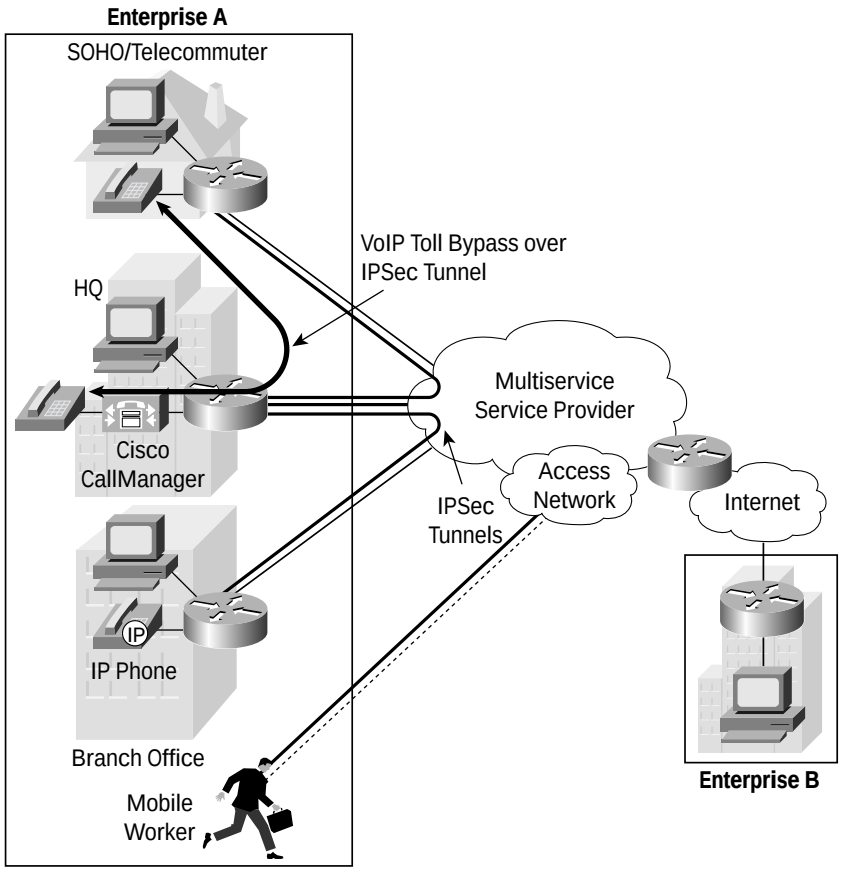
White Paper

Voice and Video Enabled IPSec VPN (V^3PN)

Solution Overview

Virtual private networks (VPNs) offer a lower cost and highly flexible alternative to replacing or augmenting dedicated private networks that use leased lines, Frame Relay, or ATM circuits. VPNs also provide seamless remote access for telecommuters and mobile workers, as well as cost-effective remote-office connectivity. VPNs provide tremendous cost savings for enterprise data networks by utilizing shared networks secured by encrypted VPN tunnels. The trend toward network convergence, however, places new demands on VPNs. With voice and video enabled IPSec VPN (V^3PN) delivered by Cisco, enterprises can leverage cost-effective VPNs to add voice and video to their data network without compromising quality and reliability. Figure 1 illustrates how IP Security (IPSec) VPNs are used to create a private network over a multiservice service provider's public network enabling the secure transport of voice and data.

Figure 1
Voice, Video Enabled IPSec VPN



This solution overview discusses some of the business drivers, deployment considerations, enabling technologies, and products, as well as two compelling case studies that illustrate the value of the Cisco V^{3}PN solution.

Business Drivers

As enterprises expand and strive to compete in today's market, network managers are seeking a network solution that economically delivers corporate voice, video, and data services to their employees regardless of their location (that is, headquarters, branch office, telecommuter, mobile worker). Business drivers include the following:

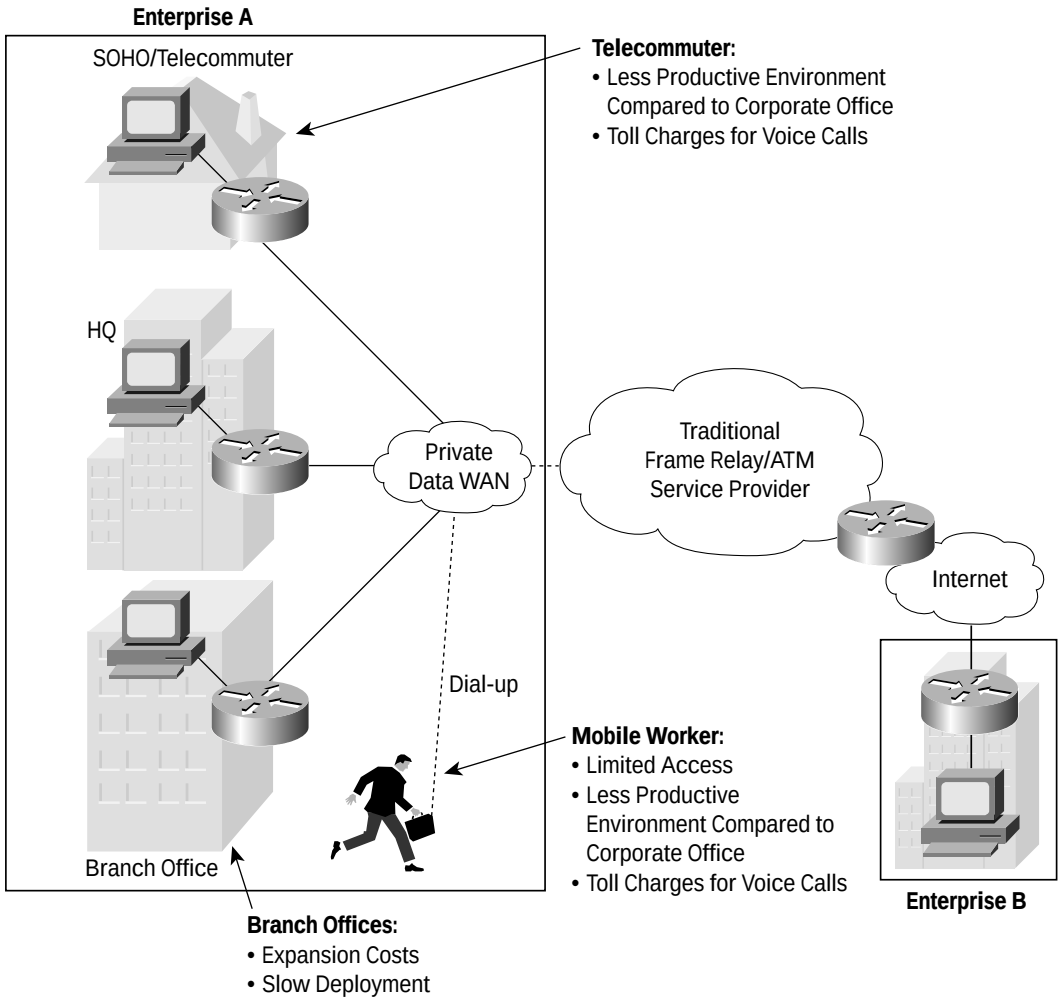
- *Cost reduction*—Enterprises are quickly converging voice, video, and data services onto a single IP network, and they require a more economical and efficient way of delivering these services to their employees. This includes reducing network operations costs, wide-area network (WAN) transport costs, telecommuter and mobile worker access costs, and voice toll charges.
- *Increase in employee productivity*—With the availability of high-speed Internet access in homes and hotels, enterprises need to extend the reach of their networks to the telecommuter and mobile worker and provide them access to the same voice, video, and data services that are available on the corporate network.
- *Speed to market*—The enterprise must be able to react to market demands and bring new branch or sales offices online quickly when geographic presence is required.

