connection. Up to 50 users can communicate quickly, securely and wirelessly. Because the threat posed by hacker attacks, viruses and trojans grows every day, particular emphasis was placed on security when developing the new Integrated Services Routers. The integrated security services comprise

- An IPv6 Stateful Inspection Firewall
- IPSec VPN support using hardware-based encoding following 3DES and AES standards
- Dynamic Multipoint VPN (DMVPN)
- An Intrusion Prevention System (IPS) with more than 700 signatures
- Network Admission Control (NAC) for an improved level of anti-virus protection and the maintenance of security guidelines.

Feature	Cisco 1801	Cisco 1802	Cisco 1803	Cisco 1811	Cisco 1812
DSL WAN Interface	ADSL/POTS	ADSL/ISDN	G.SHDSL-4W	No	No
10/100 Mbps WAN Ports	1	1	1	2	2
8-Port Switch, 802.1g	Yes	Yes	Yes	Yes	Yes
ISDN BRI Dial Backup	Yes	Yes	Yes	No	Yes
V.92 Analog Modem Dial Backup	No	No	No	Yes	No
USB 2.0 Ports	0	0	0	2	2
802.11a/b/g Wireless Model	Yes	Yes	Yes	Yes	Yes
802.1af Standard (Power over Ethernet)	Yes	Yes	Yes	Yes	Yes
AUX & Console Ports	Yes	Yes	Yes	Yes	Yes

In addition, these fixed configuration routers offer:

- An integrated ISDN, analog modem or Ethernet connection as backup for the WAN connection and for better load distribution
- A manageable 10/100 switch with 8 ports and support for up to 8 VLANs
- The possibility to connect wireless devices over 802.11a and 802.11b/g
- The Cisco Security Device Manager (SDM) in version 2.1, for fast, simple configuration
- In addition to this, the Cisco 1811 and 1812 Routers come with a USB port for future security applications using Security Tokens



Cisco 1841 Router with antenna

The modular Cisco 1841 Router

The Cisco 1841 Integrated Services Router offers a host of additional functions thanks to its modular architecture. Two HWIC connection slots (high-speed WAN interface card) and an AIM slot (Advanced Integration Module), permitting the use of over 30 different modules and interface cards in order to upgrade the router to future requirements. Existing modules can also be upgraded, thus protecting your investment. These modules include:

- Analog modems
- ISDN connections
- ADSL connections
- High-speed DSL connections (G.SHDSL)
- Switch with 4 ports
- Plus modules able to “loop through” speech applications (the Cisco 1841 is not voice-capable)

In addition, the Cisco 1841 has two high-speed Ethernet LAN ports, serving to help significantly increase data capacity (in total up to 800 Mb/s) and help make it possible to segment the LAN.

A USB port is provided for future security applications with Security Tokens. Further features of the Cisco 1841 include:

- More than 800 VPN channels with an AIM module
- Cisco Easy VPN remote and server support, plus Dynamic Multipoint VPN (DMVPN)

THE NEW CISCO 2800 SERIES INTEGRATED SERVICES ROUTERS

Integrated security services, an increase in performance over the Cisco 2600 series, the option of connecting up to 96 IP telephones and a range of latest-generation slots for the installation of new modules and interface cards: These are just some of the top features of the Cisco 2800 Integrated Services Router range, designed for small and medium-sized companies.

Additional new slots



Cisco 2800 Series Router

The new architecture of the Cisco 2800 Series offers up to five times the performance levels of the Cisco 1700 and 2600 series models. On security and voice services, performance can be increased by up to a factor of 10. Numerous new slots able to accommodate high-performance modules and interface cards help to ensure flexible upgrading. These include (depending on router model) up to four high-speed WAN interface cards (HWICs), a slot for an Enhanced Network Module (NME), a slot for an Extension Voice Module (EVM) and two Advanced Integration Module (AIM) slots. This means you can choose from over 90 modules to determine which functions your router runs.

Cisco 2800 Series Router

Fast WAN connections are made possible by two fast Ethernet 10/100 ports (2801, 2811) or two Gigabit Ethernet 10/100/1000 ports (2821, 2851). In addition, up to 44 switch ports can be added with integrated power supply (PoE - Power over Ethernet).

