Router di accesso Cisco 1720 VPN

Accesso VPN flessibile e sicuro per medie e piccole aziende e uffici di filiale

Tendenze di mercato

Internet sta modificando radicalmente il modo di operare delle aziende e il futuro ci riserverà sicuramente ulteriori cambiamenti sulla scia di rapidi sviluppi nella tecnologia di networking.

Le aziende che sono già pronte per affrontare questo futuro hanno un vantaggio competitivo sulla concorrenza. E per essere pronte, devono scegliere i dispositivi di rete con lungimiranza, considerando in particolare la presenza di caratteristiche quali il supporto alle reti private virtuali (VPN, Virtual Private Network), la flessibilità e l'integrazione.

VPN: il nuovo mondo del networking

Tradizionalmente, le aziende collegano le proprie sedi distribuite geograficamente mediante un'infrastruttura di comunicazione privata creata con linee WAN dedicate. Si tratta di reti che offrono una larghezza di banda garantita con ritardi prevedibili che l'azienda, tuttavia, paga a caro prezzo, indipendentemente dal loro utilizzo. Un simile scenario porta a un'infrastruttura con costi elevati legati alla larghezza di banda specifica e alla distanza.

Le reti private virtuali (VPN) collegano le sedi distribuite geograficamente e gli utenti remoti mediante reti condivise o pubbliche (come Internet) e garantiscono al tempo stesso sicurezza, prioritizzazione del traffico, gestione e affidabilità, proprio come nel caso di una rete privata. L'impiego di reti condivise come Internet permette alle VPN di offrire costi WAN notevolmente inferiori e nuove funzionalità quali la comunicazione sicura con le reti extranet dei partner.

Tra i principali vantaggi offerti dalle soluzioni VPN vi sono:

- Costi ridotti. Gli analisti e i media sostengono che le VPN sono in grado di ridurre i costi WAN dal 30 all'80 percento (così, per esempio, Data Communications 9/98, Network World 8/31/98) con un recupero degli investimenti nelle apparecchiature in pochi mesi e un ritorno sugli investimenti (ROI, Return On Investment) del cento percento. Per la connettività site-to-site le VPN sfruttano il basso costo dell'accesso alle intranet tramite un'infrastruttura condivisa. Per l'accesso dell'utente remoto le VPN risparmiano i costi delle chiamate long-distance chiamando un numero locale e connettendosi attraverso un'infrastruttura condivisa. Inoltre, le aziende possono semplificare le operazioni WAN delegando le proprie VPN ad una società esterna (outsourcing) come un service provider.
- Comunicazione extranet. Le VPN garantiscono una comunicazione facile e sicura con partner e fornitori e il controllo dell'accesso a risorse di rete come i database.
- Connettività migliore. Internet offre una connessione globale a siti e utenti remoti in dial-up. L'estrema diffusione e disponibilità di Internet rende quindi più facile effettuare un collegamento locale a Internet da qualsiasi città o paese.
- Affidabilità migliore. Utilizzando Internet o una grande rete condivisa di un service provider si può contare su una ridondanza automatica grazie alla presenza diffusa di nodi di instradamento.

Flessibilità

Le esigenze di networking di un'azienda si modificano costantemente in base a diversi fattori quali l'aumentata domanda

della larghezza di banda, i cambiamenti tecnologici, la liberalizzazione delle telecomunicazioni. Quando un'azienda aggiunge utenti e scopre nuove possibilità di utilizzo della propria rete, le esigenze di larghezza di banda iniziano ad aumentare. Le LAN Ethernet devono garantire una facile migrazione alla tecnologia Fast Ethernet. Inoltre, la liberalizzazione nel settore delle telecomunicazioni porta a una riduzione dei costi delle tecnologie WAN esistenti quali le linee dedicate, Frame Relay, ISDN (Integrated Service Digital Network), SMDS (Switched Multimegabit Data Service) e ATM (Asynchronous Transfer Mode), e al rapido emergere di nuove tecnologie come DSL (Digital Subscriber Line). In questo mondo in continuo cambiamento, un'azienda deve proteggere i propri investimenti affidandosi a dispositivi di rete che si adattino alle novità.

Integrazione delle apparecchiature di rete

L'integrazione di funzioni multiple in un unico prodotto riduce i tempi e i costi di gestione e di implementazione. Tra i vari componenti integrati di rete vi sono i router di accesso, i firewall, la codifica ad alta velocità , i tunnel server VPN, le DSU/CSU (Data Service Unit/ Channel Service Unit) e le unità terminali di rete. L'integrazione riduce i costi di implementazione per il minor numero di apparecchiature e cavi da installare e configurare. La possibilità di effettuare la configurazione, il monitoraggio e il troubleshooting di ogni funzione integrata in modo remoto mediante il router di accesso semplifica inoltre il supporto continuo degli uffici remoti da un sito centralizzato.

Per soddisfare queste importanti esigenze di mercato, che vanno oltre l'accesso a intranet e Internet, Cisco Systems ha sviluppato il router di accesso Cisco 1720 VPN per le medie e piccole aziende e per i piccoli uffici di filiale.

Introduzione al router di accesso Cisco 1720 VPN

Il router Cisco 1720 offre i seguenti componenti chiave.

- Software Cisco IOS®
- Una porta autosensing 10/100 Fast Ethernet
- Due slot per schede d'interfaccia WAN (WIC, WAN Interface Card)
- Una porta ausiliaria (AUX) (seriale asincrona fino a 115,2 Kbps)
- Una porta per la console
- Processore RISC con codifica ad alte prestazioni
- Uno slot di espansione interno per il supporto di futuri servizi hardware assistiti come la codifica (fino a T1/E1) e la compressione
- Memoria DRAM di 16 MB (default) espandibile a 48 MB
- Memoria flash da 4 MB (default) espandibile a 16 MB
- Desktop form factor

Figura 1: il router Cisco 1720 offre accesso VPN con la potenza del software Cisco IOS, la flessibilità e l'integrazione delle apparecchiature di rete

Il router Cisco 1720 supporta tutte le combinazioni di una o due delle seguenti WIC.

- WIC-1T: una porta seriale (synch/async) ad alta velocità
- WIC-2T: due porte seriali (synch/async) ad alta velocità
- WIC-2A/S: due porte seriali (synch/async) a bassa velocità fino a 128 Kbps
- WIC-1B-S/T: una porta ISDN BRI (Basic Interface Rate) S/T
- WIC-1B-U: una porta ISDN BRI U
- WIC-1DSU-56K4: una porta integrata per DSU/CSU 4-wire 56/64 Kbps
- WIC-1DSU-T1: una porta integrata per DSU/CSU T1/ Fractional T1

Le schede d'interfaccia WAN possono essere condivise con i router Cisco 1600, 2600 e 3600.

