Business Ready Teleworker Design Guide

January 2004

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

Customer Order Number: OL-11675-01

Business Ready Teleworker Design Guide

Preface

This design guide presents a series of design and implementation chapters intended to facilitate the creation of scalable and secure *Business Ready Teleworker* environments. The purpose of this guide is to set expectations and make recommendations so that the quality of services delivered over broadband remains usable during the worst-case situations—rather than to encourage the network managers to implement a configuration that becomes a source of frustration to the user and a support burden to the help-desk staff.

Scope

In general, this publication is split into two primary "parts" with relevant chapters addressing content specific to each part. The following summary provides an outline of the chapters presented in each part. Chapter 1, "Business Ready Teleworker Design Guide Introduction" is presented to provide an overall context for the remainder of the publication.

Part 1—Business Ready Teleworker

- Chapter 2, "Business Ready Teleworker VPN Solution Overview"
- Chapter 3, "Business Ready Teleworker CPE Deployment Models"
- Chapter 4, "Business Ready Teleworker Deployment Guidelines"

Part 2—Voice and Video-Enabled Virtual Private Networking (V^3PN) for Business Ready Teleworker

- Chapter 5, "V3PN for Business Ready Teleworker Solution Overview"
- Chapter 6, "V3PN for Business Ready Teleworker Broadband Issues"
- Chapter 7, "V3PN for Business Ready Teleworker Planning and Design"
- Chapter 9, "V3PN for Business Ready Teleworker Product and Performance Data"
- Chapter 8, "V3PN for Business Ready Teleworker Implementation and Configuration"
- Chapter 10, "V3PN for Business Ready Teleworker Verification and Troubleshooting"
- Appendix A, "V3PN for Business Ready Teleworker Solution Testbed Network Diagram"
- Appendix B, "ToS Byte Reference Chart"
- Appendix C, "Additional Performance Data Configuration Examples"
- Appendix D, "Sample Deployment"

Target Audience

This design guide is targeted for Cisco Systems Engineers, Customer Support Engineers, Cisco Partner technical support staff, and customer network support staff. It provides guidelines and best practices for Business Ready Teleworker network deployments.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can email your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Business Ready Teleworker Design Guide Introduction

This introductory chapter presents a high-level overview of the *Cisco Business Ready Teleworker* solution. Specific sections presented in this chapter:

Solution Introduction

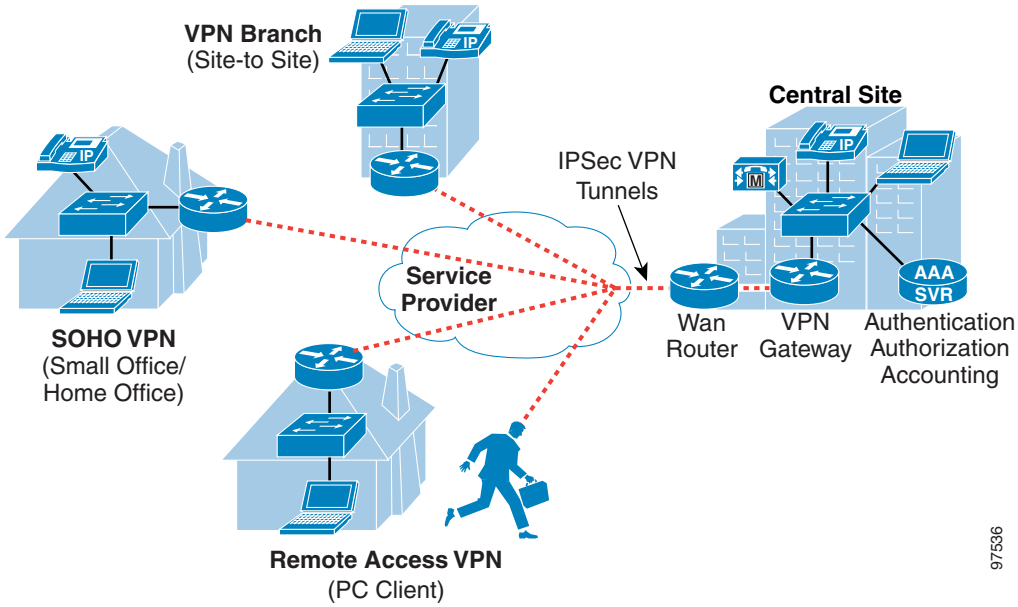
This guide provides information for deploying secure teleworker solutions supporting quality voice and data services. The focus is on the teleworker home office—the residential portion of the Small Office/Home Office (SOHO) deployment. This guide emphasizes:

- Defining the safe boundaries in which this solution may be deployed—including design and implementation considerations and caveats. Setting these boundaries will help set proper expectations early on in the planning process.
- Providing hardware platform and software code recommendations for a given deployment.
- Including or referencing performance and configuration information.

Because an IPSec Virtual Private Network (VPN) deployment involves a service provider, this document differentiates between requirements that enterprises and service providers must provide in order to ensure a successful voice over IP (VoIP) via IPSec VPN deployment.

The solution addressed in this guide extends the benefits of Cisco Architecture for Voice, Video and Integrated Data (AVVID) from enterprise sites to teleworker homes in a secure manner—and enables applications such as voice and video to be extended to home office environments using Cisco Voice and Video Enabled IPSec VPN (V^3PN) technology. This solution makes the teleworker home a functionally transparent extension of the enterprise and allows family Internet access—while protecting the enterprise network. Figure 1-1 illustrates this solution along with other remote access options.

Figure 1-1 VPN Deployment Models



Included in this guide are requirements, planning and deployment considerations, caveats and sample configurations. The technologies discussed include:

- IPSec VPNs
- Firewalls
- Quality of Service (QoS) methods

The purpose of this solution guide is to provide best practices for successful deployment of a teleworker secure voice and data network for the enterprise.

V^{3}PN for Business Ready Teleworkers

Home offices are increasingly relied upon by enterprises for connectivity of day-extenders, part-time teleworkers, and full-time teleworkers. In order for these workers to be optimally productive, they require access to the same services used at the corporate site, including data, E-mail, collaboration tools, and voice and video services.

To provide these capabilities, Cisco designed the Business Ready Teleworker solution for delivering Cisco V^{3}PN over broadband access services—such as cable and digital subscriber line (DSL). The result is an end-to-end VPN-based service that can guarantee the timely delivery of latency-sensitive applications (voice and video) to home offices in a cost-effective and reliable manner.

Solution Benefits

The Business Ready Teleworker solution offers benefits for both enterprises and service providers. These are summarized separately in the following general sections:

Business Ready Teleworker Benefits

Organizations are constantly striving to reduce costs, improve employee productivity, and keep employees within the organization. These goals can be furthered by providing employees the ability to work from home with similar quality, function, performance, convenience and security as are available in the office. Employees who are occasional or full-time teleworkers require less office space. By providing a work environment in the residence, employees can optimally manage their work schedules, allowing for higher productivity (less affected by office distractions) and greater job satisfaction (flexibility in schedule). This transparent extension of the enterprise to employee homes is the objective of the Business Ready Teleworker solution.

The capabilities addressed in this publication highlight enterprise benefits:

- A teleworker can access the central-office IP Telephone system from home with comparable voice quality, and can thereby take advantage of the higher function IP Telephony capabilities—instead of using the public switched telephone network (PSTN). This reduces PSTN costs.
- Since the IP handset at the teleworker home has all the capabilities of the enterprise handset, the user can share the same extension and applications as their office phone. Using IP for business calls also frees the home plain old telephone service (POTS) line for family use.
- With broadband cable or DSL, users can achieve similar response times for web applications, E-mail downloads and telephony.
- The solution includes strong firewall and VPN ability in the SOHO network equipment; this provides an additional layer of security for all networked personal computers in the home.
- Plug-and-play installation—The user has only to connect the VPN device into the SOHO network and perform a minimal set of operations. No further action is needed by the user on the device(s).
- Family members can access the Internet while the teleworker accesses enterprise telephony and data applications using the same broadband connection. Voice takes precedence over data.
- Employees or temporary workers can be brought on-line with reduced startup costs.

Enterprises are considering decentralizing their operations and converting many employees to full time teleworkers. Since these employees require full office functionality, such as IP telephones, networked printers, and high bandwidth for data, the SOHO VPN model meets their needs more appropriately than the Remote Access VPN.

To summarize the benefits of the teleworker voice and data solution, this solution extends the advantages of VPNs (such as cost savings, data application support, extended availability, security, and privacy) to provide secure enterprise voice services to full-time and part-time teleworkers.

V3PN Benefits for Business Ready Teleworkers

From an enterprise perspective, benefits derived from an V3PN for Business Ready Teleworker implementation fall into the following five categories:

Increased Productivity

On average, employees spend 60 percent of their time or less at their desks, yet this is where the bulk of investment is made in providing access to corporate applications.

Providing access to corporate applications in the home office for just four additional hours each month for 100 employees can result in more than $21,000 productivity savings per month.

Business Resilience

Employees can be displaced from their normal workplace by natural events (such as winter storms, hurricanes, or earthquakes), health alerts (such as SARS), man-made events (such as travel restrictions or traffic conditions), or simply by family-related events such as sick children or home repairs. These disruptions can significantly impact an organization's processes.

Providing employees with central-site equivalent access to applications and services in geographically dispersed locations (such as home offices) creates a built-in back-up plan to keep business processes functioning in unforeseen circumstances.

Cost Savings

A traditional remote worker set up involves toll charges for dial-up and additional phone lines. Integrating services into a single, broadband-based connection can eliminate these charges while delivering superior overall connectivity performance. These savings alone can pay for any initial investment associated with the Business Ready Teleworker solution.

Security

Demands for access to enterprise applications outside the campus are stretching the limits of security policies. Teleworking over VPNs offers inherent security provided by encryption of all traffic, including data, voice and video.

Also critical is integrating firewall and intrusion detection capabilities, as well as a finding ways to easily accommodate both corporate and personal users who share a single broadband connection (the *Spouse-and-Child* concern).

Employee Recruitment and Retention

In the past, enterprises recruited employees in the locations where corporate offices were located. It can be difficult to find the right skills and have them in the right cities—or to find resources willing to relocate. Today, Enterprise organizations need the flexibility to hire skilled employees where the skills exist, and to integrate remote workers into geographically dispersed teams with access to equivalent corporate applications.

Service Provider Benefits

For service providers, the teleworker solution offers a growing, profitable, deployable and manageable multi-service VPN offering. It is a competitive differentiator. As an example, industry analysts predicted that while the majority of DSL circuits are for consumer residential usage, the majority of DSL revenue comes from business circuits. This is due to the higher monthly costs which enterprises are willing to pay for an enhanced service.

A secure teleworker Cisco AVVID solution requires capabilities that combine to provide a valuable service to enterprises: basic quality network access; secure VPN; and, multi-service support. The service provider can bill for each of these services. In addition, each of these can be offered as a managed service, allowing for varying combinations and options for enterprises. For example, an enterprise might buy teleworker Cisco AVVID services with a service provider-managed circuit and VPN, but manage the IP Telephony application internally.

For service providers that also offer enterprise network design and implementation, an enterprise teleworker solution allows the advantages of Cisco AVVID solutions to be extended to employee residences. Enterprises will value a Cisco AVVID solution even more when the capabilities are available anywhere at any time.

Enterprises and service providers will be interested in the added value of network and firewall functions handled by hardware versus PC software at the SOHO site, not only for the greater performance and capability, but for the lower cost of installation, maintenance, and support. When service providers can provide end-to-end QoS, it will be possible to use this solution to support distributed call centers, allowing enterprises to provide full services without having to maintain large centralized enterprise service operations.

Solution Scope

This design and implementation guide focuses on residential broadband interface to the service provider —typically media such as asymmetric DSL (ADSL), cable, Integrated Services Digital Network (ISDN), and wireless.

This guide also focuses on the use of Cisco IOS to terminate the IPSec VPN tunnels at the SOHO. Cisco PIX 501 and Cisco VPN 3002 may also be used in one specific model (Dual Unit) as will be described in Chapter 3, “Business Ready Teleworker CPE Deployment Models.”

In addressing V^3PN for Business Ready Teleworker requirements, this design guide focuses on:

- A deployment model in which the interface to the service provider is typically a broadband media such as cable or DSL.
- Cisco IOS VPN routers to terminate the IPSec VPN tunnels. While the Cisco PIX and Cisco VPN 3000 Concentrator products can support the transport of voice and video over IPSec, they do not provide the full feature set necessary to support Business Ready Teleworker—in particular, QoS.

The topics of authentication, deployment, management, and security are all critical for an Business Ready Teleworker deployment. This design guide focuses on the V^3PN aspects of the solution. Other design guides cover the remaining topics.

IPSec with Dead Peer Detection (DPD) and Reverse Route Injection (RRI) was the primary topology evaluated.

Other features that were not evaluated for this revision of the design guide include:

- IP Multicast
- Dynamic Multipoint VPN (DMVPN)
- Advanced Encryption Standard (AES)

Public and Private IP Addressing Conventions

This publication addresses the interface between public and private address spaces typically found when interconnecting teleworker home networks to enterprise networks through an ISP over VPN.

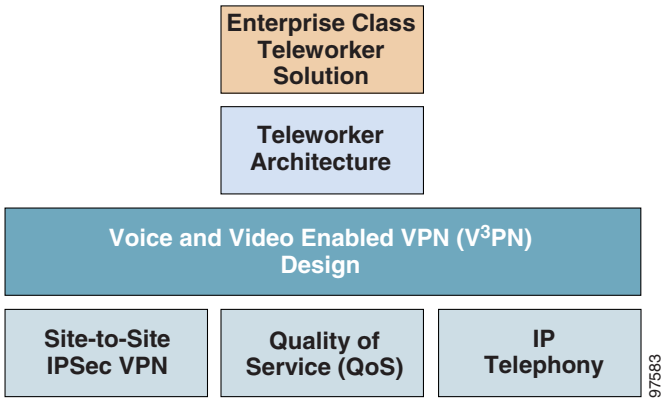
For illustration purposes, private networks (teleworker home networks) are presented here with assigned addresses in the Class C private space (192.168.0.0 to 192.168.255.255), while enterprise and ISP networks are presented with assigned addresses in the Class A private space (10.0.0.0 to 10.255.255.255) or with variables specified in the high-order address fields (such as XX.YY.123.123).

In real-world production networks, the enterprise address space would be a "legal" private address range. Cisco Systems uses private network addressing schemes in all documentation.

Supporting Designs

The Business Ready Teleworker solution is based on several supporting technologies and designs (see Figure 1-2). In an effort to minimize overlap and repetition, this guide will focus on the unique aspects of the solution and refer to supporting design guides when appropriate.

Figure 1-2 Underlying Business Ready Teleworker Design Foundation



One key related solution guide is the *Voice and Video Enabled IPSec VPN (V^3PN) Solution Reference Network Design (SRND)* guide covering the combination of Cisco IPSec VPN, Quality of Service (QoS), and IP Telephony technologies.

This content found within this guide focuses on specific issues of deploying IPSec encrypted VoIP using residential broadband service providers as transport. The reader should view content found here as a guidelines for including access media (cable and DSL) to V^3PN deployments. As such, it is expected that the reader be familiar with the concepts covered in related guides. Where appropriate, and to provide particular emphasis, these guides will be referenced in the text.

In addition, V^{3}PN is designed to overlay non-disruptively on other core Cisco AVVID designs. Relevant content includes the following:

- *Cisco AVVID Network Infrastructure Data-only Site-to-Site IPSec VPN Design*, available at:

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns142/c649/ccmigration_09186a00800d67f9.pdf

- *Cisco AVVID Enterprise Quality of Service Design*, available at:

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns17/c649/ccmigration_09186a00800d67ed.pdf

- *Cisco IP Telephony Solution Reference Network Design(s)*, available at:

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns268/c649/ccmigration_09186a008017bb4a.pdf

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns230/c649/ccmigration_09186a00800d6805.pdf

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns268/c649/ccmigration_09186a00800d6802.pdf

This guide does not cover these technologies in any detail, but will instead focus on the intersection, integration, and interactions of these functions on the network—as it applies to the Business Ready Teleworker solution.

Familiarity with design and implementation guides for underlying technologies is extremely beneficial to the reader. Please review the above mentioned guides before attempting to implement an Business Ready Teleworker design based on V^{3}PN.

The underlying VPN design principles are based on the SAFE VPN Architecture. Cisco SAFE documentation can be found at:

http://www.cisco.com/go/safe

Technical Assistance Center (TAC) Technical Tips are a valuable source of configuration examples for the technologies deployed in this design guide. Please refer to the Technical Tip section after logging on the TAC homepage at:

http://www.cisco.com/tac

Cisco Systems

PART 1

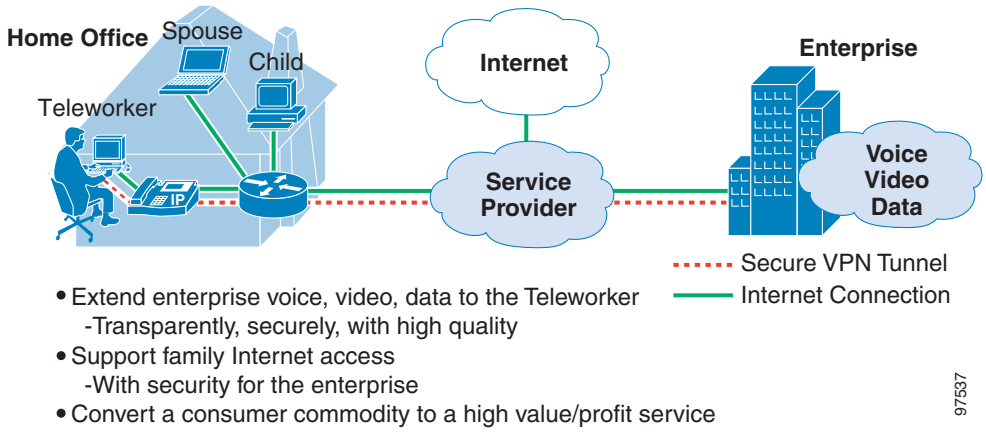
Business Ready Teleworker

Business Ready Teleworker VPN Solution Overview

This chapter provides an overview of voice and data over site-to-site IPSec VPNs for small office/home office (SOHO)/teleworker environments. High-level summaries are provided for the following topics:

Figure 2-1 depicts the deployment model covered in this design and implementation guide.

Figure 2-1 Home-office Deployment



Solution Characteristics

The following are general solution characteristics for SOHO voice and data over IPSec VPN deployments:

- This design guide is based on SOHO IPSec VPNs (concentration on home office) that assume the wide-area network (WAN) media to the service provider is best effort with no link fragmentation and interleaving (LFI). This can achieve an acceptable level of voice quality—between cellular and business quality under specific conditions. As service providers offer residential broadband QoS and LFI, guidelines will be updated. For the latest list of service providers offering QoS for multi-service VPNs, please see:

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

  Select *VPN IP Multi-Service* as the type of service.

- A SOHO voice/VPN solution is a subset of V³PN. For public information on V^3PN, please see:

  http://www.cisco.com/go/v3pn/

- Secure Triple Data Encryption Standard (3DES) encrypted VoIP and data traffic can be simultaneously transported over the same IPSec VPN tunnel—with adequate QoS for IP-based voice service quality similar to a private WAN.
- The solution is based on Cisco IOS platforms for broadband access, QoS and VPN. Cisco PIX 501 or Cisco VPN 3002 may used be for VPN function with a Cisco IOS router providing QoS.
- IP Telephony traffic traversing an IPSec VPN is transparent to all users and personnel managing the IP Telephony network.
- Admission control for IP Telephony is handled the same for IPSec tunnels as a private WAN connecting two branch offices together. Admission control is based on the maximum VoIP traffic permitted across a given IPSec tunnel.
- The IPSec tunnels can be managed by the enterprise or offered by the service provider as a managed service. Such managed services can be Cisco managed VPN solutions that require VoIP transport.
- Family (home) PCs may be optionally included behind the SOHO firewall for protection.
- PCs behind the SOHO firewall/VPN can have Internet access through the VPN tunnel and provided by the enterprise, or from the SOHO directly (split tunnel). This can be granular (teleworker PC Internet access through enterprise, home PCs split tunnel). The option chosen depends on enterprise security policy.

General Best Practices Guidelines

Best practice guidelines presented here cover:

- Basic Guidelines, page 2-3
- Quality of Service Guidelines, page 2-3
- IPSec VPN Guidelines, page 2-4
- Security Guidelines, page 2-4

Basic Guidelines

Follow these guidelines in preparing for data/voice connectivity over an IPSec VPN:

- Have realistic expectations about voice quality over best-effort service provider networks if the service provider does not provide QoS.
- Investigate broadband residential circuit options available and pilot those options before selection. Choose a provider offering QoS *service level agreements* (SLA), or if not available, the most-capable, best-effort provider (least delay, most bandwidth, greatest availability and coverage), and request QoS with a SLA often. Use the supplied selection chart in the "Choosing Broadband Access" section on page 2-18. Note that when multiple service providers are used (in the path) by an enterprise, there are additional considerations (discussed in Part 2 "V3PN for Business Ready Teleworker").
- Choose the most appropriate SOHO model, considering the number and types of residential broadband circuits, applications, security policies, and management. Use the supplied selection chart in the "Which Model to Choose" section on page 2-14.
- Plan ahead for a subnet (such as /29 or /28) or a single IP address (if using Easy VPN client mode) per SOHO, plan route summarization, and test Domain Name System (DNS) configurations to support split-tunneled environments.
- Plan for SOHO Dynamic Host Configuration Protocol (DHCP) support at the SOHO CPE (or from a centralized DHCP server) and ensure that option 150—Trivial File Transfer Protocol (TFTP) server—for an IP Phone is included.

Quality of Service Guidelines

Follow these guidelines in preparing for support for QoS over IPSec VPN:

- Use routers with hardware encryption, or a dedicated VPN device (Cisco PIX 501 or Cisco VPN 3002) to offload the SOHO CPE performing WAN/QoS function if no hardware encryption is available.
- Traffic prioritization and shaping are required at the SOHO device performing QoS to ensure priority for voice, and to ensure that a minimum number packets are in the output queue (to minimize serialization delay).
- For best effort service provider connections, measure the maximum consistent throughput to the VPN head-end gateway and use this value for traffic shaping from the SOHO CPE.
- Existing QoS implementations might be based on more than the type of service (ToS) byte. Since packets are encrypted, using only the ToS byte is recommended for traffic classification.
- Use **adjust-mss** at a low value (536-to-640 bytes) to reduce serialization delay when TCP traffic is in front of voice. Choose an optimum value for the link (542 for DSL). This is required as LFI is not available with point-to-point protocol over Ethernet (PPPoE)—the dominant residential encapsulation option offered by service providers.
- For an Ethernet-to-Ethernet router, shape and prioritize traffic via hierarchical low-latency queueing (LLQ). Refer to http://www.cisco.com/warp/public/105/pppoe_qos_dsl.pdf.
- If the enterprise's security policies permit the use of split tunneling, using this configuration might decrease the amount of data traffic that must be encrypted. QoS configurations for split tunnel traffic are shown in Chapter 7, "V3PN for Business Ready Teleworker Planning and Design," of this guide.
- Hub-and-spoke IPSec topologies are recommended. Take into account traversing the service provider network twice if teleworker-to-teleworker (spoke-to-spoke) calls are supported.

Note Dynamic Multipoint IPSec VPNs (DMVPN) will be tested and documented in a subsequent release of this guide. DMVPN supports a simplified definition of generic routing encapsulation (GRE)/IPSec tunnels.

- Use a single (contiguous) service provider between SOHO and enterprise. Enterprises that have tunnels that traverse multiple service providers should pilot test this solution, as there are special considerations for QoS between service providers.

IPSec VPN Guidelines

Follow these guidelines in preparing for support of IPSec VPN:

- Use Encapsulating Security Payload (ESP) 3DES for encryption and ESP-Secure Hash Algorithm (SHA)-Hash-based Message Authentication Code (HMAC) for integrity.
- Use Dynamic crypto-maps to support SOHO with dynamic IP addresses and to simplify head-end VPN configuration.
- Use the appropriate SOHO site (VPN device) authentication option.
  - Digital certificates when possible
  - Internet Key Exchange (IKE) shared secret using authentication, authorization, and accounting (AAA) server, when no certificate authority is available.
  - Easy VPN for ease-of-implementation and/or single-enterprise address per SOHO, if no digital certificate support is needed, and users accept logging into the VPN device to bring up the VPN tunnel.
- Consider enterprise security policies to determine whether split tunneling or sharing a connection with home PCs is acceptable.
- For large-scale implementations, consider appropriate management tools listed in the "Management" section on page 4-38.

Security Guidelines

Follow these guidelines in preparing security for IPSec VPN connectivity:

- Configure Context-Based Access Control (CBAC) on the VPN device for strong firewall security. All recommended VPN devices include stateful firewalls.
- Plan and design to meet enterprise security policy regarding spouse/child access to enterprise. The recommendation is to configure per-user authentication (Authentication Proxy) in addition to the VPN device authentication to allow enterprise data access. IP Telephony traffic can be allowed by source or destination access lists. Spouse and child traffic and teleworker Internet traffic can be allowed through the enterprise to the Internet or be split tunneled.
- Plan and design to meet enterprise security policy regarding in-home wireless access. The recommendation is to have a written policy requiring the teleworker to use PC VPN client software when connected via wireless, or disallowing the teleworker from using wireless unless supplied by the enterprise, while providing Authentication Proxy for per-user authentication to access the enterprise network.

General Solution Caveats

Many of the site-to-site V^{3}PN caveats apply to teleworker VoIP VPNs. These include:

Basic Caveats

Deploy teleworker VoIP VPN implementations with the following data and voice caveats in mind:

- The experience with providing multiple enhanced functions to teleworker devices is at an early stage. Specific pilots are recommended to ensure required features are available on the platform implemented and Cisco IOS level deployed.
- For the Cisco 800 series routers, different Cisco IOS levels vary in their support of QoS options. The "Software Releases Evaluated" section on page 9-9 summarizes the code levels and feature sets recommended.
- For ADSL circuits, the dominant encapsulation of PPPoE does not support LFI. With appropriate expectations, design and testing, it is possible to achieve voice quality between cellular wireless and toll quality. Depending on the model, configurations might require specific configuration techniques. Two examples are: implementing a service policy on the permanent virtual circuit (PVC) of an ADSL router when using PPPoE (even though the interface has no IP address); and, defining hierarchical shaping and prioritization using the modular QoS command-line interface (CLI). Examples can be found at:
  - www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt8/qcfmcli2.htm
  - www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt4/qcfcbshp.htm
- Due to processing and performance requirements, only the devices listed in Chapter 4, "Business Ready Teleworker Deployment Guidelines" are recommended, and only for the functions listed. The use of Cisco Unity VPN client and Cisco IP SoftPhone are *not recommended* at this time, due to the inability of the VPN client to carry forward the IP precedence value set by IP Softphone to the encrypted packet header.
- All telephony features should be pilot tested before deployment. While basic calling might function, advanced functions—such as conference calling—might require additional design or configuration to operate well.

QoS Caveats

Deploy teleworker VoIP VPN implementations with the following QoS caveats in mind:

- For cable, if DOCSIS 1.1 is not available, use the Integrated Unit + Access Device model and shape the Cisco 831 uplink rate less than the upstream trained rate. Without DOCSIS 1.1, cable is a best-effort service. Currently, the Cisco uBR 905 does not support DOCSIS 1.1 and does not properly shape traffic out the cable interface.
- The definition of QoS for traffic classes in a service policy includes the bandwidth needed at the IP layer. For ADSL, there can be 25 percent Layer-2 overhead.
- If a non-recommended SOHO device is used, voice quality might be unacceptable. An example is a dual-unit design where the WAN/QoS routers cannot support real-time prioritization and scheduling. Another example is an Integrated Unit + Access Device model design with spouse and children PCs connected on the access device along with the VPN/QoS device. Non-teleworker traffic might consume the bandwidth while teleworker data and voice suffer. The VPN/QoS device would contend with the spouse and children PCs, as the access device (dumb modem or non-QoS router) does not prioritize the teleworker traffic.

IPSec VPN Caveats

Deploy teleworker VoIP VPN implementations with the following general IPSec VPN caveats in mind:

- When the VPN function is on an Ethernet-to-Ethernet device with a DSL/cable router in front (Dual Unit model), configure IPSec to use ESP-SHA-HMAC authentication versus Authentication Header (AH)-SHA-HMAC. Use this configuration because Network Address Translation/Port-level NAT (NAT/pNAT) is commonly used. AH protects the IP header, which is manipulated by NAT/pNAT. The packets will not pass the integrity (hash) check when received by the head-end VPN device.
- Allowing teleworker PCs to access Internet sites directly (without traversing VPN) improves response and reduces the load on enterprise VPN gateway, but might not be allowed by enterprise security policy. In addition, if there are discontiguous or multiple networks at the enterprise, scalability of the teleworker VPN device or VPN head-end gateway must be considered.
- If IP Softphone is required for SOHO telephony (and Easy VPN is used), *network extension mode* must be used. Client mode uses pNAT across the VPN. IP Softphone uses Computer Telephony Integration (CTI) for signaling, which includes IP addressing in the payload. Cisco IOS does not support adjusting the payload with Port Address translation as it does for H.323.
- If access to servers located at SOHOs is needed, and Easy VPN is used for IPSec, use an Easy VPN remote network extension mode at the SOHO and a static DHCP entry for the SOHO server so that the server is given the same IP address and is accessible from the enterprise.

Security Caveats

Deploy teleworker VoIP VPN implementations with the following security caveats in mind:

- The use of in-home wireless requires careful coordination with enterprise security policy, and might limit in-home wireless usage to the teleworker PC or to the non-teleworker PCs (not both).
- The split tunnel design might require special DNS configuration if the enterprise uses Hypertext Transfer Protocol (HTTP) proxies and an enterprise authoritative DNS. All name resolution will send traffic through the enterprise in this case, thus Internet traffic will not be split-tunneled. Options include not split tunneling or providing separate enterprise DNS servers for teleworkers.

Solution Technology Components

The teleworker secure voice and data solution is a combination of existing VPN and IP Telephony solutions, with additional elements to deliver their joint characteristics to the SOHO. A brief overview of VPN and IP Telephony is followed with the specifics of SOHO.

Virtual Private Networks

VPNs are used to provide secure communications across non-secure networks. Users accessing enterprise services across the VPN have the same functions as when they would in the office. The common reasons for VPN use are:

- Cost savings—Internet connection costs less than private-line access.
- Flexibility—VPN makes it easy to change site locations or bring up new sites.
- Mobility—Users can securely connect to their network using any Internet connection. Mobility is not applicable to teleworker SOHO implementations.

The challenge to achieving the benefits in the "Solution Benefits" section on page 1-3 is that voice payload and signaling traffic must be encoded, encrypted, transmitted over the service provider public network, decrypted, and decoded—all with consistently short delay and low loss.

There are two types of VPNs: site-to-site and remote-access (usually a PC Client).

Site-to-site VPNs provide a relationship between two network devices to forward encrypted traffic between networks. Usually, the two devices are peers and either can create the VPN tunnel. This is used between two enterprise sites, or an enterprise site to branch office. Encrypted voice and data are supported. Below are a few characteristics for site-to-site VPNs:

- Supports multiple devices using a single VPN tunnel from a static location (such as a home)
- No dependence on the types of operating systems on SOHO end systems
- Used for SOHO sites using routing protocols, multicast applications, or non-IP transport that must be sent over the VPN via encapsulation methods such as GRE
- Supports high-security deployments using digital certificates without user authentication
- Used for high-availability scenarios where multiple SOHO CPE devices using routing protocols and GRE to provide automatic fail-over
- Configured with at least some knowledge of each other's existence, either within configurations (using RADIUS), or by sharing common access to a certificate authority

Remote access VPNs allow a user to connect securely from anywhere there is appropriate Internet or service provider access. The VPN tunnel is created between an enterprise network device (VPN gateway) and a user VPN client (usually software on the laptop). The relationship between the enterprise VPN device and the VPN client is master-slave. The VPN client requests the VPN tunnel, while the definitions and control are in the VPN gateway. This solution guide does not address remote client VPN. Below are a few characteristics for remote client VPNs:

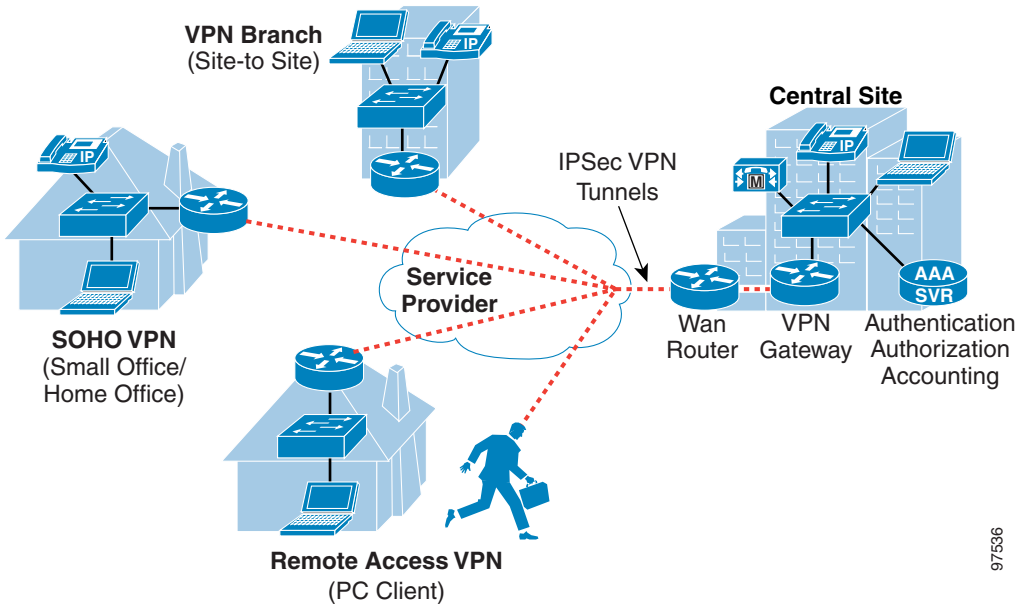
- Used for large numbers of remote users who might connect from different locations
- A user database (such as RADIUS, NT, SecureID) must exist, often for dial-in users
- Provides individual SOHO VPN user authentication (user must log in to connect every time)

Although it might be feasible to use remote access VPNs for teleworker encrypted voice and data, this configuration has not as yet been verified, and thus cannot be recommended at this time. Supporting encrypted voice with remote access VPN requires that the teleworker have both a Cisco VPN client and

Cisco Softphone installed on a PC powerful enough to support them. Additionally, tests show that the Cisco Unity VPN client does not carry forward the IP ToS marking into the encrypted packet header. Even though the SoftPhone software sets the ToS byte to IP precedence 5 for payload, the VPN client sends all encrypted packets from the PC with ToS byte to 0. The teleworker device providing QoS cannot classify the voice packets for priority delivery.

Business Ready Teleworker VPNs are site-to-site VPNs. The teleworker environment supports multiple devices (IP phones, enterprise user laptop, home PCs accessing the Internet) and is similar to a small branch office. Unlike many site-to-site VPNs, the main site generally does not request the VPN tunnel to the SOHO, and fewer definitions in the SOHO devices are preferred for easy and scalable implementation. This solution guide is focused on teleworker VPN. Figure 2-2 depicts the VPN deployment types.

Figure 2-2 VPN Deployment Models



VPNs can be delivered via function in the enterprise network equipment (main site, branch/SOHO site or PC) referred to as *enterprise-based VPNs*, or via service provider equipment (VPN created in central office VPN hardware/routers). In the latter category, the VPN function is performed in the service provider access or aggregation devices, so that the enterprise devices are off-loaded from the management and processing of IPSec. This solution guide assumes enterprise-based VPNs.

For enterprise-based VPNs, the management of VPN-related devices can be done by the enterprise itself or can be out-sourced to a service provider. Granularity in management is possible. For example, a service provider might offer management (monitoring, alerting, reporting) of DSL or cable lines to the SOHO, with the enterprise managing the devices. A second option is for the service provider to offer a service that adds monitoring, alerting and reporting of the main site and SOHO network devices, while the enterprise controls configuration and security policy. A third option is for the service provider to manage all three areas (lines, network devices, and VPN configurations/policy).

IP Telephony

IP Telephony is the convergence of traditional voice and data into a single system. This includes integration of the infrastructure (such as networks), applications (such as mail systems), and end devices (such as phones). The general architecture and benefits of IP Telephony are widely accepted, and IP Telephony is being implemented in many enterprises. Details on IP Telephony can be found at:

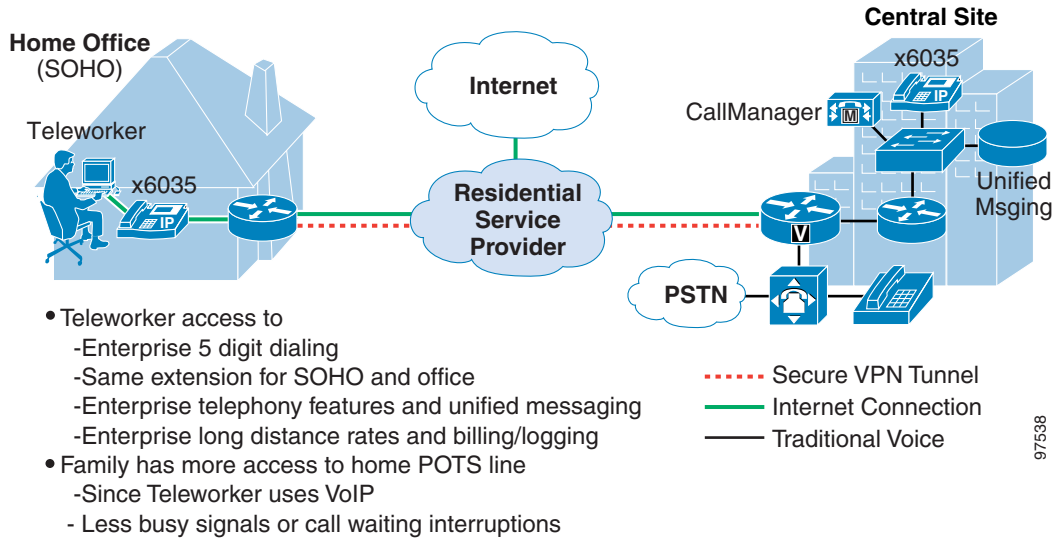
http://www.cisco.com/warp/public/779/largeent/learn/technologies/IPtelephony.html

The functions of a traditional voice system—such as a private branch exchange (PBX)—are distributed in an IP Telephony environment, allowing for cost savings, improved availability, and flexible changes and growth. The Cisco CallManager server handles call control/processing. Line (handset) connections are Ethernet, thus integrated with the data network.

Trunk connections to the PSTN or PBX are traditional analog or digital lines, made via a Cisco IP-to-time division multiplexing (TDM) voice gateway. Many Cisco routers and switches have this ability via plug-in modules. Trunk connections to IP Telephony systems are any appropriate IP connection, thus integrated with the data network.