Integrated security

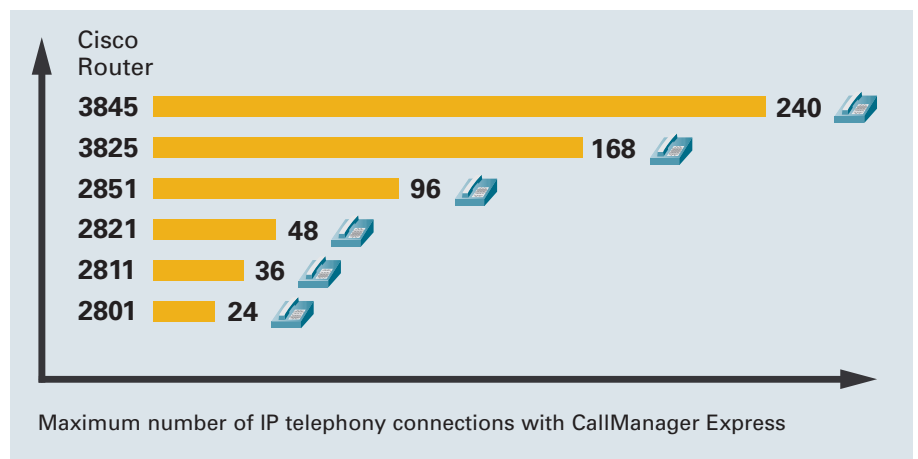
As with all other Integrated Services Routers, hardware-based encoding acceleration is integrated into the motherboard of the Cisco 2800 Series. In this way, the CPU is not burdened with having to perform encoding work and, compared to software-based solutions, an improved Isec data flow can be achieved. Depending on requirements, you can install additional security modules: VPN modules, to help increase the number and performance of tunnel connections, Content Engine Network Modules for the filtering of undesirable URLs, or Intrusion Prevention Network modules, for increased security.

From the large selection of Cisco IOS Software Security Feature Sets, you can also choose functions such as Stateful Inspection Firewall, Network Access Control (NAC), voice and video capable VPN (V3VPN) or implement Dynamic Multipoint VPN (DMVPN).

All this makes the Cisco 2800 router one of the most secure and robust routers available for small and medium-sized companies and establishments.

Telephoning over IP

With the Cisco 2800 Series, companies can deploy IP telephony solutions using digital and analog terminals: with the use of speech and fax modules, Voice-over-IP (VoIP) and Voice-over-Frame-Relay (VoFT) applications, a highly-available Cisco Survivable Remote Site Telephony (SRST) solution and even a distributed telephone switchboard solution using Cisco CallManager Express (CCME) can all be deployed. Scalability is guaranteed by way of up to 12 T1/E1 trunks, 52 Foreign Exchange Station (FXS) ports or 36 Foreign Exchange Office (FXO) ports, which also serve to handle ‘normal’ data traffic and other services.



Integration of further services

Through the use of a range of additional service modules, the Cisco 2800 series offers the opportunity to integrate into the router additional functions which would otherwise have to be carried out by standalone appliances. Many of these modules have their own processors and hard drives and can therefore operate independently of the router, while at the same time being configured and administered by the same management software. These include, for example, the Cisco Unity Express Voicemail module, the Cisco Intrusion Detection module and the Cisco Content Engine module.

THE NEW CISCO 3800 SERIES INTEGRATED SERVICES ROUTERS

The 3800 Series models are our most powerful Integrated Services Routers, combining routing services with comprehensive security services, convenient IP telephony, switchability and the capacity to set up to 2,000 VPN connections. This makes them the ideal product for large Enterprise branch offices or the central location of smaller organisations.

The open architecture of the modular Integrated Services Routers enables IT managers to integrate new services, functions and capabilities into the router, using a management tool for administration. This means that it is not necessary to install and maintain other standalone devices on the network from any other manufacturer, administration and maintenance complexity may potentially be reduced (especially when upgrades become necessary) and with it network operating costs. One further positive effect: you only need to call on one technological partner when it comes to routing, security, voice and VPN.



Cisco 3800 Series Router

Extended architecture

Not only does the new Cisco 3800 Series allow for integration of security services on the motherboard, it also aims to deliver significant performance improvement and storage capacity. The routers may offer sufficient bandwidth for the use of several Fast Ethernet interfaces from a single slot, Time Division Multiplex (TDM) connection and integrated power supply for 802.3af-configured terminals (PoE = Power over Internet). In addition, the Cisco 3845 has a range of features supporting high availability.

You can customise the 3800 Series Integrated Services Router to the specific needs of your company by way of over 90 WAN interface cards and network modules.