Il router Cisco 1720 si basa sul successo della serie Cisco 1600, cui aggiunge maggiori funzionalità e flessibilità per applicazioni di livello superiore. Oltre a soddisfare le esigenze dell'accesso Internet e intranet, il router Cisco 1720 offre i seguenti vantaggi strategici.

- Networking privato virtuale basato sul software Cisco IOS
- Flessibilità grazie all'architettura modulare
- Integrazione dei dispositivi di rete

Accesso al networking privato virtuale

Le VPN possono aiutare le aziende a cogliere i frutti della drastica riduzione dei costi WAN, di una migliore connettività globale e di un'affidabilità migliore offrendo, ad esempio, comunicazioni extranet sicure. L'accesso remoto, l'accesso a Internet, intranet ed extranet, possono essere infatti riuniti in un unico collegamento WAN verso Internet.

La potenza del software Cisco IOS per VPN. Cisco IOS, il software di networking per Internet e WAN private, diventato ormai uno standard, offre il set di funzionalità VPN più competo

per quanto riguarda la sicurezza, la QoS (Quality of Service), la gestione e l'affidabilità/scalabilità. Il router Cisco 1720 con supporto Cisco IOS completo e hardware modulare integrato è stato progettato per le VPN di oggi e del futuro. Esso definisce una nuova classe di router di accesso VPN che permette un'implementazione su vasta scala di VPN, pratica e conveniente. Prendiamo ora in considerazione le esigenze delle VPN.

Per una VPN la sicurezza è cruciale perché i dati aziendali attraversano una WAN condivisa e la rete interna di ogni ufficio è esposta a questa WAN. Il software Cisco IOS del router Cisco 1720 integra le seguenti funzionalità avanzate di sicurezza.

- *Firewall.* L'opzione Cisco IOS Firewall protegge le LAN dagli attacchi. Il controllo CBAC (Context-Based Access Control) offre un filtraggio dinamico o completo per ogni applicazione e permette al traffico autorizzato di entrare nella LAN solo mentre è attiva una sessione. Perché un firewall sia considerato efficace è necessario che integri la funzionalità CBAC. Cisco IOS Firewall supporta anche altre funzionalità chiave quali il blocco degli applet Java, l'individuazione e la prevenzione del Denial-of-Service, l'audit trail e gli allarme in tempo reale.
- *Codifica.* La codifica opzionale IPSec DES (IP Security Data Encryption Standard) e Triple DES con chiavi fino a 168 bit rappresentano il sistema più affidabile, basato sugli standard, per garantire riservatezza, integrità e autenticità della sorgente dei dati mentre attraversano la WAN condivisa.
- *Tunneling.* Cisco IOS supporta numerosi standard opzionali di tunneling quali IPSec, GRE (Generic Routing Encapsulation), L2F (Layer 2 Forwarding) e L2TP (Layer 2 Tunneling Protocol). Il supporto di L2F ed L2TP permette all'utenza mobile di chiamare i POP (Point-Of-Presence) di un provider, re-indirizzare il traffico verso il router Cisco 1720 e accedere alle risorse, come i database, situate sulla LAN del router. I router utilizzati in questo modo vengono generalmente denominati home gateway o tunnel server. Un setup di questo tipo evita la presenza di un RAS (Remote Access Server) separato nella piccola e media azienda, risparmiando sulle chiamate long-distance. Il protocollo L2TP può essere utilizzato anche per il tunneling del traffico non IP per il collegamento di uffici o utenti remoti (il tunneling IPSec supporta solo il traffico IP).
- *Autenticazione e gestione delle chiavi di accesso.* Il supporto di IKE (Internet Key Exchange), del certificato digitale X.509v3 e di CEP (Certificate Enrollment Protocol), con autorità di certificazione quali Verisign ed Entrust, garantisce l'autenticità dell'apparecchiatura e dei dati e permette di passare gradatamente a grandissime reti IPSec mediante la gestione automatica delle chiavi di accesso.
- *Software client VPN.* Con il software Cisco IOS possono interagire tutti i client standard IPSec ed L2TP.
- *Autenticazione dell'utente.* L'autenticazione dell'utente supporta i protocolli PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol), TACACS+, il servizio RADIUS (Remote Access Dial-In User Service) e l'autenticazione token.

Qualità del Servizio (gestione del traffico). Perché una VPN possa offrire il massimo livello di disponibilità e prevedibilità, è necessario disporre di comandi QoS (Quality of Service), soprattutto per quelle applicazioni e quegli utenti che accedono a un'elevata larghezza di banda. Le applicazioni time-sensitive o mission critical (per esempio, le applicazioni Enterprise Resource Planning come PeopleSoft) dovrebbero avere la priorità sul traffico meno critico (per esempio, applicazioni push come Pointcast). Il router Cisco 1720 supporta le principali funzionalità QoS sottoindicate.

- CAR (Committed Access Rate) esegue tre importanti funzioni a livello di applicazione e utente singolo. 1) Classifica il tipo di traffico (per esempio, se si tratta di PeopleSoft o di Pointcast). 2) Fissa la larghezza di banda massima consentita al traffico (denominata anche "policy di traffico" o "shaping della velocità"; per esempio, PeopleSoft riceve 1.0 Mbps e Pointcast 28 Kbps). 3) Prioritizza il traffico assegnando un "numero di precedenza IP" ad ogni tipo di traffico.
- Il routing delle policy permette di classificare e prioritizzare il traffico attraverso la "precedenza IP" e di indirizzare i vari tipi di traffico verso un'interfaccia specifica del router. Non è tuttavia in grado di fissare la larghezza di banda consentita come CAR.
- WFQ (Weighted Fair Queueing) offre tempi di risposta coerenti. Esso pianifica il traffico con larghezza di banda bassa all'inizio della coda per ridurre i tempi di risposta e condivide in modo equo la larghezza di banda rimasta tra le applicazioni ad ampio uso di banda.
- GTS (Generic Traffic Shaping) evita la congestione controllando e regolarizzando il traffico WAN out-bound verso una larghezza di banda specifica. Una funzione utile quando il router ricevente all'altra estremità della WAN non è in grado di gestire la larghezza di banda in entrata.
- RSVP (Resource Reservation Protocol) permette di riservare la larghezza di banda ad un'applicazione specifica sull'intera WAN, da un'estremità all'altra.