The teleworker requires an IP phone connected to a SOHO Ethernet LAN and appropriate IP connectivity to the enterprise central site. The CallManager at the central site controls all voice features, so no configuration or administration is required at the SOHO phone. Voice packets however flow from the SOHO phone to the actual end IP Telephony device. For example if two teleworkers are communicating, the voice path is directly between the two SOHO phones through the VPN. If a teleworker is communicating with a caller on the PSTN, the voice path is between the teleworker IP phone and the Cisco VoIP gateway. In Figure 2-3, the VoIP gateway is the router connected to the PBX for PSTN access. A higher compression codec can be used for the IP Phone to conserve bandwidth on lower speed residential access lines. The teleworker phone and the central site phone can share the same extension regardless of codec. The teleworker phone can call other IP phones or the PSTN via an VoIP gateway, since these can support multiple codecs.

Figure 2-3 IP Telephony Teleworker Benefits



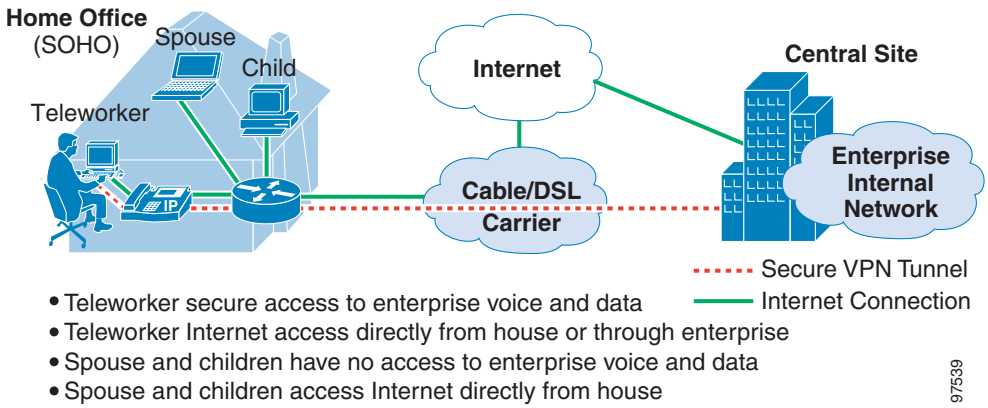
In Figure 2-3, the central site router performs WAN connection, VPN gateway, QoS and PSTN gateway functions.

These functions can be combined as shown, or separated among multiple devices depending on the router model.

Small Office/Home Office

The SOHO residence addressed in this design guide includes multiple devices that can connect to the home LAN. These include the teleworker enterprise laptop or PC, teleworker IP handset (teleworker devices), and spouse or children PCs (home devices). Both teleworker devices and home devices require some basic services, such as NAT when accessing the Internet directly, DHCP to be dynamically addressed, and basic firewall security from the Internet. There are also services or types of access available to the teleworker devices that are not available to the home devices, such as access to enterprise data and telephony. The QoS available to teleworker devices is also different. Enterprise voice traffic is prioritized over all data traffic. Figure 2-4 depicts the teleworker secure voice and data SOHO environment.

Figure 2-4 teleworker SOHO with secure IP Telephony



Below are additional characteristics of the SOHO for teleworker secure voice/data:

- There is typically a single logical path (virtual circuit, cable channel, ISDN B-channel PPP bundle) provisioned to the SOHO that transports both best-effort data and real-time traffic.
- At the SOHO end of the connection, there can be as little as a single workstation, or there can be several network devices, such as workstations, servers, printers, and IP telephones.
- The VPN is built between a specific SOHO device and a VPN termination device at the corresponding enterprise network.
- The SOHO network connects to the Internet via one of a number of possible broadband access devices, such as cable, DSL, or ISDN. The broadband access device (connects the SOHO LAN to the DSL/cable line) and the SOHO VPN device (provides the IPSec tunnel for secure connection to the enterprise) can be separate or can be integrated into a single device.
- The SOHO VPN device has an Ethernet interface to the SOHO LAN.

General Deployment Models

There are three different models for SOHO deployment for this solution. Each provides a distinct benefit, meets a constraint, or fits a service provider deployment model. The three models are:

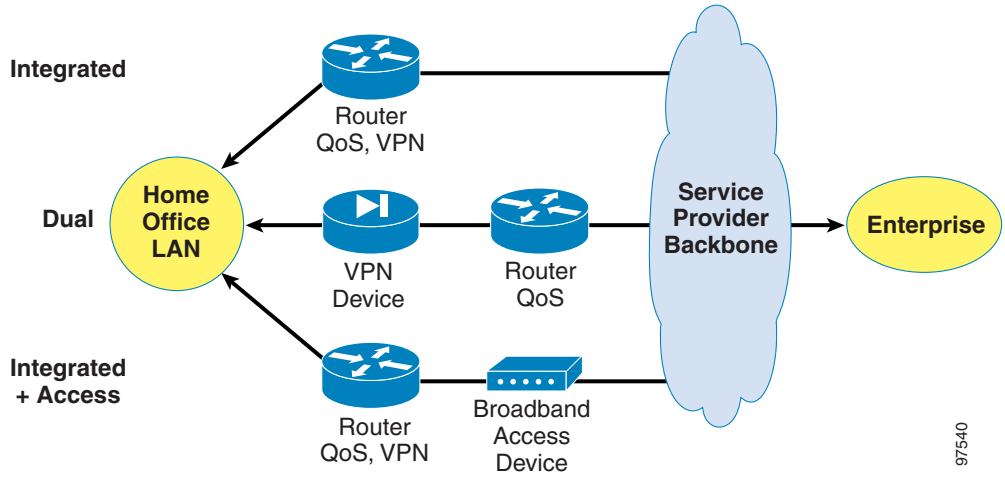
- **Integrated Unit**—Single router with all functions.
- **Dual Unit**—Router with QoS, broadband access, basic services; VPN device with VPN, security, and basic services.
- **Integrated Unit + Access Device**—Router with all functions except broadband access; the router connects via Ethernet to a broadband access device (bridges Ethernet to DSL/cable) for Internet access.

Each of the deployment models must provide the following services required for teleworkers:

- Basic Services— NAT/pNAT, DHCP, IP routing, multiple Ethernet connections for SOHO devices, and broadband connection (attachment to the WAN circuit cable, DSL, ISDN, or wireless).
- QoS—Real-time classification, prioritization, forwarding and shaping of traffic.
- VPN/Security Services—Encryption of traffic to the main site; firewall function for the SOHO.

In each of the three models, a Cisco IOS-based router provides QoS functionality. Figure 2-5 depicts the models and is followed by a description of each.

Figure 2-5 General Home Office Deployment Models



Integrated Unit

This model is a single device (router) capable of providing QoS for voice, VPN/security, and basic services including broadband connectivity.

Advantages include:

- Single device deployment and management
- Adaptability for service provider fully managed services (transport, QoS, IP Telephony application)
- Potential cost savings

Challenges include:

- Availability of a single device at an appropriate cost, with the features and performance required
- There might not be a single unit for some broadband access circuit types (ISDN and wireless).

This model is the best choice for DSL or cable fully managed services.

Dual Unit

This model consists of a VPN device that provides VPN/security services and basic services, and a router that provides QoS and basic services (including broadband access and NAT). The VPN device is a Cisco 831 as this offers the Cisco IOS CLI for consistency in function and configuration, high VPN performance via hardware encryption acceleration, firewall function, and built-in 10/100 switch ports. As an alternative, Cisco PIX 501 or Cisco VPN 3002 may be used.

Advantages include:

- Granularity of Managed Services—Service providers can manage broadband access while enterprise manages VPN/security and private network addressing, since these are two different units.
- Media Independence—Since the VPN/security device is separate from the router connecting the broadband circuit, the same VPN device can be used for cable, DSL, wireless, and ISDN by changing the router model or module in the router. This is especially valuable if one enterprise must support teleworkers with different broadband circuit types (such as DSL, cable, and ISDN).

- Superior Capability—Best of breed function and performance due to devices with dedicated function.

Challenges include:

- Packaging two units for deployment
- Ongoing management of two devices
- The cost for two devices

This model is the best choice where the service provider manages the circuit and associated CPE, while the enterprise manages the VPN.

Integrated Unit + Access Device

This model can be implemented in one of two ways:

- One solution consists of a router that performs all functions except for broadband access via the circuit. Integrated Unit + Access Device is useful when a specific broadband interface type is not available on the router. An example might be when broadband cellular wireless becomes available and there is no router with that interface available—a non-intelligent Ethernet-to-wireless bridge could be used to connect the router to the cellular wireless network.
- Another scenario would involve a non-intelligent broadband device that is already provisioned at the SOHO (some service providers require use of their access device).

Advantages to this model include:

- Use of existing broadband access device/circuit (cost savings and simplified provisioning)
- Use of the solution where no router interface is available for a specific broadband circuit type
- Might reduce cost of implementing the solution in existing SOHOs

Challenges include:

- The integration of the circuit characteristics through the non-intelligent access device. Since the router is responsible for QoS, it has responsibility for sending traffic at a rate and packet size that ensures low delay across the broadband circuit. In this model, the router does not control or see the circuit. This makes traffic shaping and LFI (if needed) more difficult.
- Troubleshooting a problem is more difficult when the broadband access device (often called a broadband modem) is not intelligent and cannot be queried, managed or controlled.

This model is the best choice for provisioning across multiple access circuit types and when the service provider supports a limited or non-intelligent access device.

Which Model to Choose

There are many factors in determining which model is best for an enterprise. Table 2-1 lists the three models and 10 top factors; X indicates that a model accommodates a factor well. Definitions of the factors follow Table 2-1.

Table 2-1 Top 10 Factors in Home Office Model Selection

Factor	Integrated Unit	Dual Unit	Integrated Unit + Access Device
Low Cost (less than $1000)	X		X
Simpler Deployment	X		X
Simpler Management	X		
Totally Managed Service	X		
Managed Service Options		X	
Limited Service Provider CPE Support (non-Cisco)			X
Support Multiple Circuit Types			X
High Performance with QoS	X	X (Except ISDN)	X (Cisco 831 or Cisco 1711/1712)
Strong Security	X	X	X
SOHO LAN Switching	X (Cisco 837 only)	X	X (Cisco 831 or Cisco 1711/1712)

Factors:

- Low Cost—Price of SOHO network equipment is cost effective for teleworker deployment.
- Simpler Deployment—Can be easily staged and drop shipped, or uses GUI or other tools for setup.
- Simpler Management—Reduced processing, data and bandwidth consumption; highly scalable.
- Totally Managed Service—Can be offered by a service provider with circuit, router, and VPN management.
- Managed Service Options—Can be offered by an service provider with just circuit and router management, or just VPN management, and enterprise managing VPN or router.
- Limited Service Provider CPE support—Service provider only supports non-intelligent access devices which do not provide for QoS or manageability.
- Support Multiple Circuit Types—Solution is configured similarly (VPN, firewall) regardless of residential broadband circuit type (DSL cable, ISDN, or wireless).
- High Performance with QoS—IPSec 3DES performance equal to residential broadband speeds (~2Mbps).
- Strong Security—Firewall capable of granular filtering, CBAC, inspection of all traffic without major performance impact, and intrusion detection system (IDS) support for many signatures.
- SOHO LAN Switching— Availability of built-in 10/100 switched Ethernet ports for SOHO device connection.

Broadband Access Technologies

In the U.S., there are four available broadband access types for SOHO. ADSL and cable dominate. ISDN, due to per minute cost, is used less. However, ISDN flat rate is becoming available which will make ISDN a good option for areas where ADSL or cable is not available. Last mile wireless is a new option. DSL, cable and ISDN options are summarized briefly in the following sections:

Broadband technology implementation considerations are summarized in the following sections:

Digital Subscriber Line

DSL service features a dedicated access circuit and offers a service similar to Frame Relay or Asynchronous Transfer Mode (ATM), in which a single permanent virtual circuit (PVC) is provisioned from the SOHO to the service provider aggregation point. DSL has a variety of speeds and encoding schemes. Most service providers today offer residences ADSL with a single best-effort PVC using PPPoE encapsulation. In DSL networks, delay and jitter are very low, but are not guaranteed. Since PPPoE is used, no LFI is available in service provider DSL networks. Residential access speeds are generally 128-to-384 Kbps upstream and 608 Kbps-to-1.5 Mbps downstream. In the future, QoS at Layer 2 might be available across service provider networks, using familiar ATM variable bit-rate (VBR) definitions. With ATM, attention is required to cell overhead.

ADSL provides for asymmetric speeds (downstream greater than upstream). Due to low cost, reasonable reach, and varying rates, ADSL is the prevalent DSL variant in use for residences. For ADSL upstream speeds below 256 Kbps, G.729 VoIP codecs are recommended.

Single-pair High Bit-rate DSL (G.SHDSL) is the new high speed standard for business DSL. Most residences will continue to be served by ADSL, while small business and branch offices will use G.SHDSL. Existing symmetric DSL (SDSL) deployments might be available to teleworkers until service providers upgrade those services to ADSL and G.SHDSL. G.SHDSL offers varying rates controlled by the service provider; the upstream and downstream rates are the same speed (symmetric). G.SHDSL is seen as an eventual replacement for T1s in the U.S, and will become increasingly available from more service providers. Table 2-2 summarizes DSL technologies and their characteristics.

Table 2-2 xDSL Technologies and Characteristics

DSL Technology	Maximum Data Rate Down/Uplink (bps)	Line Coding Technology	Baseband Voice?	Maximum Reach (feet)	Key Attributes
VDSL (Very High Bit Rate DSL)	51 to 55 M/1.6 to 2.3 M 13M/1.6. to 2.3M	TBD	No	1,000 5,000	Very fast, short reach
G.SHDSL (Single Pair High Bit Rate DSL)	2.3M/2.3M Multi-rate	OPTIS	No	26,000	Multi-rate, multi-service, extended-reach, and repeatable, two-wire

Table 2-2 xDSL Technologies and Characteristics

DSL Technology	Maximum Data Rate Down/Uplink (bps)	Line Coding Technology	Baseband Voice?	Maximum Reach (feet)	Key Attributes
HDSL (2 lines for T1)	768K/768K	2BIQ	No	10,000	Both replaced by G.SHDSL, two-wire
HDSL2	1.5M/1.5M	OPTIS	No	10,000	
ADSL	8M/1M Multi-rate	CAP, DMT, G.lite	Yes	18,000	Coexists with (POTS); technology of choice for residential, two-wire
SDSL	768K/768K	2BIQ/CAP	No	21,000	Symmetric, multi-rate; replaced by G.SHDSL
IDSL (ISDN-based DSL)	144K/144K	2BIQ	No	18,000, 45,000 with repeaters	Distance, might be able to use existing CPE

Cable

Cable offers a shared service with symmetric speeds varying from 100 Kbps-to-4 Mbps. In the past, the delay and jitter varied greatly and cable was not suitable for packet voice. With the new cable Data-over-Cable Service Interface Specifications (DOCSIS), more intelligent cable modems and routers are able to provide Layer-2 traffic shaping for transmission into the cable network. Although the circuit and frequencies are physically shared, access to the medium can be controlled by the head-end so that a device can be guaranteed specified bandwidth.

CPE configuration information is downloaded from a Cable Modem Termination Shelf (CMTS) system (available in the Cisco uBR 7100 and higher Universal Broadband Routers), so no definition is required in the CPE.

Integrated Services Digital Network

ISDN circuits offer proven dedicated-switched service for symmetric speeds of 2 x 64 Kbps via the Basic Rate Interface (BRI). Although ISDN is a switched service, it is offered by some service providers for a flat rate regardless of usage to a local point-of-presence (POP) for Internet access. In this scenario, encryption is needed, as the circuit does not terminate at the enterprise central site, but at the service provider. Using Multilink PPP (MPPP), the two B channels can be combined to provide 128 Kbps symmetric speed. ISDN is often used where ADSL reach or cable availability is an issue.

The minimum recommended broadband data rate is 160 Kbps upstream and 860 Kbps downstream. Data rates below this require more troubleshooting and are less likely to provide acceptable voice quality. ISDN is only recommended when no other broadband access is available and when pilot testing has been done to gauge voice quality.

Broadband Encapsulation

Data-link layer encapsulation is used between the home network device and the service provider aggregation device. For cable, the encapsulation used includes a DOCSIS header followed by the Ethernet header, payload and trailer. ISDN uses PPP as the encapsulation method. DSL over ISDN (IDSL) can use multiple encapsulations, with Frame Relay being common. With IDSL, the typical ISDN 2B1Q coding is used, except that both B-channels and the D-channel are used together to provide 144 Kbps symmetric bandwidth. Applicability of residential circuits below 160 Kbps and low-speed symmetric circuits for this solution are addressed in the "Quality of Service" section on page 7-7.

PPP is usually implemented because it provides for flexibility and user authentication. PPP has various forms, two of which are used across DSL access networks:

- PPP over ATM (PPPoA)—Based on RFC 1483; provides an efficient data-link layer encapsulation of IP, supports link fragmentation and interleaving (LFI) to permit real-time packets interrupting large data packets; also supports bundling multiple circuits as one logical connection.
- (PPP over Ethernet (PPPoE)—Based on RFC 2516; provides for integration of Ethernet, encapsulating another data-link layer packet. Many service providers use PPPoE due to past regulatory requirements that limited transport of network layer traffic over parts of networks. PPPoE has higher overhead than PPPoA, and no method of LFI or physical circuit bundling (such as with MPPP).

For additional information on protocols, see:

www.cisco.com/en/US/tech/tk175/tk819/tech_protocol_family_home.html.

Choosing Broadband Access

Table 2-3 highlights factors in choosing a teleworker residential broadband access technology. Two Xs means very good, one X means good, and no X means adequate. To summarize, Both DSL and cable are good choices. Where these are not available, ISDN offers excellent availability and sufficient bandwidth.

Table 2-3 Broadband Access Comparison

Factor	DSL	Cable	ISDN	Wireless
Low Cost (less than $100/month)	X	X	X (Flat rate only)	To be determined
Simple Deployment	X	XX	X	To be determined
Totally Managed Service	X	XX	X	To be determined
Managed Service Options (Enterprise Control)	XX	X (Dual unit only)	XX	To be determined
Performance	XX	XX		To be determined
Reach	X	XX	XX	To be determined
Availability (By/within a Region)	X	XX	XX	To be determined
Reliability	X	X	XX	To be determined

CHAPTER 3

Business Ready Teleworker CPE Deployment Models

This chapter presents the underlying CPE deployment models for carrying voice and data over IPSec-based VPN networks. The models for each residential broadband access technology vary according to Cisco devices available.

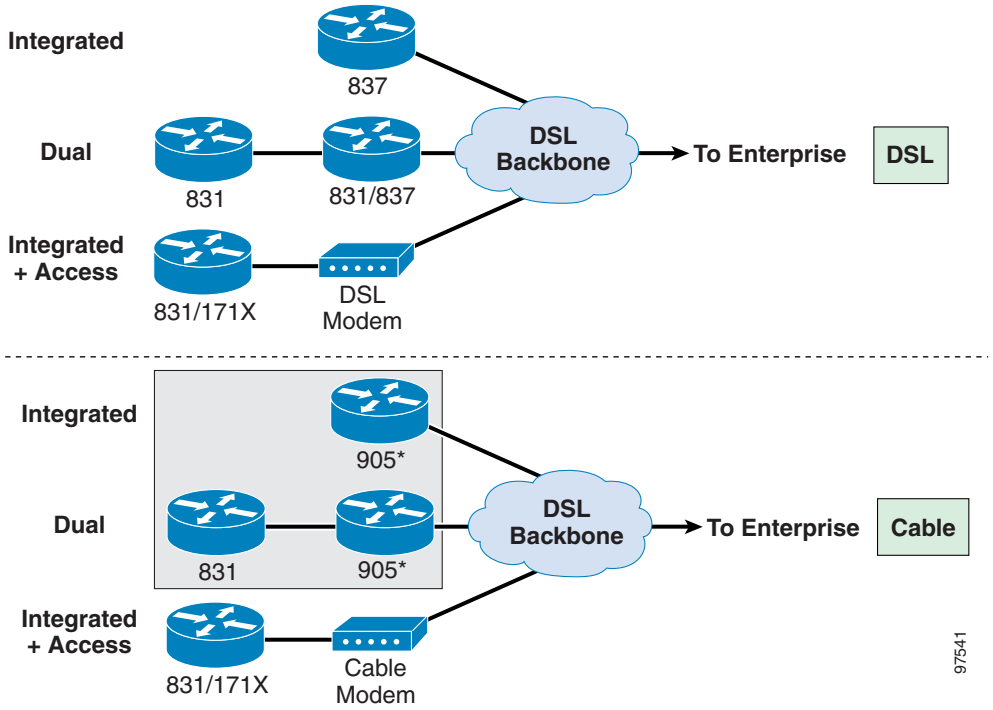
Sections presented in this chapter:

Deployment caveats follow:

- For ISDN
  - The Cisco 802 cannot perform with VPN and QoS enabled and thus no Integrated Unit model is addressed.
  - Third-party “dumb” ISDN bridges are not widely available, and thus no Integrated + Access Device model is addressed.
- For wireless—Global System for Mobile Communications (GSM); last mile cellular to the home
  - There is no Cisco router with a built-in cellular wireless interface, thus no Integrated Unit model or Dual Unit models are addressed.

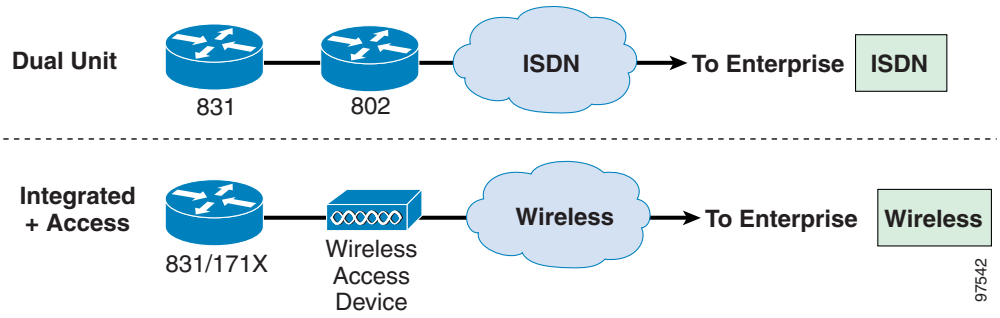
The Figure 3-1 and Figure 3-2 depict the supported models with specific recommended Cisco devices.

Figure 3-1 DSL and Cable Deployment Options



*Option not recommended until traffic shaping available (CSCea33951)

Figure 3-2 ISDN and Wireless CPE Product Deployment Options



Note For the deployments illustrated in Figure 3-2, minimum asymmetric speeds of 160 Kbps upstream and 768 Kbps downstream are recommended to provide consistently acceptable voice quality. ISDN and IDSL provide less bandwidth than this. In general, Cisco does not recommend running this solution over ISDN or wireless.

Devices Used for Models

The following list of devices were identified as usable for the solutions addressed in this publication. The accompanying descriptions include summaries of device functions. As new devices become available—or new functions are added to existing devices currently not recommended—functions and devices will be added. Notes are also included regarding devices that may be used in these solution, but that were not tested in the Cisco Enterprise Solutions Engineering lab.

- The Cisco 837 serves as the broadband access router for the DSL Dual Unit model or the device for the DSL Integrated Unit model. Feature/capability notes:
  - DSL broadband connection
  - NAT of IPSec packets (and clear packets if split tunnel is implemented)
  - QoS support
  - 10/100 Ethernet switch ports to connect SOHO devices in the Integrated model, or to connect non-secure devices and the Cisco 831 in the Dual Unit model
  - High performance IPSec 3DES encryption via hardware assisted encryption
  - Support for split tunnels, firewall
  - Copies original ToS byte to the encrypted packet for subsequent classification
  - Supports Easy VPN, shared secrets or certificates for authentication

Note **Caveat**—The Cisco 837 requires the IP/FW/PLUS 3DES feature set for teleworker voice/VPN. This feature enables the hardware-based crypto-accelerator, which is required for this solution. The IP/FW/PLUS 3DES feature set also provides—or will provide in the future—support for Easy VPN, additional IP QoS features, public-key infrastructure (PKI), IDS, Advanced Encryption Standard (AES), uniform resource locator (URL) filtering, and support for Enhanced Interior Gateway Routing Protocol (EIGRP).

Please refer to this resource:

http://www.cisco.com/warp/public/cc/pd/rt/800/prodlit/ssbro_ds.pdf.

- The Cisco 831 can serve as the Integrated Unit device for all Integrated Unit + Access Device models. Feature/capability notes:
  - Ethernet 10 Mbps broadband connection to access device (broadband modem)
  - NAT of IPSec packets (and clear packets if split tunneling is implemented)
  - QoS support
  - 10/100 Ethernet switch ports to connect SOHO devices
  - High performance IPSec 3DES encryption
  - Support for split tunnels, firewall
  - Copies original ToS byte to the encrypted packet for subsequent classification
  - Supports Easy VPN, shared secrets or certificates for authentication

Note **Caveat**—The Cisco 831 requires the IP/FW/PLUS 3DES feature set for teleworker voice/VPN. This feature enables low-latency queuing (LLQ) with class-based hierarchical traffic shaping which is required for this solution. The IP/FW/PLUS 3DES feature set also provides, or will provide in the future, support for Easy VPN, PKI, IDS, AES, URL filtering, and EIGRP.

Please refer to this resource:

http://www.cisco.com/warp/public/cc/pd/rt/800/prodlit/ssbro_ds.pdf

- The Cisco 1700 series router can serve as the Integrated Unit device for all Integrated Unit + Access Device models. Feature/capability notes:
  - Ethernet 10 Mbps broadband connection to access device (broadband modem)
  - NAT of IPSec packets (and clear packets if split tunneling is implemented)
  - QoS
  - One 10/100 Ethernet port to connect a SOHO device or Ethernet switch (the Cisco 1711 and Cisco 1712 offer a four-port 10/100 built-in Ethernet switch)
  - High performance IPSec 3DES encryption
  - Support for split tunnels and firewall
  - Copies original ToS byte to the encrypted packet for subsequent classification
  - Supports Easy VPN, shared secrets or certificates for authentication
  - Requires a separate Ethernet switch to provide connection to multiple SOHO devices

Note **Caveat**—The Cisco 1710 does not include a built-in Ethernet switch. The Cisco 1721 and 1751 support an optional 4-port 10/100 Ethernet Switch module. The Cisco 1711 and Cisco 1712 include a four-port built-in switch. The Cisco 1700 series was not Cisco Enterprise Solutions Engineering lab tested; the Cisco 831 was successfully Cisco Enterprise Solutions Engineering lab tested. Unless the SOHO IP Phone requires local PSTN access (via FXO port from the SOHO network device), the Cisco 831 is recommended as the Integrated Unit device.

Please refer to this resource:

http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/1710s_ds.htm.

- The Cisco 802 serves as the broadband access router in the ISDN Dual Unit model. Feature/capability notes:
  - ISDN broadband connection
  - NAT of IPSec packets (and clear packets if split tunneling is implemented)
  - QoS support

Please refer to this resource:

http://www.cisco.com/warp/public/cc/pd/rt/800/prodlit/isrdd_ds.htm

- The Cisco PIX 501 serves as the VPN device for Dual Unit models. Feature/capability notes:
  - High performance 3 Mbps IPSec 3DES encryption
  - 10/100 Ethernet switch ports to connect SOHO devices
  - Support for split tunnels, Cisco PIX strength firewall and NAT
  - Copies original ToS byte to the encrypted packet for subsequent classification

  - Supports Easy VPN, shared secrets or certificates for authentication
  - Cisco PIX is not used as the Integrated Unit in the Integrated + Access Device model because it does not support prioritization of packets or shaping, which are required in this model

  Please refer to this resource:

  http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/px501_ds.htm

Note **Caveat**—The Cisco PIX 501 requires an optional software activation key for 3DES support. The Cisco PIX 501 has not been tested in the Cisco Enterprise Solutions Engineering lab. The Cisco 831 has been tested in the Cisco Enterprise Solutions Engineering lab for this function and is recommended.

- The Cisco VPN 3002 serves as the VPN device for Dual Unit models. Feature/capability notes:
  - High performance IPSec 3DES encryption
  - 10/100 Ethernet switch ports to connect SOHO devices
  - Support for split tunnels and NAT
  - Copies original ToS byte to the encrypted packet for subsequent classification
  - Supports Easy VPN, shared secrets or certificates for authentication
  - Cisco VPN 3002 not used as the Integrated Unit in the Integrated + Access Device model because it does not support prioritization of packets or shaping, which are required in this model

  Please refer to the following resource:

  http://www.cisco.com/en/US/products/hw/vpndevc/ps2286/products_data_sheet09186a00801089cf.html

Note **Caveat**—The Cisco VPN 3002 has not been tested in the Cisco Enterprise Solutions Engineering lab. The Cisco 831 has been tested in the Cisco Enterprise Solutions Engineering lab for this function and is recommended.

- The Cisco 827H serves as the broadband access router for the DSL Dual Unit model. Feature/capability notes:
  - DSL broadband connection
  - NAT of IPSec packets (and clear packets if split tunneling is implemented)
  - QoS supported
  - 10 Mbps Ethernet hub ports to connect un-secure SOHO devices and the Cisco PIX 501 in the Dual Unit model
  - Cisco 827H not used as an Integrated device for DSL due to processing limitations in supporting both IPSec 3DES and QoS simultaneously

  Please refer to this resource:

  http://www.cisco.com/warp/public/cc/pd/rt/800/prodlit/827ad_ds.htm

- Cable modem, DSL modem, or wireless access devices are usually un-intelligent devices bridging the Integrated Unit via Ethernet to the broadband circuit. Feature/capability notes:
  - A cable modem can supply traffic prioritization if the device and the cable network are DOCSIS 1.1 compliant.

- The Cisco 79XX IP Phone handset or ATA-186 VoIP Gateway provides telephony services for the teleworker.

  Please refer to this resource:

  http://www.cisco.com/warp/public/cc/pd/tlhw/prodlit/index.shtml

- Non-Cisco routers are not recommended as the Integrated Unit or broadband access router for Dual Unit models, since they might not be able to perform classification, strict prioritization, and all the needed basic services—such as IPSec pass-through with NAT, authenticated NTP, DHCP with required options, and functions necessary for full management (SNMP, SSH, syslog)—and proper performance with multiple functions activated.

Although there are multiple applicable devices and models, Table 3-1 provides a comparison of the voice and data abilities that determine each device's suitability (considered in the CPE selection criteria shown in Table 3-2).

Table 3-1 Comparison of Voice and Data Capabilities for each VPN Model

CPE	Best-case Voice Quality	QoS Ability	Ability to Support Decrypted Voice and| Data	Manageability
Cisco 831/Cisco 837	Toll	Real-time hardware crypto embedded	Yes	Improving (Easy VPN)
Cisco 17xx plus hardware VPN	Toll	Real-time hardware crypto added	Yes	Improving (Easy VPN
Cisco 806/Cisco 827	Between cellular and toll	Non-real-time; no hardware crypto	Cellular quality voice at best	Improving (Easy VPN)
Cisco VPN 3002	Toll	None, but fast 3DES	No, must use with Cisco IOS router	Excellent
Cisco PIX 501	Toll	None, but fast 3DES	No, must use with Cisco IOS router	Improving (Easy VPN)

The Cisco 831 or Cisco 1700 series can be used as the Integrated Unit in an Integrated Unit + Access Device model, the Cisco PIX 501 and Cisco VPN 3002 can be used as the VPN device in the Dual Unit model, and the Cisco 837 or Cisco 1700 series can be used as the Integrated Unit in the Integrated Unit model. Cisco Enterprise Solutions Engineering lab testing was performed using the Cisco 831, Cisco 837 and Cisco 1751 routers.

CPE Selection Criteria and Recommendations

Use Table 3-2, along with the comparisons throughout this design guide, to evaluate the deployment models.

Table 3-2 CPE Product Selection Criteria[1]

	Integrated Unit	Integrated Unit + Access Device	Dual Unit
Enterprise VPN device	Cisco IOS router, Cisco PIX firewall	Cisco IOS router, Cisco PIX firewall	Cisco IOS router, Cisco PIX firewall (Cisco PIX not tested)
Cisco WAN interface	DSL, Cable	10BaseT (to broadband modem)	DSL, cable, ISDN
LAN interface	Cisco 837: 4-port 10/100 switch	Cisco 831: 4-port 10/100 switch	Combination of the ports from Cisco PIX 501 and Cisco 837 router
IPSec authentication	Pre-shared key, certificate, Easy VPN	Pre-shared key, certificate, Easy VPN	Pre-shared key, certificate, Easy VPN
IPSec encryption	DES or 3DES	DES or 3DES	DES or 3DES
Unity Client	Yes (basic functions)	Yes (basic functions)	Yes (basic functions)
Direct management interfaces	Cisco 837: CLI or browser via Cisco Router Web Setup (CRWS) Tool	CLI or limited browser	CLI for Cisco PIX 501 CLI or browser via CRWS for Cisco 83X.
Remote management	CiscoWorks 2000 VPN/Security Management Solution (VMS)/IP Solution Center (ISC)	VMS/ISC	VMS/ISC
Number of units per head-end device	Varies by head-end device see V^3PN guide	Varies by head-end device see V^3PN guide	Varies by head-end device, see V^3PN guide
3DES throughput	Varies by SOHO VPN device	Varies by SOHO VPN device	Varies by SOHO VPN device
Individual user authentication	Easy VPN allows user to authenticate the tunnel, but all home users can then go through the tunnel.	Easy VPN allows user to authenticate the tunnel, but all home users can then go through the tunnel.	Easy VPN allows user to authenticate the tunnel, but all home users can then go through the tunnel.
Multi-service application support	QoS: Yes Multicast: Yes	QoS: Yes Multicast: Yes	QoS: Yes Multicast: No
IP Telephony via VPN	Yes	Yes	Yes
Firewall	Cisco IOS firewall	Cisco IOS firewall	Cisco PIX firewall
Split tunneling	Access control lists or Easy VPN	Access control lists or Easy VPN	Access control lists or Easy VPN
DHCP client	Yes	Yes	Yes

Table 3-2 CPE Product Selection Criteria[1]

	Integrated Unit	Integrated Unit + Access Device	Dual Unit
DHCP server	Yes	Yes	Yes
Improved Availability	GRE Encapsulation, Hot Standby Routing Protocol (HSRP), RRI. Dual Tunnels or VPN gateway improved availability designs.	GRE Encapsulation, HSRP, RRI. Dual Tunnels or VPN gateway improved availability designs.	Dual Tunnels or VPN gateway improved availability designs

1. The Cisco uBR 905 is not recommended due to the lack of traffic shaping (CSCea33951) and the use of a built-in shared media hub. When traffic shaping is supported, and no devices except for the VPN device are connected to the Cisco uBR 905, it can be considered.

Business Ready Teleworker Deployment Guidelines

Deployment guidelines for implementing an IPSec VPN environment in support of voice and data are presented in this chapter in the following series of sections:

Basic Services

Basic IPSec VPN services addressed in this section include:

One Broadband Connection

All solutions addressed in this publication provide a single broadband connection. The minimum recommended broadband data rate for either cable or DSL is 160 Kbps (up)/860 Kbps (down).

Ethernet Connection for Four or More SOHO Devices

Switched Ethernet connections should be provided with this solution because SOHO devices might perform large file or print services across the SOHO LAN during IP based voice calls. Applicable product summaries follow:

- **DSL Integrated Unit**—The Cisco 837 provides four 10/100 switched Ethernet ports for secure SOHO LAN devices (devices needing VPN access to enterprise or firewall protection).
- **DSL Dual Unit**—The Cisco 831 VPN device provides four 10/100 switched Ethernet ports for the secure SOHO LAN. The Cisco 837 broadband router provides four switched 10/100 Mbps ports for non-secure SOHO LAN devices. The Cisco PIX 501 and Cisco VPN 3002 (although not Cisco Enterprise Solutions Engineering-tested as VPN devices for Dual Unit models) offer switched 10/100 Ethernet ports for the secure SOHO LAN.
- **DSL Integrated Unit + Access Device**—The Cisco 1711/1712 provides four 10/100 switched Ethernet ports that can be used for secure SOHO LAN devices.

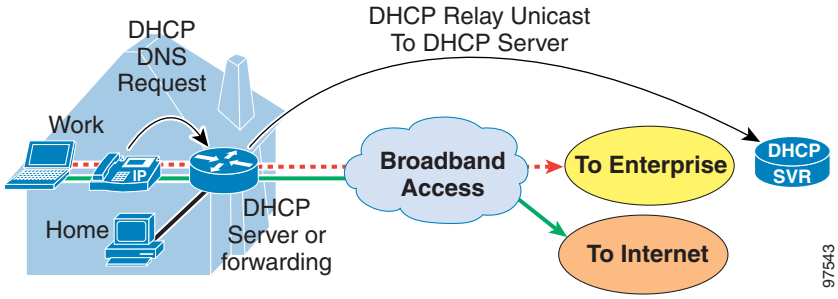
  The Cisco 831 provides four 10/100 Ethernet switch ports and one 10 Mbps Ethernet port. The switch ports can be used to connect devices to the secure SOHO LAN, with the single Ethernet port used to connect to the broadband access device (modem).
- **Cable Integrated Unit**—This model is currently not recommended due to the lack of traffic shaping on the Cisco uBR 905.
- **Cable Dual Unit**—This model is currently not recommended due to the lack of traffic shaping on the Cisco uBR 905.
- **Cable Integrated Unit + Access Device**—The Cisco 1700 series router provides a single 10 Mbps Ethernet port for secure SOHO connection, thus requiring a Cisco 1548 or other Ethernet switch to support multiple secure SOHO devices. If multiple ports are integrated into the broadband modem (access device), these should not be used, as the Integrated Unit is not able to provide QoS to voice or enterprise traffic with devices connected to these modem ports.

  The Cisco 831 provides four 10/100 Ethernet switch ports and one 10 Mbps Ethernet port. The switch ports can be used to connect devices to the secure SOHO LAN, with the single Ethernet port used to connect to the broadband access device (modem).
- **ISDN Dual Unit**—The Cisco 831 provides four 10/100 switched Ethernet ports, which can be used for secure SOHO LAN devices. The Cisco 802 broadband router provides one 10 Mbps ports that must be used to connect the Cisco PIX 501. If multiple non-secure ports are required, a Cisco 1548 or other switch can be used.
- **Wireless Integrated Unit + Access Device**— The Cisco 831 provides four 10/100 Ethernet switch ports and one 10 Mbps Ethernet port. The switch ports can be used to connect devices to the secure SOHO LAN, with the single Ethernet port used to connect to the broadband access device (modem). The ports may be configured so that the single Ethernet port is the secure LAN, allowing the four 10/100 ports to be used to connect non-teleworker PCs and the broadband access device. The non-teleworker PCs are then unprotected and do not have access to the VPN.