The hardware at a glance

The Cisco 3825 and the Cisco 3845 come with:

- Two built-in autosensing 10/100/1000 ports
- An SFP slot (small form-factor pluggable)
- Two built-in USB ports for future Security Token applications
- Four network module slots for normal or extended network modules
- Four single- or two double-sized HWICs
- Two Advanced Integration Modules (AIMs)



Cisco Wireless Access Point HWIC

- Four Packet Voice DSP Module (PVDM) slots for speech processing
- IP Security (IPSec) acceleration on the motherboard
- 802.3af-configured power supply for IP telephony or wireless access points



Cisco IP Telephone 7970G

Up to 240 telephone connections

With the Cisco 3800 Series, companies can deploy IP telephony solutions using digital and analogue terminals: with the use of speech and fax modules, Voice-over-IP (VoIP) and Voice-over-Frame-Relay (VoFT) applications, a highly-available Cisco Survivable Remote Site Telephony (SRST) solution and even a distributed telephone switchboard solution using Cisco CallManager Express (CCME) can all be deployed. Scalability is guaranteed by way of up to 24 T1/E1 trunks, 88 Foreign Exchange Station (FXS) ports or 56 Foreign Exchange Office (FXO) ports, which also serve to handle ‘normal’ data traffic and other services.

Integrated security

As with all Integrated Services Routers, the Cisco 3800 Series offers hardware-based encoding acceleration integrated into the motherboard, meaning that the CPU does not have to be burdened with encoding. Compared to software-based solutions, significantly higher IPSec data flows may be achieved. Depending on requirements, you can install additional security modules: VPN modules, to increase the number and performance of tunnel connections, Content Engine Network Modules for the filtering of undesirable URLs, or Intrusion Prevention Network modules, for increased security.

From the large selection of Cisco IOS Software Security Feature Sets, you can also choose functions such as Stateful Inspection Firewall, Network Access Control (NAC), voice and video capable VPN (V3VPN) or implement Dynamic Multipoint VPN (DMVPN).

This makes the Cisco 3800 router one of the most secure and robust routers for organisations and companies.

	Modular Slots			LAN Ports		WAN	
	WIC/HWIC*	NME*	AIM	10/100 Mbps	10/100/1000 Mbps	Data BRI	PRI
Cisco 800 Series							
Cisco 851 / 851-W				4/4			
Cisco 857 / 857-W				4/4			
Cisco 871 / 871-W				4/4			
Cisco 876 / 876-W				4/4		1/1	
Cisco 877 / 877-W				4/4			
Cisco 878 / 878-W				4/4		1/1	
Cisco 1800 Series							
Cisco 1801 / 1801-W				1/1		1/1	
Cisco 1802 / 1802-W				1/1		1/1	
Cisco 1803 / 1803-W				1/1		1/1	
Cisco 1811 / 1811-W				2/2			
Cisco 1812 / 1812-W				2/2		1/1	
Cisco 1841	2		1	2		2	4
Cisco 2800 Series							
Cisco 2801	4		2	2		2	4
Cisco 2811	4	1	2	2		12	8
Cisco 2821	4	1 + 1EVM*	2		2	12	8
Cisco 2851	4	1 + 1EVM*	2		2	12	8
Cisco 3800 Series							
Cisco 3825	4	2	2		2	20	16
Cisco 3845	4	4	2		2	36	24

*HWIC/*NME applicable for Cisco 1841, Cisco 2800, and Cisco 3800 Series only

	ADSL	SHDSL	Frame Relay	Ethernet	Firewall	VPN (IPSec)	Wireless LAN	IP phones max.
				1/1	X/X	X/X	-/802.11bg	
	1/1 POTS				X/X	X/X	-/802.11bg	
				1/1	X/X	X/X	-/802.11bg	
	1/1 ISDN				X/X	X/X	-/802.11bg	
	1/1 POTS				X/X	X/X	-/802.11bg	
		1/1			X/X	X/X	-/802.11bg	
	1/1 POTS			8/8	X/X	X/X		
	1/1 ISDN			8/8	X/X	X/X	-/802.11abg	
		1/1		8/8	X/X	X/X	-/802.11abg	
				8/8	X/X	X/X	-/802.11abg	
				8/8	X/X	X/X	-/802.11abg	
	2	2	4	8	X	x	802.11abg opt.	
	2	2	4	18	x	x	802.11abg opt.	24
	6	6	16	35	x	x	802.11abg opt.	36
	6	6	16	35	x	x	802.11abg opt.	48
	6	6	16	56	x	x	802.11abg opt.	96
	8	8	24	83	x	x	802.11abg opt.	168
	12	12	40	94	x	x	802.11abg opt.	240

Maximum capacity, check individual configuration with config tool under www.cisco.com/appcontent/apollo/configureHomeGuest.html



Corporate Headquarters

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

European Headquarters

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

Americas Headquarters

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

Asia Pacific Headquarters

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

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

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)