Gestione e facilità di installazione

Il router Cisco 1720 supporta una gamma di tool per la gestione e la semplificazione dell'installazione in rete. Cisco ConfigMaker è un tool Windows su base Wizard progettato per configurare una piccola rete di router, switch, hub e altre apparecchiature di rete Cisco Systems da un unico PC. Studiato per installatori e amministratori di rete di medie e piccole aziende, esso guida l'utente attraverso il design di rete e il processo di installazione dei nuovi dispositivi, rendendo ogni compito facile come tracciare un diagramma di rete. Cisco ConfigMaker semplifica l'implementazione VPN con il supporto della configurazione delle policy, IPSec, NAT (Network Address Translation), DHCP (Dynamic Host Configuration Protocol) Server e IPSec.

CiscoView, un'applicazione software con interfaccia grafica per la gestione dei dispositivi per piattaforme UNIX controlla i dispositivi e fornisce statistiche e informazioni complete sulla configurazione. Cisco 1720 supporta anche CiscoWorks2000, la suite web-based di amministrazione di rete. La sua interfaccia browser semplifica task quali la gestione dell'inventario di rete e dei cambiamenti dei dispositivi, la modifica della configurazione, la rapida implementazione di nuove immagini software, il troubleshooting. Per i service provider CSM (Cisco Service Management) offre una suite completa di soluzioni di gestione del service che permettono di pianificare rapidamente, controllare e fatturare le prestazioni delle VPN.

Affidabilità e scalabilità. Il software Cisco IOS è il noto software di networking più diffuso, ormai uno standard nel mondo delle reti. Le tecnologie Cisco IOS permettono di ampliare una VPN fino a dimensioni molto ampie, in modo affidabile, mediante il supporto di IKE (Internet Key Exchange), certificati digitali con le più importanti autorità di certificazione, protocolli di routing scalabili quali OSPF (Open Shortest Path First) ed Enhanced IGRP (Interior Gateway Routing Protocol) e servizi quali HSRP (Hot Standby Router Protocol).

Possibilità di codifica. Grazie al potente processore RISC di cui dispone, il router Cisco 1720 per il momento supporta la codifica su base software IPSec a 512 Kbps con pacchetti da 256 byte (dimensioni standard dei pacchetti della maggior parte delle reti). (Le prestazioni possono variare in base all'algoritmo di codifica utilizzato, alle dimensioni dei pacchetti della rete, etc.) Un slot di espansione sulla scheda madre del router Cisco 1720 permetterà invece di supportare in futuro anche i servizi su base hardware quali la codifica (fino a T1/E1) e la compressione.

Flessibilità

Per proteggere gli investimenti da esigenze di networking in continuo mutamento, le aziende devono disporre di un prodotto che sia in grado di adattarsi alle novità. Il router Cisco 1720 rappresenta la soluzione più flessibile per le medie e piccole aziende e per i piccoli uffici di filiale.

Schede di interfaccia WAN modulari. Tutte le interfacce WAN su Cisco 1720 sono intercambiabili sui due slot WAN. I clienti possono quindi combinare le schede d'interfaccia WAN che preferiscono, potenziando o modificando le tecnologie WAN in base alle proprie esigenze. Le numerose opzioni WAN disponibili comprendono due ISDN BRI duali, fino a cinque porte per l'aggregazione seriale e DSU/CSU integrate con velocità fino a T1.

Schede d'interfaccia WAN condivise con router Cisco 1600, 2600 e 3600. Le schede d'interfaccia WAN possono essere utilizzate anche su altri modelli e ciò protegge gli investimenti effettuati e facilita le modifiche di configurazione. Quando una scheda non serve più su una piattaforma, la si può riutilizzare su un'altra. Inoltre, i clienti, i rivenditori e i service provider possono ridurre il numero di unità da tenere a magazzino.

Autosensing 10/100 Fast Ethernet. Cisco 1720 dispone di una porta autosensing 10/100 Fast Ethernet che permette di migrare con facilità verso le reti Fast Ethernet. Dopo aver collegato il cavo LAN la porta individua automaticamente il tipo di velocità LAN (10 o 100 Mbps) e negozia la modalità simplex o duplex. Per gli uffici con hub 100BaseTX, la porta autosensing 10/100 di Cisco 1720 elimina la necessità di un bridge 10/100.

Nuovi livelli prestazionali dalle tecnologie emergenti a banda larga. Il processore RISC di Cisco 1720 permette infine al router di supportare le tecnologie a banda larga emergenti come DSL (Digital Subscriber Line). In futuro, le schede d'interfaccia WAN Cisco Systems includeranno anche la tecnologia DSL.

Integrazione dei dispositivi di rete

Con l'integrazione di funzioni multiple in un'unica apparecchiatura si riducono i tempi e i costi di implementazione e gestione. Il router Cisco 1720 offre i vantaggi dell'integrazione all-in-one in due modi.

Apparecchiature integrate in un unico alloggiamento. Cisco 1720 è in grado di combinare funzioni multiple agendo da router, firewall, codificatore, tunnel server VPN (home gateway),

DSU/CSU ed NT1 (Network Termination 1). Tra i vantaggi offerti vi sono:

- supporto semplificato e costi ridotti grazie alla possibilità di effettuare dal router, in modo remoto, la configurazione, il monitoraggio e il troubleshooting di ogni funzione integrata;
- configurazione VPN semplificata: il software Cisco IOS supporta il tunneling VPN di tipo L2TP e funzionalità di sicurezza quali la codifica IPSec e l'autenticazione dell'utente;
- installazione e configurazione di un numero inferiore di apparecchiature e cavi;
- maggiore affidabilità (minori componenti come gli alimentatori);
- risparmio di spazio.

Soluzione integrata LAN/WAN Cisco Network Office Stack. Le medie e piccole aziende, che generalmente dispongono di poche o nessuna risorsa per amministrare la rete, possono beneficiare dell'implementazione di soluzioni integrate con componenti LAN e WAN, che operano insieme in modo semplice e trasparente. Inoltre, adottando soluzioni Cisco per vari aspetti della rete, in caso di richiesta di assistenza, basta interpellare un unico interlocutore. Il router Cisco 1720 fa parte dello stack CNO (Cisco Networked Office), la soluzione LAN/WAN integrata di Cisco Systems. Tra gli altri componenti CNO vi sono i router della serie Cisco 1600, Cisco Secure Integrated Software (in precedenza denominato Cisco IOS Firewall Feature Set), l'hub 10/100 Cisco 1528, lo switch 10/100 Cisco 1548 e il tool di configurazione della rete Cisco ConfigMaker.