Dynamic Host Configuration Protocol Support

DHCP is required for serving SOHO PCs an IP address and mask, IP default gateway, DNS server IP address(es), and option 150 (TFTP server IP address needed by Cisco 79XX IP telephones to register to CallManager). The CPE must be able to provide either DHCP server function, or relay the teleworker PC (or IP phone) DHCP requests by forwarding the request as a unicast to an enterprise DHCP server through the VPN. Figure 4-1 depicts the DHCP function, and is followed by each model's support.

Figure 4-1 DHCP Support



- **All Integrated Unit models**—All Cisco IOS routers support these functions.
- **All Dual Unit models**—Cisco 831 and Cisco PIX 501 support these functions for all secure SOHO devices.
- **All Integrated Unit + Access Devices**—The Cisco 831 and Cisco 1700 series routers support these functions.

Below is a Cisco PIX 501 DHCP server configuration example:

```
dhcpd address 10.100.200.3-10.100.200.14 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable inside
dhcpd option 150 10.1.2.10 10.1.2.11
```

Below is a Cisco IOS router DHCP server configuration example:

```
ip dhcp pool test
   network 192.168.200.0 255.255.255.240
   default-router 192.168.200.1
   dns-server 10.2.2.5 XXX.YYY.0.38
   option 150 ip 10.1.2.10 10.1.2.11
```

Below is a Cisco IOS router DHCP forwarding configuration example:

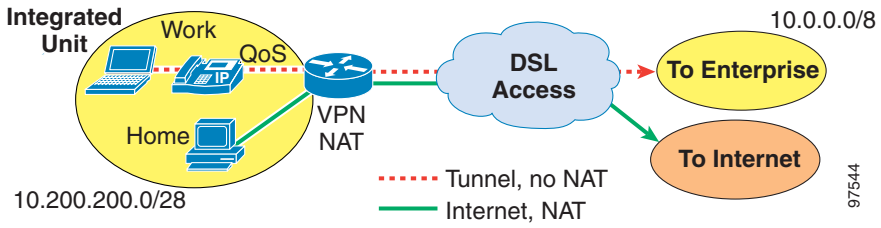
```
interface ethernet0
 description inside interface and dhcp forwarding
 ip address 10.200.200.1
 ip helper-address 10.10.10.10
```

Note Some enterprises use HTTP proxies to provide caching and security for web access. In this environment, the enterprise DNS is authoritative for all name resolution (resolves all entries) in order to point all web access through the enterprise proxy. If the SOHO network uses split tunneling to provide Internet access directly (outside of the VPN), but the Home PCs receive an enterprise DNS entry only, no split tunneling will occur, as all resolutions will point to the enterprise proxy through the VPN. A workaround is to provide a separate enterprise DNS server for teleworkers that will not be authoritative; this allows for a response to a request, with the real IP address of the named service and, if on the Internet, the traffic can be split tunneled.

Network Address Translation

Most service providers allow a single IP address, often dynamically assigned to the SOHO CPE. If the solution allows for split tunneling (Internet access directly from the SOHO) it will provide pNAT to allow for multiple devices to access the Internet. The IP address range of the SOHO, which is allocated from the enterprise range, is connected using pNAT to the public IP address assigned to the CPE. Packets destined for the enterprise are not connected using NAT/pNAT, but are tunneled so that upon decryption at the enterprise VPN gateway they are intact and can be routed as if they traversed a private WAN. Figure 4-2 depicts pNAT for the Integrated Unit model.

Figure 4-2 pNAT and VPN for Integrated Unit Model

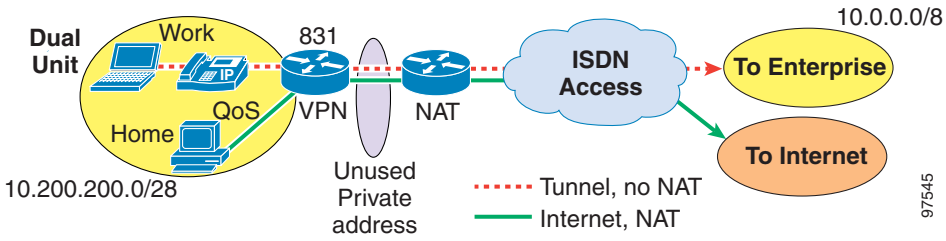


Below is a sample configuration fragment pertaining to pNAT for the DSL Integrated Unit model in Figure 4-2:

```
interface Ethernet0
 ip address 10.200.200.1 255.255.255.240
 ip nat inside

interface Dialer0
 bandwidth 134
 ip address negotiated
 ip nat outside

ip nat inside source list 101 interface Dialer0 overload
!(pNAT)
ip route 0.0.0.0 0.0.0.0 Dialer0
!#(default route to PPPoE virtual interface)

access-list 101 permit ip 10.200.200.0 0.0.0.15 any
!(the 10.200.200.0/28 net is 'interesting')
```

For the Dual Unit model, a private address subnet (not used by the enterprise) is required between the VPN device and broadband access router. No NAT is required on the VPN device, however the VPN device requires a static default route to the broadband router Ethernet interface, and the broadband router requires a static route to the subnet behind the Cisco PIX 501 (10.200.200.0/28, unique within the enterprise). Figure 4-3 depicts the Dual Unit model.

Figure 4-3 pNAT and VPN for Dual Unit Model



In the Dual Unit model, NAT support of IPSec packets (IPSec NAT raw pass-through) is required if there are any home PCs between the VPN device and broadband router (thus unprotected, requiring a larger unique subnet, and the use of NAT for that subnet in addition to the private subnet). This feature is part of Cisco IOS at 12.2(2)XI and 12.2(8)T, and requires no additional configuration besides standard pNAT.

In the Dual Unit model, in addition to the IPSec pass-through capability in the broadband device, the VPN device must use IPSec ESP without AH for authentication. AH includes the outer IP header as part of its integrity check. If this mode is used and the broadband router performs NAT, the packet is rejected when it reaches the enterprise VPN gateway, as the source IP address is altered and the integrity check fails.

Below is a partial Cisco IOS example of encryption and authentication *without* using AH:

crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac

Below is a partial Cisco PIX 501 example of encryption and authentication *without* using AH:

crypto ipsec transform-set espset esp-3des esp-sha-hmac

Below is a partial configuration example pertaining to pNAT for the DSL Integrated Unit model above:

```
interface Ethernet0
 ip address 172.16.12.1 255.255.255.240
!(network between 8X7 and PIX)
 ip nat inside

interface Dialer0
 ip address negotiated
 ip nat outside

ip nat inside source list 101 interface Dialer0 overload
!(pNAT)
ip route 0.0.0.0 0.0.0.0 Dialer0
!(default route to PPPoE virtual interface)
ip route 10.200.200.0 255.255.255.240 172.16.12.2
!(route to subnet behind PIX)

access-list 101 permit ip 172.16.12.16 0.0.0.3 any
```

Network Time Protocol and Simple Network Time Protocol

The Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP) provide a common time base for networked routers, servers, and other devices. A synchronized time enables correlation of error logs and debugging output across multiple devices to specific events.

NTP might also be required for VPN, when the SOHO VPN devices authenticate using digital certificates and the SOHO VPN devices do not have internal real-time clocks. The VPN device, Cisco 800 series and Cisco 1700 series do not have internal real-time clocks. Time synchronization might be required to check the certificate lifetime (depends on Cisco IOS version), so all VPN devices should use the NTP protocol (or SNTP if NTP is not supported) to synchronize the time. Although there are publicly accessible NTP servers, the enterprise should provide a publicly reachable NTP server to ensure its availability. Note that NTP is supported on the Cisco 831, but not the Cisco 837 (which only supports SNTP). One difference between NTP and SNTP is that SNTP does not offer an authentication option. NTP servers can usually support both NTP and SNTP.

Below is an example of how to enable NTP on an Cisco IOS SOHO VPN gateway:

```
ntp server XX.YY.41.41
!(or sntp server XX.YY.41.41)
ntp server XX.YY.41.40
!(or sntp server XX.YY.41.40)
clock timezone PST -8
clock summer-time PDT recurring
```

Enterprise-based Telephony Services

Unified IP-based messaging or connection to legacy voicemail systems are needed to provide teleworker users enterprise-based telephony and applications, and access to a CallManager, VoIP gateways, and DSP resources. The servers centralized at the primary enterprise location normally supply these services.

Support of E911 service is not normally included as part of the teleworker solution. It is assumed that the home POTS line is available to the teleworker in the SOHO location. If E911 support is needed, then the following deployment considerations apply:

- **DSL Integrated Unit**—Use a Cisco 1751-2V [with VPN module, ADSL WIC, FXO VIC, and Survivable Remote Site Telephony (SRST) software option] as the Integrated Unit. The FXO VIC allows the Cisco 1751 to connect to a POTS line for (and route teleworker IP Telephony calls for) 911 or a WAN circuit failure.
- **DSL Dual Unit**—Use a Cisco 1751-2V (with ADSL WIC and FXO VIC) as the broadband router. VoIP traffic from a Cisco 79XX IP handset behind the VPN device to the Cisco 1751 VoIP gateway during WAN outages does not require encryption. The FXO VIC allows the Cisco 1751 to connect to a POTS line for (and route teleworker IP Telephony calls for) 911 or a WAN circuit failure.
- **Cable Integrated Unit**—No feasible solution, use the cable Integrated Unit + Access Device model.
- **Cable Dual Unit**—No feasible solution, use the cable Integrated Unit + Access Device model.
- **All Integrated Unit + Access Device Implementations**—Use a Cisco 1751-2V (with VPN module, FXO VIC, and SRST software option) as the Integrated Unit. The FXO VIC allows the Cisco 1751 to connect to a POTS line for (and route teleworker IP Telephony calls for) 911 or WAN circuit failure.

Below is a configuration fragment illustrating SRST and Media Gateway Control Protocol (MGCP) for a Cisco 1751-2V:

```
ip dhcp pool PHONE1
```

```
        host 10.100.200.2 255.255.0.0
        client-identifier 0100.3094.c337.cb
        option 150 ip 10.1.2.10 10.1.2.11
        default-router 10.100.200.1

!
voice-port 2/0
 description My Home Phone Line
!
!
dial-peer voice 45 pots
 destination-pattern 9
 port 2/0
!
call-manager-fallback
 ip source-address 10.100.200.1 port 2000
 max-ephones 2
 max-dn 2
 access-code fxo 9
```

There would be a separate address DHCP pool for PCs that would not map an IP address to a specific PC.

Quality of Service

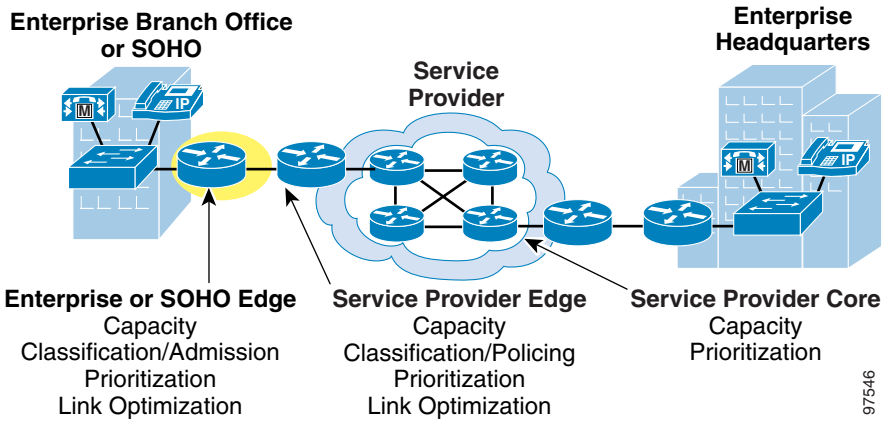
QoS considerations addressed in this section include:

General

The techniques required to provide QoS are not changed for encrypted teleworker packet voice. The goal is to provide acceptable voice packet delay, variation in delay (jitter) and packet loss—levels low enough to provide consistently acceptable voice quality. The existing methods include traffic classification, prioritization, shaping, and fragmentation/interleaving.

Figure 4-4 illustrates the QoS tools needed to provide business class voice.

Figure 4-4 QoS for Business-Quality Voice



CPE Performance

For all deployment models, cryptographic processing with minimal delay and throughput equivalent to the access link speed are required to achieve acceptable voice quality. Notes regarding specific VPN implementation-model cryptographic recommendations follow:

- For **DSL Integrated Unit models**, the recommended single devices is a Cisco 837. It provides hardware-assisted cryptography.
- For **all Integrated Unit + Access Device models**, the recommended Ethernet-to-Ethernet Integrated Units (Cisco 831 and Cisco 1700 series VPN bundles) provide hardware-assisted cryptography
- For **all Dual Unit models**, the Cisco 831 offers sufficient cryptography performance.

End-to-End QoS

Although not the focus of this guide, an important part of the teleworker solution is the ability of the service provider's network to offer QoS. Cisco has documented these requirements as part of the Multi-Service Cisco Powered Network designation. Providers meeting these requirements can be found at the following web resource:

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

To use this tool, select *IP/VPN Multi-service* from the top drop-down menu.

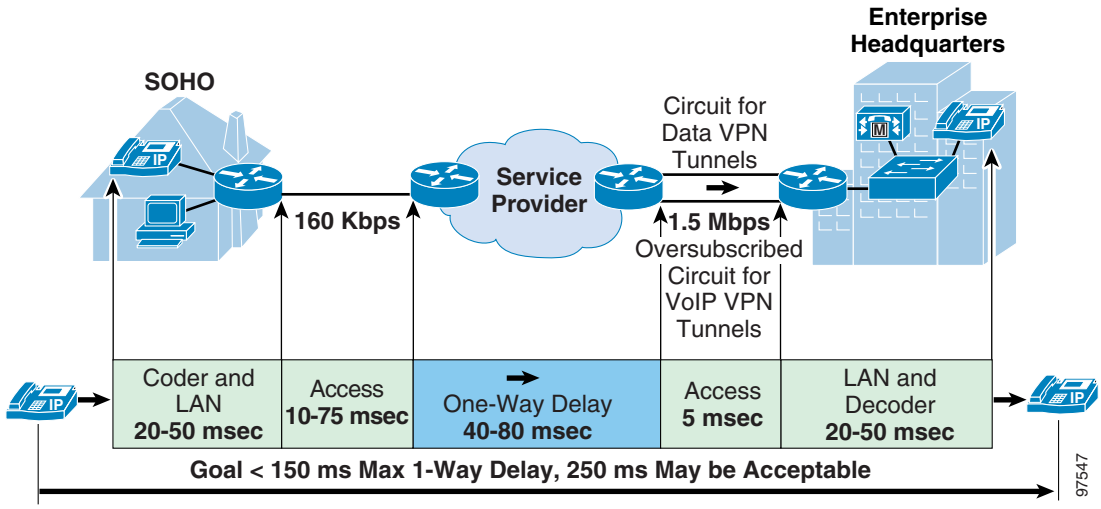
The requirements across the service provider networks are enforced by the service providers themselves, and include:

- 60 msec or less delay one way across the service provider core (access link delay not included)
- 20 msec or less jitter across the service provider core
- 0.5 percent voice packet loss or less across the service provider core

However, many service provider core networks are not QoS-enabled. Nonetheless, enterprises can deploy quality-sensitive services over VPN with appropriate expectations, if the end-to-end delay, jitter and loss can support acceptable voice quality. This quality can only determined by the enterprise via a pilot test, but can generally be characterized as better than cell phone, but inferior to toll quality.

Figure 4-5 illustrates an example of the teleworker environment with 160 Kbps upstream bandwidth and delay variables.

Figure 4-5 End-to-End Quality of Service Objectives



Note Regardless of the access link speed, testing should be done to determine the maximum bandwidth that can be consistently achieved between the CPE and the VPN head-end gateway. This value should be used to determine the maximum bandwidth guaranteed to traffic classes at the SOHO CPE.

The example in Figure 4-5 shows a 40-to-80 msec delay in the service provider network. The goal here is 60 msec or less with 20 msec of jitter, thus 80 msec is shown as an upper bound.

Access Circuit QoS

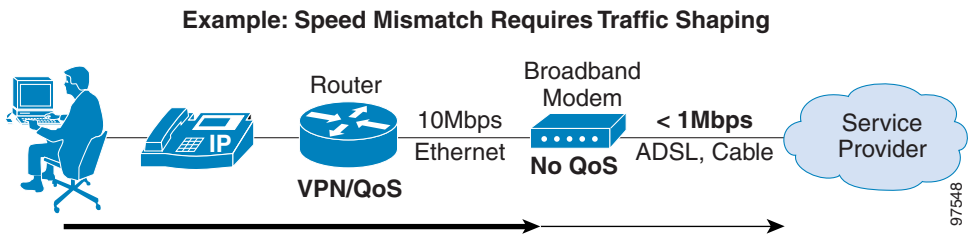
Although service providers are planning to offer QoS for residential SOHO, it is generally not available. However, the performance of the best-effort networks deployed today is improving. It is possible to achieve fairly consistent delay, jitter and loss performance during normal business hours from broadband service providers. However, this is not guaranteed. Testing with hundreds of Cisco employees in a pilot for encrypted voice/data VPN, and testing at two service providers has yielded the following results:

- Best-effort service provider networks for residential broadband (DSL and cable) allow for encrypted voice quality better than cellular, but lower than business class. It is acceptable for many teleworking solutions (not distributed call center). Service providers are beginning to develop offerings for teleworkers with QoS.
- For **all models:** Due to the lower uplink speed of most residential broadband circuits, upstream voice traffic can be delayed when a data packet is in front of voice traffic. For DSL (which uses PPPoE encapsulation) and some cable networks (using DOCSIS 1.0), no method exists for interrupting data packets in favor of voice (LFI). Since LFI is not available, voice cannot achieve toll quality. However, acceptable teleworker quality voice (between cell phone quality and toll quality) can be achieved, if:
  - This maximum one-way delay is 250 milliseconds or less
  - The variation in delay can be accommodated by the de-jitter buffer of the receiving voice device (IP handset, VoIP gateway, multi-party voice-conference device)
  - Voice Activation Delay (VAD) is not used or is tested within the teleworker environment

  To reduce serialization delay, Cisco routers provide a method to reduce the maximum packet size for TCP sessions. The **ip tcp adjust-mss** interface command provides this capability. For example, if this value is set to 542, devices communicating with TCP across the router will send smaller packets, which can reduce the serialization delay of a voice packet behind a data packet by as much as 64 percent. On a 160 Kbps uplink, this equates to a maximum potential reduction in serialization delay of 39 milliseconds. Use of **adjust-mss** is recommended for all circuits with uplink speeds less than 768 Kbps.
- For **all Integrated Unit + Access Device models**—Ethernet-to-Ethernet routers (Cisco 831, Cisco 171X) do not know the upstream access speed available because the circuit is terminated on the broadband access device (modem or a transparent bridge). These routers must have traffic shaping enabled on the trunk side Ethernet interface (connecting to the DSL/cable/wireless modem). The shaped speed should match the upstream ability of the DSL or cable line or the speed of the modem, whichever is lower.

Figure 4-6 below depicts this scenario.

Figure 4-6 Speed Matching with Traffic Shaping



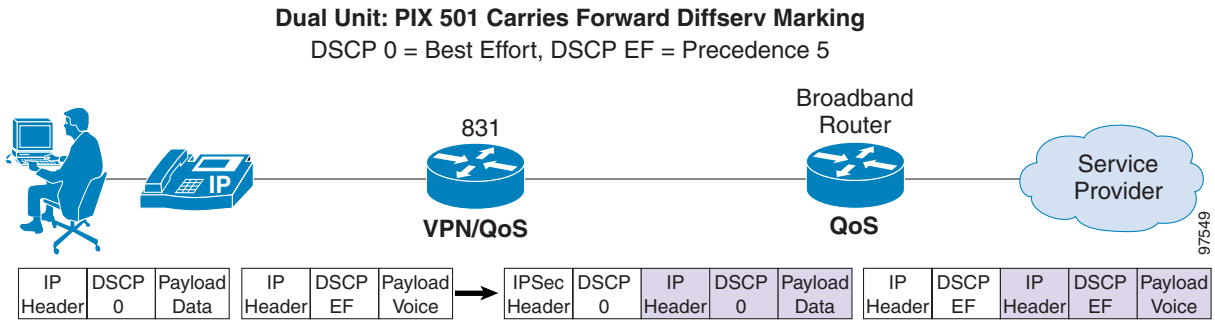
QoS Classification Persistence through VPNs

For all models, the original QoS classification contained in the IP header ToS byte is preserved. This allows the broadband router (and in the future the service provider network) to classify encrypted packets and prioritize those representing voice payload and signaling (traditionally IP precedence 5 and 3 respectively).

Since the encrypted packets cannot be examined for address and port information, relying solely on the ToS byte for classification and prioritization is recommended. The device carrying forward the ToS byte is the one performing VPN gateway. This varies by the three general deployment models.

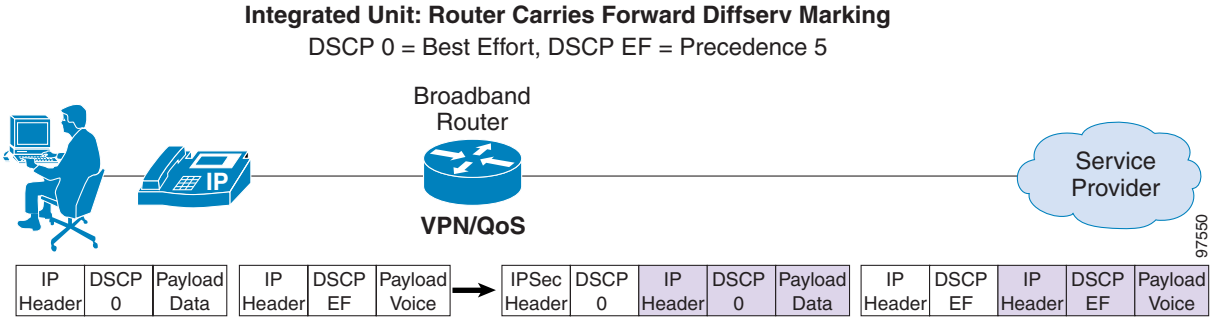
All Dual Unit Models—The VPN device encrypts the packets sent by SOHO devices before they reach the broadband router. As the packets are encrypted, the router cannot classify these packets based on the original IP header. The VPN device copies the value of the original packet ToS byte to the encrypted packet's ToS byte. The broadband router (and in the future the service provider network) can classify encrypted packets and prioritize those representing voice payload and signaling (traditionally IP precedence 5 and 3 respectively). Figure 4-7 represents QoS persistence. The ToS byte shown separately is actually byte 2 in the IP header, and is depicted separately for emphasis.

Figure 4-7 QoS Classification Persistence—Dual Unit Model



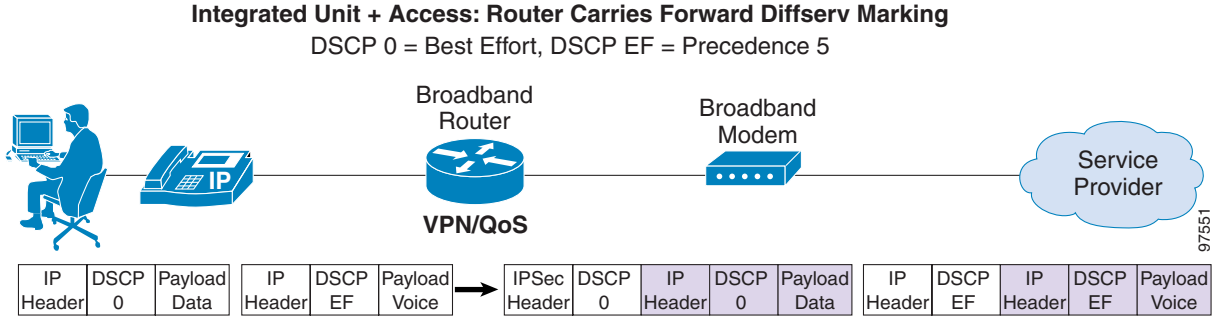
All Integrated Unit Models—The broadband router encrypts the packets sent by SOHO devices and carries forward the ToS byte. This allows the service provider network (in the future) to classify and prioritize the encrypted packets. See Figure 4-8.

Figure 4-8 QoS Classification Persistence—Integrated Unit Model



All Integrated Unit + Access Device Models—The Cisco 1700 series Ethernet-to-Ethernet routers encrypts the packets sent by SOHO devices and carries forward the ToS byte. This allows the service provider network (in the future) to classify and prioritize the encrypted packets. See Figure 4-9

Figure 4-9 QoS Classification Persistence—Integrated Unit + Access Device Model



IPSec VPN and Security

This section addresses the following IPSec VPN security considerations:

Technique for Strong Encryption

The 3DES and AES algorithms provide strong encryption. Because 3DES is widely implemented and secure, it is recommended for both key negotiation via Internet Key Exchange (IKE) and payload encryption via ESP.

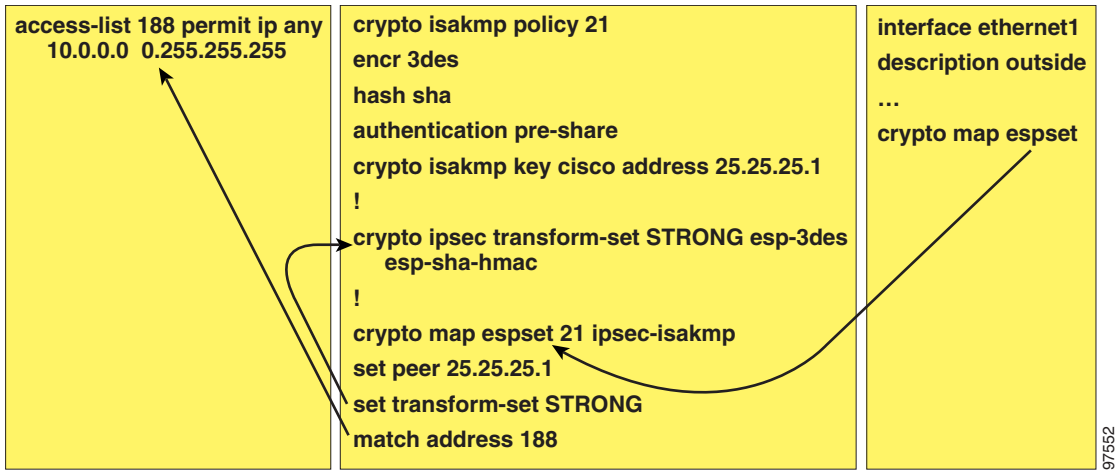
Packet Authentication Options

Hashing provides for data integrity and is configured along with encryption method. In addition to device authentication, the teleworker and head-end VPN devices use a hash function to authenticate the integrity of encrypted packets. This protects against packets being altered during transport because the hash is incorrect for an altered packet, and thus the receiving VPN device discards the altered packet. Two general hashing algorithms can be used: Message Digest 5 (MD5) and SHA. Both hashing options span 12 bytes in the IPSec packet. Although both are the same length due to truncation, SHA is generally preferred because it is a 160-bit hash (versus MD5's 128-bit algorithm), even though the hash in either case is truncated.

For **all models** use SHA for both IKE and ESP.

Figure 4-10 illustrates an example of IPSec definition with 3DES and SHA used for both IKE and ESP.

Figure 4-10 IPSec Basics with 3DES and SHA



VPN Network Design

Several options are available for designing IPSec VPN networks for the teleworker. Each option has benefits and specific considerations related to function, performance, and scalability. These are summarized in the following notes:

- *Traditional IPSec Design*—Provides for either statically defined or dynamically defined remote sites. Dynamic definition of remote sites is required for SOHOs with dynamic IP address assignment from the service provider. Dynamic crypto-map definition provides for simple definition at the central site VPN head-end because there can be a single configuration for all remote nodes. What is to provided with traditional IPSec design is the support of broadcast and multicast applications—including Routing Information Protocol (RIP), EIGRP and Open Shortest Path First (OSPF).
- *Traditional IPSec with GRE* (GRE encapsulated packets that are encapsulated with IPSec, specifically ESP)—Provides for the same encryption and integrity as traditional IPSec, and allows for broadcast and multicast applications (including routing protocols). However, since traditional GRE requires each VPN device to configure the specific IP address of each neighbor, the central site VPN head-end must define each remote. This requires significant definitions at the VPN head-end device.

Dynamic Multi-point VPN (DMVPN)—Also known as Dynamic multi-point GRE; a new option that combines the function of IPSec, dynamic crypto-maps, GRE and Next Hop Resolution Protocol (NHRP). This combination provides the benefits of the above two methods (simplified definition, support for remote nodes with dynamic addresses, and broadcast/multicast support). This became available in Cisco IOS 12.2(13)ZG, which also offers other enhancements such as IPSec pre-fragmentation. A potential benefit is the ability for SOHOs to dynamically set up IPSec tunnels directly between SOHO sites, thereby allowing the VPN head-end to off-load this responsibility and helping to reduce delay (no double encryption/decryption and latency to/from hub). DMVPN is a new feature with significant capabilities. Full testing of all DMVPN functions in a V^3PN environment has yet to be completed. This guide will be updated as DMVPN scenarios are tested and documented.

For **all models,** traditional IPSec VPNs with dynamic crypto-maps are recommended, as routing protocols are not usually required for teleworker home offices, and the VPN head-end configuration is simplified.

VPN Authentication

There are multiple options that can be used—separately or together—to provide authentication for teleworker sites. This authentication is for the network device itself. Please refer to "Per-User Authentication" section on page 4-16 for per-user authentication options that can be used with any of these device authentication methods. Although there are various combinations, three recommended SOHO authentication methods are listed below, with each having specific benefits depending on security policy:

- *Shared secrets* with a radius server back end provides scalable authentication
- *Digital certificates* allows for highly secure and scalable authentication
- *Easy VPN* provides for simplified scalable by simple definitions and a preset combination of authentication options.

Shared secrets has traditionally provided easy definition and pre-configured SOHO equipment for drop shipping and easy user installation, but difficult VPN gateway definition and manageability. This difficulty stems from the shared secret for each remote VPN device being stored on the head-end VPN gateway. In this situation, if the shared secret is not changed, or if the same shared secret is used for multiple SOHOs, there is more of a security threat. If the VPN unit is stolen or inappropriately used, manual enterprise head-end VPN device reconfiguration is needed to disable the shared secret used by the specific device.

With the addition of a feature in Cisco IOS 12.2, a VPN head-end gateway can use pre-shared keys for authentication with teleworker sites without storing the keys internally. A Remote Authentication Dial-In User Service (RADIUS) server is used to store the key for each teleworker VPN device. This allows for an individual key per teleworker VPN device without the need to define the key in the VPN head-end gateway. A device can also be revoked via the RADIUS server instead of requiring the head-end VPN gateway to be altered.

Digital certificates provide strong authentication for the teleworker VPN device. Authentication management is centralized at the enterprise server acting as the Certificate Authority (CA). If broadband availability fails and then becomes available, no user action is required to resume secure communications. If the VPN device is stolen or inappropriately used, that specific teleworker VPN device's certificate can be revoked, which does not require a change in the enterprise VPN gateway (revoked at the CA). Digital certificates have a range of validity (time), and require updating via re-enrollment of the certificate. This can be done automatically across the VPN tunnel with appropriate CPE configuration (**auto-enroll** and **source interface** configuration commands under **crypto ca trustpoint**).

Easy VPN provides a pre-set combination of IKE and IPSec authentication and encryption options to provide very simple remote VPN device definition and to provide user-level authentication of the VPN device (not granular authentication per user; once the device is authenticated, all home users can access the VPN). Easy VPN combines shared secrets, Extended Authentication (Xauth), and 3DES for key negotiation and encryption. Strong authentication can be enabled by using a RADIUS server and a hard or soft token to generate a one-time password (OTP) that must be entered by the teleworker to initiate the VPN tunnel. Once the tunnel is established, it remains active due to the keepalive messages to and from the IP telephone (if using SCCP, SIP does not do keepalives). Although the authentication is user level, it is not per user. Once the tunnel is up, any traffic from the SOHO LAN behind the VPN device can traverse it. If the VPN device is stolen or inappropriately used, that specific teleworker VPN profile can be deleted or changed, which does not require a change in the enterprise VPN gateway (done at RADIUS server). If broadband availability fails and then becomes available, the user might need to input the userid and password again to resume secure communications. This is done in one of the following ways:

- **For all Integrated Unit + Access Device models**—The teleworker accesses a web page from the Cisco 831 and inputs userid and password. Group name and password definitions need not be retyped. UserID and password are cached.
- **For all Dual Unit models**—Cisco 831 process is as above. The Cisco PIX 501 provides for pre-configuration of the userid and password, or both can be entered via command line.
- **For DSL Integrated Unit model**—The teleworker accesses a web page from the Cisco 831 and enters userid and password. The group name and password definitions need not be retyped. UserID and password are cached.
- **For Cable Integrated Unit model**—This model is not recommended at this time.

Note If the teleworker VPN device is a Cisco IOS router, and if the VPN connection becomes inactive (power or broadband circuit loss), the user must log in again via Easy VPN before data and voice services can be used.

IPSec authentication interoperability between Cisco PIX, Cisco IOS and Cisco VPN 3000 with software levels is shown in Table 4-1.

Table 4-1 SOHO VPN to Central Site VPN Device Interoperability

	Cisco IOS Router (such as 7140 and 7200)	VPN 3000 Concentrator	PIX 515, 525, 535
Cisco 800/900/1700 Routers	IKE aggressive mode + RADIUS requires 12.2(8)T Certificates for dynamic addressing Easy VPN—Requires greater than or equal to Cisco IOS12.2(4)YA on SOHO device (client) and Cisco IOS 12.2(8)T at head end (server)	IKE aggressive mode + RADIUS not available Certificates for dynamic addressing Easy VPN (requires Cisco IOS greater than or equal to 12.2(4)YA on SOHO device) or 12.2(12)T Does not support multicast (GRE) Untested as a head end during Cisco Enterprise Solutions Engineering lab testing. Cisco IOS head end VPN devices used.	IKE aggressive mode + RADIUS not available Certificates for dynamic addressing Easy VPN—Requires Cisco IOS greater than or equal to 12.2(4)YA or 12.2(12)T on SOHO device and PIX 6.1 or later at head end Untested as a head end during Cisco Enterprise Solutions Engineering lab testing.
Cisco PIX 501 Untested; Cisco 831 used during Cisco Enterprise Solutions Engineering lab testing.	IKE aggressive mode + RADIUS not available Certificates for dynamic addressing Easy VPN—requires greater than or equal to 6.2 on Cisco PIX 501 and Cisco IOS 12.2(8)T at head end	IKE aggressive mode + RADIUS not available Certificates for dynamic addressing Easy VPN (requires PIX 6.2 on SOHO device)	IKE aggressive mode + RADIUS not available Certificates for dynamic addressing Easy VPN—Requires greater than or equal to 6.2 on Cisco PIX 501 and greater than or equal to PIX 6.1 at head end

Table 4-2 provides a comparison of the three recommended authentication models by ability. Two Xs indicates capability is very good, one X indicates good, and no X indicates adequate.

Table 4-2 Authentication Comparison

	Digital Certificates	Pre-Shared Keys + RADIUS	Easy VPN
Works Across All Platforms (Cisco IOS, PIX, VPN3000)	XX	Cisco IOS only	XX
Strong Security	XX	X	XX
Improved Availability	X Can define multiple head-ends	X Can define multiple head-ends	Maximum of one head end defined
Easy Definition	Requires CA and processes, must be renewed over time	X Easy on remote device	XX Few remote definitions sent from head-end
Easy for Teleworker to use	XX No end-user interaction	XX No end-user interaction	Requires end-user to enter password

Note IKE aggressive mode offers somewhat less security during initial key exchange, but is faster.

Per-User Authentication

The following features are required to limit VPN access to appropriate traffic:

- Split tunneling (Internet access to all non-teleworker traffic and teleworker non-enterprise traffic is handled using NAT)
- A method to allow only IP Telephony traffic across the VPN without authentication
- A method to require per-user authentication for all enterprise data traffic

There are two recommended methods for per-user authentication:

- *Authentication Proxy* uses an existing functionality in Cisco IOS to perform authentication at the network layer.
- *802.1X* uses a functionality in Cisco IOS to perform authentication at the data-link layer.

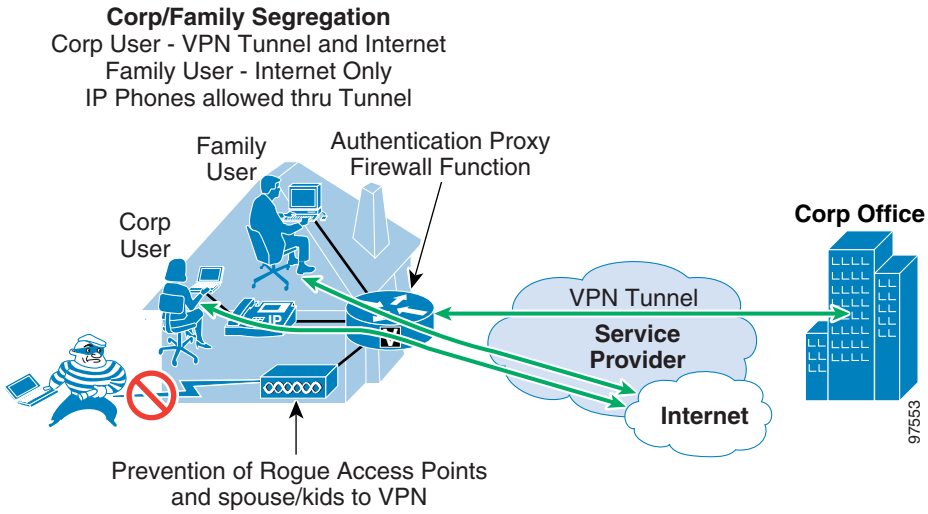
Both methods are described in the following sections—along with guidelines on which to use for specific environments:

- Authentication Proxy, page 4-17
- 802.1X for VPN Access Control, page 4-20

Authentication Proxy

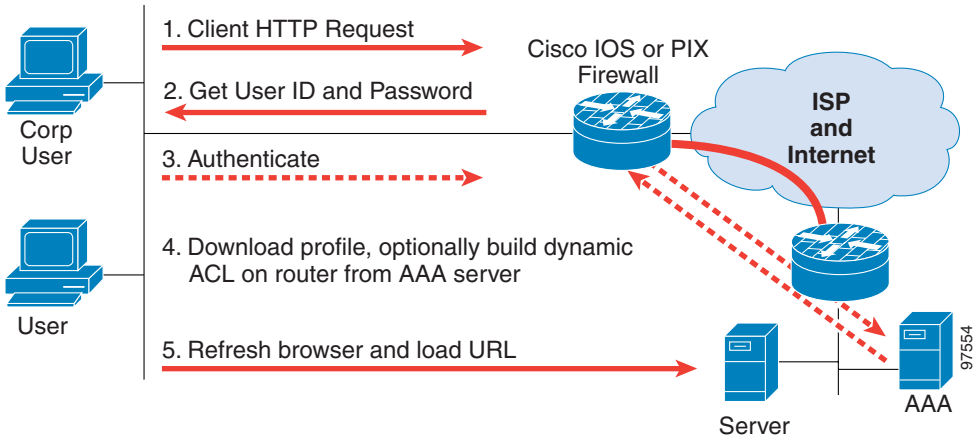
By using the Cisco IOS or Cisco PIX firewall functions—along with access control features—per-user authentication can be achieved through an authentication proxy capability. Cisco IOS and PIX firewall provide for an authentication proxy function which requiries users to authenticate with the local (in this case SOHO) firewall function. This function can be customized to provide for different network access per user—based on RADIUS server user definitions. Authentication proxy can also be customized to require only authentication for access to specific sites or from specific devices—and to use HTTPS to securely transmit the login userid/password. Figure 4-11 represents this environment.