The following sections describe some of the challenges of doing business in this expanding and mobile workforce environment and how the Cisco V^{3}PN IPSec VPN solution overcomes these challenges.

Today's Challenges

Today, extending the enterprise network and services to branch offices, telecommuters, and mobile workers presents unique challenges and introduces new technologies. Figure 2 illustrates these challenges, followed by additional details and examples.

Figure 2
Business Challenges



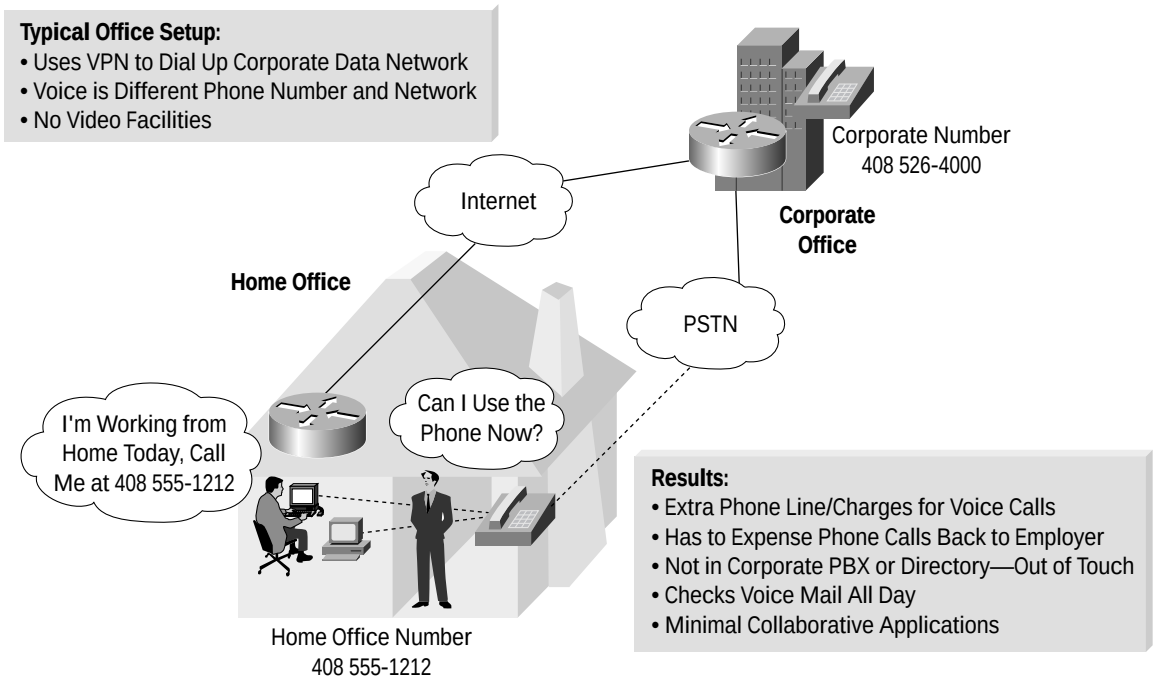
Challenges include the following:

- *Branch offices*-Being able to add branch offices to the enterprise network quickly at a lower cost than using leased lines, Frame Relay, or ATM circuits while maintaining the stringent performance and security requirements of a private network
- *Telecommuters/mobile workers*—Cost-effectively providing telecommuters and mobile workers the same level of productivity they experience in the office, with a high level of security and usability

For example, today a telecommuter typically accesses corporate data services through either a dialup modem or an ISDN line. Typically, 800 toll charges are associated with these calls, in addition to a monthly connection charge. As a result of these low-speed links, productivity is low and costs are high.

With the advent of digital subscriber line (DSL) and cable high-speed Internet access and new VPN technologies, the telecommuter is experiencing significant improvements in productivity and cost reduction for higher-bandwidth access to corporate data services. However, access to corporate voice services is almost nonexistent, and conducting business over the phone in a home office is quite cumbersome. Telecommuters resort to using their private home phone, using their mobile phone, or paying for an additional business line. This requires telecommuters to maintain at least two phone numbers and voice mailboxes (for example, corporate office and home office) and juggle incoming calls among them all. Figure 3 illustrates telecommuting challenges.

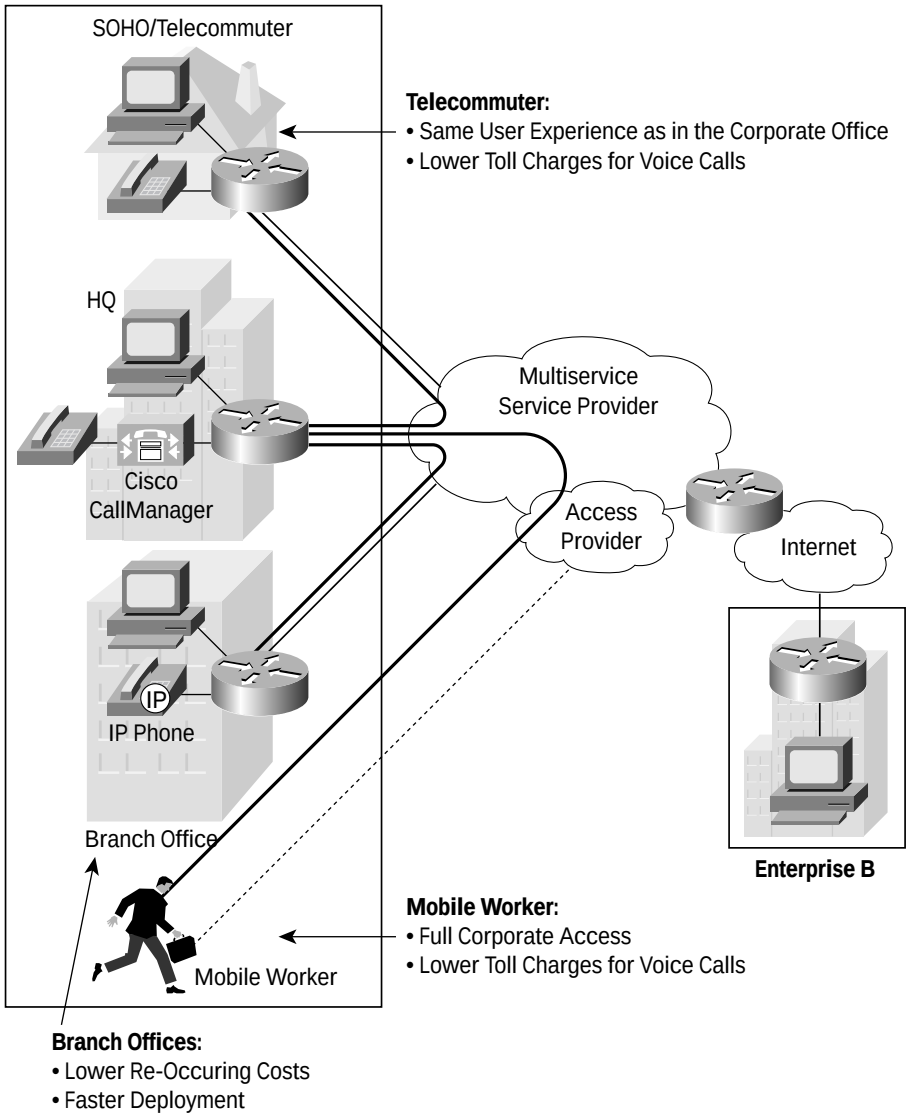
Figure 3
Typical Telecommuter Challenges