Figura 2: il router Cisco 1720 VPN fa parte dello stack Cisco Networked Office che comprende hub e switch autosensing 10/100.

Principali caratteristiche e vantaggi

Cisco 1720 offre il supporto VPN, caratteristiche di flessibilità e integrazione di rete come evidenziato nella tabella sottostante.

Tabella 1: caratteristiche fondamentali della serie Cisco 1720

Caratteristiche	Funzioni/Vantaggi
Supporto VPN	
Supporto completo Cisco IOS Con routing multiprotocollo (IP, IPX, AppleTalk, IBM/SNA) e bridging	• Software di networking, standard de facto nel settore, per Internet e WAN private • Il più ampio ed affidabile supporto software a numerosissime funzionalità di rete • Parte integrante della strategia di rete end-to-end Cisco Systems
Firewall Cisco Secure Integrated Software con CBAC per il filtraggio firewall dinamico, individuazione e prevenzione del Denial-of-Service, blocco degli applet Java, allarmi in tempo reale	• Accesso a Internet sicuro per gli utenti interni, controllo degli accessi dinamico per singola applicazione con prevenzione dell'accesso alla LAN interna di utenti Internet non autorizzati
Codifica IPSec ESP DES e Triple DES. Slot di espansione per una futura codifica hardware assistita ad alta velocità	• Creazione di VPN grazie a livelli standard di riservatezza, integrità e autenticità dei dati mentre attraversano le reti pubbliche • Possibilità di potenziamento con codifica hardware assistita ad alta velocità fino a T1/E (non appena disponibile)
Processore RISC **Autenticazione dell'apparecchiatura e gestione delle chiavi di codifica** IKE, certificato digitale X.509v3, CEP con le principali autorità di certificazione (CA, Certification Authorities) quali Verisign e Entrust	Codifica software assistita con velocità di 512 Kbps per le VPN • Identificazione/autenticazione delle apparecchiature e dei dati • Scalabilità verso grandissime reti IPSec mediante la gestione automatica delle chiavi di codifica
Autenticazione dell'utente PAP/CHAP, RADIUS, TACACS+, Token	Certezza sull'identità del cliente
Tunneling IPSec, GRE, L2F, L2TP	• Numerosi metodi di tunneling basati sugli standard per la creazione di VPN per traffico IP e non IP • Interoperabilità con le tecnologie di tunneling Cisco Systems da parte di tutti i client IPSec o L2TP basati sugli standard
Gestione Tramite SNMP (CiscoView, CiscoWorks2000), Telnet e la porta della console	Integrate nel router Cisco 1720 con riduzione dei tempi e dei costi gestionali
Facilità d'uso e di installazione Cisco ConfigMaker, utility di configurazione SETUP, AutoInstall, porte/cavi colorati, LED di stato NAT e Easy IP	• Semplificazione e riduzione dei tempi e dei costi di implementazione con configuratore grafico delle policy LAN/WAN, domande di configurazione interattive di tipo command line, cablaggio diretto • LED per una diagnosi e un troubleshooting rapidi • Implementazione semplificata e riduzione dei costi di accesso a Internet
Quality of Service CAR, routing delle policy, WFQ, GTS, R SVP	Allocazione della larghezza di banda WAN per le applicazioni prioritarie con prestazioni di rete migliori
Affidabilità e scalabilità Software Cisco IOS, routing dial-on-demand, memoria flash a banco doppio, protocolli di routing scalabili (p. es. OSPF e Enhanced IGRP), HSRP	• Maggiore affidabilità della rete e scalabilità verso reti più grandi

Caratteristiche	Funzioni/Vantaggi
Flessibilità	
Architettura modulare (slot per schede WAN)	• Scelta flessibile delle schede WAN sul router Cisco 1720 ad ulteriore protezione degli investimenti
Schede d'interfaccia WAN condivise con i router Cisco 1600, 2600 e 3600	• Costi di manutenzione e di magazzino ridotti • Minori costi di training per il personale di supporto • Protezione degli investimenti con il riutilizzo delle stesse schede su piattaforme diverse
Autosensing 10/100 Fast Ethernet	• Possibilità di migrazione immediata a Fast Ethernet
Slot di espansione sulla scheda madre	• Espandibilità per il supporto di servizi futuri come la codifica hardware assistita e la compressione
Integrazione delle apparecchiature di rete	
Router, firewall, codifica, tunnel server VPN, DSU/CSU e NT1 integrati in un'unica apparecchiatura	• Riduzione dei costi di implementazione e semplificazione della gestione rispetto alle soluzioni basate su apparecchiature multiple separate
Parte integrante dello stack Cisco Networked Office	• Soluzioni complete e compatibili per le reti dei piccoli uffici

Set di funzioni software

I set di funzioni di Cisco 1720 sono analoghi a quelli della serie Cisco 1600 con Cisco IOS V. 12.0. I set disponibili sono tredici: quattro versioni Base e nove Plus. A partire della versione 12.0, i set Base comprendono alcune funzioni che prima appartenevano ai set Plus, in particolare NAT, OSPF, RADIUS (Remote Access Dial-In Service) e NHRP (Next Hop Resolution Protocol). I set Plus comprendono tutte le funzioni dei set Base più altre come L2TP, L2F, BGP (Border Gateway Protocol), IP Multicast, SVC (Switched Virtual Circuit) Frame Relay, RSVP, NLSP (NetWare Link Services Protocol), SMRP (Simple Multicast Routing Protocol) AppleTalk, NTP (Network Timing Protocol).

Le tabelle 2 e 3 riassumono i set di funzioni di Cisco 1720.