Figure 4-11 Authentication Proxy



Authentication proxy requires per user authentication initiated via a web interface, even if the traffic is not web traffic. Users must first access an enterprise VPN reachable web page before using a non-Web enterprise application. As the user accesses an enterprise Web page, they are presented with a login web page instead. Once the user authenticates via the web page, (only) that user can access all enterprise data applications. This process is illustrated in Figure 4-12.

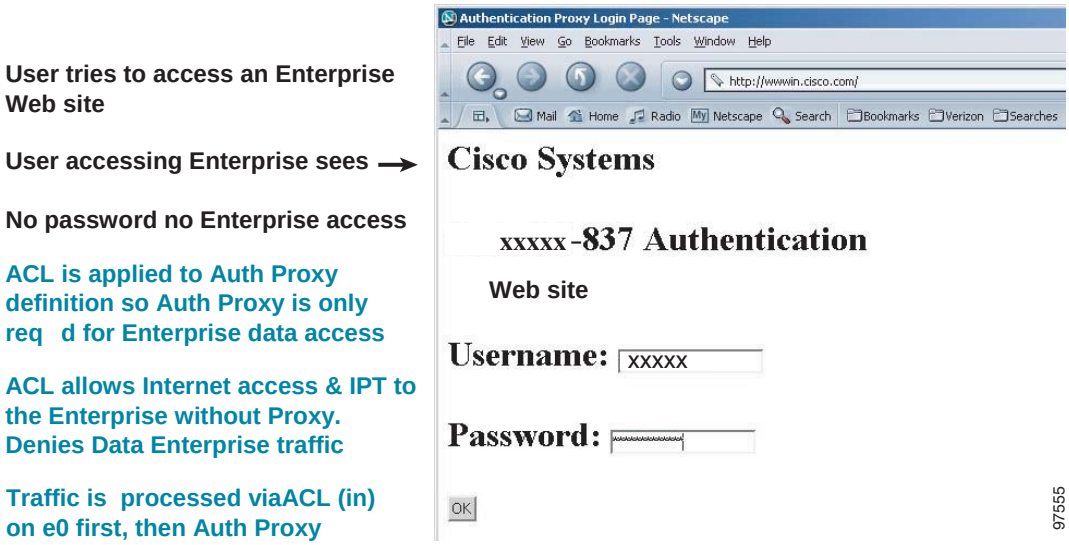
Figure 4-12 Authentication Proxy Flow



Note AAA authentication and enterprise traffic are transported through a VPN tunnel.

The user at step 2 in Figure 4-12 sees a login web page instead of the expected enterprise web page. Again, the user does not see this page for Internet traffic, and the IP Telephony traffic is allowed to bypass the authentication proxy function. The Internet and IP Telephony traffic bypass the proxy by the use of access lists on the SOHO VPN device inside interface. Traffic matching this access-control list is permitted and bypasses the authentication proxy process (which has its own access-control list permitting this traffic to pass without authentication). Traffic that is denied by the access-control list on the inside interface then is processed by the authentication proxy function. Figure 4-13 represents what the user sees when authentication is needed.

Figure 4-13 Authentication Proxy Login



After filling in an authorized user name/password and clicking OK, the user sees a new small browser window with an authentication successful message (Figure 4-14), that disappears after a few seconds. The original Web page is then automatically refreshed with the expected enterprise Web page originally requested.

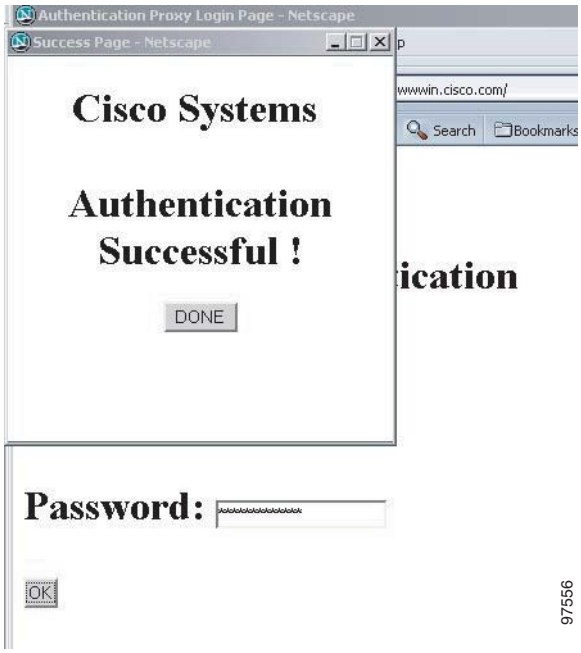
Figure 4-14 Authentication Proxy Login Successful

User types in ID and password and clicks OK button, small authentication window appears

The Small Authentication window disappears after ~3 seconds, and the Web site accessed appears on the web browser as usual

After Logging in, Teleworker can access all enterprise services (email, Web, Client-Server, etc.)

Must use the Web browser first (to authenticate the user) before user accesses non-Web Enterprise applications

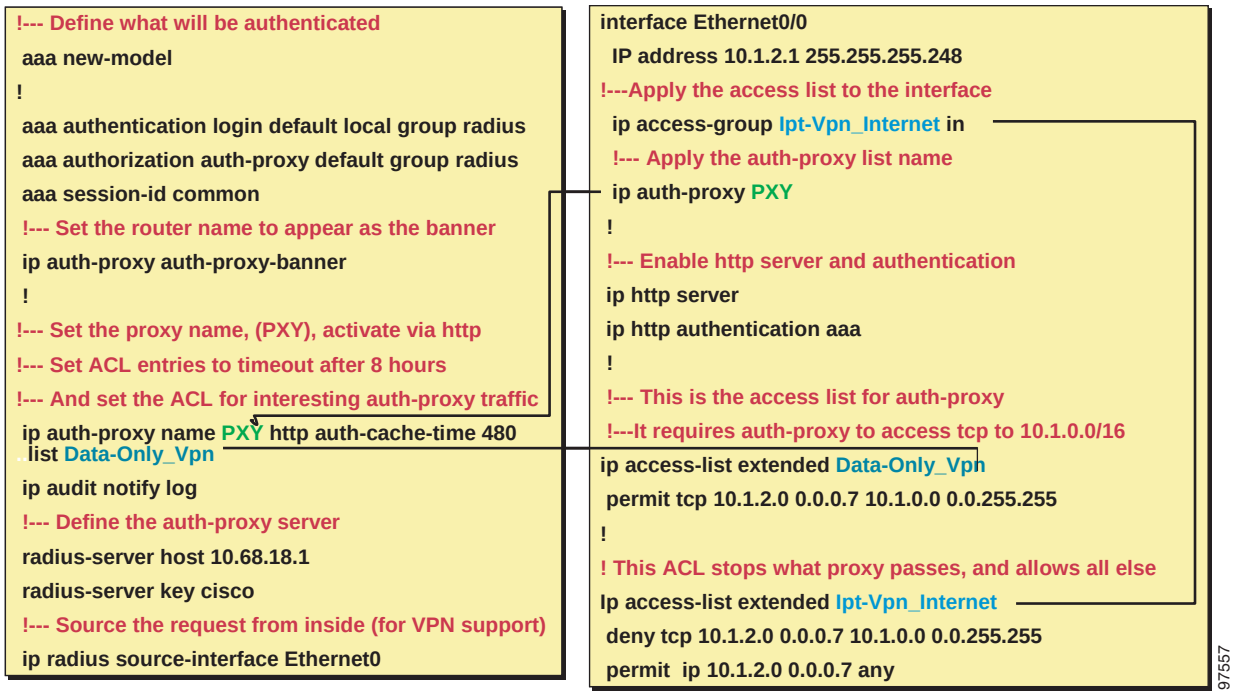


To accomplish per-user authentication for enterprise data traffic only (via VPN), while allowing NAT-based Internet traffic and IP Telephony traffic (via VPN) through, the following steps occur:

1. Define all traffic requiring NAT (Internet traffic).
2. Define the traffic which must be VPN tunneled (enterprise data and IP Telephony).
3. Define the traffic which may bypass the authentication proxy (Internet and enterprise IP Telephony).
4. Define the traffic which requires per-user authentication (enterprise data traffic).
5. Allow Internet and enterprise IP Telephony traffic past firewall authentication.
6. Require user authentication before allowing any enterprise data traffic through the VPN tunnel.
7. Apply NAT to all Internet traffic.
8. Send all VPN traffic through the VPN tunnel(s).

Figure 4-15 depicts the key Cisco IOS commands to accomplish this process. IPSec configuration is not shown.

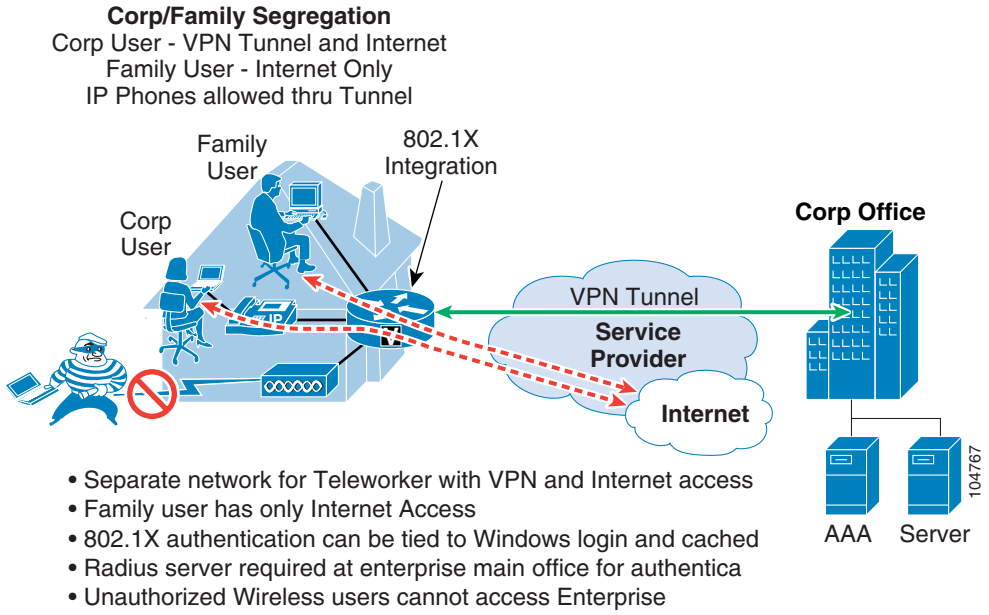
Figure 4-15 Authentication Proxy Configuration



802.1X for VPN Access Control

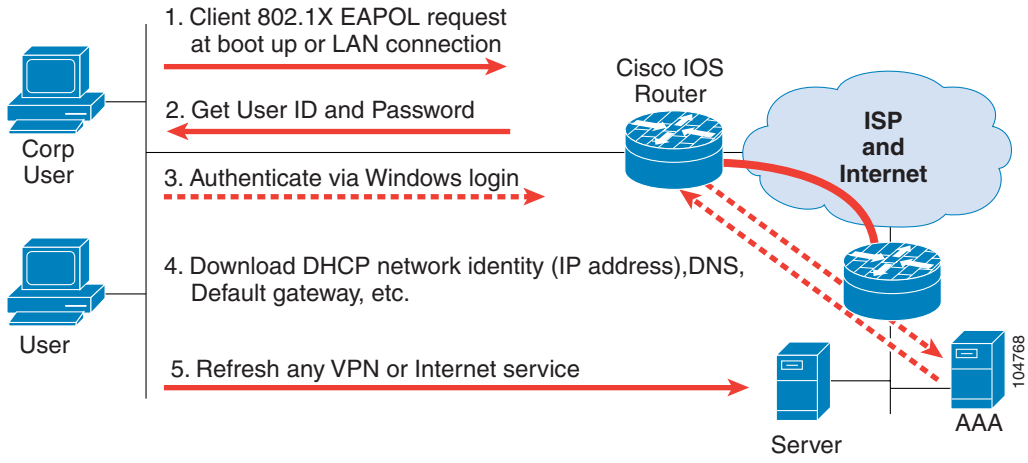
To distinguish between the teleworker and non-teleworker users, IEEE 802.1X protocol-based VPN authentication allows end hosts to send user credentials on Layer-2 via a login prompt from the PC operating system. Unauthenticated users (such as spouse-and-children users) are allowed access to the Internet, but are blocked from accessing the enterprise via the VPN. This Cisco IOS feature of Cisco 831/837 routers expands the scope of the 802.1X standard to authenticate devices regardless of the specific Ethernet LAN port to which they are attached, so that multiple devices can be independently authenticated for any given port (the Cisco 83x router has a single internal Ethernet port attached to the built-in switch). This feature separates traffic from authenticated and unauthenticated users so that separate access policies can be applied. The separation is done by supporting two IP networks—each with a separate DHCP scope—on the same home LAN. Figure 4-16 represents this environment.

Figure 4-16 802.1X Overview



When the teleworker starts up or connects the PC on the home LAN, the PC usually first requests its network identity (IP address) and other needed information from a DHCP server. For PCs enabled for 802.1X, the first request is an Extensible Authentication Protocol over LAN (EAPOL) request. When the VPN device (such as a Cisco 83x router) sees this request, it challenges the PC, which responds with the appropriate credentials (userid and password for example). The router checks with the AAA server across the VPN to authenticate the user's credentials via RADIUS. If the teleworker logs in successfully, the PC is provided a network identity and other information via DHCP which allow access to the enterprise via the VPN. If a PC is not 802.1X capable, or the user does not log in successfully, the PC will be provided a network identity that only allows Internet access. This process is pictured in Figure 4-17.

Figure 4-17 802.1X Flow



The following are VPN access control using 802.1X authentication feature advantages:

- User is prompted upon PC start up or plug-in to the LAN. Web access to a protected site to initiate challenge is not required (as in Authentication Proxy)
- The IP phone can be automatically allowed through the VPN. Just one configuration statement is required (requires multiple access lists in using Authentication Proxy method). CDP is used for IP phone discovery. See Figure 4-23.
- A separate address range for spouse-and-child PCs allows for standardized addressing and access control, and a smaller enterprise addressable subnet for each teleworker home. The spouse-and-child subnet can be the same in every SOHO, as it only has Internet access via NAT/pNAT (address translation).
- The teleworker can still communicate with non-enterprise PCs, print servers, and the like, if permitted—allowing for sharing between all home workstations. Or this communication can be limited using access-lists in the router.
- Multiple authentication types are supported, including two-way authentication and the use of certificates, as permitted in the 802.1X standard. EAP-MD5, PEAP, and EAP-TLS are among the supported authentication methods.
- PCs with static IP addresses in the enterprise addressable subnet cannot access the VPN until 802.1X authentication occurs. This reduces rogue access.
- Any wireless PC (teleworker, spouse, child, or rogue) by default cannot gain enterprise access. This reduces rogue access.

The following caveats apply when considering 802.1X implementation:

- The teleworker PC must have IEEE 802.1X supplicant (client) code. This is part of Windows XP, Windows 2000 at service pack 4 or above, or a Solaris or Linux system with an 802.1X supplicant (such as www.mtghouse.com).
- For detailed information about installing and using Microsoft 802.1X Authentication Client for Windows 2000, see Microsoft Knowledge Base Article 313664, “Using 802.1X Authentication on Computers Running Windows 2000.”
- The Cisco IOS VPN device requires Cisco IOS 12.3(2)XA, Cisco IOS 12.3(4)T, or above, and enough DRAM/flash memory (48 Mbytes/12 Mbytes for a Cisco 83x router)
- By default, teleworker PCs and IP phones must be directly connected to the built-in switch of the Cisco 83x router. EAPOL packets use a multicast address that is not forwarded by external LAN switches or wireless access points. For a wireless teleworker, PC software VPN client can provide secure access across a home wireless network and the Internet to the enterprise. The Cisco 83x router can also be configured to allow a specific device VPN access (via MAC address) by bypassing 802.1X authentication.
- Windows operating system with the supplied supplicant can request DHCP information before completing the 802.1X process. Although third party supplicants are available, a workaround follows for this condition with the Microsoft supplicant for the Teleworker.

The *Microsoft Registry Editor* (regedit.exe) enables you to change settings in your system registry. Making incorrect changes can damage your system. A Windows registry entry must be included:

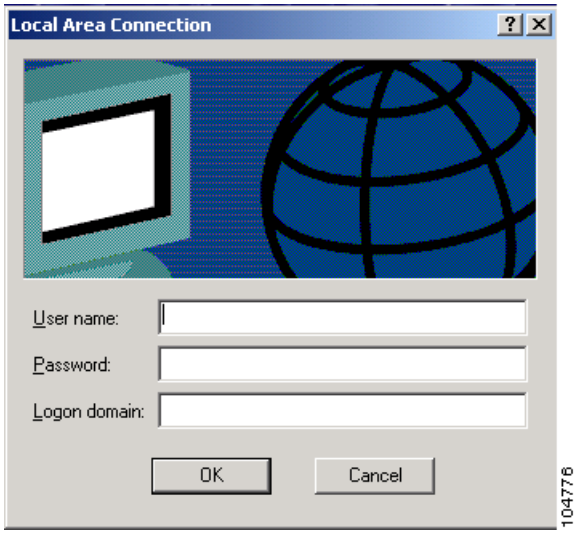
- `HKey_Local_Machine\Software\Microsoft\EAPOL\Parameters\General\Global\SupplicantMode REG_DWORD 3`

Note The `SupplicantMode` entry does not exist by default under the *Global* option in the registry. Create a new entry by including the name *SupplicantMode* as the `REG_DWORD` and then setting its value to 3.

The PC must be rebooted and 802.1X enabled on both Windows 2000 and XP. Do this as follows:

1. Open the *Network and Dial-up Connections* window.
2. Right click on the Ethernet interface (Local Area Connection) to open the properties window.
3. It should have a tab named *Authentication*. Click on the *Authentication* tab.
4. Select the check box named *Enable network access control using IEEE 802.1X*.
5. After connecting the PC to the Cisco 831 LAN interface, the dialog box shown in Figure 4-18 should appear.

Figure 4-18 802.1X Login



Using a command prompt window (Windows Start/Run), the user determines that the teleworker PC has a network address derived from the spouse-and-child network (192.168.99) instead of the enterprise network (10.81.7).

```
D:\Documents and Settings>ipconfig

Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : NONCORPUSER.org
        IP Address. . . . . . . . . . . . : 192.168.99.8
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.99.1
```

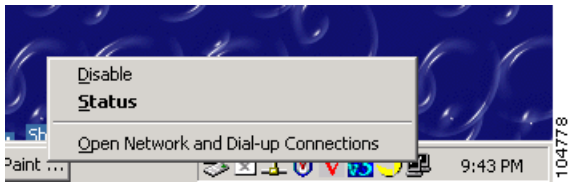
This can be rectified by typing *ipconfig /release* followed by *ipconfig /renew* in this same command prompt window. However, most users do not access a Windows command line interface, and some enterprises IT organizations disable it. The following process illustrates another method to rectify this access problem.

Step 1 Look for the icon of two connected PCs on the Windows action bar (usually bottom right). See Figure 4-19.

Figure 4-19 Network Icon

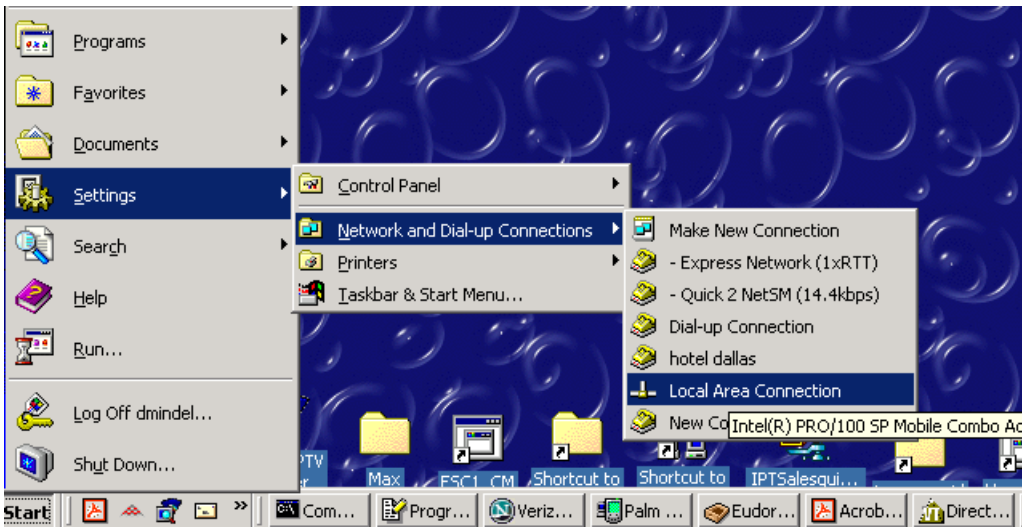
Step 2 Right mouse click this icon, and select *disable*. See Figure 4-20.

Figure 4-20 Disable NIC



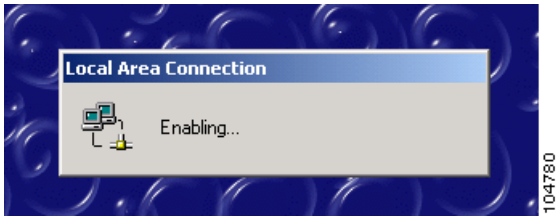
Step 3 Click *Start/Settings/Network* and *Dial-up Connections/Local Area Connection*. This automatically enables the PC LAN adapter again. See Figure 4-21.

Figure 4-21 Enable NIC



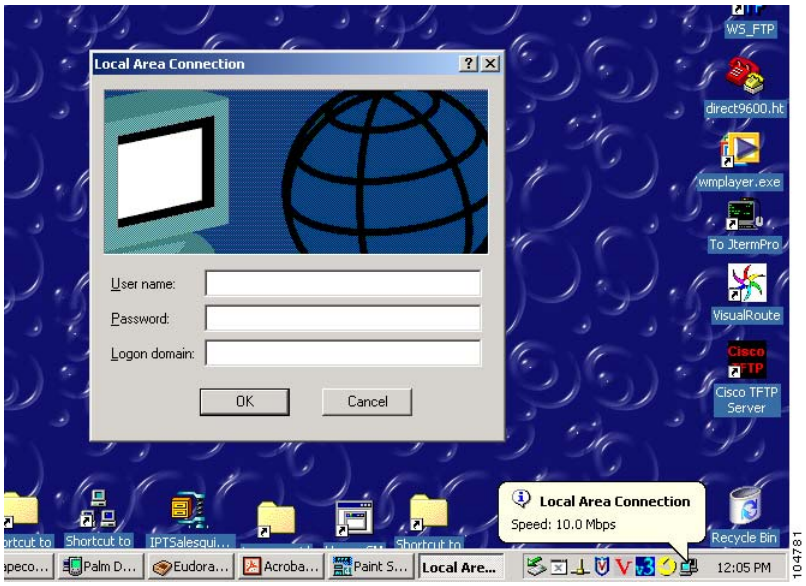
Step 4 The small window stating the NIC is enabling appears. See Figure 4-22.

Figure 4-22 NIC Enabling



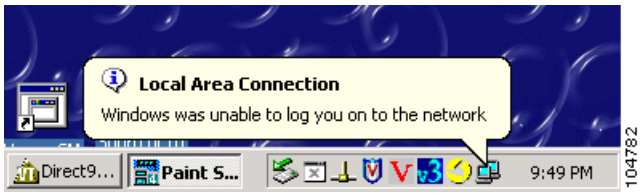
Step 5 The 802.1X login window appears again. See Figure 4-23.

Figure 4-23 802.1X Login



Step 6 Logging in successfully will now provide full access to the VPN. If the Teleworker does not log in with a few minutes, the message below is seen, and the process above needs to be repeated. See Figure 4-24.

Figure 4-24 Login Unsuccessful



As can be seen from the command prompt windows, the following information has changed:

```
D:\Documents and Settings>ipconfig

Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cisco.com
        IP Address. . . . . . . . . . . . : 10.81.7.83
        Subnet Mask . . . . . . . . . . . : 255.255.255.248
        Default Gateway . . . . . . . . . : 10.81.7.81
```

Configuration of VPN access control using 802.1X authentication requires three steps:

1. Configuring the PC
2. Configuring the IOS VPN device
3. Configuring the AAA server.

All steps are documented at:
www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xa/gt_802_1.htm

Figure 4-25 illustrates a partial IOS configuration highlighting 802.1X options.

Figure 4-25 802.1X Partial Configuration

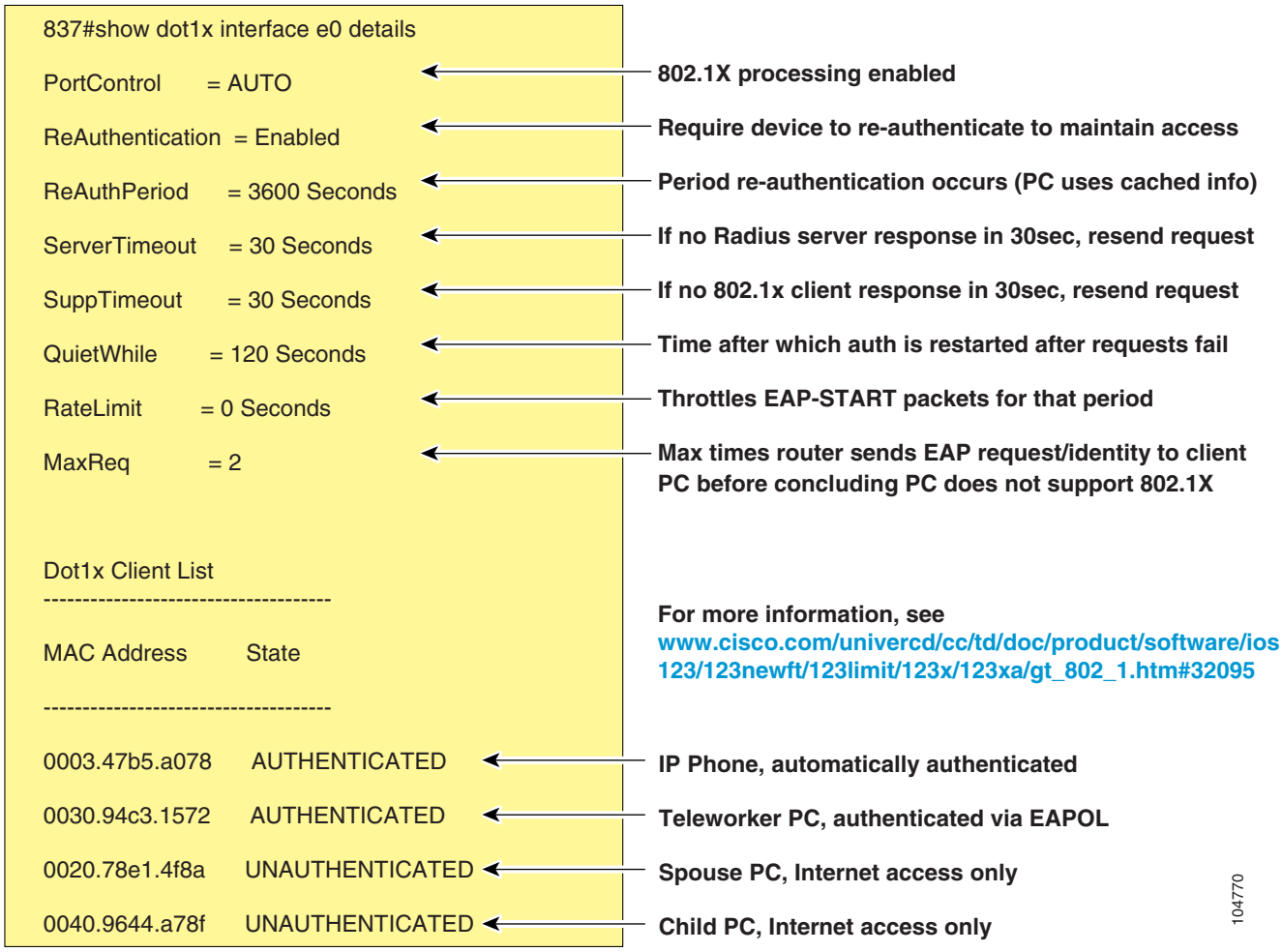
```
!---Define what will be authenticated
aaa new-model
aaa authentication login default local group radius
aaa authorization dot1x default group radius
aaa session-id common
!---Define DHCP pools: Teleworker and Home devices
ip dhcp pool CORPUSER
  network 10.81.7.80 255.255.255.248
  default-router 10.81.7.81
  dns-server 6x.10x.x.247 17x.6x.22x.120
  domain-name cisco.com
  option 150 ip 10.87.110.11
  netbios-name-server 17x.6x.23x.228 17x.6x.23x.229
!
!ip dhcp pool NONCORPUSER
  import all
  network 192.168.99.0 255.255.255.0
  default-router 192.168.99.1
  domain-name NONCORPUSER.org
!
ip audit notify log
!---Source the request from inside (for VPN support)
ip radius source-interface Ethernet0
!---Define the 802.1x server
radius-server host 10.81.0.19 auth-port 1645 acct-port 1646
radius-server key cisco
```

```
!---Enable spawning virtual interfaces for home devices
template Virtual-Template1
 !---Define 802.1X and options
 dot1x system-auth-control
 identity profile default
 description 802.1x configuration
template Virtual-Template1
 device authorize type cisco ip phone
 !
 !---Define gateway interface used by home devices
 interface Loopback0
 description NONCORPUSER inside interface
 ip address 192.168.99.1 255.255.255.0
 !---Define 802.1 X on inside interface
 interface Ethernet0
 ip address 10.81.7.81 255.255.255.248
 ip nat inside
 ip tcp adjust-mss 542
 dot1x port-control auto
 dot1x reauthentication!
 !
 !---Define template used for each home device
interface Virtual-Template1
 ip unnumbered Loopback0
 ip nat inside
 ip tcp adjust-mss 542
```

104769

The router keeps track of which devices are authenticated. To see the current status of 802.1X function on the router, use the **show dot1x1** command as shown in Figure 4-26.

Figure 4-26 802.1X Monitoring



For all models: 802.1X is recommended to provide per-user authentication except for the scenarios listed below, where Authentication Proxy is recommended:

- Teleworker PCs do not have an 802.1X client installed or enabled.
- The existing Cisco 831 or Cisco 837 devices do not have enough DRAM or flash to run the new Cisco IOS images with this function (Cisco IOS 12.3(2)XA, Cisco 12.3(4)T, or above).
- There is a LAN switch between the Cisco IOS VPN device and teleworker PC or IP phone. EAPOL frames will be discarded by a LAN switch.
- The teleworker wishes to use wireless to communicate across the VPN and the enterprise does not support remote access VPN. Wireless access points will discard EAPOL frames.
- The VPN device is not based on Cisco IOS (for example, Cisco PIX 501).

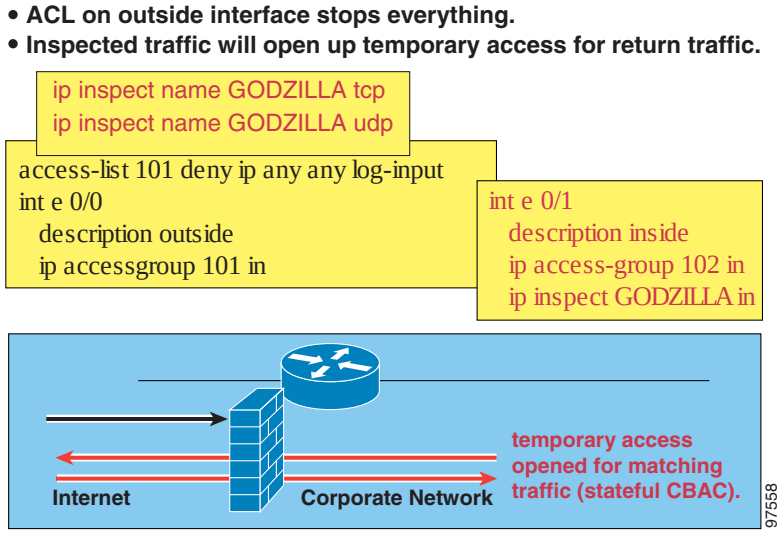
Note Caveat: When using Authentication Proxy and NAT, Context Based Access Control (CBAC) must also be configured. Please see the link below.
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d981d.html#1001127

Note Caveat: Authentication Proxy requires multiple access lists to use for Teleworker; enterprises with discontiguous or multiple networks will require longer access lists.

Context-Based Access Control

CBAC inspects the activity behind a firewall. CBAC specifies what traffic is allowed in, and what traffic is allowed out by using access-control lists (in the same way that Cisco IOS uses access-control lists). However, CBAC access-control lists include **ip inspect** statements that allow the inspection of the protocol to make sure that it has not been tampered with data before the protocol reaches systems behind the firewall. By using CBAC, additional security is provided for teleworkers and home users. It only allows traffic to the SOHO from sessions initiated by the SOHO users. Figure 4-27 represents how CBAC works; the SOHO router inspects all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic.

Figure 4-27 CBAC Operation



For all models—CBAC is recommended to provide security to all SOHO systems.

Firewall Options

To provide security, Cisco 8XX and Cisco 9XX routers, and Cisco PIX firewalls offer multiple features:

- Access-Control Lists
- Context-Based Access Control
- Intrusion-Detection System
- Authentication Proxy
- Port-To-Application Mapping

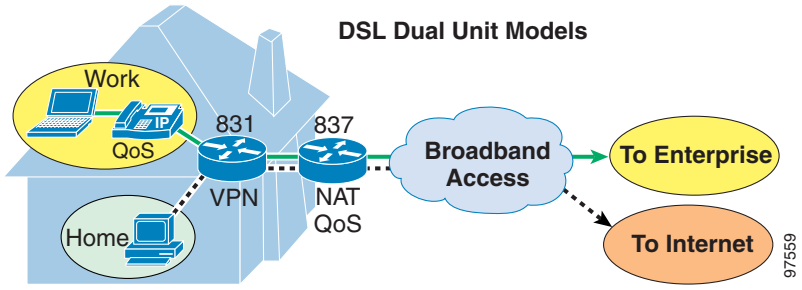
Split Tunneling

Split tunneling is the ability to allow traffic that is not part of enterprise communication to go directly to the Internet without being encrypted. Split tunneling is efficient because it encrypts only business-related traffic and avoids sending Internet traffic in and out of the enterprise network. Although split tunneling poses a security risk if any of the machines on the SOHO LAN become compromised from the Internet, it can address security risks from home PCs (non-teleworker) accessing the enterprise network. The *SAFE VPN IPSec Virtual Private Networks in Depth* white paper discusses the security issues of split tunneling in detail.

Split tunneling might not be allowed by the enterprise security policy. If not, there are two options:

- **All Models**—All Internet traffic from teleworker and home PCs must traverse the VPN. This model is easiest to implement, but is a risk to the enterprise from non-teleworker users.
- **DSL Dual Unit Deployment Model**—Connect home PCs to the Cisco 837. The Cisco 837 broadband router provides four 10/100 switched Ethernet ports. This allows for three home devices connected for Internet access, but blocks access to the VPN tunnel. The fourth Cisco 837 Ethernet port is used to connect the VPN device. Figure 4-28 depicts this option.

Figure 4-28 Spouse-and-Child Network Outside VPN



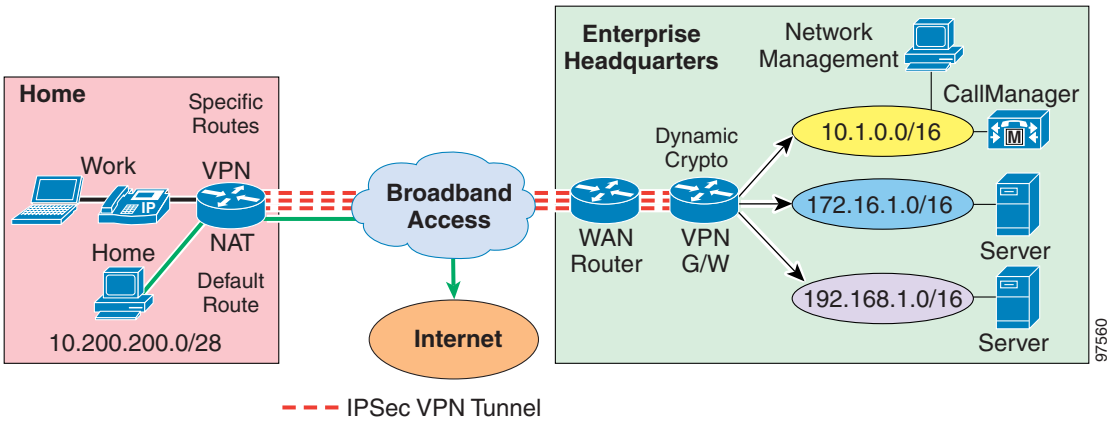
For **all deployment models**, if split tunneling is allowed, there are specific *caveats* to be addressed:

- If the SOHO VPN device or PPPoE session is restarted, an obsolete entry may exist in the enterprise VPN device. This entry points to the SOHO subnet as being behind a public IP address that is no longer valid. Using IKE keepalive, the VPN tunnel session loss can be detected after three lost keepalives, thus clearing the obsolete entry and allowing a new entry to be created when the SOHO VPN device next requests a VPN tunnel. The default IKE keepalive value is 10 seconds.
- If the enterprise network does not consist of a single contiguous IP address space—and the SOHO receives a dynamic IP address from the service provider (requiring dynamic crypto maps at the central site VPN gateway)—multiple VPN tunnels to each SOHO might be created. This requires additional resources in the enterprise VPN gateway. Without split tunneling, all traffic from the SOHO is sent via the VPN tunnel. With split tunneling, the default route is out to the Internet and specific routes are defined to be sent via VPN. If an enterprise has 10 separate subnets and traffic is sent to all those networks from a SOHO, then 10 VPN tunnels—each with separate security association (SA)—are created (in addition to the IKE SA). For the central site VPN gateway, there is a potential for more VPN tunnels than there are teleworker sites. This should be considered for enterprise VPN device sizing.
- The Cisco 831 and Cisco 837 support a maximum of 10 SAs; the Cisco PIX 501 supports a maximum of five SAs, limiting the use of split tunneling in enterprises with non-contiguous subnets or multiple classful networks. If split tunneling is still preferred in this environment, Cisco routers support the use of GRE and IPsec, providing the ability to run routing protocols across the IPSec tunnel.