The Cisco V^{3}PN Solution

The Cisco V^{3}PN solution offers the enterprise a lower-cost multiservice WAN and remote access alternative that optimizes employee productivity while maintaining the stringent performance and security requirements of a private network. This solution provides a consistent way of connecting all users to the enterprise network regardless of location. Figure 4 illustrates the advantages of using the Cisco V^{3}PN solution over the traditionally disparate ways of connecting to the enterprise network.

Figure 4
The Cisco V^{3}PN Solution



Solution Considerations

This section discusses the considerations the network manager has to make when deploying the Cisco V^{3}PN solution:

Quality of Service

- Voice and video quality is only as good as the quality of the weakest network link, so end-to-end quality of service (QoS) is critical. Latency, jitter, and packet loss all contribute to degraded voice and video quality. The network manager must understand the impact of the enterprise local-area network (LAN) as well as the level of service

that the service provider must deliver to maintain satisfactory voice/video quality. This document refers to service providers that provide low-latency bandwidth and service-level agreements (SLAs) to support multiple services (voice, video, and data) as multiservice service providers.

Security

- *Transport security*—Traffic traversing public access and backbone networks must be properly secured. IPSec VPNs provide this security by ensuring data confidentiality (using encryption), data integrity, and data authentication between participating peers.
- *Network security*—Cisco firewalls provide stateful perimeter security critical to any public-facing network, such as a VPN. When deploying voice and video across VPNs, it is critical to statefully inspect all multiservice traffic traversing the firewall.
- *Intrusion detection*—Intrusion detection plays an integral part in securing a Cisco V^3PN by providing additional network perimeter protection and shielding IP telephony hosts from intruders and malicious traffic such as worms.

Network Availability

- *Redundant components and paths*—Critical-component (that is, VPN headend) and data-path redundancy must be supported to provide fast and automatic network convergence in case of component or service provider network failure.

Network and Service Interoperability

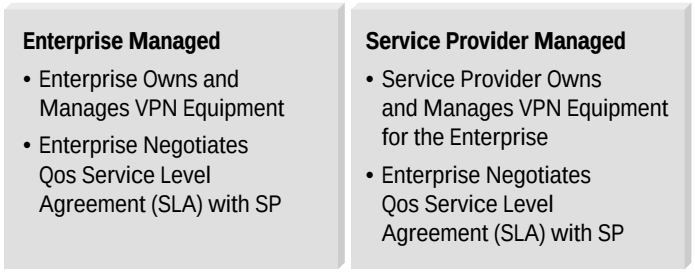
- *QoS and IPSec interaction*—IPSec encrypts packets, including QoS markings; therefore, having VPN devices that can support QoS on IPSec-encrypted traffic is a crucial element for toll-quality voice and video across the VPN.
- *Multicast support over the VPN*—Much voice and video traffic is multicast. IPSec does not natively support multicast traffic. Having VPN devices that can support multicast across the VPN is critical to a Cisco V^3PN solution.
- *Support for low-latency network topologies*—Having a meshed network topology is often important to reduce latency and jitter. The VPN device must be able to support meshed topologies, not just basic hub and spoke.
- *Firewall support for VoIP protocols*—Many firewall solutions require pass-through of IP telephony traffic because they cannot statefully inspect the traffic. Having a firewall that can support IP telephony is critical to the security of the Cisco V^3PN solution.

Service Management Options

Following the trend of outsourcing noncore business functions—and growth of the private VPN in both size and complexity—enterprises may choose to employ the service provider to manage the VPN. They may choose to manage the customer premises equipment (CPE) and negotiate an SLA with the service provider or have a service provider manage the whole WAN, including the CPE.

The next section describes the multiservice service provider and the general SLA requirements necessary to support toll-quality voice and video.

Figure 5
VPN Service Management Options



Multiservice Service Provider

A critical step the enterprise faces when deploying the V^{3}PN solution is finding and contracting an SLA with a multiservice service provider. Cisco has worked closely with large service providers tuning their IP networks to support multiservice and has developed a Cisco Powered Network program to enable enterprise customers to identify capable multiservice service providers.

General SLA Requirements

Fundamental to negotiating the SLA is understanding the latency, jitter, and packet loss budgets in each section of the network required to support high-quality voice, video, and data transport. The network manager must determine the budget values for the LAN sections of the network and use those values to set the limits negotiated in the SLA. Following are the latency, jitter, and packet-loss metrics that the multiservice service provider must support to qualify for a Cisco Powered Network designation. Note that the service provider may offer other metrics such as network availability or guaranteed bandwidth based on traffic type.

- Latency (equal to or less than 60 ms within the United States or Europe)
- Jitter (equal to or less than 20 ms)
- Packet loss (equal to or less than 0.5 percent)

For more information on choosing a multiservice service provider, see the following URL:

Cisco Powered Networks

http://www.cisco.com/pcgi-bin/cpn/cpn_pub_bassrch.pl

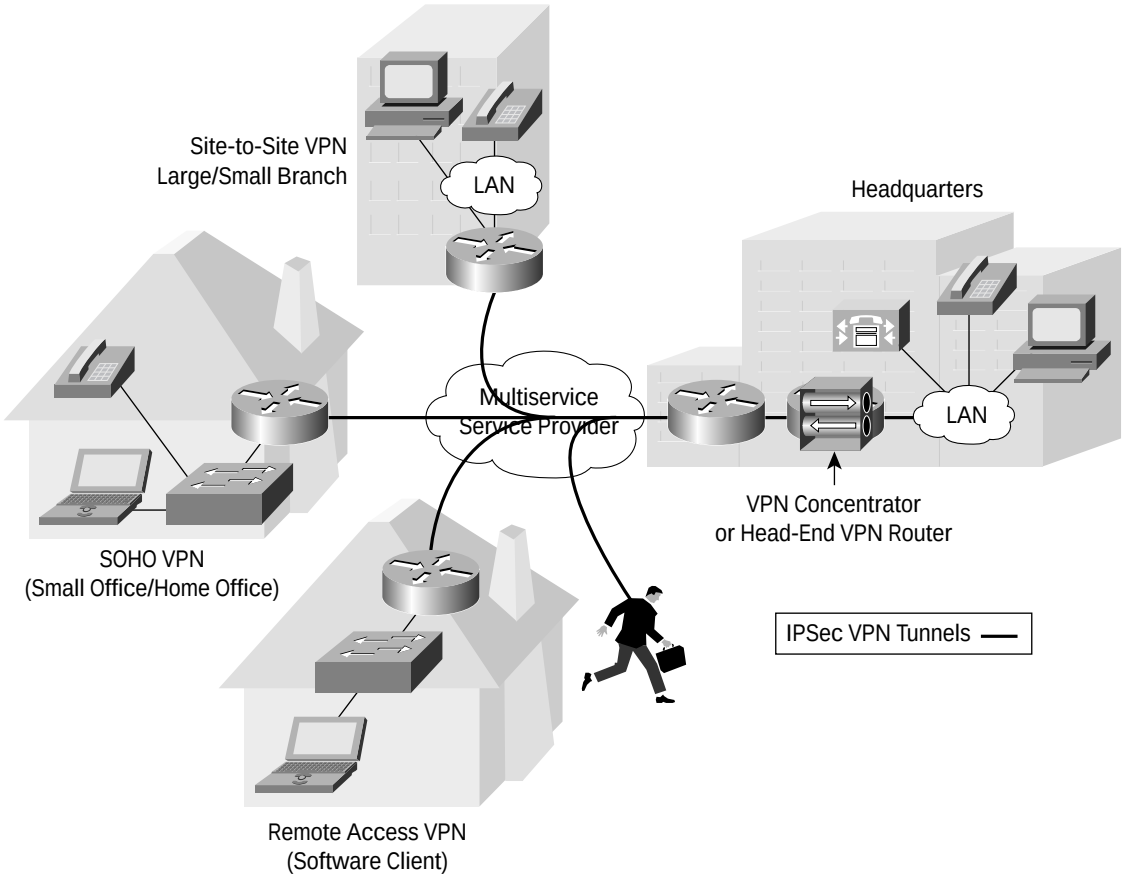
Deployment Models

The Cisco V^{3}PN solution supports three deployment models: site to site, small office/home office (SOHO), and remote access. Although the deployment models use similar technologies and topologies, they each require a different level of support from the service provider network. The following sections illustrate the deployment models and highlight the different levels of service provider support. Figure 6 shows the composite view of the Cisco V^{3}PN deployment models.

For in-depth discussions of general VPN deployment architectures, see “SAFE VPN: IPSec Virtual Private Networks in Depth” at:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm.

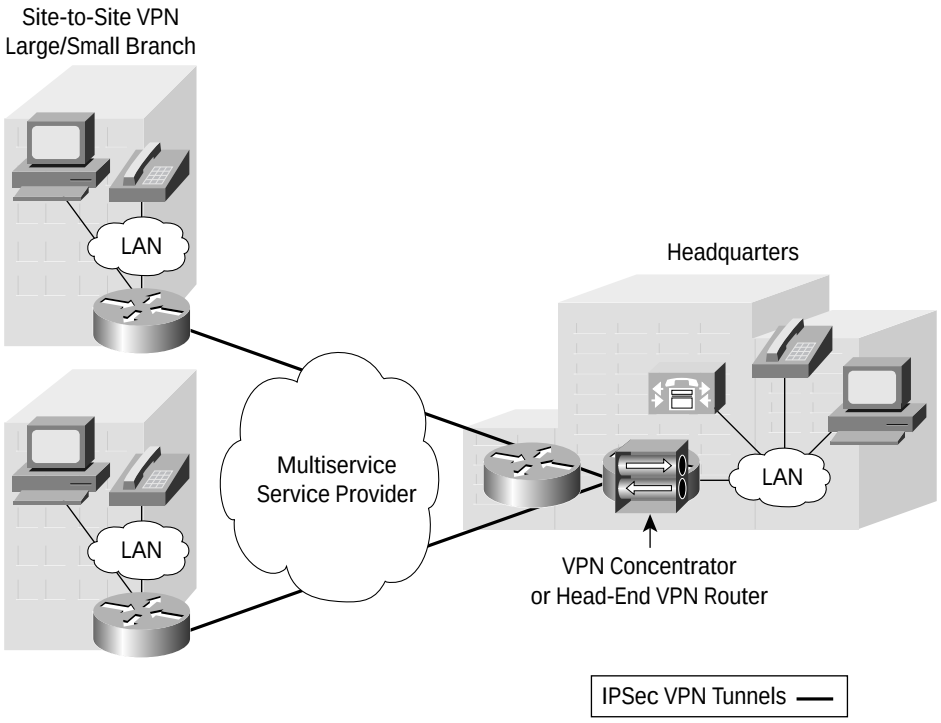
Figure 6
V3PN Deployment Models



Site-to-Site Deployment

The site-to-site deployment model consists of IPSec tunnels between corporate headquarters and branch offices. This deployment model utilizes a backbone multiservice service provider and provides the same capabilities as a traditional enterprise WAN with support for hub-and-spoke and mesh topologies. Backbone service providers are the first providers that are upgrading their network to support multiservice, and they soon will be offering a viable multiservice VPN-based WAN alternative to the enterprise. Figure 7 shows an example of a site-to-site VPN hub-and-spoke deployment.

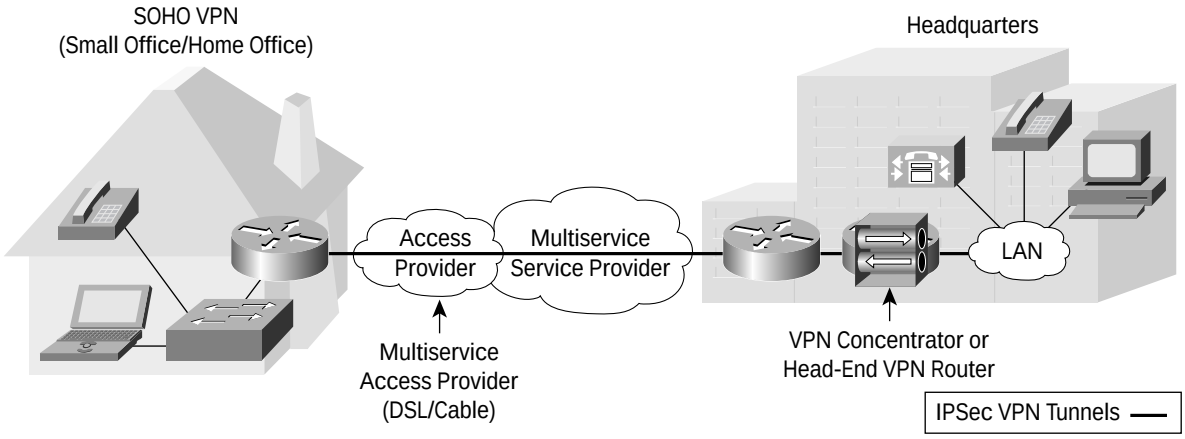
Figure 7
Site-to-Site Deployment Model



Small Office/Home Office

The SOHO deployment model consists of IPSec tunnels between corporate headquarters and small or home offices (that is, telecommuters). This deployment model likely utilizes multiple multiservice service providers (that is, backbone and access) and provides the same capabilities as a traditional enterprise hub-and-spoke WAN. Cisco is working closely with both access and backbone providers to help facilitate this end-to-end multiservice capability to provide a viable transport option for the V^3PN SOHO solution. Figure 8 shows a SOHO VPN deployment and how the VPN connection traverses multiple service providers.