Tabella 2: set di funzioni base

Categoria	Protocolli base /caratteristiche	IP	IP/PX	IP Firewall	IP/IPX/AT/IBM
LAN	Bridging trasparente	x	x	x	x
	IP	x	x	x	x
	IPX, liste di accesso NetBIOS, caching dei nomi		x		x
	AppleTalk fasi 1 e 2				x
WAN	Linee dedicate, Frame Relay, Switched 56, SMDS, HDLC	x	x	x	x
	Linea dedicata ISDN (IDSL) a 64 e 128 Kbps	x	x	x	x
	ISDN caller DI callback	x	x	x	x
	PPP, compressione PPP	x	x	x	x
	Async, SLIP	x	x	x	x
	X.25, X.25 PAD, X.25 su canale ISDN D	x	x	x	x
	LLC2, LAPB	x	x	x	x
Routing IP	RIP, RIP2, IGRP, Enhanced IGRP, OSPF, NHRP	x	x	x	x
	Routing delle policy IP	x	x	x	x
	Tunneling GRE	x	x	x	x
Altri routing	IPX-RIP		x		x
	(AppleTalk) RTMP				x
Sicurezza	PAP/CHAP, password locale	x	x	x	x
	Liste di accesso estese, Lock and Key	x	x	x	x
	RADIUS, TACACS+, Token	x	x	x	x
Quality of Service	WFQ (Weighted Fair Queueing)	x	x	x	x
Ottimizzazione WAN	Larghezza di banda on-demand, dial-on-demand	x	x	x	x
	Spoofing IPX ed SPX		x		x
	Snapshot routing	x	x	x	x
	Frame Relay FRF.9	x	x	x	x
Facilità d'uso	ConfigMaker	x	x	x	x
e di implementazione	Easy IP (PAT, IPCP, server DHCP)	x	x	x	x
	NAT (Network Address Translation)	x	x	x	x
	AutoInstall per linee dedicate e Frame Relay	x	x	x	x
Gestione	SNMP, Telnet, porta della console	x	x	x	x
	CiscoView, CiscoWorks2000	x	x	x	x
	SNTP (Simple Network Timing Protocol)	x	x	x	x

Nota: il routing e il bridging AppleTalk non vengono supportati per le interfacce asincrone.

Tabella 3: set di funzioni Plus – Funzioni aggiuntive

Categoria	Protocolli/caratteristiche aggiuntive	IP Plus	IP Plus 40	IP Plus IPSec c56	IP Plus IPSec 3 DES	IP FW Plus IPSec 56	IP FW Plus IPSec 3DES	IP/IPX FW Plus	IP/IPX/ AT/IBM FW Plus IPSec 56	IP/IPX/ AT/IBM FW Plus IPSec 3DES
WAN	Frame Relay SVC	x	x	x	x	x	x	x	x	x
Routing IP	BGP	x	x	x	x	x	x	x	x	x
Altri routing	NLSP (NetWare Link Services Protocol)							x	x	x
	AppleTalk AURP, ATIP								x	x
VPN/Sicurezza	IPSec DES			x	x	x	x		x	x
	IPSec Triple DES				x		x			x
	Tecnologia di codifica Cisco Systems a 40 bit		x	x	x	x	x		x	x
	Tecnologia di codifica Cisco Systems a 56 bit			x	x	x	x		x	x
VPN/Tunnel	L2TP, L2F	x	x	x	x	x	x	x	x	x
Quality of Service	RSVP (Resource Reservation Protocol)	x	x	x	x	x	x	x	x	x
	RED (Random Early Detection)	x	x	x	x	x	x	x	x	x
	CEF (Cisco Express Forwarding) *	x	x	x	x	x	x	x	x	x
	CAR (Committed Access Rate) *	x	x	x	x	x	x	x	x	x
	NetFlow *	x	x	x	x	x	x	x	x	x
	RTP-HC (RTP Header Compression)	x	x	x	x	x	x	x	x	x
Multimedia	IP Multicast (PIM, Protocol Independent Multicast)	x	x	x	x	x	x	x	x	x
	AppleTalk SMRP (Multicast)								x	x
Gestione	NTP (Network Timing Protocol)	x	x	x	x	x	x	x	x	x

Nota: FW indica Cisco IOS Firewall (ora Cisco Secure Integrated Software). La codifica viene offerta in set di codifica speciali (Plus 40, Plus IPSec 56, Plus IPSec 3DES). *CAR, CEF e NetFlow supportati da Cisco IOS V. 12.0(3)T e superiori. Per creare una VPN IP si consigliano le immagini software IP Firewall Plus IPSec 56 o IP Firewall Plus IPSec 3DES.

Applicazioni

Il router Cisco 1720 estende le potenzialità della serie Cisco 1600 alla medie e piccole aziende e ai piccoli uffici di filiale. Oltre alle soluzioni di accesso Internet /intranet, sicure e flessibili, offerte dai router Cisco 1600, Cisco 1720 è ideale anche per le applicazioni di seguito descritte.

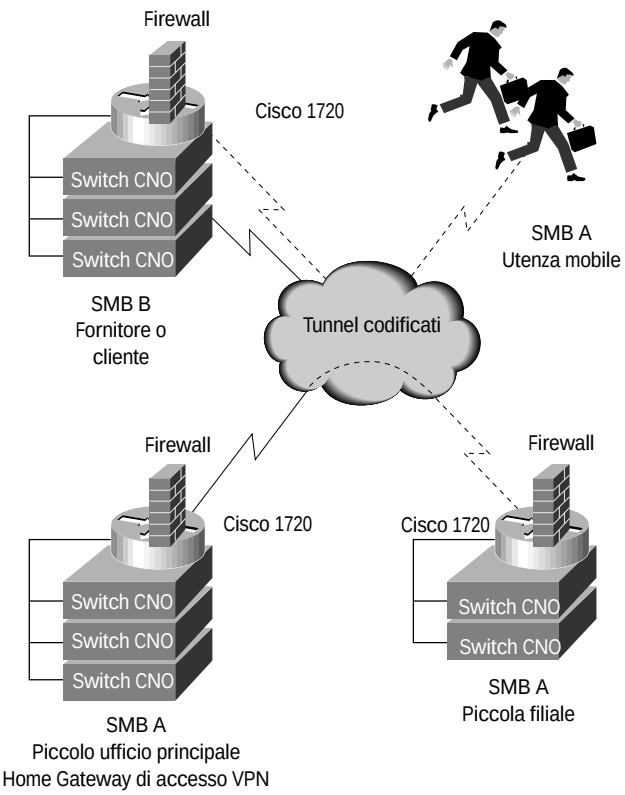
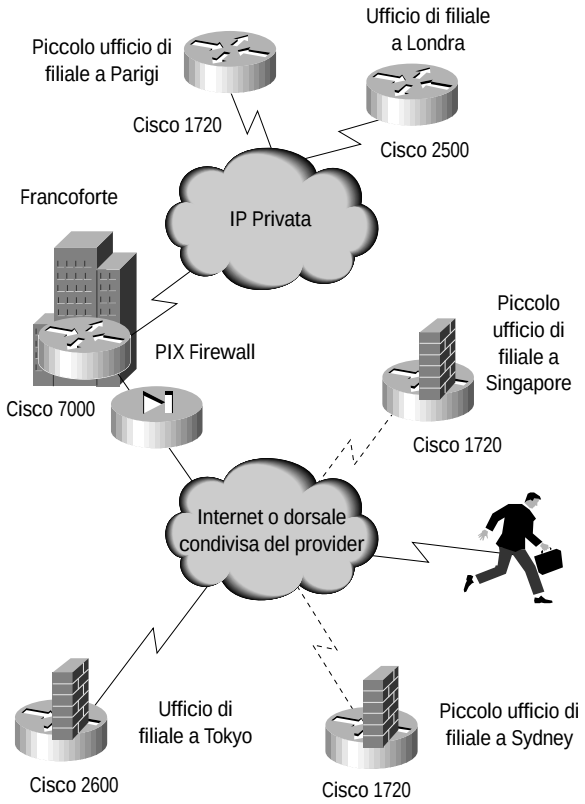