- In the split tunnel case with non-contiguous enterprise subnets and dynamic crypto maps, a tunnel might time out if the SOHO LAN has no traffic to send to that enterprise subnet—because the SOHO VPN device creates the tunnel. If the SOHO is to be managed by the enterprise, the management station must be on an enterprise subnet to which the SOHO VPN device has an active tunnel. SAs time out after 60 minutes by default. To keep management communications active:
  - Put the management station on the same subnet as the call managers because the IP phones send keepalives—if Skinny Client Control Protocol (SCCP)—and will keep the tunnel active.
  - Configure NTP or Cisco Service Assurance Agent (SAA) response time reporter on the SOHO device with the server on the same network (hitting the same access-control list) as the management station to keep the tunnel active.

Figure 4-29 represents the issues with discontiguous enterprise networks:

Figure 4-29 Issues with Discontiguous Enterprise Networks



For **all Integrated Unit and Integrated Unit + Access Device models** using split tunnels with service provider dynamic addressing, inactive SAs are not a concern if the SOHO is to be managed by the service provider. The Integrated Unit can be managed via its public IP address. The method used should be Simple Network Management Protocol (SNMP) V3 with authentication and console access via Secure Shell (SSH). Service providers can use the mapping between PPP session (by username) and IP address to determine the public IP address currently in use by a specific user.

For the **Dual Unit model**, using split tunneling with a single dynamic address from the service provider requires pNAT. Because the port numbers used by IPSec negotiation are meaningful and pNAT dynamically maps port numbers to accomplish translation, the broadband router must have application knowledge to track associated IPSec port numbers. This is called IPSec *raw pass-through* and is currently supported by the Cisco 800 Series routers.

Note If there is a significant number of discontiguous subnets or networks, or the networks change, then GRE and an IP routing protocol can be used to reduce configuration.

Two-Teleworker Homes

Homes with two teleworkers from different organizations face a number of options:

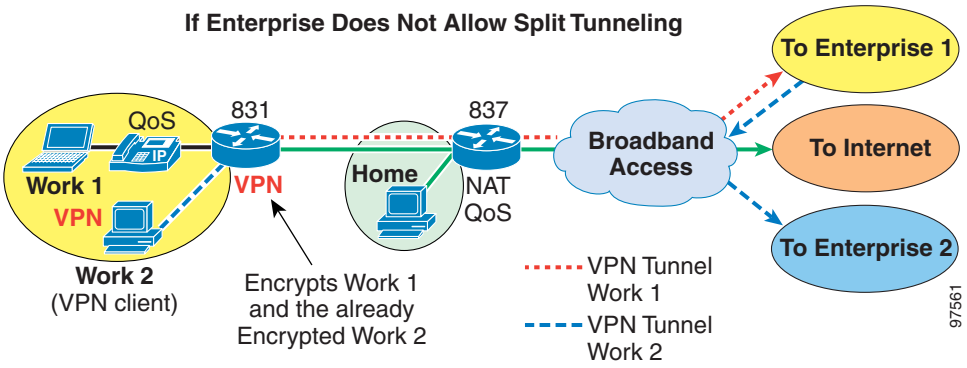
- For **all deployment models**, the entire SOHO environment can be duplicated—resulting in two separate deployments in the home. This can be done with two DSL, ISDN or wireless circuits, or any combination of DSL, ISDN, cable, or wireless. Cable providers might not provision two separate cable access circuits to the home. This option is recommended.
- For **all deployment models**, if the second teleworker PC is on the SOHO LAN behind the VPN device, a VPN software client can be installed on the second teleworker PC for secure communications.

  Secure IP telephony would not be available for the second teleworker.

  If the first teleworker enterprise's security policy does *not* allow for split tunnels, this option only works if the first teleworker enterprise allows encryption from their internal network to the Internet. In addition, there might be maximum transmission unit (MTU) issues, because the IPSec packet from the second teleworker's VPN client is encrypted again by the first teleworker's VPN device.

  Figure 4-30 illustrates this alternative.

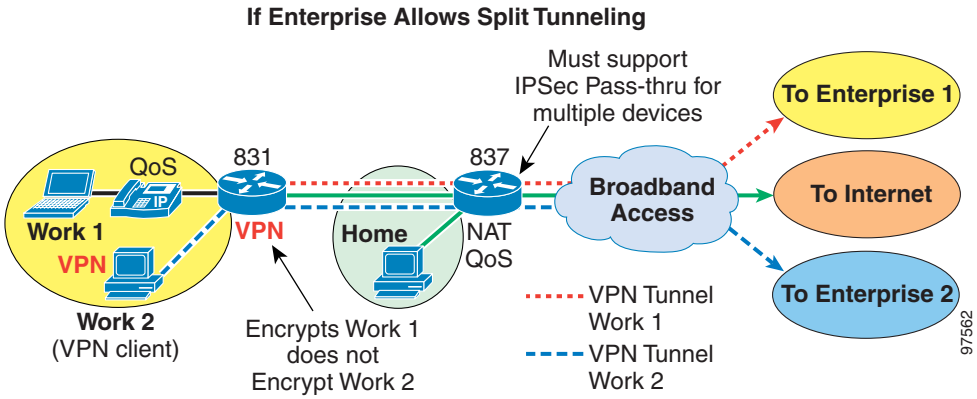
Figure 4-30 Special Considerations for Dual-Teleworker Home (Split Tunnelling Not Allowed)



- For **all Dual Unit models**, if the first teleworker enterprise's security policy allows for split tunnels, the second teleworker can use VPN client software to securely access that user's respective enterprise. For this to function, either the broadband access router must support IPSec pass-through of multiple devices with pNAT, or the VPN device must support IPSec NAT transparency.

Figure 4-31 illustrates this alternative.

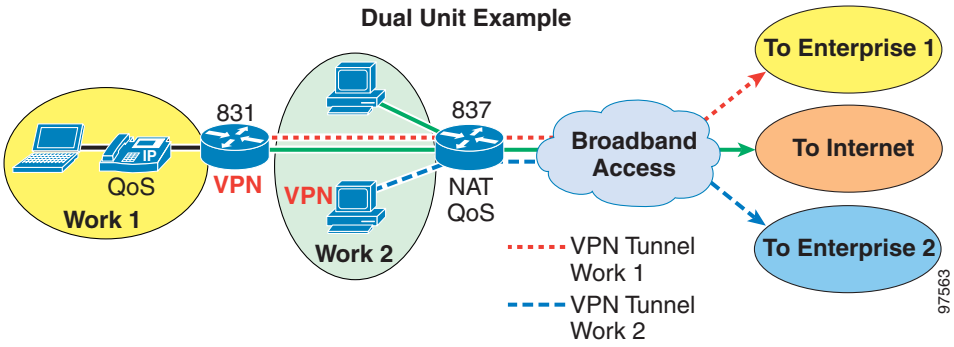
Figure 4-31 Special Considerations for Dual-Teleworker Home (Split Tunnelling Allowed)



- For **all Dual Unit models**, the second teleworker has secure access if the second teleworker PC is on the non-secure network, however:
  - Secure IP telephony would not be available for the second teleworker.
  - The service provider must support multiple PPPoE tunnels across a single PVC.
  - This option requires the access router (such as the Cisco 837 or Cisco 905) to support IPSec pass-through of multiple IPSec sessions because it is performing pNAT.

  Figure 4-32 illustrates this option.

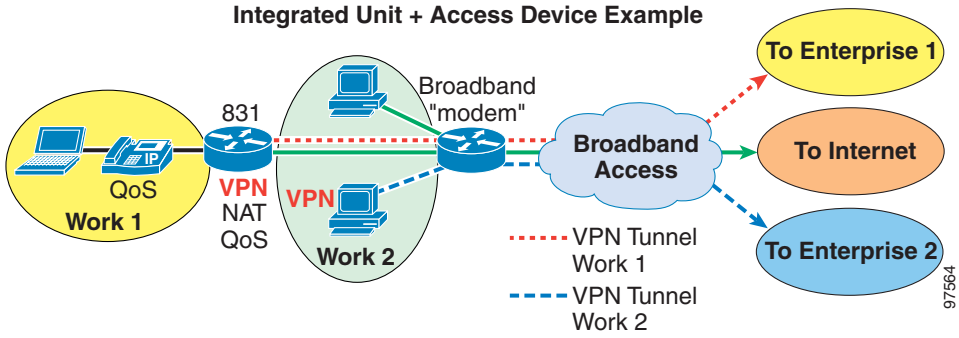
Figure 4-32 Dual-Teleworker with Dual Unit Model



- For **all Integrated Unit + Access Device models**, the second teleworker has secure access if the second teleworker PC is on the non-secure network, however:
  - Secure IP telephony would not be available for the second teleworker.
  - The service provider must support multiple PPPoE tunnels across a single PVC.
  - The second teleworker must run a PPPoE software client on their PC.
  - This option is not recommended due to the lack of QoS for *Work 1* PC and telephone illustrated in Figure 4-33. Competing traffic from PCs connected to the broadband modem can cause delay and loss since the broadband modem has no QoS. Also, there is a risk of running PPPoE software on the second teleworker PC; enterprises might prohibit the installation of non-authorized software on work PCs.

This option is illustrated in Figure 4-33.

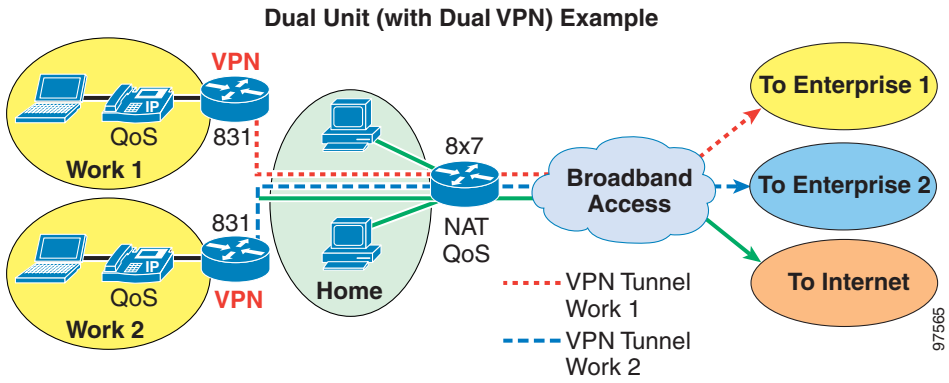
Figure 4-33 Dual-Teleworker with Integrated Unit Model



- For **all dual unit models**, a second VPN device can be added, with both running in parallel. This option requires sufficient bandwidth if both teleworkers use IP Telephony. The required bandwidth depends on coder-decoder (codec) and access circuit type. For encrypted G.729 using PPPoE, assume 64 Kbps per call is needed. Implementation considerations:
  - This option requires the access router to support IPSec pass-through of multiple IPSec sessions, since it is performing pNAT.
  - If both teleworkers use IP Telephony, the broadband access circuit must have sufficient bandwidth for two simultaneous calls. Using a G.729 codec is recommended.

  Figure 4-34 illustrates this option.

Figure 4-34 Dual-Teleworkers with IP Telephony



IP Multicast

Each teleworker site is connected via an IPSec VPN tunnel, which creates a hub and spoke network. IP multicast is used by some IP routing protocols (OSPF, EIGRP). Additionally, teleworkers typically wish to participate in a one-way multicast. Supporting IP multicast requires GRE to be used between the teleworker VPN device and the enterprise VPN gateway. As most teleworker environments do not require IP routing protocols to the remote site, and teleworkers can participate in one-way communications via unicast, GRE is generally not required.

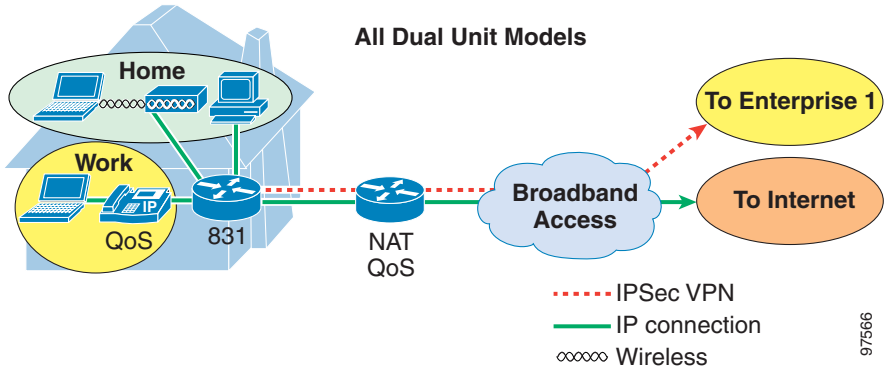
In-Home Wireless

In-home wireless provides for the convenience and function of working online regardless of the location in the home. Using 802.11b wireless technology via a Cisco access point, such as the AP-1100, provides high performance (up to 11 Mbps), long reach and enterprise-level security. Since there are likely to be few simultaneous users of shared wireless bandwidth, and this bandwidth exceeds the available broadband access bandwidth using cable or DSL, performance should not be affected by in-home wireless connection for data or voice (using an 802.11b IP handset for example).

Along with the flexibility of wireless comes risk. If incorrectly configured, wireless traffic can be easily captured and analyzed outside of the home. A wireless device from outside the home can easily use a wireless network. In order to protect the enterprise from these, certain models and security method combinations are recommended.

For **all Dual Unit models**, and **all Integrated Unit + Access Device models**, the wireless network can be used by non-teleworker PCs and laptop computers. Although the use of WEP is recommended, wireless security does not affect the enterprise or teleworker, and enterprise traffic does not traverse the wireless network, and the wireless network has no access to the unencrypted teleworker traffic. Figure 4-35 depicts this set up.

Figure 4-35 In-Home Wireless Access for Spouse-and-Child Network



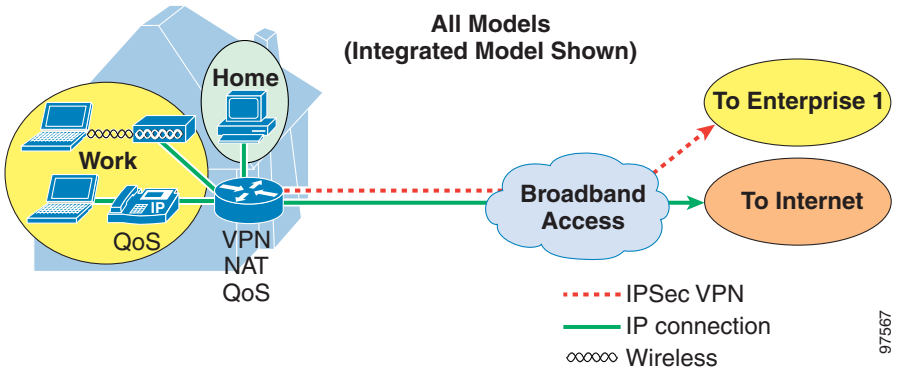
For **all models,** if only the teleworker uses the wireless network, and appropriate wireless security is used, the teleworker has flexibility while the enterprise is not exposed to undue risk. Appropriate wireless security includes:

- Using Extensible Authentication Protocol-Cisco (EAP-Cisco) and Cisco-enhanced Wired Equivalent Privacy (WEP) for authentication and encryption respectively. These methods provide for authentication without statically defined WEP keys in wireless access points or clients. This is accomplished by centrally controlling the keys (via a RADIUS server for example) and tying the key to the user by network logon.

- Using Cisco-enhanced WEP to provide authentication and encryption. This method provides for authentication without a statically defined WEP key in wireless access points. This is accomplished by centrally controlling the keys (via a RADIUS server for example) and defining the WEP key (128 bit recommended) on the teleworker wireless client software.

Figure 4-36 depicts this setup.

Figure 4-36 In-Home Wireless Access for Teleworker

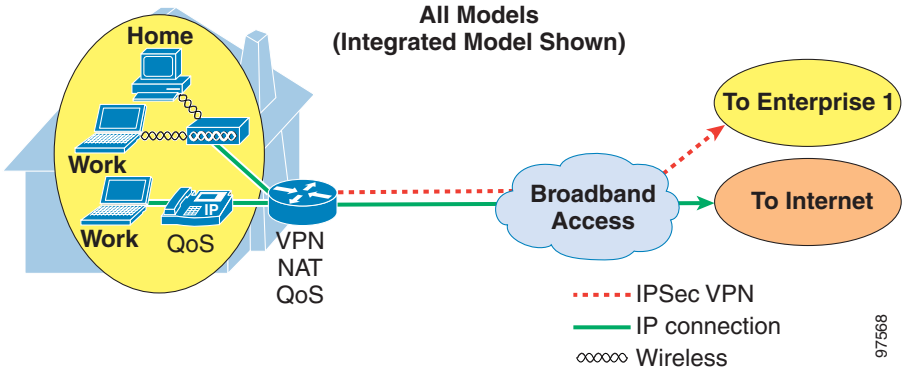


For **all models**, if both the teleworker and non-teleworkers are to use wireless, there is one option, which is *not recommended*:

- All SOHO users would have access to the enterprise VPN; hand out cards with WEP keys put in the wireless card flash during staging at the enterprise. Although the WEP key is statically configured, the user never has the key (not retrievable from wireless card). The security weakness of static WEP keys is mitigated by Cisco techniques of creating temporary keys for encryption. These temporary keys are based on a per packet dynamic key creation by hashing the WEP key and the value of the initialization vector used in 802.11b (which changes per packet per wireless association).
- If EAP-Cisco is used, the enterprise must create a userid and password per spouse/child.

Figure 4-37 depicts this.

Figure 4-37 In-Home Wireless for Shared Usage



Improved Availability

For this design guide, the SOHO LAN device is assumed to be non-redundant. While this creates a single point of failure per SOHO LAN, it is assumed that the SOHO LAN has constraints for cost. Failures at the SOHO are more likely to result from power and network failures rather than from individual device failures. At the SOHO, the important factor for improved availability is the ability of the device to recover from interruptions in service—both on the communications link and at the enterprise head end.

- For **all Dual Unit models**—The Cisco 831 supports dial-up networking via the console port.
- For **all Integrated Unit + Access Device models**—The Cisco 831 supports dial-up networking via the console port.
- For the **DSL Integrated Unit model**—The Cisco 837 supports dial-up networking via the console port.
- For the **Cable Integrated Unit model**—The Cisco 905 is currently not recommended due to the aforementioned QoS issues.

Although the Cisco 831 and Cisco 837 routers support dial-back in case of DSL (Cisco 837) or Ethernet (Cisco 831) outages, the function is limited. If an outage is caused by PPP (negotiation failure, service provider aggregation router failure, or failure inside the service provider network between the SOHO router and the service provider aggregation router), the virtual access interface is down, but the dialer and physical interfaces remains up. Thus dial-back does not occur even though the line is down.

For teleworker locations, availability can be achieved via fall back to dial-up networking through a POTS connected to the teleworker PC line for data—and a POTS line or cell phone for voice.

Improved availability is more important for the enterprise VPN gateway. Ideally, there can be dual VPN gateways and ISP connections. Each type of device has methods for providing device redundancy at each location.

For **all deployment models**, the teleworker VPN device supports multiple definitions for enterprise VPN gateways. If the first VPN tunnel fails and cannot be re-established, the teleworker VPN device initiates a VPN tunnel with the secondary gateway. The following configuration fragment lists a partial Cisco IOS example of multiple tunnel definitions:

```
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
!
crypto map test 1 ipsec-isakmp
 set peer xx.xx.223.3
 set peer xx.xx.223.4
 set transform-set t1
 match address 101!
```

Management

Due to the potentially large number of teleworkers, and their potential lack of technical networking expertise, it is important for CPE configuration and upgrade to be centrally controlled and automated. Initial configuration (a stub configuration) can be provided by Cisco during product manufacturing. Alternately, this can be done using the Cisco Router Web Setup (CRWS) tool built into all Cisco 83X and Cisco 9X5 routers.

Using tools such as the IE2110, Cisco IOS-based CPE can be automatically configured without manual intervention. The solution also provides for configuration backup-and-restore functionality and Cisco IOS image upgrades.

Teleworker device management generally requires capability in the CPE and management applications. Below are the capabilities or programs available to provide large scale teleworker deployment.

For the CPE, the following functions are available:

- SNMP agent—Providing for sending of traps or responding to polls by an SNMP manager
- Syslog—Providing configurable event logging on the local device and to a remote managing device
- SAA—Providing response time statistics to track delay
- NetFlow—Providing configurable traffic statistics gathering, summarization and reporting
- CNS Agents—Providing a robust API for automated configuration and device management

The following list summarizes Cisco management applications that provide allow device or function management by enterprises or service providers:

- Cisco Networking Services (CNS) Configuration Registrar—IE2100-based configuration management automation
- CNS NetFlow Collector Engine—Collection and summarization of traffic statistics and reporting
- CNS Performance Engine (CNS-PE)—Gathers and reports response-time information from SAA
- Internet Performance Monitor (IPM)—Gathers and reports response-time information from SAA; software only
- CNS Notification Engine (CNOTE)—Gathers and processes Syslog messages; sends SNMP traps
- IDS Director—Collects intrusion alerts and sends new signatures to firewall devices
- IP Solutions Center (ISC)—Provides for large scale VPN provisioning and management
- Cisco Info Center (CIC)—Event acquisition, consolidation and correlation

Basic Device Provisioning

Device provisioning for teleworkers can be done in multiple ways:

- Central staging devices via copy/paste from the console. Fast and easy, few changes required to make each device unique.

  Recommended for **all models**.

- Configuration Express is offered by Cisco to pre-configure equipment during manufacturing using the supplied configuration during ordering. The CPE can be shipped directly to the end user already customized, with an appropriate end-user setup page.

  Recommended for **DSL Integrated** and **All Integrated Unit + Access Device models** using fixed port CPE (Cisco 8XX).

- Automatic provisioning via IE2100 to provide an automated method to customize each teleworker device.
- CRWS allows the end user to customize the configuration via a web browser. The tool was enhanced to support Easy VPN authentication and basic provisioning.

  Recommended for **DSL Integrated Unit or All Integrated Unit + Access Device models** only if Easy VPN is used for VPN provisioning.

Provisioning IPSec VPN

This solution must scale to potentially thousands of users for large enterprises, and be simple to deploy for small and medium enterprises. Site-to-site VPN deployment has traditionally required non-trivial definitions in the remote CPE. There are two methods to accomplish scalable deployment and management for VPN: central staging with traditional IPSec definitions and Easy VPN.

Using traditional IPSec definitions and centrally staging and testing all CPE, while more resource intensive, provides a plug-and-play solution for teleworker installations. If changes are required in the teleworker VPN device, this must be done manually with Telnet or with a management application such as VMS. VPN problem resolution after installation might require console access (Telnet) to the teleworker VPN device. Central staging also allows for secure installation of digital certificates onto teleworker VPN devices. With a well-tested remote VPN device configuration template, traditional IPSec definitions are a highly reliable and proven method of provisioning VPNs for SOHO.

Easy VPN provides for automatic central provisioning of VPNs for teleworker devices, and is a function included in Cisco IOS IPSec images and the Cisco PIX firewall. Easy VPN enables the teleworker VPN device to automatically establish and maintain a VPN tunnel with a minimal configuration in the teleworker VPN device. The specific definitions required in the teleworker VPN device—including IPSec, Internet Security Association and Key Management Protocol (ISAKMP), authentication, and access-control lists—are downloaded from the head-end VPN gateway via IKE extensions known as *Mode-Config*. The terminology for Easy VPN devices includes the server (head-end VPN gateway) and client (remote VPN device such as a Cisco 8XX router with IPSec image or a Cisco PIX 501). There are two modes of operation for the Easy VPN client. The *network extension mode* is currently recommended for teleworkers because this provides the ability to access the remote site from the central site (the remote site has an enterprise addressable subnet). This is required for IP Telephony because incoming calls require central site session initiation. *Client mode* also functions appropriately, and was tested in the Cisco teleworker pilot.

Below is a summary of the items that Easy VPN automatically manages:

- Negotiating VPN tunnel parameters (IP addresses, algorithms, SA lifetime)
- Establishing VPN tunnels according to these parameters
- Dynamic creation of the NAT/pNAT definitions and associated access lists
- Authentication via group name and password, and username and password
- Managing security keys for encryption/decryption
- Support for multiple VPN central gateways (IPSec peers) for improved availability

Below are examples IPSec Cisco IOS configuration fragments that highlight the definitions required with traditional Cisco IOS crypto definitions and using Easy VPN.

Traditional crypto teleworker VPN device definitions:

```
crypto isakmp policy 1
 encr 3des
crypto isakmp key cisco address <VPN gateway IP address>
```

```
crypto isakmp keepalive 10
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
!
crypto map test 1 ipsec-isakmp
 set peer <VPN gateway IP address>
 set transform-set t1
 match address 101

interface Dialer1

 crypto map test

access-list 101 permit ip <local subnet> <local wildcard mask> any
```

Easy VPN teleworker VPN device definitions:

```
crypto ipsec client ezvpn hw-client
 group <thegroupname> key <thepassword>
 mode network-extension
 peer <VPN gateway IP address>

interface Dialer1

 crypto ipsec client ezvpn hw-client
```

The difference is that Easy VPN does not require IPSec specific definition—only group name and password, user name and password, and enterprise VPN gateway IP address (or name if using DNS).

Recommendations for which method to use follow.

For **all models:**

- If digital certificates are used for authentication, use traditional crypto definitions. Easy VPN does not yet support digital certificates.
- If no user involvement with VPN initiation is preferred, use traditional crypto definitions (Digital Certificates or pre-shared keys). As will be discussed in the "Management" section on page 4-38, Easy VPN requires the teleworker to initiate the VPN tunnel via web GUI on the Cisco 837 and Cisco 831 (CRWS).
- For other environments—Use Easy VPN.

Easy VPN Client minimum software levels are:

- Cisco IOS 12.2(8)YJ or later
- For Cisco 831/837 multiple-VPN peer support, Cisco IOS 12.2(13)ZG or later
- PIX 6.2 or later

Easy VPN Server minimum software levels are:

- Cisco IOS 12.2(8)T or later
- PIX 6.2 or later
- VPN3000 3.1.1 or later

Provisioning Authentication

IPSec VPN networks can be designed in different manners for the teleworker. Each option has benefits and caveats related to function, performance and scalability. Please refer to the discussion provided in the "VPN Network Design" section on page 4-13 for discussions of the following available design options:

- Traditional IPSec
- Traditional IPSec with GRE
- Dynamic Multi-point VPN (DMVPN)

The "VPN Authentication" section on page 4-14 reviewed the following authentication methods:

- Shared secrets with a RADIUS server back-end—Provides scalable authentication
- Digital certificates method—Allows for highly secure and scalable authentication
- Easy VPN method—Provides for a simplified and scalable solution by implementing simple definitions and a preset combination of authentication options.

Due to the number of issues with authentication, the following recommendations are general and might not fit every deployment.

- Digital certificates should be used where there is in-house skill and infrastructure for X.509 and a certificate authority (CA).
- Shared secrets with IKE aggressive mode and RADIUS should be used where no CA server or skill is available.
- Easy VPN should be used where simple SOHO VPN deployment, user authentication and/or one-time passwords via tokens are required. It should not be used if improved availability VPN is required (does not currently support multiple VPN tunnel definitions for backup enterprise VPN gateways).

Policy and Device Management

The controlling requirement is that the SOHO LAN users do as little management of the system as possible. The enterprise security/network managers must manage configuration and security policy on the SOHO VPN devices remotely. As required by the SAFE blueprint (please refer to http://www.cisco.com/warp/public/779/largeent/issues/security/safe.html) the management connections must be protected by IPSec or equivalent, such as SSH or SSL. The management tools must be scalable to the expected number of SOHO LAN devices. Besides the venerable command-line interface for each device, the following VPN management products or tools currently exist:

- **CiscoWorks 2000 VPN/Security Management Solution (VMS)**—This package includes a number of relevant tools, including Cisco Secure Policy Manager (CSPM) for central control of VPN and security policies on routers and firewalls, and VPN Device Manager (VDM) for VPN configuration on Cisco 7100 and Cisco 7200 routers. CSPM is a powerful tool, but it is intended for large site-to-site deployment and does not handle more than 500 nodes.
- **IP Solution Center (ISC)**—This is a service-provider oriented product for deployment, provisioning, and management of multiple VPNs. It is currently being modified to also support large enterprises.
- **PIX Device Manager (PDM)**—This is a built-in code module available for all Cisco PIX firewalls running current software. It provides a browser user with control of most Cisco PIX configuration and management, including IDS and VPN support.
- **Security Device Manager (SDM)**—This is a built-in code module available for Cisco 831, Cisco 837, and Cisco 1700 Series routers. It is a web-based configuration tool that allows you to configure LAN and WAN interfaces, routing, NAT, firewalls, and VPNs. SDM and CRWS can be used together.
- **Syslog**—Provides for logging to a management device. Secure console access is available via SSH and Secure Socket Layer (SSL), depending on platform. For platforms not supporting SSH, if the VPN tunnel is up, Telnet is secure.
- **SSH**—Provides for secure command line access to Cisco IOS routers. As many service providers offer dynamic addressing to residential CPE, the WAN IP address of the teleworker router can change. If the service provider provides dynamic DNS, the CPE can be accessed by domain name. Otherwise, the CPE address can be found by the user using the web browser interface (CRWS web-based GUI supplies this).

For these management methods or tools (except SSH), the teleworker devices must be reachable via the VPN. This can be accomplished using an enterprise internal IP address for **all models**, either an inside interface or loopback address on Cisco IOS SOHO routers.

If the VPN tunnel is down, but access is still available to the Internet, SSH (preferred) or Telnet can be used to gain access to the device. However, the public IP address must be known.

- For **Cable Integrated Unit model**, this can be known to the cable provider via SNMP traps.
- For **DSL Integrated unit** and **all Integrated Unit + Access Device models**, the user can assist the enterprise or service provider help desk by supplying the broadband interface's IP address, which is dynamically provisioned and also can change. This is done for the Cisco 837 and Cisco 831 by using CRWS. The user can be instructed by the help desk to bring up the web browser and type in the appropriate IP address (the inside LAN address of the router). The user can then provide the help desk with the broadband IP address so that the help desk can gain console access via SSH.

Service Provider Managed Services

The market for providing enterprise-managed services for teleworkers is growing and has many of the same characteristics as small-and-medium businesses (SMB). As the routers used for the teleworker solution are Cisco IOS-based, their capabilities are a significant portion of those in Cisco 1700, Cisco 2600, and Cisco 3700 routers.

This topic is beyond the scope of this publication.

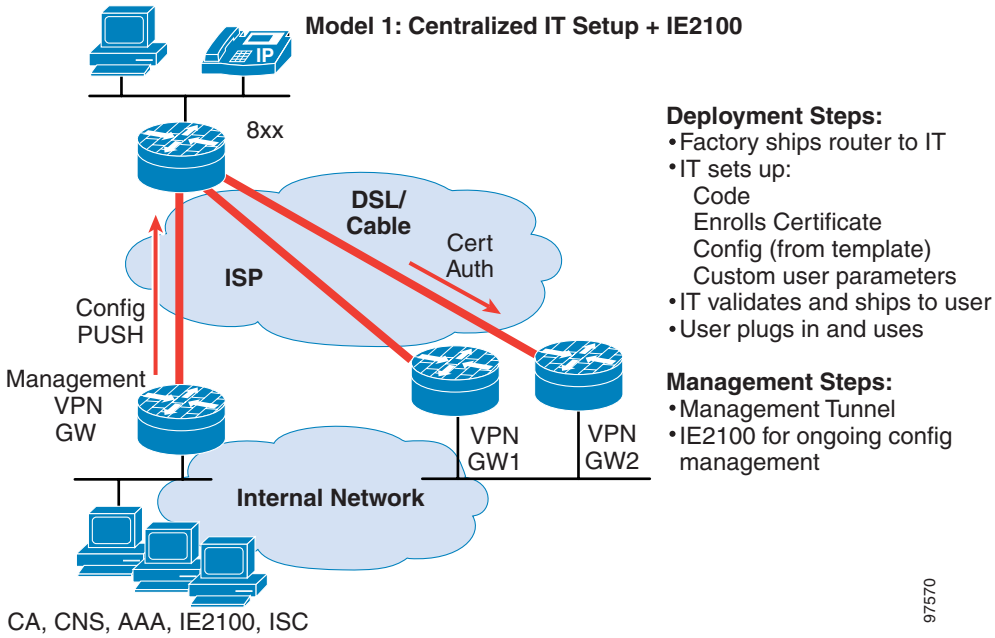
Ongoing Solution Creation for Provisioning

Although the techniques and tools mentioned in the preceding sections can provide for management of a function, service providers and enterprises require a solution that supports basic provisioning, IPSec provisioning, and ongoing configuration management for basic functions, security, VPN and QoS.

An ongoing internal Cisco teleworker trial is providing the environment to test, develop and deploy a comprehensive management solution for teleworkers. The solution includes ISC, IE2100, customized scripts, and Cisco 8XX functions (CNS, CRWS). All the scenarios include a separate VPN tunnel for management, and some provide for an initial configuration and VPN tunnel used for bootstrap, followed by a loading of digital certificates and production configuration. Figure 4-38 through Figure 4-41 illustrates some of the environments being tested. Table 4-3 compares the different options.

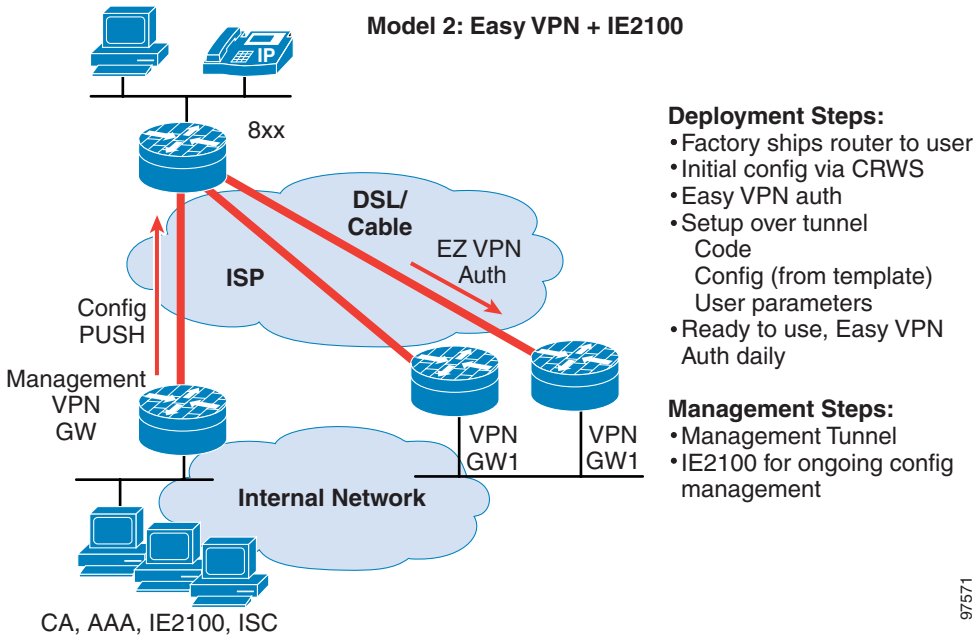
The first model (Figure 4-38) provides for an enterprise information technology (IT) setup and test for each teleworker network device and shipment to the teleworker for plug in.

Figure 4-38 Model 1—Centralized IT Setup + IE2100



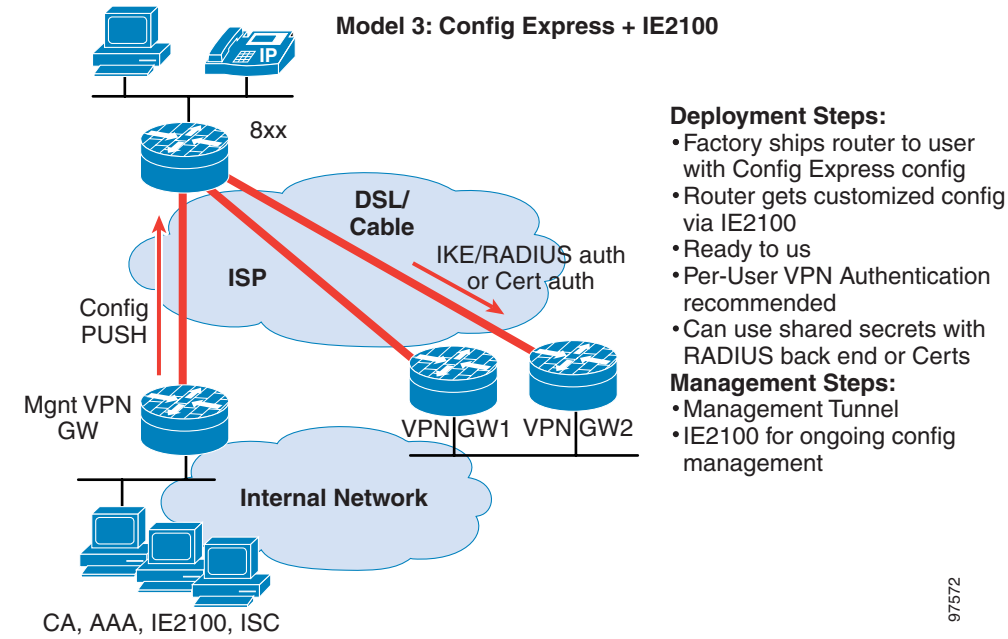
The second model (Figure 4-39) provides for user set up and configuration for initial basic service and VPN, followed by a customized configuration.

Figure 4-39 Model 2—Easy VPN + IE2100



The third model (Figure 4-40) provides for user set up and configuration for initial basic service and VPN, followed by a customized configuration.

Figure 4-40 Model 3—Config Express + IE2100



The fourth model (Figure 4-41) provides for user set up and configuration for initial basic service and VPN, followed by a customized configuration. The customized configuration includes a digital certificate downloaded through the initial Easy VPN tunnel.

Figure 4-41 Easy VPN/Cert Bootstrap + IE 2100

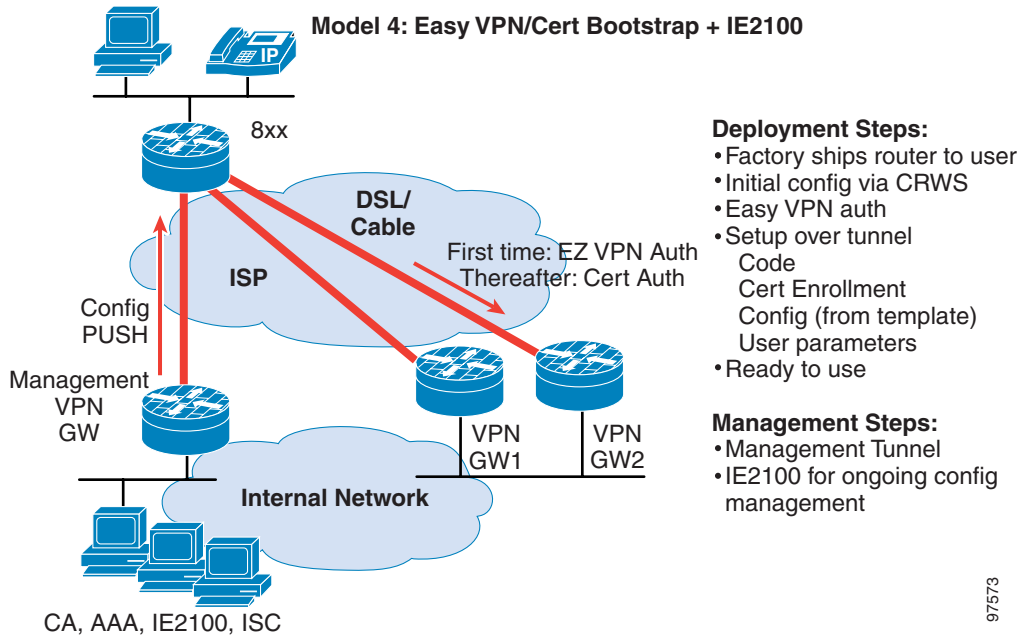


Table 4-3 compares the above four options.