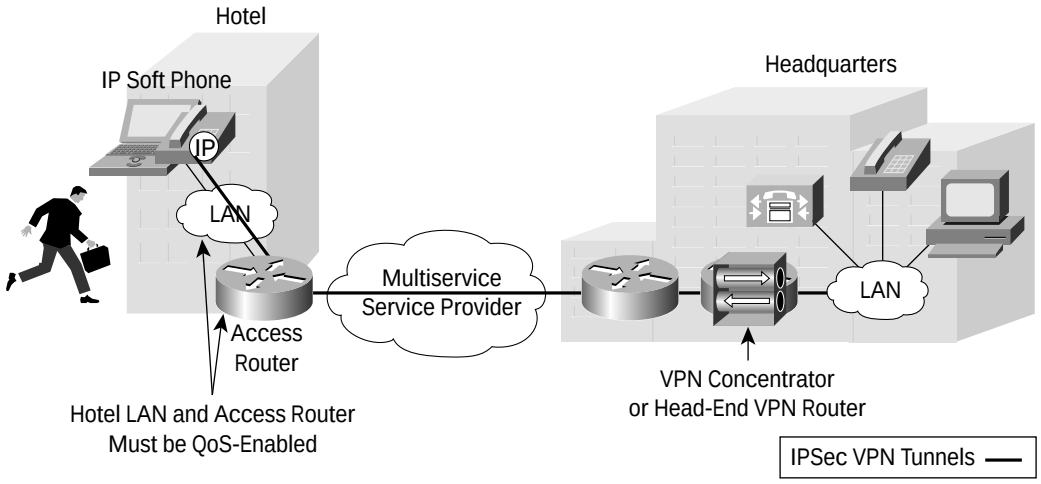
Figure 8
SOHO Deployment Model



Remote Access

The remote access deployment model consists of IPSec tunnels between corporate headquarters and a mobile worker's laptop computer. This deployment model also utilizes multiple multiservice service providers (that is, backbone and hotel network) and provides the same capabilities as a "high-speed" enterprise remote access network. Figure 9 shows a remote access VPN deployment and how the VPN connection traverses multiple service providers.

Figure 9
Remote Access Deployment Model



QoS Tools

End-to-end QoS is critical for delivering toll-quality voice and video services over VPN. Cisco has enabled numerous QoS tools available in Cisco IOS® Software to work in concert with the VPN features. This section discusses the QoS issues the network manager must be concerned with when deploying the V^3PN solution and the tools that Cisco provides to address each.

For more detailed information on IP telephony network design, see:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/.

The basic steps required for end-to-end QoS are given as follows, with details in the following sections.

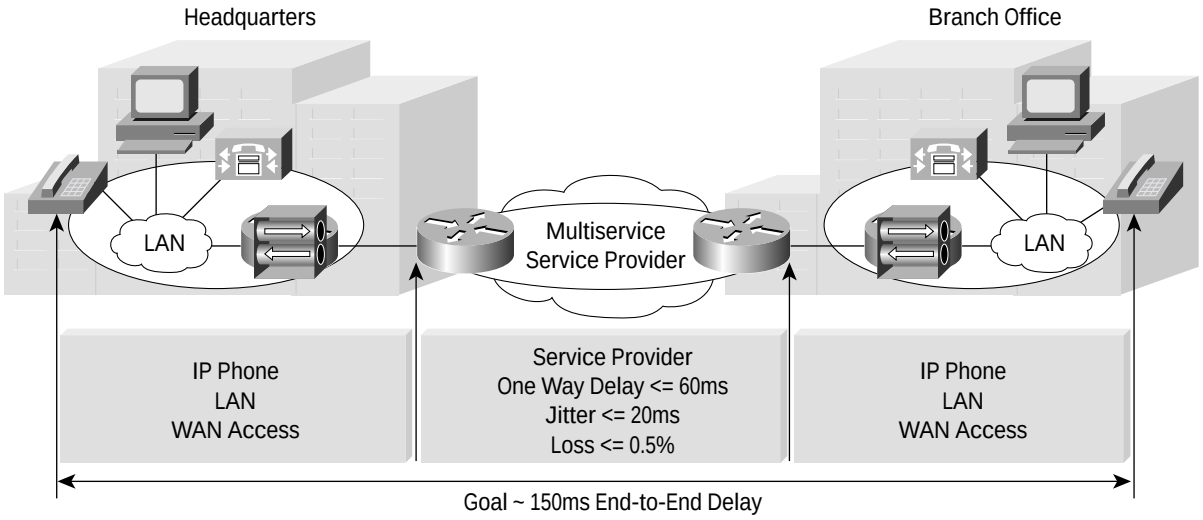
Step 1. Classify voice, video, and data traffic such that it matches the appropriate classifications used by the service provider to ensure that the traffic is assigned the proper class of service.

Step 2. Implement the appropriate QoS tools in the LAN and enterprise edge router to properly queue traffic toward the service provider network.

Step 3. Implement Call Admission Control (CAC) to limit the number of voice or video calls allowed to traverse the access link.

Figure 10 illustrates where QoS must be managed with the goal of meeting the recommended end-to-end latency, jitter, and packet-loss constraints for toll-quality voice and video transport.

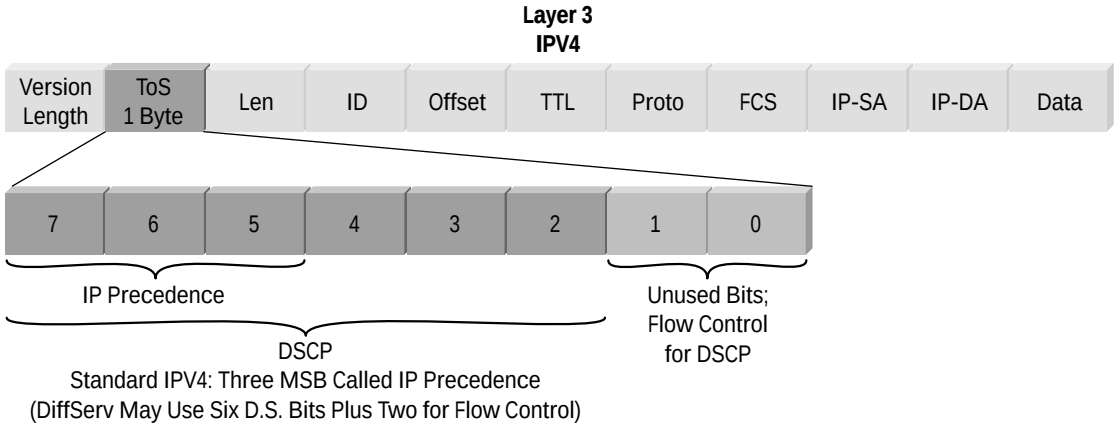
Figure 10
End-to-End QoS Management



Classification

Classification is the marking of a packet or flow with a specific priority. Classification takes place in the enterprise LAN, typically in the wiring closet or within the IP phones or voice/video endpoints themselves. Packets must be marked for priority handling within the network with the IP Precedence or differentiated services code point (DSCP) bits in the type-of-service (ToS) byte of the IPv4 header. Figure 11 shows the ToS field and the bits that are used for both IP Precedence and DSCP QoS markings.