Figura 4: VPN Access /Intranet/ Extranet per le medie e piccole aziende (SMB)

La figura 4 illustra le applicazioni VPN per due medie e piccole aziende (SMB A ed SMB B). SMB A ha un ufficio principale e un ufficio di filiale collegati attraverso un tunnel VPN sicuro. SMB B è un client o fornitore strategico con un collegamento sicuro extranet verso la SMB A. Le applicazioni VPN considerate comprendono quanto segue.

- *Intranet VPN (connettività branch-to-branch).* Invece di una linea dedicata privata, long-distance, tra l'ufficio principale e quello di filiale della SMB A, ogni ufficio si abbona a una linea di accesso Internet locale e un tunnel IPSec codificato trasporta il traffico long-distance via Internet. La codifica IPSec DES o Triple DES garantisce la riservatezza, l'autenticità e l'integrità dei dati mentre Cisco Secure Integrated Software, integrato nel router Cisco 1720, evita accessi indesiderati o attacchi non autorizzati alle LAN di ogni ufficio. Il traffico viene prioritizzato mediante funzionalità QoS, come il routing delle policy o una velocità di accesso prefissata, per garantire che le applicazioni mission critical ricevano la larghezza di banda maggiore. Cisco ConfigMaker semplifica la configurazione della VPN per la rete della media e piccola azienda con un tool basato su interfaccia utente grafica (GUI), che configura i parametri base del router, Cisco Secure Integrated Software e le policy di codifica IPSec. La configurazione IPSec viene semplificata al minimo grazie all'impiego di valori di default standard, stabiliti con Cisco ConfigMaker (modalità di tunneling, ESP-HMAC-MD5, una diffusa variante di IPSec, chiave precondivisa per la policy IKE). I tunnel VPN sicuri possono essere definiti rapidamente specificando il tipo di algoritmo di codifica (DES o Triple DES), la password per la chiave condivisa, gli indirizzi IP dei router di destinazione.
- *VPN di accesso (accesso remoto per l'utente mobile).* Gli utenti mobili o i dipendenti in telelavoro A possono chiamare un POP locale Internet ed effettuare il tunneling del traffico long-distance verso la LAN dell'azienda tramite Internet o la dorsale condivisa di un service provider. La soluzione elimina le onerose tariffe long-distance con un conseguente risparmio sui costi. I tunnel delle VPN di accesso possono essere attivati dal client o dal server di accesso alla rete (NAS, Network Access Server). Per il tunneling attivato dal client, un client standard IPSec o L2TP sul PC dell'utente mobile attiva un tunnel tra il PC e il router Cisco 1720. Il router funge da home gateway (denominato anche VPN tunnel server o L2TP network server) e chiude il tunnel. Per il tunneling attivato da NAS, quando un utente chiama un NAS sul POP locale, il service provider autentica l'utente verso l'azienda e attiva il tunnel L2TP dal NAS verso l'home gateway Cisco 1720. L'utente viene quindi autenticato su un security server, il tunnel chiuso e l'utente può accedere alle risorse sulla LAN, in base alle policy stabilite.
- *Extranet VPN (connettività con partner dell'azienda).* La connettività tra la piccola o media azienda A e quella B riduce la durata dei processi di business (per esempio, per la fatturazione, l'evasione degli ordini, la progettazione in collaborazione) e rafforza le relazioni commerciali, poiché permette a clienti, fornitori o partner strategici di accedere a determinate risorse sulle rispettive reti. La tecnologia di creazione delle extranet VPN è analoga a quella utilizzata per le intranet VPN. Si configura Cisco Secure Integrated Software, integrato nel router Cisco 1720 di ogni sito, con policy firewall personalizzate che permettono l'accesso alle risorse per singola applicazione e interfaccia.
- *Soluzione stackable LAN/WAN integrata.* In ogni sito, il router Cisco 1720, combinato a hub e switch Fast Ethernet 10/100 della serie Cisco 1500, offre una soluzione LAN/WAN completa e integrata da un unico fornitore. Cisco ConfigMaker costituisce il tool comune di configurazione della rete che guida, passo dopo passo, attraverso il design, l'indirizzamento e la configurazione delle reti LAN e WAN.

Figura 5: rete privata virtuale/privata ibrida



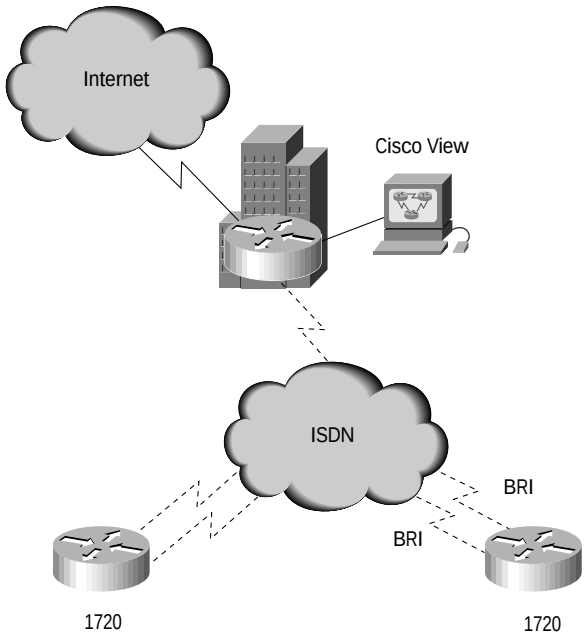
La figura 5 illustra un'organizzazione multinazionale con sede a Francoforte. La WAN dell'azienda fu inizialmente stabilita in Europa, con linee private dedicate che collegavano la sede principale agli uffici di filiale. Ora l'azienda migra alcuni suoi siti verso una VPN, iniziando con quelli di Tokyo, Singapore e Sydney, per risparmiare sui costi WAN internazionali e per diminuire la complessità delle linee richieste a compagnie telefoniche straniere. L'azienda potrebbe anche decidere di affidare all'esterno l'implementazione dell'intera VPN a un service provider globale e inviare così il traffico sulla dorsale IP condivisa del provider o effettuare al proprio interno l'implementazione, abbonandosi a una linea di accesso locale Internet per ogni sito e configurando tunnel IPSec su Internet.