Table 4-3 Solution Provisioning Options Comparison

	Advantage	Disadvantages	Comments
IT set up plus IE2100 Model #1	No end-user action Configuration validated Highly secure	IT touches box before user receives IT must know user userid and password to configure	User Easy VPN or classic IPSec definition with Auth-Proxy
Easy VPN plus IE2100 Model #2	IT touchless Simple process	Configuration not validated User authenticates daily (until Easy VPN Phase 3) No management tunnel (until Easy VPN phase 3)	Shared key with RADIUS back end; currently no certificate support with Easy VPN User configures initially via web GUI
Config Express plus IE2100 Model #3	IT touchless No end-user action	IT must know user userid and password to configure Configuration not validated	Initial configuration from TFTP boot or Config Express Certificates or shared key
Certificate "bootstrap" plus IE2100 Model #4	IT touchless Highly secure	Configuration not validated User authenticates daily (until Easy VPN phase3) No management tunnel (until Easy VPN phase 3)	Initial tunnel configuration via TFTP boot, CRWS, or Config Express; certificates installed via IE2100

Cisco Systems

PART 2

V3PN for Business Ready Teleworker

CHAPTER 5

V3PN for Business Ready Teleworker Solution Overview

This chapter summarizes teleworker V3PN solutions delivered over broadband links, such as DSL and cable. Specific sections include:

Teleworker Applications Overview

With the evolution of remote access from dial-up connectivity to broadband access services, the nature of offsite work has dramatically changed. Teleworkers can now be transparently integrated into every aspect of enterprise online applications. The implications of this level of access stretches far beyond simple E-mail retrieval, online calendar management, web browsing, or file transfer.

The bandwidth and high performance of these services is enabling applications that were previously not possible unless employees worked at the central corporate site. These applications include:

- **Office Productivity**—Applications rich in media and graphics and near real-time information synchronization
- **Collaboration**—Tools for sharing documents, spreadsheets, presentations, and other applications in real-time with peers and colleagues
- **Voice**—Services that are integrated with the corporate voice network
- **Video Conferencing**—Two-way video with employees at the central site or other teleworkers

Note Video conferencing might require 768 Kbps or greater uplink bandwidth.

- **E-learning**—Streaming media from training library archives, such as slides, audio, and video-on-demand

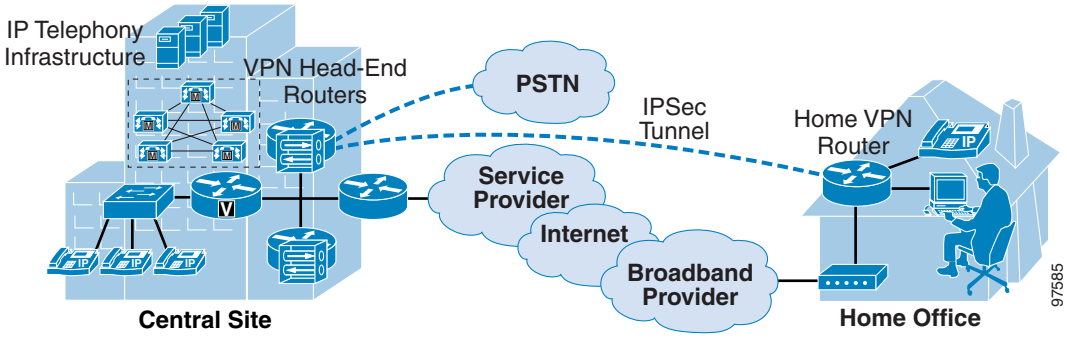
Large-scale organizations spend considerable funds to ensure that these applications are made highly available to each and every staff member—at their desks. But increasingly, employees are not at their desks—work is an *activity*, not a *place*. What is pulling employees away from their desks?

- **Meetings**—Wireless LAN deployments can extend desk services to other areas of the enterprise campus, such as conference rooms and open spaces.

- **Travel**—Many airports and hotels are being outfitted with wireless LAN and high-performance broadband-like access services to accommodate visitors.
- **Home**—It is now possible to extend the full range of enterprise applications and services to employees working at home, with no degradation in productivity or performance. The Cisco Business Ready Teleworker solution is the enabling architecture for implementing a transparent work-at-home environment.

Enterprise Class Teleworking can be differentiated from other forms of *work-at-home* or *telecommuting* scenarios in that the emphasis is on delivering transparent accessibility to the full range of applications and services critical to the operational effectiveness of large-scale organizations. The Business Ready Teleworker solution is part of an overall secure enterprise VPN infrastructure**.** Figure 5-1 illustrates the general Business Ready Teleworker VPN solution for the case where the enterprise has already deployed IP Telephony and is seeking to extend its reach to teleworkers:

Figure 5-1 Business Ready Teleworker, End-to-End IP Telephony



Key characteristics of the solution include:

- **High-Speed Broadband**—Enables cost-effective office applications
- **Site-to-Site VPN**—Promotes high-bandwidth services with the stability of an *always-on* VPN connection from central site services to any remote location
- **Advanced Security Functions**—Combine to facilitate the extension of the central-site LAN to the home office
- **Comprehensive Application Support**—Supports the full range of converged desktop applications, including high-quality voice, video, and real-time collaboration tools
- **Seamless Remote Networking**—Provides teleworkers with the same services at home as their office desktop

To be optimally effective, the Business Ready Teleworker environment requires a level of feature integration that appliance-based telecommuting solutions cannot support. Cisco has the only product suite capable of reliably delivering voice, video, multimedia, and traditional data over the same connection.

The key elements of the Cisco teleworker solution at the home office location include:

- Home-office VPN router enabled with QoS
- IP Phone (typically with the same number as the employee's desk phone)
- Laptop (or desktop) computer
- Broadband cable or DSL access

Corporate components that compliment the home office and facilitate central-site integration:

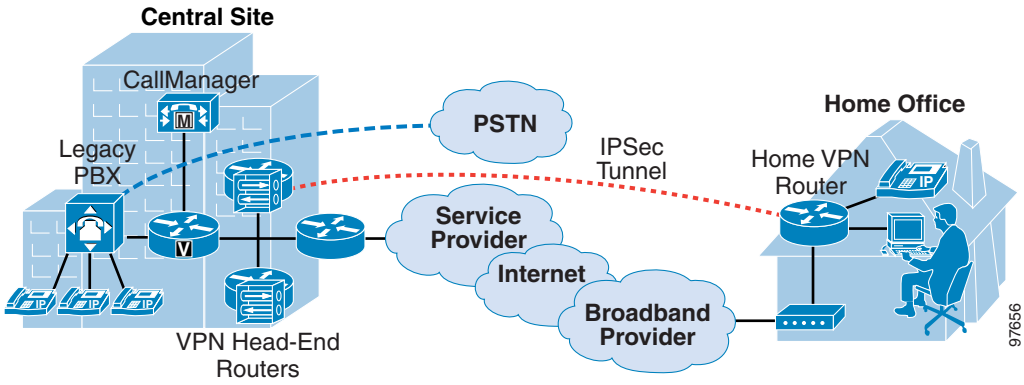
- VPN head-end aggregation routers designed for resiliency and scalability
- CallManager and IP Telephony infrastructure (or legacy PBX)

Notice that the IP Telephony deployment remains unchanged, but in this deployment connectivity between the central site and branch locations is through a V^{3}PN tunnel over broadband DSL or cable. Signaling traffic (such as H.323) flows *encrypted* over the VPN (IPSec) tunnels to the CallManager cluster at the central site. Voice conversations are established and bearer traffic also flows encrypted over the VPN tunnels.

The encryption provided by IPSec provides an additional level of security for voice conversations. However, the IP Phones, CallManager Cluster, and voice applications (such as voice mail servers) are unaware—and need not be aware—that their respective traffic is being transported over a VPN tunnel and being encrypted during transport. The VPN is transparent to these applications.

In the event the enterprise has not yet deployed IP Telephony and still uses a traditional PBX, it is still quite possible to deploy Enterprise Class Teleworking. Figure 5-2 shows how such a deployment might be accomplished:

Figure 5-2 Business Ready Teleworker, Legacy PBX



In this design, the home office phones are IP phones, with a Cisco CallManager providing the switching intelligence. However, the phones at the corporate site are proprietary PBX stations. Internetworking with the PBX can be accomplished such that the employee's phone in the corporate location and home office location still have the same number and same voice mail access.

Cisco's Business Ready Teleworker solution delivers a best-in-class, end-to-end integrated approach to VPN connectivity. Unlike appliance-based solutions, Cisco's solution provides an industry-leading feature set supporting enterprise-class applications and services over a secure, high-bandwidth ISP-based connection.

Providing a secure connection is only the first step. Cisco's solution provides the ability to deliver V^{3}PN-based services (such as voice, video-on-demand, or IP TV) by taking advantage of integrated QoS capabilities—allowing enterprise network implementers to explicitly shape traffic using QoS-based prioritization. No other solution offers this powerful capability.

Furthermore, the Business Ready Teleworker solution is fully integrated with Cisco's robust suite of VPN products—including the broadest portfolio of aggregation routers—and fully integrated with Cisco's IP Telephony solution.

Solution Characteristics

The following are general solution characteristics for Business Ready Teleworker deployments:

General

- *Always on* connection is a secure extension of the corporate LAN in the home office.
- Users have access to the same applications and services in the home office as when they are working at the corporate location, and access them exactly the same way.
- Works with existing residential or business class broadband cable/DSL subscriptions, including dynamic IP addressing via DHCP or PPPoE.

Voice Support

- Possible to have *single number reachability* with employees having same phone number at their corporate desk and in the home office.
- Full access to integrated corporate voice applications in the home office, including extension dialing, voice mail, voice mail notification, conference bridging, caller ID and call forwarding.
- Frees up personal PSTN line at home, so that others in the home can use that line. Also prevents other home users from inadvertently picking up the phone while in use by the corporate user.
- Possible to achieve high quality voice, simultaneous with data, over existing broadband cable and DSL networks by enabling QoS on the home-office VPN router.
- Hardware-based encryption in both the home-office VPN router and the VPN head-end routers at the central site insure minimal delay and jitter for VoIP packets.
- “On net” calls are free, since they are transmitted over the same VPN tunnel as data traffic. Only the cost of the broadband cable/DSL connection is incurred each month.
- Can be deployed as an extension of existing IP Telephony deployment or “along side” a legacy PBX.

Security

- All traffic, including data and voice, is encrypted with 3DES.
- Firewall and intrusion detection functions can be enabled on the home-office VPN router, protecting the connection from Internet-based security breaches.
- Broadband cable and DSL connections can be securely shared by corporate and home users, with authentication of corporate users providing access to the VPN tunnel.

Scalability and Manageability

- Based on Cisco IOS VPN routers for resiliency, high availability, and a building-block approach to high scalability that can support thousands of home office users.
- Digital certificates can be deployed to provide a highly scalable approach to authentication of the home-office VPN routers.
- The home office routers can be centrally managed by the enterprise using a highly scalable and flexible management product, such as ISC.
- Integrated home office routers providing VPN tunnel origination, QoS, and firewall (and other security functions) are possible—reducing the number of devices to be managed.

General Best Practices Guidelines

The following are a list of "best practice" notes and guidelines established through a combination of design experience, scalability and performance evaluation, and internal Cisco trials:

- Select Cisco IOS VPN routers with hardware encryption accelerator cards. Software based encryption adds unacceptable latency and jitter that significantly degrades voice quality.
- Follow all applicable V^3PN design guidelines.
- G.729 (20 msec sampling at 50 pps) is recommended due to bandwidth consumption after IPSec and cable/DSL overhead are added to the voice packets.
- Use QoS, LLQ/class-based, weighted fair queuing (CBWFQ), on the uplink.
- Use traffic shaping on Ethernet-to-Ethernet routers for the broadband cable/DSL uplink.
- Decrease data packet size by configuring the router to adjust the maximum segment size (MSS) of TCP packets.
- Implement dynamic IP addressing via DHCP or PPPoE as appropriate.
- Implement IPSec with DPD/RRI as appropriate to provide redundancy and suitable availability.
- Use digital certificates as appropriate for secure scalable deployments.
- A minimum uplink broadband cable/DSL bandwidth of 256 Kbps is recommended and the downlink bandwidth should be in the 1-to-1.5Mbps range.
- Implement fault and performance management tools such as NetFlow, SAA and IPM.
- Use Cisco Powered Network Services providers where possible. Head-end placement should minimize ISP exposure.

General Solution Caveats

The following is a list of caveats for the solution:

- Cisco PIX 501X and Cisco VPN 3002 are not recommended as home-office VPN devices unless a Cisco IOS router is providing the QoS features that are mandatory to achieve simultaneous data and high quality voice transmission.
- Cisco uBR 900 series devices are currently not recommended for deployment as the integrated home-office VPN device, as they do not support needed QoS in DOCSIS 1.0.
- Uplink speeds less than 160 Kbps require additional support costs due to lower quality voice.
- Asymmetric link speeds minimize impact of having no downlink QoS. Symmetric link speeds are not preferred unless downlink QoS is available.
- LFI is not supported on DOCSIS 1.0 (cable) or PPPoE (DSL).
- Enterprise is exposed to issues relating to E911 service, rogue WLAN access points and network access by non-teleworker (spouse-and-children) home-network users.
- IP multicast is not supported in IPSec-only implementations.
- Supporting two-way video conferencing might require link speeds in the business class service level—greater than 768 Kbps—and might require higher performance routers.
- Compressed real-time protocol (cRTP) currently provides no bandwidth savings when used in conjunction with IPSec and generally is not supported by broadband service providers.

CHAPTER 6

V3PN for Business Ready Teleworker Broadband Issues

This chapter summarizes issues specific to deploying V3PN over broadband links—DSL and cable—and ways to deal with each. Specific sections include:

Avoid Known Issues

A common mistake is to ignore the empirical results derived from both Cisco lab testing and deployments. Many voice quality issues can be directly attributed to not following these recommendations:

- **Implement Hardware Encryption Acceleration**—Chariot test results presented in this design guide validate the importance of hardware encryption acceleration in producing acceptable latency and jitter for voice calls.
- **Use Asymmetrical Links**—Some service providers offer symmetrical links (upstream and downstream provisioned at the same data rate) for business class services. Often these services also include fixed IP addresses and enhanced system support. These services are targeted at competing with traditional Frame Relay service providers. However, they are in nearly all cases, lacking any downlink QoS policies. With Layer-2 services (Frame Relay), the enterprise can deploy techniques (such as Frame Relay Traffic Shaping per PVC) to manage downlink QoS on the head-end router. With broadband services—Layer-3 services—the responsibility of downlink QoS is the responsibility of the service provider. If the service provider does not offer downlink QoS, symmetrical links are of no advantage to the enterprise. Speed mismatches—asymmetrical links—are a better choice and benefit the enterprise. The greater the downlink bandwidth the less need for QoS. Since QoS is not generally available by broadband service providers, the speed mismatch is desirable.
- **Minimum Recommended Bandwidth**—The minimum recommended broadband data rate for most deployments is 160 Kbps (uplink)/860 Kbps (downlink). Data rates below this speed require more troubleshooting by the support staff and are less likely to provide acceptable voice quality. The

recommended data rate is 256 Kbps/1.4 Mbps or higher rates, such as 384 Kbps/1.5 Mbps. While V^3PN can be deployed at rates less than 160 Kbps/860 Kbps, generally the voice quality at that service level is in the cell phone quality range and support costs are higher.

- **Cable incurs less Layer-2 overhead than DSL**—DSL is at a disadvantage to cable due to higher Layer-2 overhead requirements associated with ATM/AAL5 and PPPoE. Cable media has less Layer-2 overhead—a DOCSIS header and the Ethernet header and trailer—and generally produces lower latency and jitter than the same data rate as DSL. Additionally, cable service providers tend to deploy a high percentage of Cisco uBR routers at the head-end, which can support DOCSIS 1.1 by a software upgrade and a DOCSIS 1.1 remote cable MODEM. DOCSIS 1.0 and 1.1 can be deployed on the same cable plant. DSL service providers have less Cisco equipment deployed and in many cases the DSLAM or ATM aggregation switch has no QoS capabilities.

  However, cable is a shared media between the enterprise premise cable MODEM and the cable head-end router. DSL is a dedicated circuit between the enterprise's DSL MODEM (bridge) and the DSLAM or DSL router. Both cable and DSL offerings utilize shared uplinks between these aggregation devices and the service provider's core network.

Link Fragmentation and Interleaving

The common installed base of broadband services today is made up of DOSCIS 1.0 for cable, while DSL providers typically implement PPPoE. PPPoE is popular with ISPs as it provides a consistent means of authenticating users (RADIUS for example) regardless of the access method—traditional dial-up or DSL.

Neither DOCSIS 1.0 or PPPoE have any means within the protocol to implement LFI of data packets within voice packets. DOCSIS 1.1 *does* define fragmentation and interleaving.

Most broadband services are offered at data rates that require LFI to minimize the impact serialization delay on voice packets—56 Kbps to 768 Kbps. To address this limitation, the design presented in this publication assumes a realistic traffic profile, made up of:

- One voice call
- TCP applications
- UDP applications suitable for a WAN topology

Suitable UDP applications include: DNS, port 53; Lightweight Directory Access Protocol (LDAP), port 389; Network Basic Input/Output System Name Service (NetBIOS NS); port 137; and, NetBIOS destination service access port address (DS), port 138. These applications usually have a Layer-3 packet size of less than 300 bytes and a transaction rate of less than one packet per second. UDP applications that generate MTU-sized packets—such as Network File System (NFS) version 2 or video conferencing—cannot be supported without an LFI technique. All TCP applications and TCP-based video applications—like Video-on-Demand (VOD) and NetMeeting—have been demonstrated to produce good results.

To address the lack of LFI, the TCP Maximum Segment Size (MSS) is adjusted by the Cisco IOS router to reduce the TCP packet size to manage, but not eliminate, serialization delay.

Use QoS where Available

QoS techniques provide the greatest benefit on links that have the highest probability of experiencing congestion—low-speed links. Broadband service providers might not be in a position to offer QoS to the home or small office; however, the enterprise-owned remote router can be configured to implement QoS techniques such as CBWFQ and Weighted Random Early Detection (WRED). Shaping is also deployed on routers with dual high-speed (Ethernet-to-Ethernet) interfaces to provide the appropriate congestion feedback when the upstream link is not directly terminated on the router—as is the case with a Cisco 837 or Cisco 1700 series routers with an DSL WIC.

While an end-to-end, QoS-enabled network connection between the SOHO and the enterprise head-end is ideal, that goal might not be attainable or practical in the immediate future. If the service providers can meet the Cisco Powered Network (CPN) SLA requirements for a VPN/IP multi-service provider, the lack of QoS availability in the core networks might not be a major problem. Service providers with high-speed cores (OC3 and above) and that are adept at capacity planning/management should be able to offer viable transport for V^3PN.

In most instances, the greatest exposure to the enterprise is the broadband service provider—the Tier 2/3 ISP. In Cisco internal trials and during all lab testing, downlink QoS was not applied since most broadband service providers do not offer this service.

In a nutshell, always implement the QoS techniques defined in this and other QoS design references if they are available.

Minimize ISP Exposure

In this design guide, the traditional voice delay budget illustrations are presented to illustrate that the encryption and decryption process adds a minimal amount to the total delay budget.

Many of the components of the voice delay budget are fixed or cannot be influenced by the enterprise network manager. Examples are the codec, jitter buffer, and propagation (speed of light) delay. However the network portion of the delay budget—the service provider—can be influenced by choice of service providers and location of head-end routers.

Direct peering (links) to the broadband service provider from the head-end location is one means of minimizing ISP delay and jitter. Placement of multiple head-end routers in different geographies to avoid long hauls over the Internet is another method. In Cisco internal trials, the service provider portion of the delay budget for cable, DSL and T1 links to the Internet range from 15 msec to more than 60 msec. As a rule of thumb, less than 30 msec in the ISP network is ideal, 30-to-60 msec is acceptable, and more than 60 msec is not optimal.

In subsequent chapters, techniques will demonstrate how to measure service provider delay and jitter and how to validate the available uplink bandwidth. These methods can be used to plan for a successful deployment as well as to provide ongoing troubleshooting of V^3PN problems.

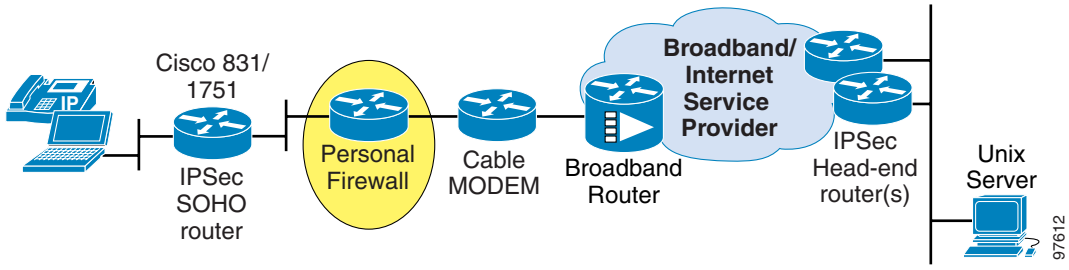
Personal Firewalls

While outside the scope of Cisco Enterprise Engineering lab testing and the primary focus of this document, the Cisco internal trials have encountered issues which might be applicable to many deployments. This section addresses the following topics:

Issues with Personal Firewalls

Personal firewalls are inexpensive teleworker site products and are commonly deployed to provide access for multiple PCs in the home over a single IP address a NAT/pNAT function. The personal firewall is illustrated in Figure 6-1.

Figure 6-1 Personal Firewall



There are two issues with supporting a personal firewall.

- First, the recommended configuration applies QoS to the uplink on an Ethernet-to-Ethernet router by shaping traffic on the output interface to a rate below the uplink speed. If a personal firewall is inserted into the topology between the IPSec/QoS-enabled router and the cable/DSL modem, packets from a spouse or child PC will not be subject to the QoS policy. If the cable or DSL modem does not support a suitable QoS policy, voice packets might be dropped as they contend with the spouse or child PCs packets. This will lead to voice quality issues.
- Second, not all personal firewalls or service provider-provided cable/DSL routers properly support IPSec pass through by default or might need additional configuration to eliminate specific voice-related issues. For the IPSec router to establish an IPSec tunnel to the head-ends, the personal firewall must invoke a NAT/pNAT function for the IPSec ESP and UDP port 500 packets. NAT transparency is one means to address this issue, however it does add additional overhead to the resulting encrypted packet size—which might be undesirable. The performance impact of NAT transparency has not yet been scale-tested internally.

An advantage to including a personal firewall for DSL/PPPoE broadband connections is that this eliminates the need to terminate the PPPoE session on the enterprise-configured IPSec router. To terminate the PPPoE session on the IPSec router, the employee/user PPPoE username and password must be given to the network administrator and included in the IPSec router configuration. The PPPoE username and password are not encrypted with the strong MD5 hash in the Cisco IOS configuration file and can easily be cracked by anyone with access to the configuration—for example when stored on a TFTP server. This allows the enterprise network administrators to have full access—and to be able to masquerade as—the employee on the employee's personal ISP account. The alternative would be to

terminate the PPPoE session on the personal firewall and the IPSec router would then receive its IP address via DHCP. The PPPoE username and password would be under employee/user control on the personal firewall.

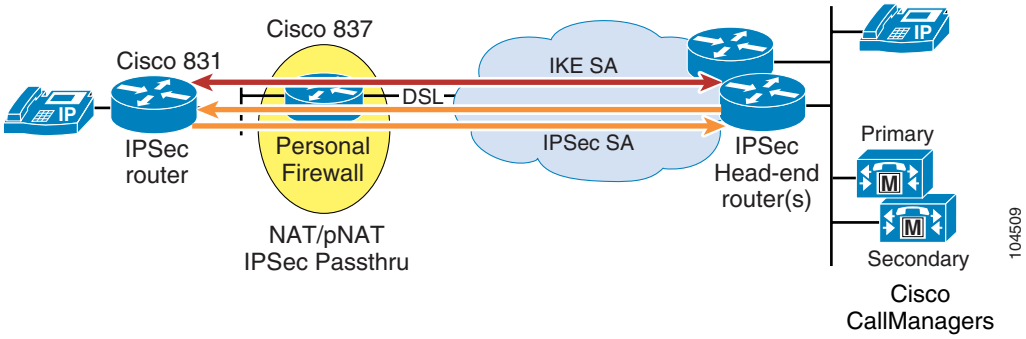
IPSec Pass-through—Calls Drop When Muted

In specific circumstances, active calls placed on mute can cause the voice call to drop shortly after the call is placed on mute. The specific criteria are:

- The IPSec router has no other device generating network traffic—for example, a Cisco 7960 IP Phone is in us, but no PC is attached to the remote LAN.
- The personal firewall is supporting IPSec pass-through or NAT/pNAT of IKE on UDP port 500 and ESP on protocol 50.
- The NAT/pNAT inactivity timeout for UDP translations are less than the IPSec SA lifetime—by default this value in Cisco IOS is one hour (3600 seconds). The default NAT/pNAT inactivity timeout for UDP defaults to five minutes in Cisco IOS.
- This is an IPSec-only deployment (no GRE) and the head-end routers have IKE keepalive/DPD and RRI enabled with a value that will cause the IP route and SA to be invalidated in less time than specified with the SCCP keepalive interval. The default values are a Cisco CallManager cluster-wide value—every 30 seconds for the active CallManager and every 60 seconds for the standby Call Manager.

Refer to Figure 6-2.

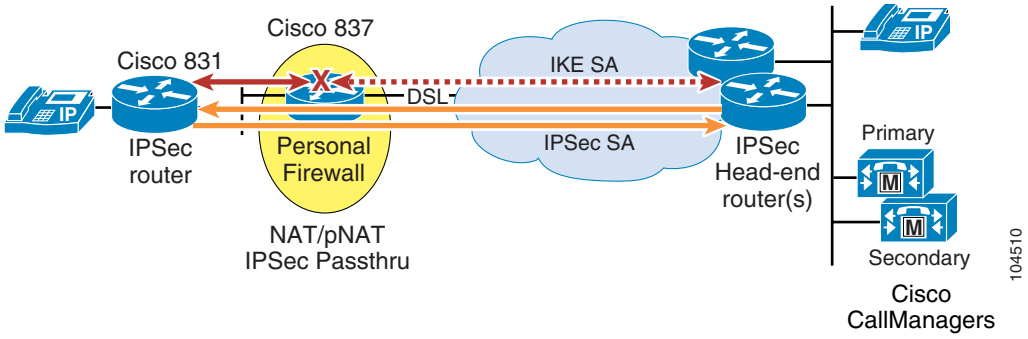
Figure 6-2 Mute Issue



The scenario illustrated in Figure 6-2 assumes the two IP Phones are in an active call. A Cisco 837 terminates the DSL connection via PPPoE and has served an RFC 1918 IP address to the Cisco 831 using DHCP. The Cisco 837 is supporting IPSec pass-through. Since there are packets flowing through the transmit and receive IPSec tunnels, the IKE keepalive/DPD packets on UDP port 500 will not be exchanged between the remote and head-end router.

In Figure 6-3, the NAT/pNAT entry for IKE (UDP port 500) has expired from the IPSec pass-through router; however, neither IPSec router is aware of this event. While the remote router can re-establish the NAT/pNAT entry for IKE, the head-end router cannot. The voice call is still functioning normally through the ESP translation entries in the NAT/pNAT router.

Figure 6-3 Mute Issue—NAT/pNAT Timeout



From the console of the Cisco 837 router, the following output illustrates that the UDP port 500 NAT entry has timed out. The ESP translations continue to function normally.

```
837-FW#sh ip nat trans udp verb
Pro Inside global      Inside local       Outside local      Outside global
udp xx.32.92.50:500    192.168.1.4:500    xx.xxx.223.24:500  xx.xxx.223.24:500
    create 00:04:52, use 00:04:52, left 00:00:07, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 2961, lc_entries: 0
```

The following display was captured more than seven seconds from the previous display. The NAT entry is no longer in the translation table.

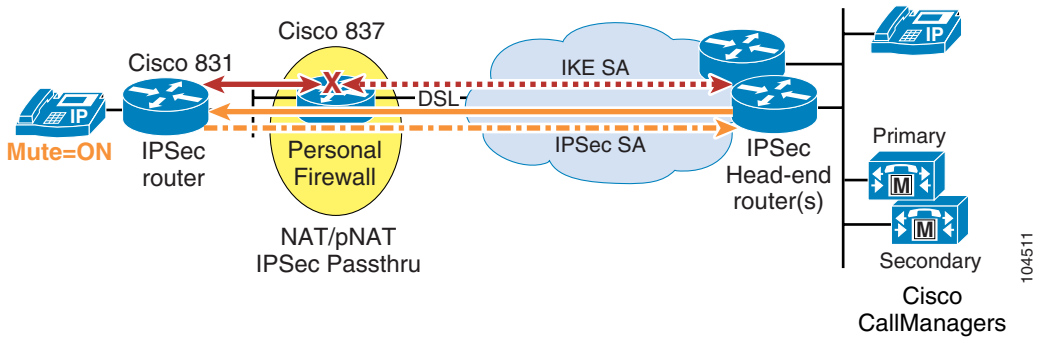
```
837-FW#sh ip nat trans udp verb
Pro Inside global      Inside local       Outside local      Outside global
```

Note The ESP translations remain in the ESP translation table.

```
837-FW# sh ip nat trans esp
Pro Inside global      Inside local       Outside local      Outside global
esp xx.32.92.50:0      192.168.1.4:0      xx.xxx.223.24:0    xx.xxx.223.24:BCE29552
esp xx.32.92.50:0      192.168.1.4:1EE78B67 xx.xxx.223.24:0  xx.xxx.223.24:0
```

At this point the remote user places the call on mute by depressing the mute button on the lower right side of the Cisco 7960's base. The net effect of this action is to stop the upstream RTP (voice) stream. The phone continues to generate SCCP keepalives to the primary and secondary call managers. See Figure 6-4.

Figure 6-4 Mute Issue—Phone Placed on Mute



In Figure 6-4, the call is placed on mute. Only the SCCP keepalives are flowing through the IPSec tunnel and these are by default 30 seconds apart for the primary CallManager and 60 seconds apart for the secondary CallManager. There are four packets in a keepalive: the phone initiates a packet to the call manager; the CallManager responds; the CallManager immediately initiates a packet; and the phone responds. The SCCP keepalives can be configured in CallManager. They are cluster-wide parameters. Configuration is as follows:

1. Under Service Parameters then under Sever* select the publisher.
2. Under Service* select Cisco CallManager
3. Scroll down to Cluster Wide Parameters (Device-General)
   - Station and Backup Server Keep Alive Interval (sec)*: Default is 60
   - Station Keep Alive Interval (sec): Default is 30

With thirty seconds between keepalives, the phone on mute, and no PC attached to the home network, there will be no packets encrypted to the head-end for up to 30 seconds. This will cause the head-end IPSec router to initiate IKE keepalives to verify connectivity to the remote IPSec router. Since the UDP port 500 entry is no longer in the NAT/pNAT translation table, the head-end router cannot initiate a connection to the remote IPSec router. The NAT/pNAT router will drop the IKE keepalive packets.

In this example the head-end IPSec router configured with the **crypto isakmp keepalive 10** command. This option instructs the router to adopt a *worry interval* of 10 seconds and by default initiate DPD/R_U_THERE messages every two seconds once the worry interval has expired and no packets are seen from the remote peer. Refer to Figure 6-6.

Figure 6-5 Mute Issue—Worry Interval Exceeded

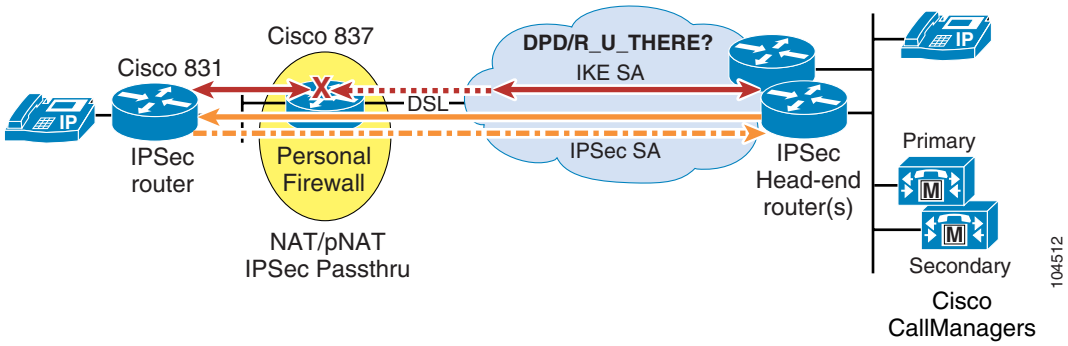


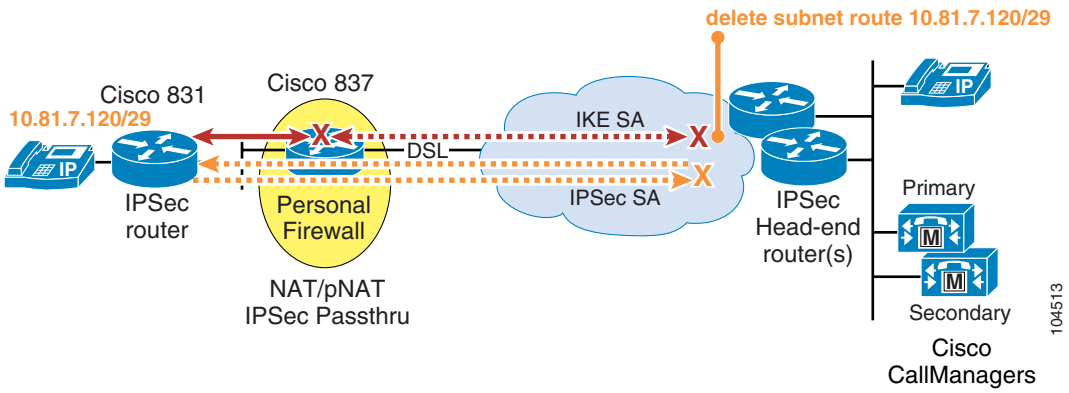
Figure 6-5 and the following abbreviated **debug crypto isakmp** output illustrate the process and the related messages.

```
10:01:51 edt: ISAKMP (0:10): more than 10 seconds since last inbound data. Sending DPD.
10:01:51 edt: ISAKMP (0:10): sending packet to xx.xx.xx.24 my_port 500 peer_port 500 (I)
10:01:53 edt: ISAKMP (0:10): sending packet to xx.xx.xx.24 my_port 500 peer_port 500 (I)
10:01:55 edt: ISAKMP (0:10): sending packet to xx.xx.xx.24 my_port 500 peer_port 500 (I)
10:01:57 edt: ISAKMP (0:10): sending packet to xx.xx.xx.24 my_port 500 peer_port 500 (I)
10:01:59 edt: ISAKMP (0:10): sending packet to xx.xx.xx.24 my_port 500 peer_port 500 (I)
10:02:01 edt: ISAKMP (0:10): peer xx.xx.xx.24 not responding!
```

Note Once the worry interval has expired, the peer will be declared non-responsive after five DPD/R_U_THERE messages are not answered. Total elapsed time between last packet seen and the peer declared dead will be as little as 20 seconds. Since the SCCP keepalive messages (30 seconds apart) are

the only packets flowing to the head-end in this example, the keepalive packets are not sufficient activity to maintain the tunnel in this configuration. The result is that the head-end IPSec router causes a connectivity failure. This is illustrated in the Figure 6-6.

Figure 6-6 Mute Issue—Connection Torn Down



The IPSec tunnels will be torn down by the head-end router. The routes to the remote subnet will be removed from the head-end's routing table—effectively dropping the voice call. At this point, the remote IPSec router no longer receives encrypted traffic from the head-end and which triggers IKE keepalive/DPD on the remote router. Subsequent SCCP keepalives from the IP Phone will cause the remote router to re-contact the IPSec head-ends to establish a new tunnel and the phone will then be able to function normally; however, the remote user will probably need to dial back into the conference bridge or call the other party.

One solution to this problem would be to increase the worry interval configured in the **crypto isakmp keepalive** command to a value aligned with the phone's keepalive interval. Another alternative would be in increase the NAT/pNAT timeout value for the IPSec pass-through router.

The NAT/pNAT timeout issue also presents a problem at the expiration of the IPSec SA lifetime. This is discussed in the next section.

IPSec Pass-through—Calls Drop During Rekey

The use of a personal firewall and IPSec pass-through can also cause a service disruption at the expiration of the IPSec SA lifetimes. By default, the lifetime of IPSec tunnels is 3600 seconds or one hour. The lifetime of an IKE SA is 24 hours.

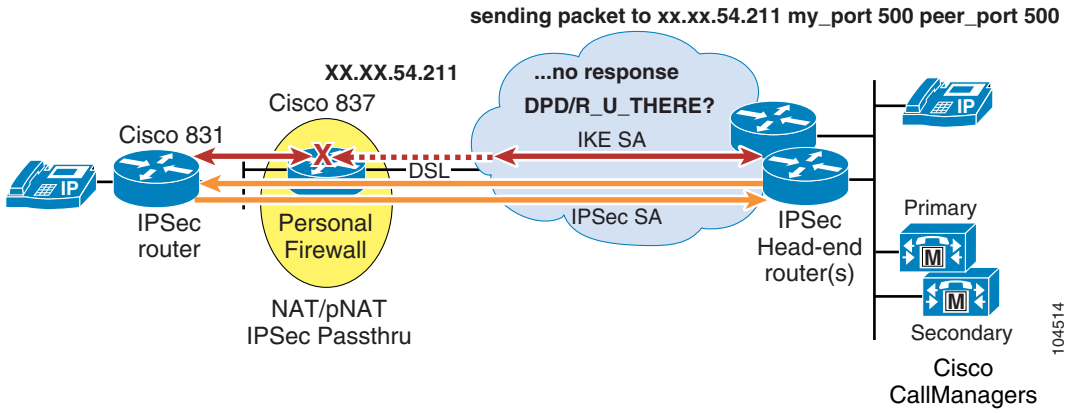
With dynamic crypto maps on the head-end IPSec routers, the remote router initiates the IKE connection to the head-end initially. However, once the IPSec SAs have been established, either the remote router or the head-end router can initiate the IKE transactions that build replacement IPSec SAs to maintain the logical tunnel between remote and head-end. With a default lifetime of 3600 seconds, this typically occurs two to three minutes prior to the expiration of the lifetime.