Figure 11
QoS Layer 3 Classifications



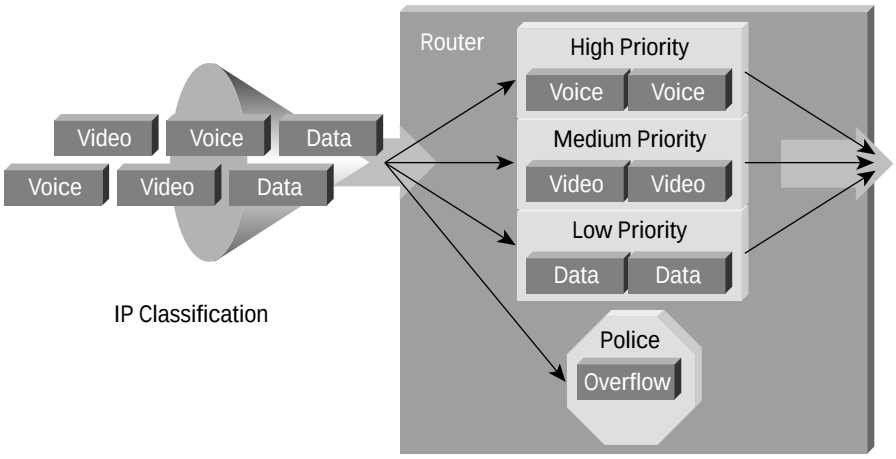
As mentioned previously, these markings may be placed in the packet by the endpoints (for example, IP phones) or at the enterprise edge router; they are the selection criteria for determining the class of service the packet is given in the service provider's network. Note the overlapping relationship between the IP Precedence value and the DSCP. This is done intentionally for compatibility between the two marking schemes, and Cisco equipment can support both. Configuring the endpoint to classify with DSCP also maintains the proper handling of packets in an IP Precedence-based QoS network. In fact, the router in the enterprise edge can even be configured to translate from one scheme to the other.

Queuing

Queuing tools assign a packet or flow to one of several queues, based on classification, for appropriate treatment in the network. When data, voice, and video are placed in the same queue, packet loss and variable delay are much more likely to occur. By using multiple queues on egress interfaces and placing voice packets into a different queue than data packets, network behavior becomes much more predictable.

Interface queuing is one of the most important mechanisms for ensuring voice quality within a data network. This is even more vital in the WAN because many traffic flows are contending for a very limited amount of network resources. When traffic is classified, the flow can be placed into an interface egress queue that meets its handling requirements. Voice over IP (VoIP), because of its extremely low tolerance for packet loss and delay, should be placed into a high-priority queue. However, other traffic types may have specific bandwidth and delay characteristics as well. These requirements are addressed with the low-latency queuing (LLQ) feature in Cisco IOS Software. Figure 12 illustrates the queuing of traffic based on classification.

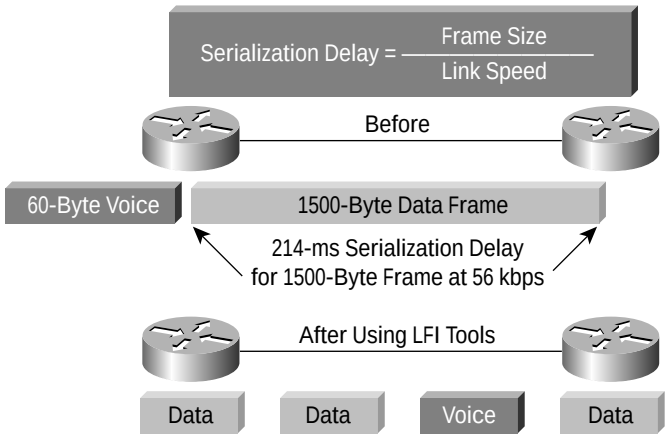
Figure 12
Queuing Based on Traffic Classification



Link Fragmentation and Interleaving

For low-speed WAN connections (in practice, those with a clocking speed of 768 kbps or below), link fragmentation and interleaving (LFI) is required to reduce jitter incurred when large frames are introduced into the data stream. LFI tools are used to fragment large data frames into regularly sized pieces and to interleave voice frames into the flow so that the end-to-end delay can be predicted accurately. This places bounds on jitter by preventing voice traffic from being delayed behind large data frames, as illustrated in Figure 13.

Figure 13
Using LFI Tools to Reduce Frame Delay

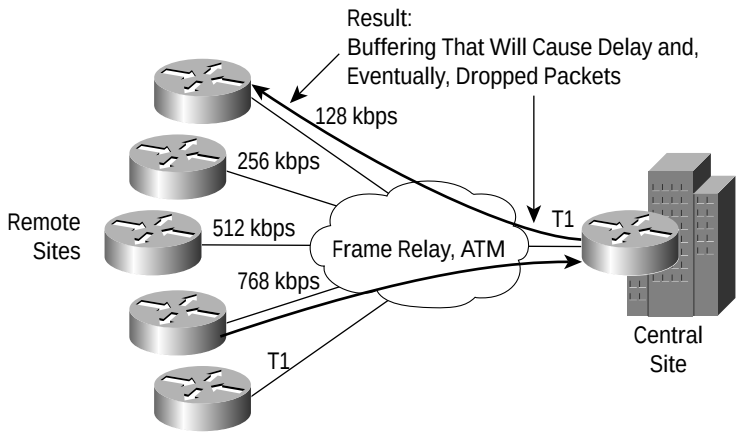


Traffic Shaping

In ATM and Frame Relay networks, where the physical access speed varies between two endpoints, traffic shaping is used to prevent excessive delay from congested network interface buffers caused by these speed mismatches. Traffic shaping is a tool that meters the transmit rate of frames from a source router to a destination router. This metering is typically done at a value that is lower than the line or circuit rate of the transmitting interface. The metering is done at this rate to account for the circuit speed mismatches that are common in hub-and-spoke topologies.

For example, as illustrated in Figure 14, the many remote sites, each with small WAN connections, when added together can oversubscribe the provisioned bandwidth or circuit speed at the central site.

Figure 14
Variable Delay Caused by Buffering



In summary, all of these QoS tools that have been available in Cisco IOS Software now may be used in concert with the VPN features to implement the V^3PN solution.

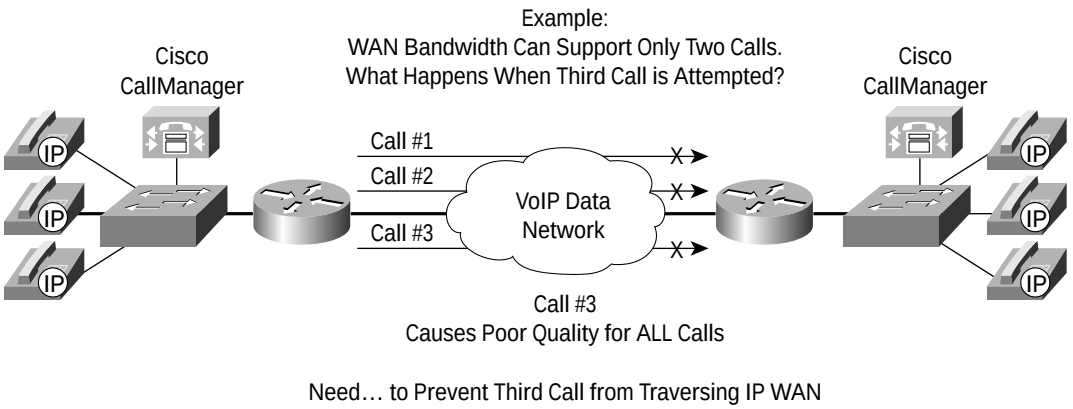
Call Admission Control

CAC is a mechanism for ensuring that voice flows do not exceed the maximum provisioned bandwidth allocated for voice conversations.