Il software Cisco IOS offre una soluzione end-to-end su questo ibrido di reti private virtuali e private. I piccoli uffici di filiale a Singapore e Sydney possono usare un router Cisco 1720 ciascuno con Cisco Secure Integrated Software integrato. L'ufficio di filiale più grande a Tokyo può utilizzare invece un router Cisco 2600. Tutti i router collegati alla VPN dispongono di tunnel IPSec codificati, l'uno verso l'altro.

Anche l'accesso remoto per gli utenti mobili viene migrato su una VPN. Un dipendente che viaggia in tutto il mondo può chiamare un POP locale e stabilire così un tunnel IPSec dal proprio PC verso il Cisco PIX Firewall nella sede di Francoforte. In tal modo si evitano i costi delle chiamate long-distance, poiché il traffico viene trasportato attraverso Internet o la dorsale condivisa del provider. PIX Firewall è la soluzione ideale per i siti enterprise più grandi che richiedono la codifica su larghezza di banda alta, un livello di sicurezza avanzato e funzionalità fail-over.

Dopo aver acquisito esperienza con le VPN, l'azienda può migrare in tutta tranquillità un numero superiore di siti dalla propria WAN privata alla VPN.

Figura 6: accesso al piccolo ufficio di filiale



La figura 6 illustra come il router Cisco 1720 rappresenti la soluzione ideale per fornire l'accesso Internet o intranet ai piccoli uffici di filiale di un'azienda, con il maggior livello di flessibilità e protezione degli investimenti di ogni altro router della sua classe. L'autosensing 10/100 Fast Ethernet garantisce la flessibilità necessaria per una facile migrazione verso le LAN Fast Ethernet. I due slot per schede d'interfaccia WAN garantiscono la massima flessibilità permettendo di scegliere i servizi WAN d'interesse immediato e di cambiarli in futuro in base a nuove esigenze. Il processore RISC e lo slot di espansione per i servizi futuri hardware assistiti, quali la codifica o la compressione, offrono invece la flessibilità di pianificare le VPN per il futuro.

Il router Cisco 1720 con due schede d'interfaccia WAN di tipo ISDN BRI è ideale per gli uffici di filiale in cui il servizio

ISDN non è costoso. Con Multilink PPP i quattro canali B possono essere "legati" per supportare fino a 256 Kbps oppure una BRI può fungere da WAN primaria e le altre da backup. La seconda BRI può essere configurata per un uso on-demand, quando si registra un picco d'uso nella larghezza di banda. Cisco 1720 supporta numerose funzionalità di ottimizzazione dell'uso della larghezza di banda quali dial-on-demand, larghezza di banda on-demand, snapshot routing, routing di circuito on-demand OSPF, compressione di payload, link e header, filtraggio, spoofing.

Con una gestione delle applicazioni tramite CiscoView e CiscoWorks2000 gli amministratori dei siti centralizzati possono gestire localmente il router Cisco Systems del sito centralizzato e i router Cisco 1720 di quelli remoti, riducendo così i tempi e i costi di amministrazione, implementazione e installazione.

Posizionamento del prodotto

Il router Cisco 1720 è un'estensione della serie Cisco 1600 ed offre maggiore funzionalità alle medie e piccole aziende e ai piccoli uffici di filiale. Oltre alle funzionalità della serie Cisco 1600, il router Cisco 1720 offre anche la codifica ad una velocità superiore per le VPN, l'autosensing 10/100 Fast Ethernet, una maggiore flessibilità con uno slot supplementare per schede d'interfaccia WAN, ulteriori interfacce seriali e prestazioni superiori per le tecnologie WAN emergenti a banda larga.