During Cisco internal trials, the likelihood of the head-end router initiating the IKE transaction appeared to increase between Cisco IOS releases 12.2(8)T5 and 12.3(3); however, this issue will occur under all applicable releases.

Figure 6-7 depicts the IPSec head-end router generating an IKE packet that initiates a rekey to build new IPSec SAs. Referring to the examples in the "IPSec Pass-through—Calls Drop When Muted" section on page 6-5, the NAT/pNAT translation for UDP 500 has expired on the personal firewall and the head-end

router cannot contact the remote IPSec router. This triggers DPD/R_U_THERE messages that also cannot reach the remote router and the IKE and IPSec SAs are deleted from the head-end, causing a loss of connectivity.

Figure 6-7 Rekey Initiation



Solution for Cisco IOS Personal Firewalls

For Cisco IOS-based personal firewalls, the solution to this problem is to increase the NAT/pNAT timeout value for the IKE NAT entry. This can be accomplished by configuring the following command on the personal firewall router (the Cisco 837 in this illustration):

ip nat translation port-timeout udp 500 7200

This command increases the default NAT/pNAT timeout value for UDP port 500 to 7200 seconds. The NAT/pNAT entry can be observed as follows:

```
Router1750-adsl#show ip nat translations udp ver | begin :500
udp 68.18.12.197:500   192.168.2.4:500    xx.xx.xx.24:500  xx.xx.xx.24:500
    create 20:34:20, use 00:26:55, left 01:33:04, Map-Id(In): 1,
    flags:
extended, use_count: 0
    initiator cookie: 0x199CABFA 1
```

Note ISAKMP Header has an 8 byte Initiator Cookie field, and this distinguishes multiple IKE sessions between the same pair of hosts.

Increasing the timeout value does not create an issue even if the IPSec router is reloaded or power cycles while the personal firewall router maintains connectivity. This solution permits the configuration of the IPSec router to continue to obtain its outside IP address via DHCP. There is no need to provide a static mapping in the personal firewall's DHCP server configuration for the IPSec router.

Solution for Linksys Personal Firewalls

Linksys routers do not have an equivalent feature to the Cisco IOS **ip nat translation port-timeout** command function. Instead, they can be configured to map an inbound UDP port 500 request to the IPSec router. The options are illustrated in Figure 6-8 and Figure 6-9 (on the pages that follow).

Configure the Linksys router options as follows:

- Forwarding Tab (Figure 6-8)—Use the *Forwarding* menu tab and map UDP 500 to the IPSec router's IP address. The IPSec router must be configured with a static outside IP address. In this example the Linksys is at 192.168.1.1.
- DMT HOST Tab (Figure 6-9)—Use the *DMZ HOST* tab, and enter the IPSec router's IP address. The IPSec router must be configured with a static outside IP address.

Note Both options require the IPSec router to use a static IP address—for example 192.168.1.100—on the outside interface and a default route must be configured to the Linksys router's IP address (by default 192.168.1.1). From a provisioning standpoint, this is undesirable as it requires configuration changes for insertion or removal of a personal firewall.

Figure 6-8 Linksys Forwarding

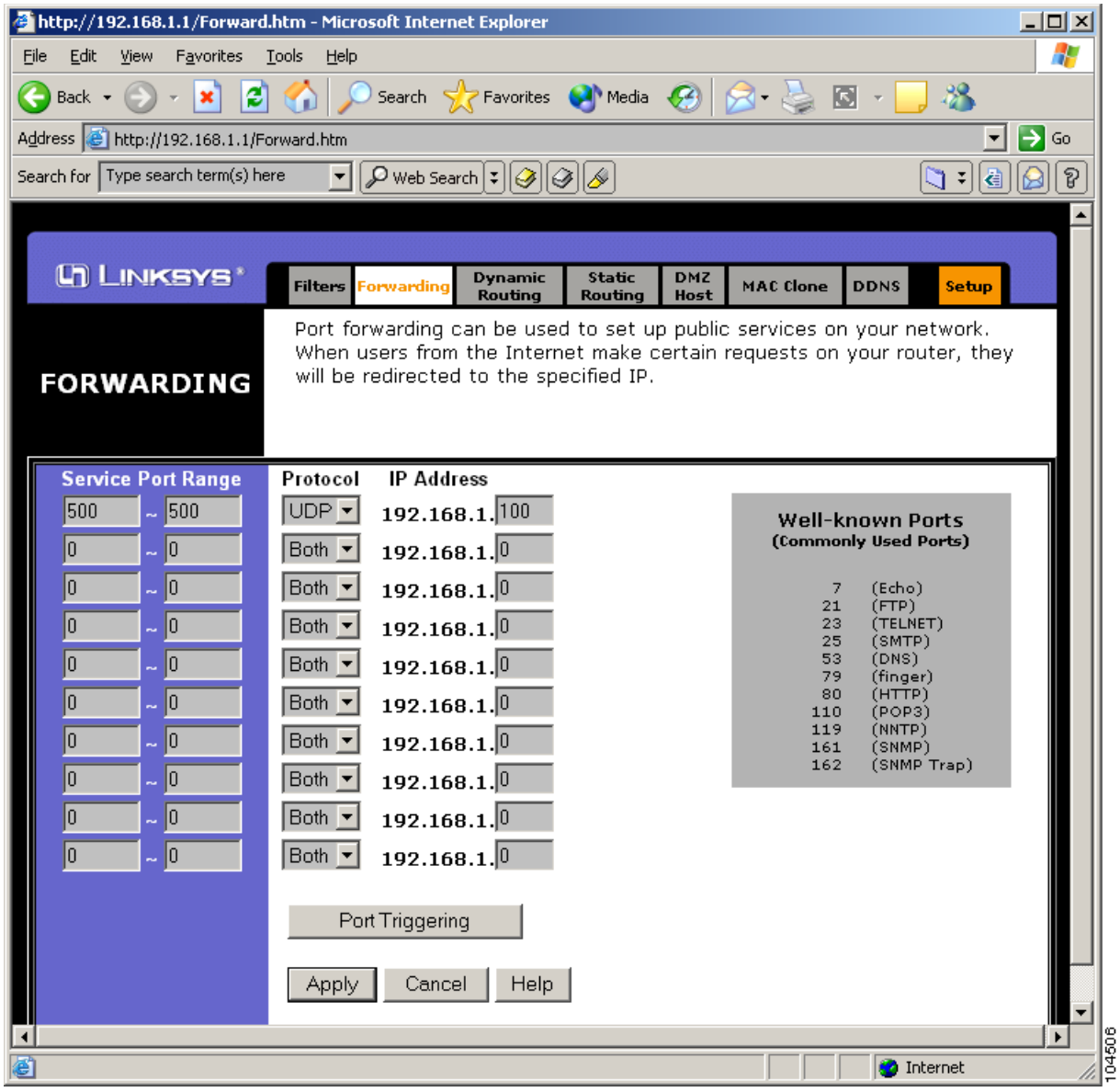
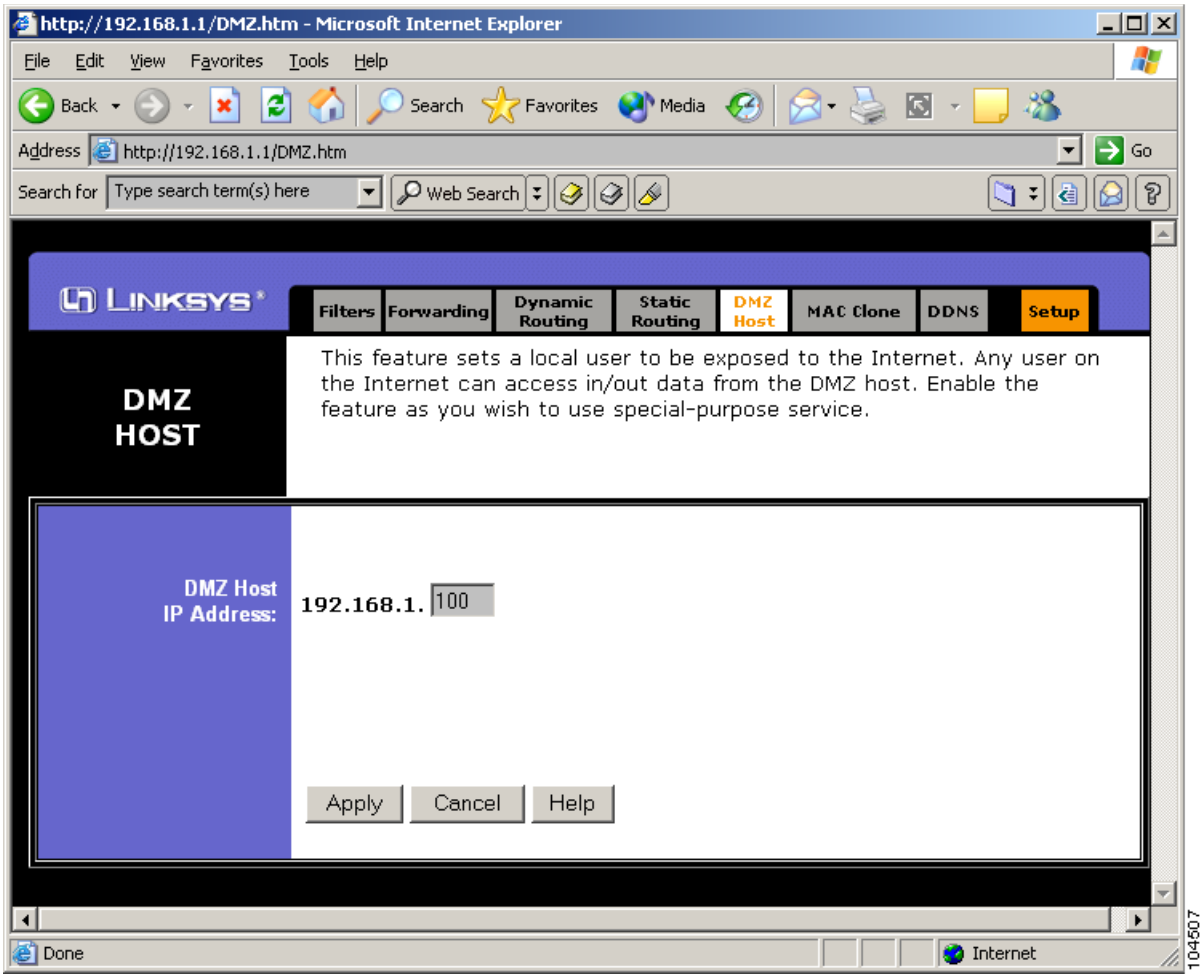


Figure 6-9 Linksys DMZ Host



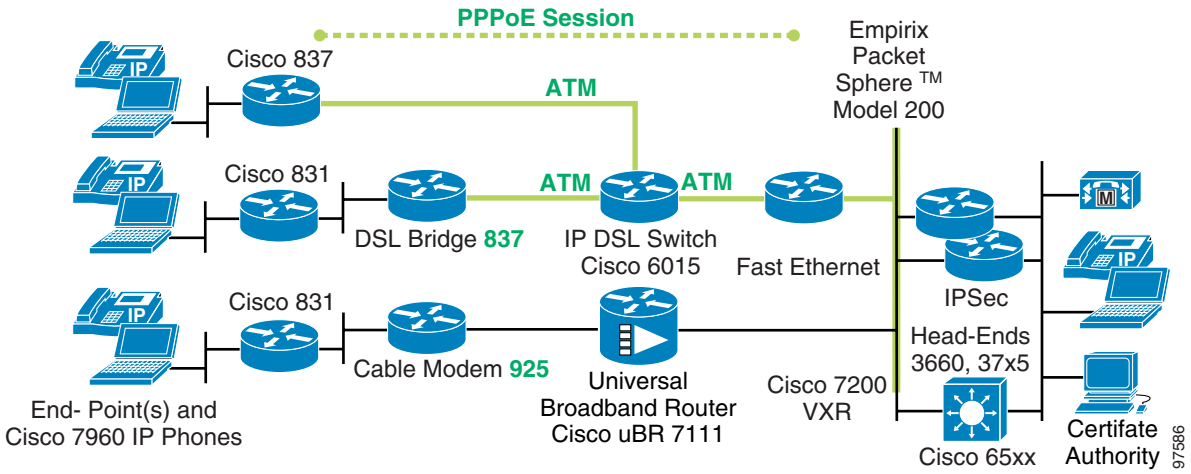
V^{3}PN for Business Ready Teleworker Planning and Design

This chapter addresses planning and design considerations for enabling V^{3}PN. It reviews issues and design considerations specific to IP Telephony, QoS and IPSec. An overview of service provider and head-end deployment considerations is also provided and the chapter ends with a checklist that can be used for V^{3}PN planning. Specific sections provided include:

Teleworker Deployment Model

Figure 7-1 represents the deployment models tested.

Figure 7-1 Deployment Model/Test Bed



The lab test environment emphasizes two deployment models:

- Cisco 831 (Dual Ethernet) behind a DSL bridge or cable modem
- Cisco 837 (Ethernet/DSL) connected to an IP DSL Switch

Both configurations share these same general characteristics. The IPSec configuration is based on IPSec only (no GRE tunnels) with multiple **set peer** statements in the **crypto map** configuration. IKE keepalives are configured. Digital certificates and a certificate authority server are used to provide keying material. Split tunneling and CBAC are not configured; however, an inbound access-control list is applied to the outside interface similar to that used by enterprises in actual deployments. SNMP, Telnet and rsh are used during testing to gather statistics about the device under test. NTP or SNTP is configured to provide accurate clocking. Cisco Express Forwarding (CEF) is configured on all interfaces. PPPoE is configured on DSL to obtain the outside IP address; for cable, the address is obtained via DHCP. WRED is configured in QoS **class class-default**.

Cisco 831 Dual Ethernet

On the outside interface (facing the WAN), hierarchical CBWFQ (HCBWFQ) is configured to provide congestion feedback for the uplink QoS policy.

Cisco 837 Ethernet/DSL

The DSL (ATM) interface's PVC is configured with the **vbr-nrt** keyword at the DSL trained rate. The output peak cell rate and sustained cell rate are equal values. The **tx-ring-limit** is set to 3.

An Empirix Packet Sphere™ is included in the test bed to simulate an ISP induced delay, jitter and loss. For more information refer to http://www.empirix.com/.

NetIQ Chariot™ and Agilent Technologies Voice Quality Tester (Agilent Telegra VQT) 2.1 test tools were used in a similar manner as described in the V^3PN SRND guide.

IP Telephony (Voice over IP)

When implementing VoIP over broadband WAN media, no change is required to the IP Telephony component as deployed for a site-to-site deployment over Frame Relay or a site-to-site VPN deployment. Call admission control and E911 issues are similar in the various deployments.

Topics addressed in this section include:

Call Admission Control

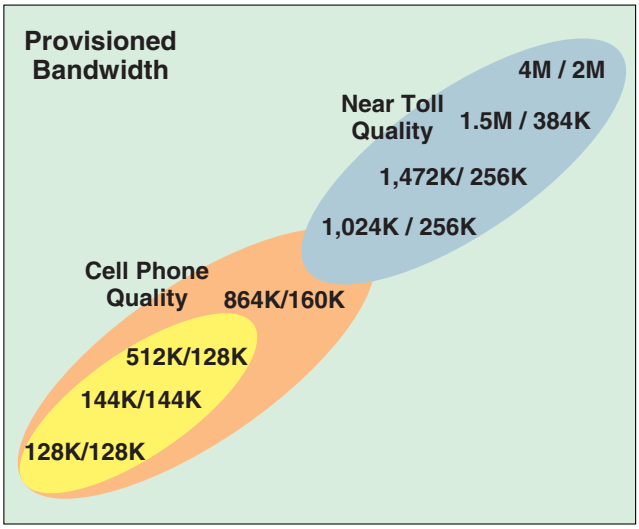
Call admission control for the teleworker does not present an issue when there is a single IP Phone in the employee's home office. Only one RTP stream is present over the broadband connection, even if using conference call features. When the home user creates a conference bridge, the RTP stream from the IP Phone is terminated on a DSP resource with all other conference-participant RTP streams. For this reason, all tests accompanying this design guide provision one voice call regardless of the available bandwidth.

Recommended Broadband Link Speeds

Two common deployment mistakes when deploying IP Phones over IPSec encrypted residential broadband are: not using the correct hardware; and, providing insufficient bandwidth. In the "Product Selection" section on page 9-6, specific product issues are identified. As a general rule, the IPSec termination device must have hardware encryption acceleration and QoS must be provisioned on the uplink portion of the broadband connection. Additionally, since QoS typically is not available on the downlink from most service providers, asymmetrical links are preferred—with downlink speeds of 1-to-1.4 Mbps.

As for provisioned bandwidth, the minimum recommended is 160 Kbps (uplink) and 864 Kbps (downlink). Speeds below these values are perceived as delivering cell phone quality voice. At uplink speeds of 256 Kbps and above, the voice quality is near toll quality with some occasional breakups. Generally, 256 Kbps/1.4 Mbps delivers acceptable voice quality for all but the most demanding applications, like agents at call centers speaking with customers. Figure 7-2 represents the range of speeds and where they fit within a subjective scale.

Figure 7-2 Voice Quality and Provisioned Bandwidth



As part of the lab testing that supports this document, wave file captures were created using the various link speeds and the QoS techniques discussed in this guide. Customers interested in copies of the wave file captures should contact their respective Cisco account team.

All wave files include service provider delay and jitter using the Empirix Packet Sphere by a random packet delay of 0-to-60 msec. The estimated delay values are ear to mouth, as calculated by the Agilent Telegra VQT. These tests were run with a traffic profile that includes voice and data, as do all tests represented in this guide. Users frequently comment that they get acceptable voice quality using non-recommended configurations. An example might be using a device that does not use hardware encryption acceleration or at speeds below the minimum recommended. This perception generally will change once the uplink is congested with data traffic and the service provider delay and jitter increase.

The purpose of this guide is to set expectations and make recommendations so that voice quality over broadband remains usable during the worst-case situations rather than to encourage the network managers to implement a configuration that becomes a source of frustration to the user and a support burden to the help-desk staff.

The criteria used in Cisco Enterprise Solutions Engineering lab testing, as reported by Chariot and with no induced service provider delay is:

- Less than or equal to one percent of voice packet loss
- Average jitter less than or equal to 10 msec
- Average one-way delay less than or equal to 50 msec

Chariot measures delay from LAN to LAN—not including the delay components of coder and jitter buffer (which can consume 100 msec between these two functions). There is little or no service provider induced delay and jitter when performance testing. Some of the tests in this guide included 0-to-60 msec of service provider simulated delay. The ITU recommended maximum delay budget value is 150 msec; however, acceptable voice quality can be achieved with up to approximately 250 msec of delay. The wave file captures that exceeded the 250 msec threshold are those broadband link speeds that were below 160 Kbps uplink. For this reason, those speeds are characterized as cell phone quality in the Voice Quality and Provisioned Bandwidth chart (see Figure 7-2).

A single average jitter value has in the past been reported for Cisco Enterprise Solutions Engineering test results. This was an average of the transmit and receive portion of the call leg. Chariot reports jitter for each half of the call leg. For testing with symmetrical speeds that have QoS enabled in both directions, the values of each call leg are similar, and the *average* value is a good representation of the jitter value. However, the speeds are often asymmetrical and QoS is only applied in one direction with the broadband testing. As a result, the jitter values are reported in both directions in many cases and the average value does not report a jitter value that is higher than the criteria.

Generally voice packet loss is not an issue in any tests. An exception is when the hardware platform does not use hardware encryption acceleration and QoS. The tests in which voice loss exceeded one percent are presented for illustrative purposes and product comparison. These are not recommended configurations.

The two most important criteria for voice quality are delay and jitter. They can be managed if suitable hardware is implemented and the appropriate bandwidth is ordered from the service provider.

Voice Quality Comparison

The challenge to the lab and design engineer is to determine how to represent test results so they are meaningful to the layman in the field. To this end, a special round of testing was completed. The output of NetIQ Chariot, Cisco SAA and the Agilent Telegra VQT 2.1 (Voice Quality Tester) wave file capture utility were tabulated on the same topology using the same test methodology.

NetIQ Chariot and the Agilent Telegra are common tools for a large-scale lab test environment, but are something which the small enterprise might not be able to afford. Cisco SAA is imbedded into Cisco IOS and is available on virtually all router platforms. Producing test results which compare the reported values of these three tools provides a means for the network manager to hear the voice quality recording and then equate this to the various delay, jitter and drop statistics from the reported test results.

Since the lab environment does not adequately simulate an ISP, an Empirix Packet Sphere Model 200 was used to introduce random delay of 0-to-60 milliseconds. The delay option selected was the reverse sawtooth 1.6. No packet loss was configured. During testing it was determined that using the Packet Sphere to drop packets actually decreased the average jitter values. Lost packets are not counted as having any jitter value. Our goal was to introduce as much jitter as practical with the Empirix by varying the delay. Dropping packets did not contribute to that goal.

NetIQ Chariot reports jitter according to the RFC 1889 algorithm and has a default jitter buffer of either 40 msec or two voice packets. Cisco SAA reports both positive and negative jitter, but has no concept of a jitter buffer and packets arriving out-of-order are not calculated as jitter.

For the purposes of this testing, the jitter value on the Cisco SAA columns were calculated by adding the sum of positive jitter with the sum of negative jitter and dividing that by the number of packets. For source to destination (SD) this is represented as:

- SumOfPositivesSD + SumOfNegativesSD / NumOfRTT

And for destination to source DS it is:

- SumOfPositivesDS + SumOfNegativesDS / NumOfRTT

These values are obtained from a **show rtr collection-statistics** that is an accumulation of all successful iterations. Configuration details are shown later in this guide.

Both Chariot and Cisco SAA delay values do not include coder and jitter buffer delay elements. The Agilent tool was connected into the handset jack of the IP or analog phone and calculates the total ear to mouth delay. The Agilent delay values represent the total delay budget. Comparison of the Chariot and Agilent delay should be noted. These tests were performed with a traffic mix of voice and data as documented in the "Traffic Profiles" section on page 9-2. The only deviation from the standard configuration was the provisioning of two G.729 calls in the QoS service policy because both Chariot and Cisco SAA generate a simulated RTP stream. The priority (LLQ) queue was increased to 128 Kbps to accommodate both calls.

Tests were run on both cable and DSL—cable at 256 Kbps/1024 Kbps and DSL at 256 Kbps/1.4 Mbps—with and without the service provider delay of the Empirix Packet Sphere. The comparison charts are shown in Table 7-1 and Table 7-2.

Table 7-1 DSL Delay and Jitter Comparison

	Chariot RFC 1889 Jitter (msec)	Cisco SAA Computed Jitter (msec)	Chariot One-Way Delay (msec)	Agilent One-Way Delay (msec)
Branch to Head	9.5	6.9	62	230
Head to Branch	2.5	4.4	25	135
ISP Added Delay Range of 0-to-60 msec				
Branch to Head	10	7.4	93	274
Head to Branch	2.1	4.7	54	230

Table 7-2 Cable Delay and Jitter Comparison

	Chariot RFC 1889 Jitter (msec)	Cisco SAA Computed Jitter (msec)	Chariot One-Way Delay (msec)	Agilent One-Way Delay (msec)
Branch to Head	6.6	6.0	21	132
Head to Branch	2.1	10.6	6	110
ISP Added Delay Range of 0-to-60 msec				
Branch to Head	7.2	6.1	52	246
Head to Branch	2.4	5.9	36	169

As a visual comparison of the waveform, Cool Edit 2000 was used to graph the waveform of the files. Please refer to Figure 7-3. For the 256 Kbps/1.4 Mbps DSL test, the branch to campus (remote to head-end) RTP stream was compared between the source and the captured output with and without the Empirix Packet Sphere.

Note In Figure 7-3 there are slight differences in the waveform from the original because the voice stream was captured with and without the simulated ISP delay.

Figure 7-3 Wave Form Comparison

Several observations should be noted from reviewing the charts, graphs and audio files presented in this section. First, the G.729 codec generally does not provide voice quality as good as G.711, but the limited amount of bandwidth—rates below 256 Kbps—require its use. Cable broadband service for the same link speed as DSL generally provides lower jitter and delay values than DSL—primarily due to the greater Layer-2 overhead of ATM on the DSL network. Cable, however is a shared media, where DSL is dedicated at the local loop to a single subscriber. DSL does have an advantage over cable in this regard—up to the first DSLAM/ATM aggregation switch or ATM IP switch, where under provisioning can be an issue.

Even with service provider simulated delay, the ear-to-mouth delay as reported by the Agilent tool was in most instances below the threshold of 250 msec—the upper limit for acceptable one-way delay. Ideally this value should be less than 150 msec and was achieved in the head-to-branch flow with no additional service provider delay. However, it is not practical to assume one-way delay of 150 msec is achievable, if the service provider component of the delay budget is in the 30-to-60 msec range. It cannot be emphasized enough that minimizing the time a voice packet spends on the Internet is crucial to achieving acceptable voice quality.

For both cable and DSL, the average jitter values were considerably higher from branch to head when compared to head to branch. In all these tests, QoS was applied on the uplink but not on the downlink. The uplink always experiences congestion in our traffic profile and as such, QoS is frequently engaged. The downlink (head to branch) has a higher clockrate and as such is not as susceptible to serialization delay as the uplink.

In the lab testing, the ideal value for average jitter as calculated by Chariot using the RFC 1889 algorithm is 8 msec or less. From 8-to-10 msec is acceptable. Only the branch-to-head DSL did not meet the less than 8 msec objective. The resulting quality of the wave files—while not toll quality voice—is at least as good or better than cell quality and is acceptable for many applications.

The Cisco SAA jitter calculations are included here so you can test this in your network. By configuring the Cisco SAA agent on routers in an existing network, in trial deployments, or as a troubleshooting tool, the network administrator has a yardstick to compare the results presented here against an actual deployment. If the Cisco SAA calculated jitter values obtained on the enterprise network are similar to the results shown in the charts, the expectation should be that voice quality sounds similar to the audio files. These Cisco SAA values help predict voice quality of a deployment. Additionally, Cisco SAA is an extremely useful troubleshooting tool for existing deployments. It is not uncommon for network problems to exist for a few hours or days. Service providers do change their BGP peering and the path today over the Internet cannot be guaranteed tomorrow. Cisco SAA—in conjunction with Cisco IPM—is valuable to the network manager for both new and ongoing implementations.

Quality of Service

This section addresses QoS issues that are specific to a SOHO site connected to the enterprise by a commercial broadband service. Specific sections address the following considerations:

Bandwidth Provisioning for WAN Edge QoS

The following issues specific to provisioning the proper bandwidth on the WAN edge are addressed in this section:

Voice over IP

To support VoIP, configure the priority (LLQ) for voice packets to allocate bandwidth capable of accommodating the underlying Layer-2 overhead for cable or DSL—as well as the overhead associated with IPSec headers and trailers. It is assumed that 3DES and SHA-1 are configured in the IPSec transform set and GRE encapsulation will not be used.

Any teleworker deployment includes a mixture of cable and DSL. Within DSL deployments, the DSL interface might be terminated directly on a Cisco 837 or Cisco 1700 series or via an Ethernet-to-Ethernet router (such Cisco 831 or Cisco 1700 series) behind a firewall/cable/DSL bridge/router.

To simplify provisioning, the following minimal configuration can be used as a template:

```
policy-map V3PN_SOHO
 description Used for both cable and DSL
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
    priority bandwidth-kbps [burst]
  class class-default
   fair-queue
   random-detect
```

In the configuration above, *bandwidth-kbps* is **128** for G.711 or **64** for G.729. It is desirable to code 128 even if the deployments plan to use only G.729—otherwise someone inadvertently using a G.711 codec might experience voice drops. The only issue with this method is that, with lower link speeds, a value of 128 allocates more of the underlying bandwidth than can accommodate the seven percent required for CALL-SETUP and INTERNETWORK-CONTROL—while still accounting for the default value of 75 percent for **max-reserved-bandwidt**h.

The *burst* parameter is optional; the default value for 128 Kbps is 3200 bytes. In some instances very minor drops can be eliminated by increasing the burst parameter to 6400 bytes.

The following example shows a burst value of 3200 and associated drops.

```
beta837-vpn#show policy-map interface ethernet 0/0 | begin VOICE
        Class-map: VOICE (match-all)
          268664 packets, 72539160 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp ef
          Queueing
            Strict Priority
            Output Queue: Conversation 40
            Bandwidth 128 (kbps) Burst 3200 (Bytes)
            (pkts matched/bytes matched) 68493/18493110
            (total drops/bytes drops) 95/25650
```

The number of packets dropped in the output illustrated above is less than 0.1 percent. To eliminate these drops, increasing the burst size to 6400 has proven to be effective. The following output illustrates the result of changing the burst to 6400.

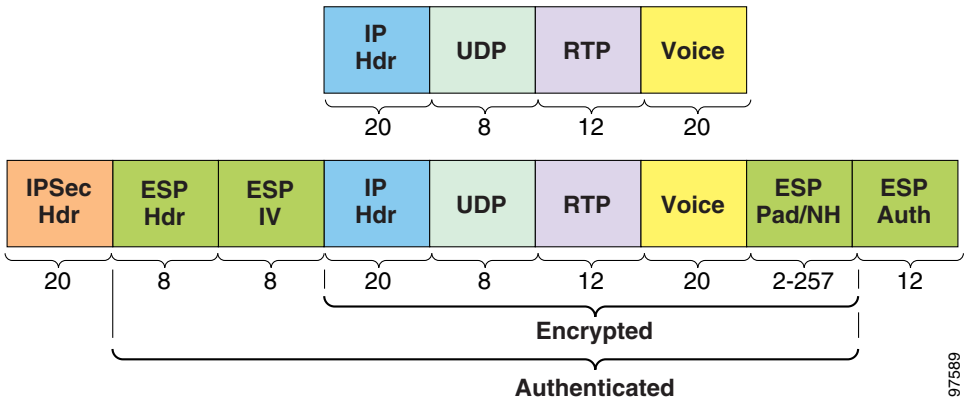
```
beta837-vpn#show policy-map interface atm 0.35 | begin VOICE
Class-map: VOICE (match-all)
      3273 packets, 955716 bytes
      30 second offered rate 104000 bps, drop rate 0 bps
      Match: ip dscp ef
      Queueing
        Strict Priority
        Output Queue: Conversation 40
        Bandwidth 128 (kbps) Burst 6400 (Bytes)
        (pkts matched/bytes matched) 3328/971776
        (total drops/bytes drops) 0/0
```

Bandwidth allocated to the priority (LLQ) that is not used by voice is not wasted. It is available to the other bandwidth classes and **class-default**. Provisioning 128 Kbps greatly simplifies deployment. There might be instances where the bandwidth savings of G.729 verses G.711 is less important—that being 256 Kbps and greater uplinks—than the slightly better voice quality obtained by G.711. Cisco's internal teleworker trial deployment used both G.729 and G.711 on a mix of cable and DSL. The standard configuration provides for 128 Kbps allocated to the priority queue.

DSL Packet Size—IPSec (only) Encrypted G.729

The Layer-3 packet size is 112 bytes per packet for a G.729 codec voice packet encrypted using a transform set which includes **esp-3des esp-sha-hmac**, 3DES as the encryption algorithm, and SHA-1 as the hash (for authentication). See Figure 7-4.

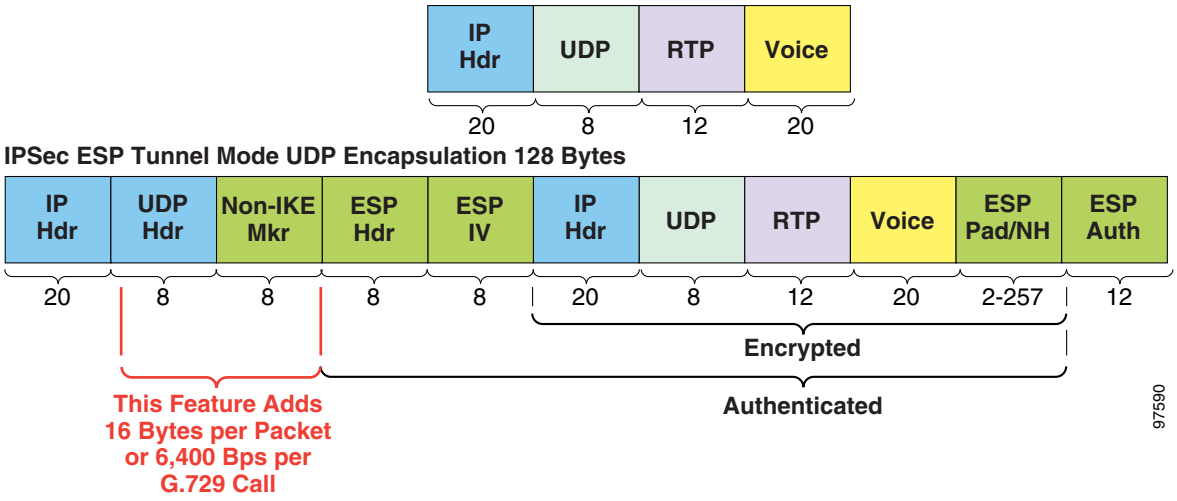
Figure 7-4 IPSec-Encrypted G.729 Packet Detail



Beginning in Cisco IOS release 12.2(13)T, NAT transparency was introduced and is enabled by default provided both peers support the feature. It is negotiated in the IKE exchange between the peers. While this feature addresses the environment where IPSec packets must pass through a NAT/pNAT device, it adds 16 bytes to each voice and data packet. For a G.729 call over DSL using PPPoE, this does not increase the number of bits on the wire, as there is AAL5 padding to absorb the 16 additional bytes and there is no need for an additional ATM cell. In cable implementations the 16 additional bytes increases the number of bits on the wire. At the head-end, it increases the bandwidth consumption of the voice traffic by 1 Mbps for approximately every 82 concurrent calls. The data packet sizes also increase and represent additional bandwidth consumed.

Unless there is a need to implement this feature, the recommendation is to disable it as a bandwidth conservation technique, which can be accomplished by the **no crypto ipsec nat-transparency udp-encapsulation** global configuration command. See Figure 7-5 for an illustration depicting overhead associated with NAT transparency.

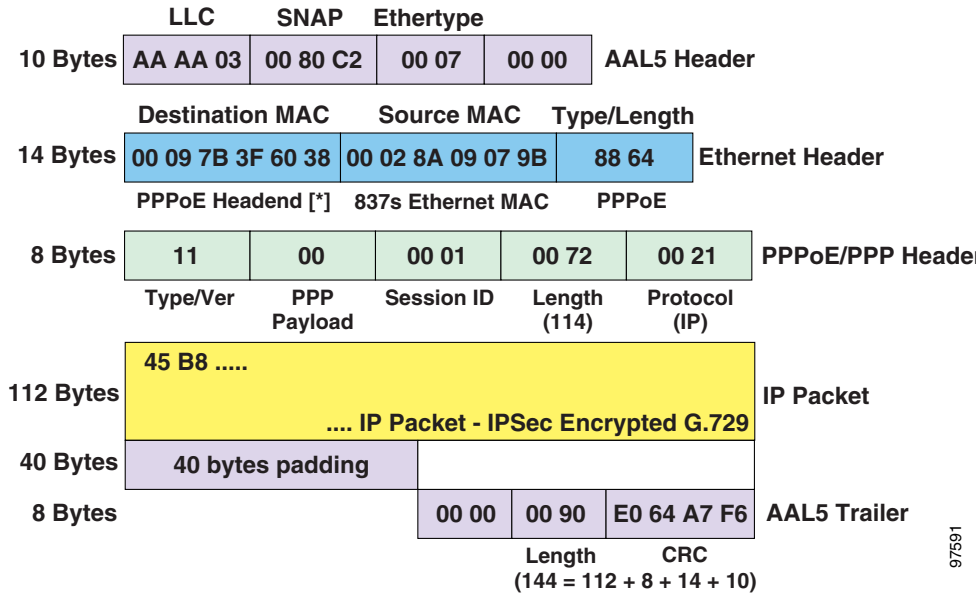
Figure 7-5 NAT Transparency Additional Overhead



Packet Size—Layer-2 Overhead

For DSL broadband connections PPPoE is the most commonly implemented deployment. Given the 112-byte, Layer-3 sized, G.729-encrypted voice call, the pre ATM Software Segmentation and Reassembly (SAR) size of the packet is 192 bytes as shown in Figure 7-6.

Figure 7-6 G.729 Packet Size Through AAL5 Encapsulation

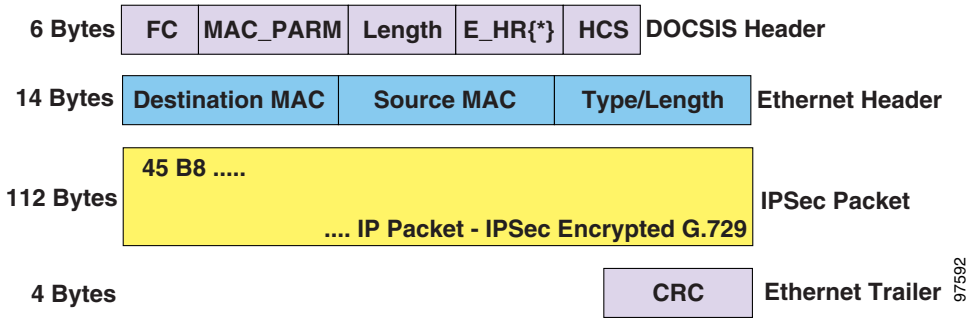


The 192 bytes of payload is incorporated via SAR into the payload (48 bytes) of four 53 byte ATM cells (192/48 = 4 cells). At 53 bytes per cell and four cells at 50 pps this represents (50 * 53 * 4 * 8) 84.8 Kbps. A G.711 call encrypted is 256 bytes and requires 7 ATM cells or 148,400 bits per second on the wire. Cisco IOS does not include the ATM cell header and the AAL5 overhead in the calculation for an output service policy on an ATM interface. For configuration purposes, the priority (LLQ) bits per second is configured at 64 Kbps for a G.729 and 128 Kbps for a G.711 call.

Cable—Packet Size, IPSec (only) Encrypted G.729

For cable deployments the Layer-2 overhead is less than DSL. The IPSec packet encapsulated in an Ethernet header (and trailer) that includes a 6-byte DOCSIS header, as shown in Figure 7-7.

Figure 7-7 G.729 Packet Size Through DOCSIS Encapsulation



If Baseline Privacy is enabled (Baseline Privacy encrypts the payload between a cable modem and the head-end), the Extended Header is used—adding an additional 5 bytes.