After doing the calculations to provision the required bandwidth to support voice, data, and possibly video applications, it is important to ensure that voice does not oversubscribe the portion of the bandwidth allocated to it. Although most QoS mechanisms are used to protect voice from data, CAC is used to protect voice from voice. This is illustrated in Figure 15, which shows an environment in which the bandwidth has been provisioned to support two concurrent voice calls. If a third voice call is allowed to proceed, the quality of all three calls is degraded. To prevent this degradation in voice quality, you can provision CAC in Cisco CallManager and Cisco IOS gatekeepers to block the third call.

For more information on CAC, see the Cisco IP Telephony Network Design Guide, which is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/index.htm.

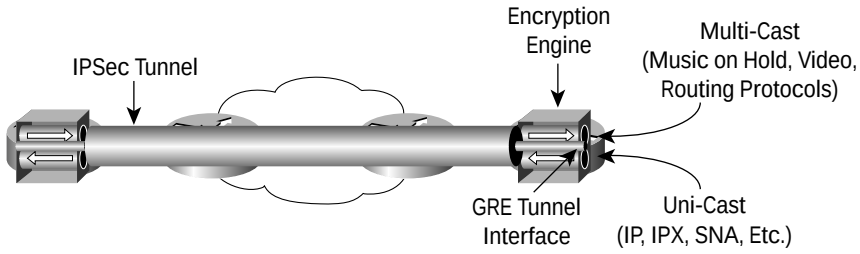
Figure 15
Call Admission Control



IPSec-Protected Generic Routing Encapsulation

A critical component in the V^{3}PN solution, the IPSec-protected generic routing encapsulation (GRE) tunnel provides the secure transport of diverse traffic types and topologies and enables the use of dynamic routing to ensure network availability. Figure 16 shows the IPSec-protected GRE tunnel.

Figure 16
IPSec-Protected GRE

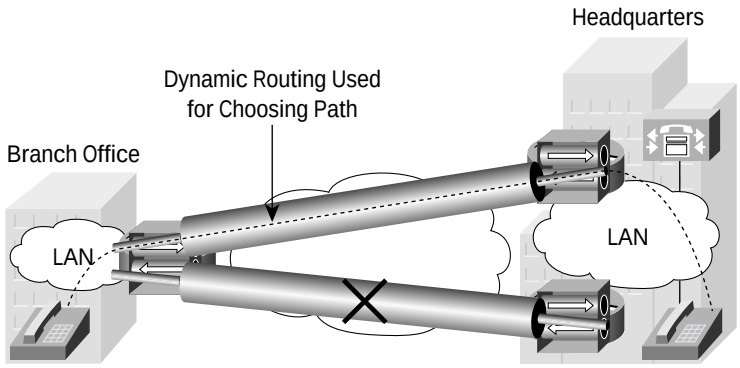


- *Diverse traffic types*—GRE supports the transport of both unicast and multicast traffic and is useful for tunneling both IP and non-IP protocols (for example, Internetwork Packet Exchange [IPX], Systems Network Architecture [SNA]).
- *Diverse topologies*—Logically, GRE is a point-to-point tunnel between endpoints and supports hub-and-spoke and mesh topologies. In cases where latency must be minimized to maintain voice or video quality, a tunnel may be configured directly to the far endpoint rather than being forced to traverse a hub site and encounter multiple encryption cycles.
- *Independent enterprise routing and IP addressing*—IP packets are placed inside a GRE header and encapsulated in an IP datagram and "tunneled" to the remote end. By terminating the tunnels on the VPN devices, the *enterprise* address space and routing information is independent of the address space and routing information of other customers or the service provider. This provides maximum flexibility for both enterprise and the service provider.

- *Network availability*—Inherently, native IPSec does not support an effective failover capability, but the V^{3}PN solution addresses this issue by using GRE coupled with dynamic routing. Because IPSec tunnels send data without any acknowledgment or feedback mechanism from the remote peer, an IPSec endpoint has no way to know if its remote peer is reachable. So if the remote peer is down or unreachable, the IPSec endpoint continues to blindly send data to what is often referred to as a "black hole."

The V^{3}PN solution uses dynamic routing protocols over IPSec-protected GRE tunnels to track remote network reachability. A remote site using dynamic routing for high availability will establish two IPSec-protected GRE tunnels, one to each headend. Routing updates traverse both tunnels to the remote site, which then forwards the traffic to the headend with the most favorable path to the destination network. Figure 17 illustrates a failed link and how traffic is diverted to a viable path.

Figure 17
Dynamic Routing Used for Network Availability



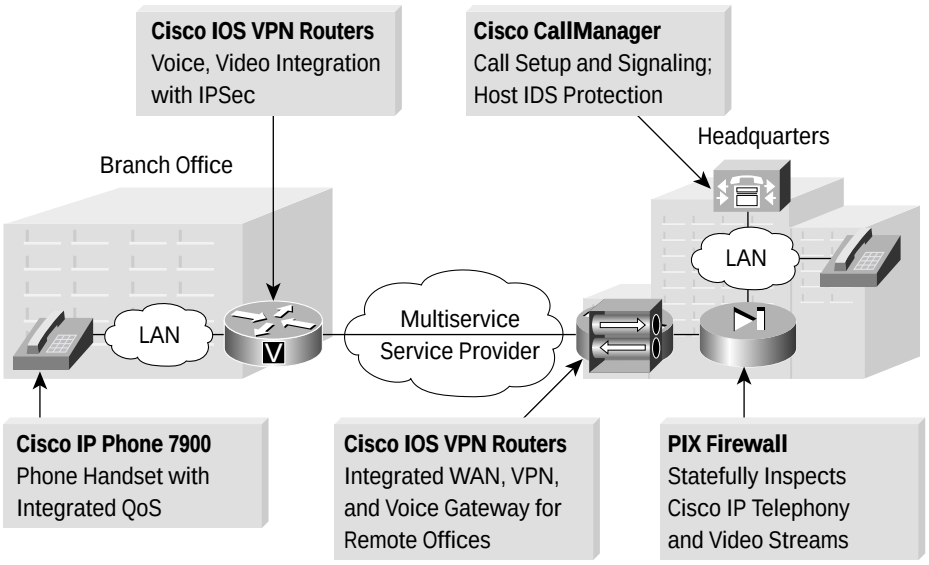
Products

Providing end-to-end products for IP telephony and video, IPSec VPNs, and security, Cisco is distinctively positioned to deliver the converged network solution offered in the Cisco V^{3}PN solution. Deploying V^{3}PN solution developed by Cisco ensures interoperability of multiservice over an IPSec VPN and provides a single source for network design guidance and support (Figure 18).

- *Cisco IOS VPN Routers*—Cisco Routers such as 1700, 2600, 3600, 3700, 7100, and 7200 series are the foundation of the V^{3}PN solution. Cisco VPN Routers provide encryption, QoS, and routing for multiservice traffic over the VPN. At remote sites Cisco IOS VPN Routers serve as a single box solution for VPN, telephony, WAN access, and firewall, thus providing a cost-effective remote office solution.
- *Cisco CallManager*—Cisco CallManager provides scalable call control and signaling services for the IP telephony infrastructure.
- *Cisco IP phones*—The Cisco IP voice handset provides the same user interface as traditional phones, but with enhanced functionality such as directory services and news feeds.
- *Cisco IOS voice gateways*—Cisco IOS voice gateways provide connectivity to the Public Switched Telephone Network (PSTN) from the VoIP network.
- *Cisco PIX® firewalls*—Cisco PIX firewalls provide stateful inspection of voice and video traffic, including protocols such as H.323, Session Initiation Protocol (SIP), and Skinny.