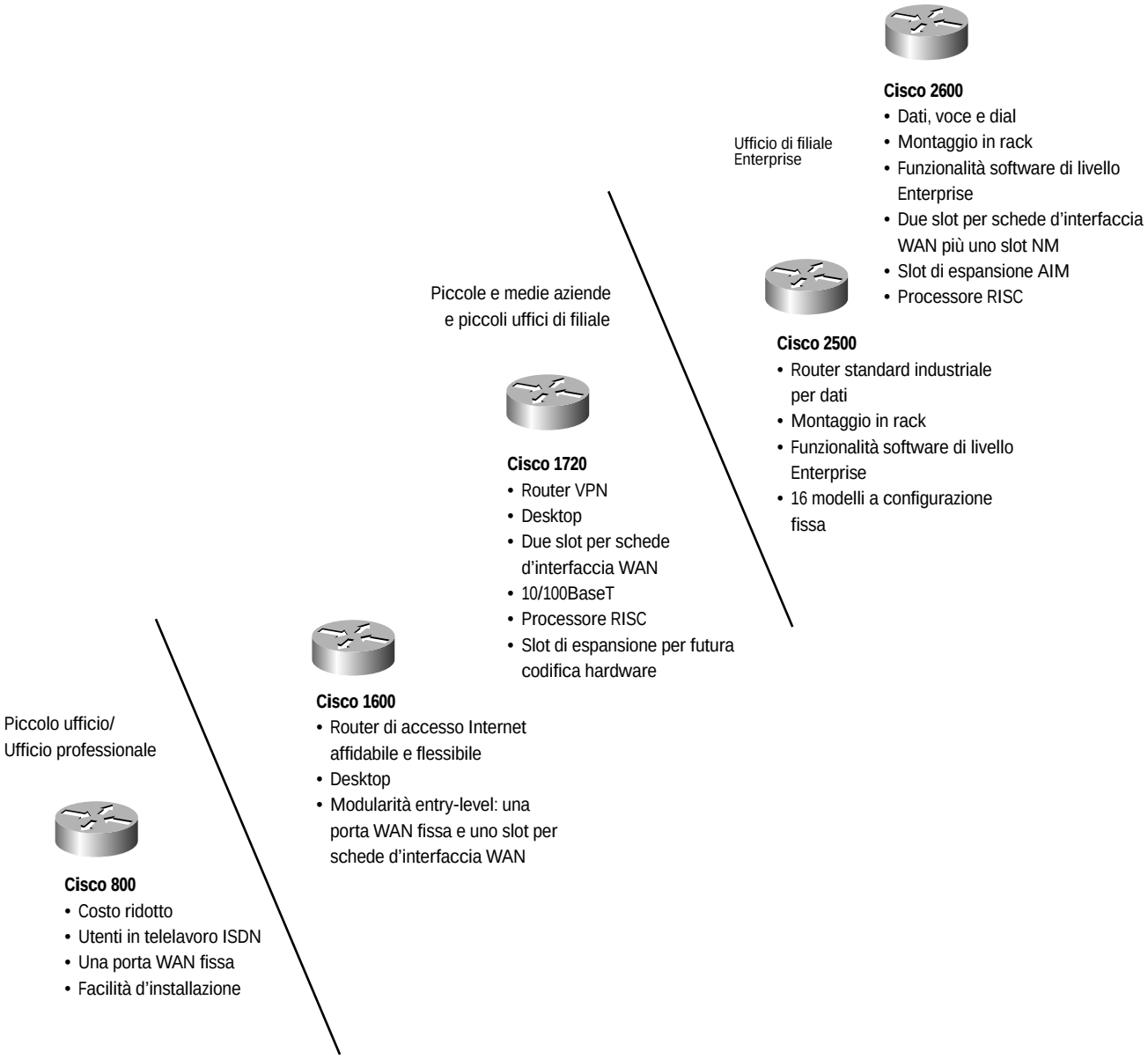
Rispetto alla serie Cisco 1600, il router Cisco 1720 è particolarmente adatto ad ambienti e applicazioni che prevedono:

- l'implementazione immediata o entro un paio di anni di VPN con velocità di codifica da 128 Kbps e T1/E1 (Cisco 1720 è attualmente in grado di effettuare la codifica software assistita a 512 Kbps mentre in futuro riuscirà a garantire velocità di T1/E1 con una codifica hardware assistita mediante una scheda installata sulla motherboard);
- LAN Fast Ethernet;
- una rapida crescita e cambiamenti che potranno beneficiare dello slot per schede d'interfaccia WAN supplementare;
- l'uso di un maggior numero di interfacce seriali (fino a cinque compresa una porta AUX) come nel caso dei POS (Point Of Sale) o dei piccoli uffici di filiali bancarie;
- collegamenti duali ISDN BRI;
- la compressione a velocità superiori a 128 Kbps;
- ADSL (Asymmetric Digital Subscriber Line) in futuro (quando sarà disponibile la scheda d'interfaccia WAN ADSL) con prestazioni superiori che sfruttino la larghezza di banda ADSL.

Tabella 4: funzioni Cisco 1720 di livello superiore rispetto ai router della serie Cisco 1600

	Serie Cisco 1600 Router di accesso Internet /intranet flessibile e sicuro	Cisco 1720 Router di accesso VPN flessibile e sicuro
Velocità di codifica IPSec DES (software assistita con pacchetti di 256 byte)	128 Kbps	512 Kbps
Velocità di codifica IPSec DES (hardware assistita con pacchetti di 256 byte)	Non disponibile	2,0 Mbps (quando sarà disponibile la scheda di codifica hardware)
Supporto della codifica	DES	DES, Triple DES
Slot di espansione interno per la futura codifica hardware assistita ad alta velocità	No	Sì
LAN	Ethernet	Autosensing 10/100 Fast Ethernet
WAN	Una porta WAN fissa più uno slot per scheda d'interfaccia WAN	Due slot per schede d'interfaccia WAN
Supporto delle schede d'interfaccia WAN (WIC)	WIC-1T, WIC-1B-S/T, WIC-1B-U, WIC-1DSU-56K4, WIC-1DSU-T1	Tutte le schede d'interfaccia WAN della serie Cisco 1600 più WIC-2T e WIC-2A/S
Numero di schede d'interfaccia WAN supportate	Seriali (sync/async): due ISDN BRI: una (più una seriale)	Seriali (sync/async): cinque (compresa una porta AUX) ISDN BRI: due
Supporto dell'ISDN BRI duale	No	Sì
Porta AUX (async fino a 115,2 Kbps)	No	Sì
Memoria DRAM max	24 MB	48 MB

Figura 7: posizionamento dei prodotti e caratteristiche fondamentali



Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
Sito World Wide Web:
http://www.cisco.com
Tel: 001 408 526-4000
001 800 553-NETS (6387)
Fax: 001 408 526-4100

Sede europea
Cisco Systems Europe
11 rue Camille Desmoulins
92787 Issy-les-Molineaux Cedex 9
France
Tel: 0033 1 5804 60 00
Fax: 0033 1 5804 61 00

Sede italiana
Cisco Systems Italy
Palazzo Faggio
Via Torri Bianche 7
20059 Vimercate (Mi)
Tel: 039 6295 1
Fax: 039 6295 299
Sito World Wide Web:
http://www.cisco.com/it

Filiale di Roma
Cisco Systems
Viale della Grande Muraglia 284
00144 Roma
Tel: 06 52301 1
Fax: 06 5220 9952

Le filiali Cisco Systems nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono e fax sono disponibili sul sito
Cisco Connection Online all'indirizzo http://www.cisco.com.

Arabia Saudita • Argentina • Australia • Austria • Belgio • Brasile • Canada • Cile • Cina • Colombia • Corea • Costarica • Danimarca • Emirati Arabi • Filippine • Finlandia • Francia • Germania • Giappone • Gran Bretagna • Grecia • Hong Kong • India • Indonesia • Irlanda • Israele • Italia • Lussemburgo • Malesia • Messico • Norvegia • Nuova Zelanda • Olanda • Perù • Polonia • Portogallo • Repubblica Ceca • Russia • Scozia • Singapore• Spagna • Stati Uniti • Sud Africa • Svezia • Svizzera • Tailandia • Taiwan • Turchia • Ungheria • Venezuela