- *Cisco IDS Host Sensor*—The Cisco IDS Host Sensor delivers real-time analysis and reactions to security attacks for IP telephony equipment, such as Cisco CallManager.

Figure 18
Cisco Products



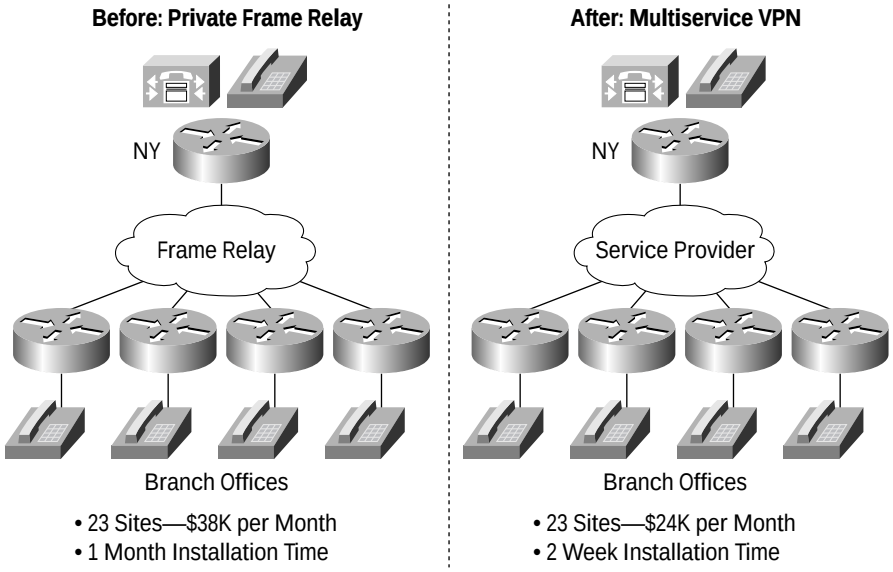
Case Studies

The following two case studies illustrate how the V^3PN solution offers a lower-cost alternative to a private Frame Relay WAN network and provides the telecommuter a cost-effective and highly productive work environment.

Site-to-Site VPN

This company prepared a business case comparing the deployment of a private Frame Relay network versus the Cisco V^3PN solution. The company realized significant costs savings on the recurring monthly charge, saving more than US$168,000 per year with a deployment timeline half that of a Frame Relay installation (Figure 19).

Figure 19
V^3PN Site-to-Site VPN Case Study



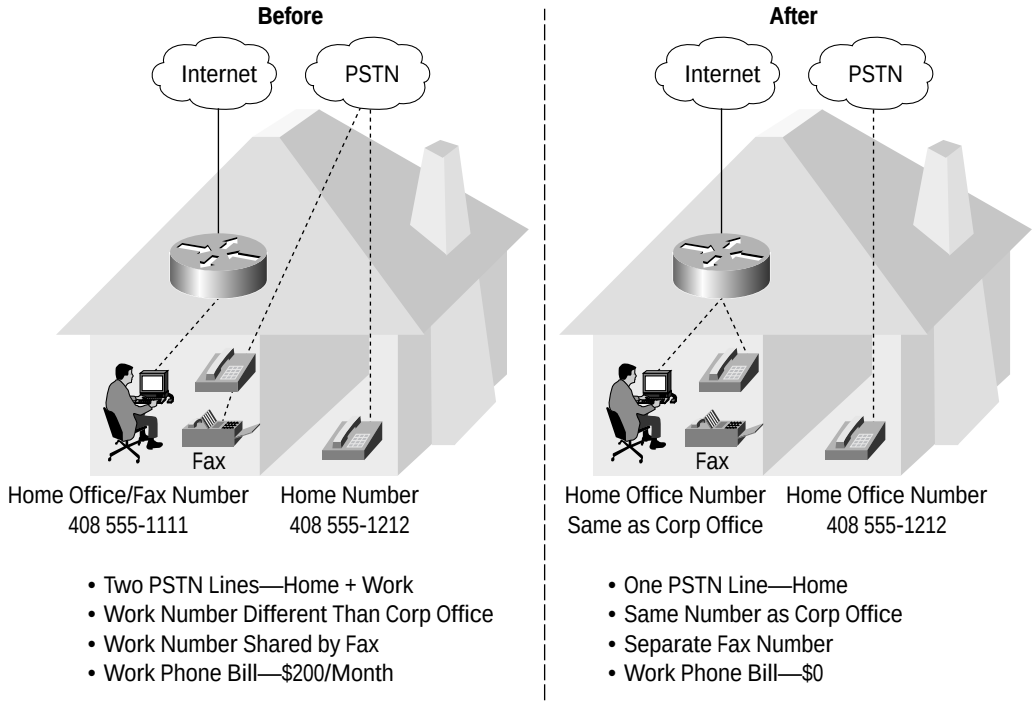
Remote Access VPN

This case study takes the example presented earlier in this document and applies actual costs to show the value of the V^3PN solution used in a SOHO deployment.

This telecommuter accesses the corporate data network via a VPN client installed on a PC. However, access to corporate voice services is almost nonexistent, and conducting business over the phone in a home office is quite cumbersome. This telecommuter resorts to paying for an additional business line with its associated phone number. This requires the telecommuter to maintain two phone numbers and voice mailboxes (for example, corporate office and home office) and juggle incoming calls between them. Between the monthly costs for the business line and long-distance charges incurred when dialing corporate offices, the total monthly phone bill is about $200 per month.

This company then deployed the V^3PN solution and coupled it with IP telephony to save significant monthly business-line and long-distance call charges and provided the identical data and voice services the employee has when in the corporate office. The telecommuter uses a VPN router connected to the high-speed connection from the multiservice service provider to establish a secure IPSec tunnel to the *enterprise* network. The telecommuter's IP phone registers with the appropriate Cisco CallManager IP private branch exchange (PBX) and the phone then receives its profile with all the speed dials, corporate directory, and its assigned corporate phone number. The telecommuter's productivity rivals that of being in the corporate office at a significantly reduced cost to the company (refer to Figure 20).

Figure 20
Remote Access Case Study



Conclusion

Providing end-to-end products and deployment architectures for both IP telephony and IPSec VPNs, Cisco is distinctively positioned to deliver the converged network solution offered in the V^3PN solution. Deploying V^3PN solutions developed by Cisco ensures interoperability of the components and technologies not only in the *enterprise* LAN but also with the service provider network and provides a single source for network design guidance and support.

Reference Documents

Cisco Multiservice VPN Solution
http://www.cisco.com/warp/public/779/servpro/solutions/telephony/multiservice-vpn.html

Cisco Virtual Private Networks
http://www.cisco.com/public/vpn.html

Cisco SAFE Blueprint for Network Security VPN: IPSec Virtual Private Networks in Depth
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm

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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia 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

LW3270 5/02