The packet size of a G.729 call with a zero length Extended Header is 136 bytes at 50 pps or 54,400 bps and a G.711 call is 280 bytes at 50 pps or 112,000 bps.

To simplify configuration and deployment, use the values of 64 Kbps (for G.729) or 128 Kbps (for either G.729 or G.711) for the priority queue with either DSL or cable.

Bandwidth Classes and Class-Default

In addition to provisioning for the voice bearer (RTP) stream, the other bandwidth classes and **class class-default** must be provisioned. The following configuration template is used for Cisco Enterprise Solutions Engineering lab testing and can be used as a guide for deployment.

```
class-map match-all VOICE
  match ip dscp ef
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
policy-map VoIP_IPSec
  class CALL-SETUP
   bandwidth percent 2
  class TRANSACTIONAL-DATA
   bandwidth percent 22
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
    priority 64
  class class-default
   fair-queue
   random-detect
!
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
!
```

Class CALL-SETUP is allocated two percent and matches on either Differentiated Services Code Point (DSCP) AF31 or CS3. The default value set by gateways and IP Phones is AF31. CS3 is being phased in for use as a DSCP class of AF31 per RFC 2475 which permits AF classes to be *marked with a new codepoint* (re-marked) if the traffic is out-of-profile. CALL-SETUP traffic is both delay and drop sensitive. If CALL-SETUP packets are lost, the effect is that the caller cannot dial the number to place the call—a user presses the keypad but nothing happens. Voicemail and other applications that require the processing of DMTF tones are not usable. The delay aspect might manifest itself as a ringing (and answered) phone that the first part of the greeting is missed. The bandwidth of two percent is a guideline and is suitable for most deployments. In the event packets are dropped in this class, increase the allocation appropriately.

Class INTERNETWORK-CONTROL includes traffic to manage and control the network. NTP packets are marked IP Precedence 6 (DSCP CS6) and as such falls into this class. Routing protocols (if used) also fall into this class. Currently IKE (ISAKMP) packets are not marked with DSCP value of CS6, (CSCdz01484 IKE Keepalive packets should be IP Precedence 6) and one way to address dropping these packets on the WAN edge is to include them in a bandwidth class, which is shown.

Class TRANSACTIONAL-DATA is used to simulate business critical data. During lab testing this class includes TN3270 traffic as well as HTTP text traffic. The raw test results from Chariot™ include response time values for this traffic category and as such can be used as a gauge of the *screen-to-screen* response time for an end user. This class is optional and is implementation dependent.

The **class class-default** configuration includes all traffic not otherwise classified. Initial testing was done with and without WRED enabled in this class. In Cisco internal trial deployments, WRED was included in the configuration templates and has observed to trigger random drops as well as tail drops. WRED was included as in most all cases it proves to be beneficial to total throughput without any

detrimental impact. Real-world deployments in the tested environment demonstrated engagement of the feature. An added benefit is the default configuration is IP Precedence aware—showing drops by IP Precedence—and as such is a beneficial troubleshooting tool. This allows a means to validate traffic classification. In other words, if packets of IP Precedence 4 are being shown in the WRED display in class-default, the network administrator should determine whether a bandwidth class should be allocated to accommodate this non-default marked traffic.

Broadband Downlink QoS

With both DSL and cable, the uplink connection can be enabled with QoS, either in the form of a service policy on the DSL (ATM PVC) interface or via a HCBWFQ service policy which shapes the uplink and prioritizes packets within the shaped rate. This half of the link is under the enterprise's control and can easily be configured.

The downlink connection is under the control of the broadband service provider and any QoS policy must be configured by the service provider. Most service providers do not offer QoS-enabled broadband services. Cable providers have an avenue to do so as DOCSIS 1.1 becomes more widely deployed. However, DSL providers have often implemented non-Cisco equipment (DSLAM or other ATM concentration devices) that might have no QoS features available.

Fortunately, most service offerings are asymmetrical—256 Kbps uplink and 1.4 Mbps downlink, for example. The downlink is rarely congested to the point of degrading voice quality with this type of broadband service offering for a one-teleworker deployment with a single IP phone. Using Chariot™ to generate traffic in the Cisco Enterprise Solutions Engineering lab tests, the congestion on the uplink and the resulting delay of data packet acknowledgements decrease the arrival rate of downlink data traffic in a way that does not congest the downlink. The scripts used for these tests attempted to consume all available bandwidth—in both directions. To summarize results of these tests: Asymmetrical links are beneficial with QoS on the uplink only, as long as the lower of the two speeds is viable for transporting voice and data.

Some service providers, for business class services, offer symmetrical links in an effort to compete with Frame Relay providers; 384 Kbps/384 Kbps and 768 Kbps/768 Kbps are examples. With no QoS on the service provider edge, this offering is non-optimal for the enterprise. An asymmetrical link such as 384 Kbps/1.5 Mbps is a better choice for the V^3PN network. When cable providers begin offering QoS via DOCSIS 1.1 this configuration might be acceptable.

Another common deployment is ISDN over DSL (IDSL). This can be offered to enterprises when distance to the central office is too great for a typical ADSL deployment. The rate is 144 Kbps/144 Kbps. In these deployments, uplink voice quality can be acceptable, with the aid of QoS, but downlink voice quality does suffer. In an attempt to influence the downlink congestion, shaping on both directions was configured both on internal deployments as well as lab testing.

An example configuration follows:

```
policy-map Shaper
  class class-default
   shape average 102000 1020
   service-policy VoIP_IPSec
!
interface Ethernet0/0
 description Outside
 …
 ip tcp adjust-mss 542
 service-policy output Shaper
 crypto map test
!
interface FastEthernet0/0
 description Inside
 …
 ip tcp adjust-mss 542
 service-policy output Shaper
```

The intent here would be to drop TCP packets—although on the wrong side of the link—which causes the TCP session to back-off and reduce its arrival rate, and thus reduce the congestion on the downlink. In Cisco Enterprise Solutions Engineering lab testing this did not improve the loss, delay and jitter values of a voice call sufficiently to make this a viable recommendation.

Note On the release tested on the Cisco 837, HCBWFQ is not supported. This technique can only be used on Cisco 1700 series and Cisco 831 routers at the current time.

Broadband Serialization Delay

The majority of the broadband implementations are DSL with PPPoE and cable with DOCSIS 1.0. Neither of these technologies includes any means to fragment data packets and interleave voice packets at Layer 2 to minimize the impact of serialization (blocking) delay on voice packets. Refer to Table 7-3, for the theoretical approximate maximum delay values.

Table 7-3 Approximate Maximum Delay Values

	ip tcp adjust-mss			
Line Rate (Kbps)[1]	**512 Byte (in msec)**	**640 Byte (in msec)**	**768 Byte (in msec)**	**1500 Byte (in msec)**
128	32	40	48	92
256	16	20	24	46
384	12	14	16	32
512	8	10	12	24
768	6	8	8	16

1. 128 Kbps, 256 Kbps, and 384 Kbps are common DSL and cable line rates.

There are several issues to note regarding the values presented in Table 7-3. These values represent the worst-case values—values calculated from line rate and the number of bytes that must be transmitted on the wire. Not every voice packet must wait for an entire 1500-byte data packet to be transmitted. Voice is very *packets per second* intensive when compared to a file transfer on the same speed link. During

testing a protocol analyzer capture was analyzed cell by cell (frame by frame) to better understand the traffic profile. It is not uncommon to see three voice packets in sequence and then see a data packet. Not every voice packet experiences serialization delay. Voice packets might follow other voice packets. Therefore, the average jitter of a voice steam is going to be much lower than the theoretical numbers presented. Also, Table 7-3 does not take into account ATM cell tax, AAL5, and IPSec padding and overhead.

There are dramatic differences in serialization delay between 128 Kbps and 768 Kbps. At the common DSL and cable speeds (256 Kbps/384Kbps), reducing the packet size from 1500 bytes to 640 bytes saves approximately 18-to-26 msec. To put that into perspective, voice packets are expected to be exactly 20 msec apart; there are 1,000 msec per second and a RTP stream of 50 pps—translating into 1,000/50 = 20 msec as an interval. The recommendation on configuring the interval for LFI or Frame Relay Forum.12 (FRF.12) is 10 msec. A jitter value of 10 msec represents 50 percent of the expected inter-packet interval. Saving 18-to-26 msec is substantial when viewed as a percent of the zero jitter value of 20 msec.

The DOCSIS 1.1 specification for cable includes this fragmentation and interleaving component and DSL providers can implement MPPP over ATM which also includes LFI support. However, these do not represent the majority of the current deployed base of enterprise networks. An alternative means to minimize the issue is provided by the **ip tcp adjust-mss** interface command**.**

TCP Maximum Segment Size

The TCP MSS value influences the resulting size of TCP packets. The majority of data packets on a network are TCP. Other than video, suitable UDP applications (such as DNS and NTP) exhibit an average packet size of less than 300 bytes. Use the router to influence/set the TCP MSS for TCP flows so as to reduce the data packet size. The effect is to reduce the impact of serialization delay—where no Layer-2 fragmentation and interleaving (LFI/FRF.12) technique exists.

Prior to the implementation of path MTU discovery (RFC 1191), the maximum IP packet size for off-net (hosts not on a directly connected interface) was 576 bytes. The TCP MSS is the number of bytes following the IP and TCP header, so the default MSS size was 536 bytes. The IP and TCP header are each 20 bytes, so 576 - 40 = 536. The MSS option can only appear in a TCP SYN packet and each end announces its own MSS. Although not required, they are frequently the same in both directions.

The recommended behavior changed with the introduction of path MTU discovery—allowing greater data throughput by transmitting more payload in each packet. This is fine for data, but given the relatively low-speed links of broadband connections and lack of LFI, it introduces serialization delay for voice packets.

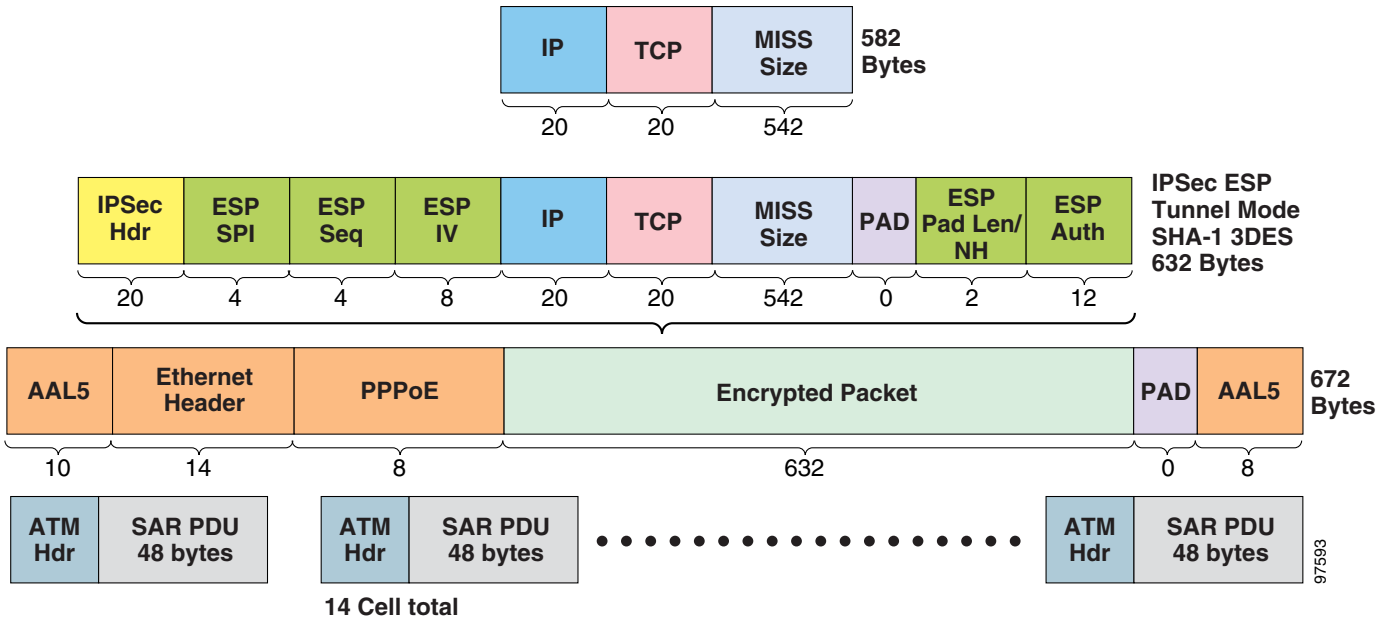
Path MTU discovery is disabled by default for TCP sessions originated by the router.

Cisco IOS has an interface configuration command to override the value of the MSS option for TCP SYN packets received through that interface, allowing the router to override the host-provided MSS value and substitute one that is optimal. The command is:

```
!
ip tcp adjust-mss 542
!
```

The value of 542 was calculated to eliminate the IPSec crypto algorithm (3DES) padding as well as the ATM AAL5 padding in DSL implementations. Cable implementations have 3DES padding but no AAL5. The value is valid for cable but was optimized for DSL. Figure 7-8 illustrates a TCP packet with a MSS size of 542.

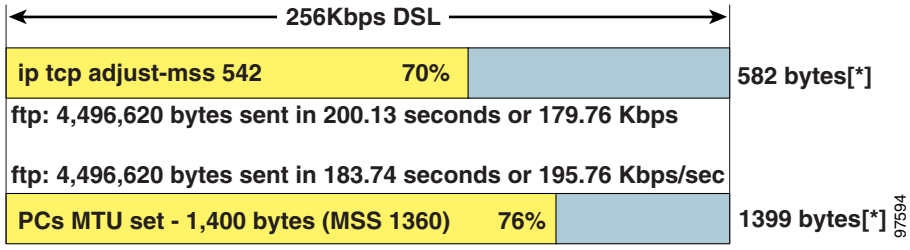
Figure 7-8 Optimized MSS Value



Note Both the ESP and AAL5 pad length are 0. A TCP packet with a MSS value of 542 fits in 14 ATM cells with no wasted bytes due to padding.

The impact of using the router to adjust the MSS value is illustrated in the Figure 7-9:

Figure 7-9 Impact of Adjusting MSS



Two tests are represented. Both were run using an Internet-connected (DSL 256 Kbps/1.4 Mbps) Cisco 837 configured similarly for QoS and IPSec to what is represented in this design guide. NetFlow was enabled on the Ethernet 0 and dialer interfaces; the flows were exported to the PC to verify average packet sizes—as shown with [*]. The FTP application-reported number of bytes sent (a binary file transfer to /dev/null on the server) are represented as a percentage of the DSL trained rate.

By making the FTP session's packets smaller, the clock time to complete the file transfer increased approximately nine percent and the number of packets increased from 3309 to 8299, or approximately 150 percent. Much of the data traffic is small, short duration flows, as is represented with HTTP requests. However, this file transfer example also represents application data such as E-mail attachment downloads/uploads and network backups.

The obvious negative aspect of using this technique to minimize the impact of serialization delay is the decreased efficiency of large data transfers and an increase in the number of packets per second that must be switched. The higher packets-per-second rate is not as much of an issue at the remote router as at the

head-end, where hundreds or thousands of remote connections are concentrated. Adjusting the MSS value provides a means for the network manager to deploy voice over broadband connections at data rates less than 768 Kbps.

Broadband Video Conference Support

Implementing video conference support on the typical broadband connection uplink (384 Kbps or less) is not practical if a VoIP call is also sharing the uplink connection, either as a separate IP Phone or as a voice stream element of a video conference-capable unit.

Both voice and video quality are sensitive to latency (delay) and jitter. As such, both video and voice should be configured in a priority (LLQ). Video packets however can generate MTU-sized packets and are typically of type UDP. Recall in the previous discussion on TCP MSS, the assumption was that the traffic over the broadband connection was a combination of VoIP (UDP), normal UDP applications such as DNS and NTP, and the remainder of the traffic TCP. The normal UDP application packets average less than 300 bytes and do not represent a serialization delay issue. The TCP application packet size is reduced via adjusting the MSS size to minimize the impact of serialization delay.

Video's large UDP packets present a problem for these low-speed connections because their presence in the LLQ incurs a serialization delay for the voice packets. The only means to decrease the size of the packets is to change the MTU of the workstation's interface. This has a negative effect on the quality of the video.

For these reasons, video conference implementations are not currently recommended for interfaces exposed to serialization delay (768 Kbps or less) and are not currently being tested in the Cisco Enterprise Solutions Engineering lab.

QoS Pre-Classify

The release of Cisco IOS tested—12.2(11)YV (versions c831-k9o3sy6-mz.122-11.YV and c837-k9o3sy6-mz.122-11.YV)—does not support QoS Pre-Classify; however, QoS Pre-Classify is configurable in release 12.2(13)ZG and the recommendation is to enable it if available. Implementations that include classification that match on fields in the Layer-3/Layer-4 header of the unencrypted packet require this feature to successfully classify.

In the "Split Tunneling—Prioritizing Enterprise Traffic over Spouse-and-Children Traffic" section on page 7-23, QoS Pre-Classify was not a requirement because all packets are classified on fields in the IPSec header—the ToS byte (DSCP values) and the destination IP address of the IPSec head-end peers. The INTERNETWORK-CONTROL class includes an access-list to select IKE (ISAKMP) packets. The following configuration fragment illustrates this feature:

```
beta837-vpn# sh ip access-list IKE
Extended IP access list IKE
    10 permit udp any eq isakmp any eq isakmp (31 matches)
```

Note IKE packets are not encrypted within the IPSec tunnel and these UDP port 500 packets can be classified by the output interface service policy.

LLQ for Crypto Engine

LLQ for crypto-engine was not available with the Cisco IOS software releases used by Cisco Enterprise Solutions Engineering in lab testing.

Determining Available Uplink Bandwidth

In the Integrated + Access Device deployment model, the access device is a cable or DSL bridge not capable of providing any Layer-3 QoS capabilities. The IPSec termination router is an Ethernet-to-Ethernet (optionally FastEthernet) router that must shape traffic to the available uplink bandwidth, and then prioritize and allocate bandwidth between the voice packets and the different classes of data packets within the shaped bandwidth (via HCBWFQ).

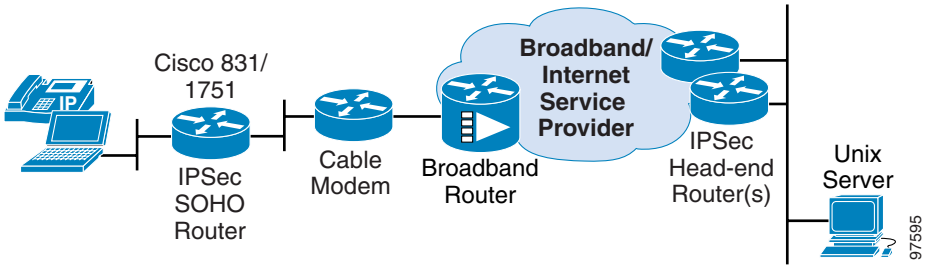
The challenge for the enterprise is determining or verifying the provisioned uplink rate so the shaper can be appropriately configured. The goal is to eliminate congestion at the access device for the link to the service provider, since this device is not capable of providing QoS. Online resources, such as the "Broadband Tests and Tools" available at www.broadbandreports.com, provide useful and available tools, but they have several disadvantages:

- The servers used for these tests might be overloaded.
- The server might reside on the Internet topology at very different locations than where the enterprise is deploying the IPSec head-end termination point.
- There might be a fee for use.
- The PC's network configuration or system configuration might influence the results.

Ideally the network manager should have a tool or means to estimate the uplink bandwidth without assistance from the end user and should be able to control the network parameters of the test to provide consistent and optimal results. This procedure provides for that, and can be executed from the central site via Telnet/SSH. It can be executed once the IPSec tunnel is up or can also be done unencrypted. The example shows the procedure assuming that the IPSec tunnel is up but with no QoS (HCBWFQ) configuration on the output Ethernet interface.

For the purposes of this example, please familiarize yourself with the simplified topology in Figure 7-10.

Figure 7-10 Topology for Determining Uplink Bandwidth



This example is from a Cisco 831 running Cisco IOS c831-k9o3sy6-mz.122-11.YV. The Unix Server is at IP address 172.26.156.10, for which we have a valid username and password. FTP daemon is running.

On the IPSec SOHO router, there is no QoS configuration; however, the IPSec tunnel is up and active to the IPSec head-end routers and packets sourced from the inside Ethernet interface are encrypted. On the Cisco 831 router, the inside interface is Ethernet 0. The following commands must be included in the router's running configuration:

```
!
ip ftp source-interface e 0
!
ip tcp path-mtu-discovery
!
```

This speed test uses FTP, and the router should source FTP requests off the inside interface so the packets are encrypted in the IPSec tunnel and can reach the Unix Server. This configuration does not permit split tunneling and the Unix server is only reachable via the IPSec tunnel by the IPSec SOHO router. All IPSec routers in this example are using hardware encryption accelerators; the overhead incurred is minimal and does not invalidate the performance of this test.

TFTP should not be used since it uses UDP, typically at 512 bytes per packet and must receive an acknowledgement from the server before sending additional packets. The file transfer rate when using TFTP is not an accurate indicator of uplink speed, especially as the latency in the path increases. The throughput of TFTP degrades greatly as the latency increases because of the *lock step* nature of the application.

By default, Cisco IOS uses a default value of 536 bytes for the TCP MSS when sessions are initiated by the router. This can be seen by issuing the command:

```
Router#show tcp | inc max data segment
Datagrams (max data segment is 536 bytes):
Datagrams (max data segment is 536 bytes):
Datagrams (max data segment is 536 bytes):
Datagrams (max data segment is 536 bytes):
```

In the above display, the router had four TCP sessions active and each advertised a MSS of 536 bytes. When the command **ip tcp path-mtu-discovery** is included in the configuration, the router can derive the appropriate maximum data segment size without manual calculations on the network administrator's part. The goal is to send as large a packet as possible without incurring any Layer-3 fragmentation. This provides a reasonable estimate of the uplink bandwidth.

With **ip tcp path-mtu-discovery** in the configuration, **show tcp** indicates the FTP TCP connection has a maximum data segment size of 1460 (1500 bytes minus 40 bytes for IP and TCP headers). When the file transfer starts, following the first packet (illustrated by a "!" in the display), the crypto card issues the following to the console:

```
: CRYPTO_ENGINE: locally-sourced pkt w/DF bit set is too big,ip->tl=1500, mtu=1442
```

This indicates that path MTU discovery is functioning and the file transfer is sending the largest packet possible without fragmenting.

In the event **ip tcp path-mtu-discovery** is not supported, **ip tcp adjust-mss** can be used instead to increase the packet size. Depending on the crypto transform set options, a value between 1360 and 1420 bytes is normally sufficient.

Determine the file name of the image in flash by issuing the following:

```
router#show flash

System flash directory:
File  Length   Name/status
  1   5315104  c831-k9o3sy6-mz.122-11.YV.bin
```

Upload this file to the Unix host generating network traffic on the uplink. Given the above file name from flash, and a username of username with a password of password, initiate a copy of the system image file from the router's flash memory to the Unix system using FTP. The file name on the Unix system is /dev/null (two slashes "//" in the URL indicate an absolute rather than a relative file reference) which discards the output on the host without incurring the expense of writing the file to the disk subsystem.

```
router#copy flash:c831-k9o3sy6-mz.122-11.YV.bin
ftp://username:password@172.26.156.10//dev/null
Address or name of remote host [172.26.156.10]?
Destination filename [/dev/null]?
Writing /dev/null !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 [repetition removed]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
5315104 bytes copied in 129.688 secs (40984 bytes/sec)
```

From the above output, the transfer rate was 40,984 bytes per second or 327,872 bits per second. This rate does not include the Layer-2, IPSec and Layer-3/Layer-4 overhead. Given a FTP throughput of 320 Kbps, plus the additional overhead, it can be assumed that the cable provider is likely limiting the uplink to 384 Kbps. Some commonly provisioned rates are shown in Table 7-4.

Table 7-4 Common Broadband Data Rates

Provider	Down Rate (bps)	Up Rate (bps)	Monthly Charge
Residential iDSl	144K	144K	$69.99
Residential aDSL	128K	128 K	$50 to $65
	512K	128 K	
	864 K	160 K	
	1,472 K	256 K	
	1.5 M	384 K	
Residential Cable Modem	1,024 K	256 K	$39.99 to $50
	1.5 M	384 K	
Business Cable Modem	4 M	2 M	$384
T1	1.5 M	1.5 M	$200 to $800

Generally both cable and DSL providers offer uplink rates at 128 Kbps, 160 Kbps, 256 Kbps, and 384 Kbps.

It can be assumed from the previous example, the uplink for this broadband cable user is rate limited to 384 Kbps.

Note Some service providers might offer a guaranteed rate of 256 Kbps with a burst rate of 384 Kbps or the burst and guaranteed rate might be the same value—shaping at the guaranteed rate is the recommended configuration. This and other speed tests might be taking advantage of the additional burst capacity and reporting higher than guaranteed values.

As an illustration, a test was run on a DSL broadband connect where **ip tcp mss** was used to influence the packet size instead of **ip tcp path-mtu-discovery.** The connection was known to train up at 256 Kbps on the uplink by previously having a Cisco router with a DSL WIC connected to the circuit and observing the rate with the **show dsl int atm 1/0** command. During this test the Cisco 1751 was configured as a FastEthernet/Ethernet router with a DSL bridge (modem) providing the termination of the DSL circuit.

The router was configured with the following command:

```
!
ip tcp mss 1400
!
```

This yields a Layer-3 packet size of 1440 (adds a 20-byte TCP header plus a 20-byte IP header). With a transform set that included **esp-3des** and **esp-sha-hmac**, the resulting encrypted packet is 1496 bytes —which is under the 1500 byte MTU of the output interface.

The results of this test were as follows:

```
router#show flash

System flash directory:
File  Length   Name/status
  1   12048716  c1700-k9o3sv8y7-mz.122-13.T1
[12048780 bytes used, 4728436 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

router#copy flash c1700-k9o3sv8y7-mz.122-13.T1
ftp://username:password@172.26.156.10//dev/null
Address or name of remote host [172.26.156.10]?
Destination filename [/dev/null]?
Writing /dev/null !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 [repetition removed]
!!!!!!!!!!!!!!!!!!!!!!

12048716 bytes copied in 546.276 secs (22056 bytes/sec)
```

From the above output, the transfer rate was 22,056 bytes per second or 176,488 bits per second. In this example, the payload throughput for this file transfer on the 256 Kbps trained rate DSL connection was approximately 69 percent.

The reported rates documented in this section are similar to those calculated by online broadband test servers.

Limiting High Priority Traffic

Implementing QoS can be described as *managed unfairness*, where the organization makes a decision to prioritize packets based on application requirements and relative importance to the operation of the business. When implementing a QoS policy in the enterprise network, the network manager must guard against theft of service.

Every organization has employees who either deliberately (or sometimes inadvertently) mark data packets with the same IP Precedence or DSCP values used to characterize voice packets—DSCP value EF for voice bearer or AF31/CS3 for call setup. The intent might be to optimize application response time and throughput. However, this is done at the expense of another employee's voice quality.

Cisco IP Phones will set the Layer-2 IEEE 802.1P class of service (CoS) value and the Layer-3 ToS (DSCP) value for both the RTP stream and the call control traffic. However, SOHO routers are unable to support these features and are unable to do anything with these settings. Because of that, the emphasis here is in illustrating how to rate-limit based on the values that SOHO routers can influence.

To rate-limit (police) the packets marked DSCP EF/AF31/CS3 received by the SOHO router's inside Ethernet port, an input QoS service policy can be applied. The rate selected should be sufficient for the number of concurrent calls (the teleworker's environment only involves one call), plus some margin to accommodate bursts and jitter.

If employees mark data traffic with DSCP value EF, both data and voice packets will be subject to policing (and can be dropped) and voice quality will suffer. Affecting the employee's voice quality should be a sufficient deterrent to stealing bandwidth allocated for voice.

Assuming some deployments might use G.711, the following configuration permits 184 Kbps of DSCP EF traffic and 48 Kbps of AF31/CS3 traffic into the remote router's inside Ethernet interface.

```
class-map match-all VOICE
  match ip dscp ef
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
!
policy-map Limit_Hi_Pri
  class VOICE
   police cir 184000
     conform-action transmit
     exceed-action drop
  class CALL-SETUP
   police cir 48000
     conform-action transmit
     exceed-action drop
!
interface Ethernet0
 description Inside
 …
 service-policy input Limit_Hi_Pri
```

To illustrate the operation of this configuration, a **show policy interface e0**, output is captured while one voice call (G.711) is active through the Cisco 837's Ethernet 0 interface as well as other data traffic.

```
beta837-vpn#show policy-map interface ethernet 0
 Ethernet0

  Service-policy input: Limit_Hi_Pri

    Class-map: VOICE (match-all)
      2938 packets, 628732 bytes
      30 second offered rate 73000 bps, drop rate 0 bps
      Match: ip dscp ef
      police:
          cir 184000 bps, bc 5750 bytes
        conformed 2938 packets, 628732 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 73000 bps, exceed 0 bps

    Class-map: CALL-SETUP (match-any)
      30 packets, 1884 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
        30 packets, 1884 bytes
        30 second rate 0 bps
      Match: ip dscp cs3
        0 packets, 0 bytes
        30 second rate 0 bps
      police:
```

```
    cir 48000 bps, bc 1500 bytes
  conformed 30 packets, 1884 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
  3086 packets, 1243856 bytes
  30 second offered rate 118000 bps, drop rate 0 bps
  Match: any
```

In the preceding **show** command output example, the CALL-SETUP class includes both DSCP AF31 and CS3 and packets matched on AF31—which is the default value for the Cisco 7960 IP Phone. Additionally, all non-voice related packets fall into **class-default** and are not policed. There is a service policy configured on the output ATM interface to prioritize voice and data traffic appropriately.

Split Tunneling—Prioritizing Enterprise Traffic over Spouse-and-Children Traffic

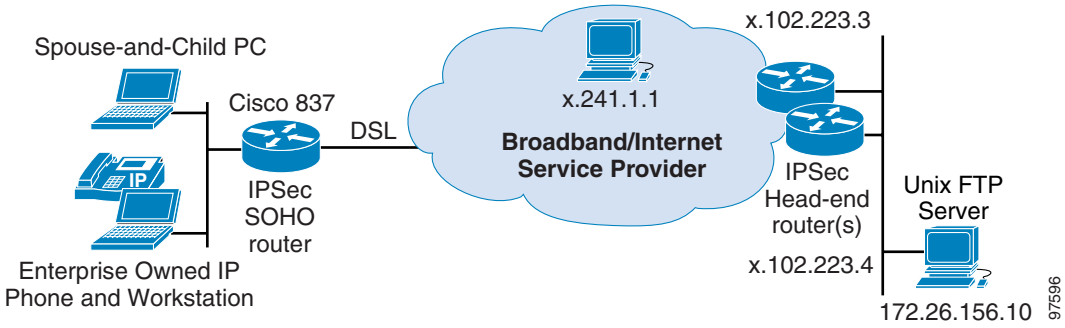
In a configuration where the Spouse-and-Children workstations are behind the enterprise-owned SOHO router and split tunneling is deployed, it is desirable to favor the data traffic to the enterprise core over the data traffic to the Internet. The enterprise-owned workstation might not be configured to set the ToS byte (DSCP) of the corporate traffic. Even if this technique was implemented for transactional or mission critical data, there will be applications on the workstation classified as best-effort by the enterprise.

In this situation, prioritization must be made based on the destination address of the traffic. Traffic to the enterprise core should be higher priority than traffic to the Internet. One method to accomplish this is to create a separate bandwidth class and prioritize all traffic in the IPSec tunnel not specifically selected by ToS byte (VOICE, CALL-SETUP, INTERNETWORK-CONTROL) over the remaining traffic going to the Internet.

Given the sample topology illustrated in Figure 7-11, a suitable QoS configuration should allocate and prioritize traffic in the following categories:

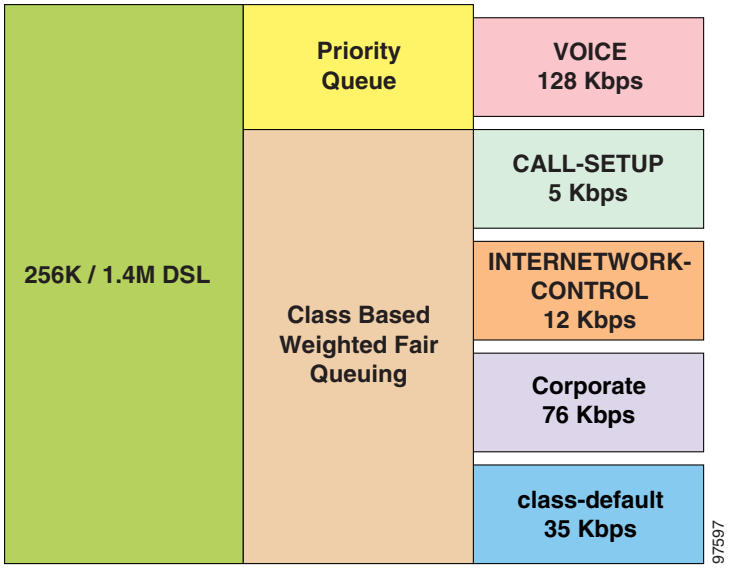
- Voice packets in the Priority Queue (LLQ) allocation based on codec
- Call Setup traffic in a bandwidth queue allocated two percent
- Internetwork control traffic in a bandwidth queue allocated five percent
- All other traffic that is destined to the enterprise via the IPSec tunnel allocated 30 percent
- Traffic to the Internet (outside the IPSec tunnel) will fall into class default

Figure 7-11 Split Tunneling Sample Topology



Given these allocations, for a 256 Kbps/1.4 Mbps ADSL link, the actual bandwidth allocations are shown in Figure 7-12.

Figure 7-12 Split Tunneling Bandwidth Allocations



The following configuration fragment provides the means to implement this policy. It assumes that the head-end IPSec crypto peers reside on network xx.102.223.0/29. In this example environment, there are two peers configured at xx.102.223.3 and xx.102.223.4. Packets within the IPSec tunnel—those matching the ENCRYPT_This access control list (not shown)—will be encapsulated in an ESP (IPSec-IP protocol 50) IP header. A **class-map** *Corporate* is configured which references the *Corporate* extended access-list.

A policy map named *Split_Tunnel* is created which includes classes for VOICE, CALL-SETUP, and INTERNETWORK-CONTROL, as well as a bandwidth class for *Corporate*. *Corporate* will be allocated a bandwidth percent of 30 percent. This is an arbitrary allocation. In this example the VOICE class is provisioned for a G.711 codec, allocating 128 Kbps. If G.729 is used, then 64 Kbps is sufficient. Note that the burst size of the priority keyword is configured at 6400 rather than the default of 3200. In testing some voice drops were observed in the priority queue and the burst size was increased which eliminated the voice drops. The relevant configuration fragment follows:

```
crypto map test 1 ipsec-isakmp
 set peer xx.102.223.3
 set peer xx.102.223.4
 set transform-set t1
 match address ENCRYPT_This
!
ip access-list extended Corporate
 permit esp any xx.102.223.0 0.0.0.7
!
class-map match-all Corporate
  match access-group name Corporate
!
policy-map Split_Tunnel
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
    priority 128 6400
```

```
  class Corporate
   bandwidth percent 30
  class class-default
   fair-queue
   random-detect
!
interface ATM0.35 point-to-point
 pvc dsl 0/35
  vbr-nrt 256 256
  tx-ring-limit 3
  max-reserved-bandwidth 90
  service-policy output Split_Tunnel
  pppoe-client dial-pool-number 1
 !
```

In the above example, note that the **max-reserved-bandwidth 90** command was added to the PVC configuration. This was required since the allocations for the LLQ and bandwidth queues exceed the default value of 75 percent of the 256 Kbps link: 128 Kbps + 5 Kbps + 12 Kbps + 76 Kbps = 221 Kbps and 221 / 256 = 86 percent. If a G.729 codec was in use for this example, the **max-reserved-bandwidth** command default of 75 percent need not change: 64 Kbps + 5 Kbps + 12 Kbps + 76 Kbps = 157 Kbps and 157 / 256 = 61 percent, which is less than 75 percent.

To illustrate the functioning of this configuration, traffic was generated by an enterprise owned PC. A file transfer (PUT) was started to a Unix FTP Server 172.26.156.10 which is reachable via the IPSec tunnel. This traffic is selected for inclusion into the *Corporate* class. An IP Phone call was placed, and a Perl program was run from the PC that continually sent UDP packets to x.241.1.1, an address that is accessible via the Internet and is not encrypted. Samples of the output are shown.

```
D:\>perl udp.pl 800 1004 5 x.241.1.1 x.241.1.1 x.241.1.1 x.241.1.1 x.241.1.1
To x.241.1.1- sending 1004 buffers, length 800, delaying 5 seconds.
To x.241.1.1- sending 1004 buffers, length 800, delaying 5 seconds.
To x.241.1.1- sending 1004 buffers, length 800, delaying 5 seconds.
To x.241.1.1- sending 1004 buffers, length 800, delaying 5 seconds.
To x.241.1.1- sending 1004 buffers, length 800, delaying 5 seconds.

ftp> put c837-k9o3y6-mz.bin /dev/null
200 PORT command successful.
150 Binary data connection for /dev/null (10.81.3.26,3332).
################################################################################
...
################################################################################
################################################################################

226 Transfer complete.
ftp: 5571044 bytes sent in 414.57Seconds 13.44Kbytes/sec.
```

While the test traffic was active along with the IP Phone call, a **show policy-map** is issued to observe the packet classification. Several items to note are:

- Packets are matched by DSCP value and are placed in the appropriate class even though these packets flow into the IPSec tunnel.
- The file transfer rate was 13.44 KBps (107 Kbps) is greater than the allocated bandwidth of 76 Kbps. The Perl UDP packet blaster sends a burst of data and then waits for 5 seconds before sending again. When the interface was not congested by this simulated Internet traffic, the FTP was able to use the available bandwidth.
- Packets were dropped from the default class—which represented the traffic going to the Internet. The WRED configuration in this class produced both random and tail drops.

The **show policy-map** output follows:

```
beta837-vpn#show policy-map interface atm 0.35
 ATM0.35: VC 0/35 -

  Service-policy output: Split_Tunnel

    Class-map: CALL-SETUP (match-any)
      32 packets, 4336 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31
        32 packets, 4336 bytes
        30 second rate 0 bps
      Match: ip dscp cs3
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
        Output Queue: Conversation 41
        Bandwidth 2 (%)
        Bandwidth 5 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 32/4336
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: INTERNETWORK-CONTROL (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs6
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name IKE
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
        Output Queue: Conversation 42
        Bandwidth 5 (%)
        Bandwidth 12 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: VOICE (match-all)
      3273 packets, 955716 bytes
      30 second offered rate 104000 bps, drop rate 0 bps
      Match: ip dscp ef
      Queueing
        Strict Priority
        Output Queue: Conversation 40
        Bandwidth 128 (kbps) Burst 6400 (Bytes)
        (pkts matched/bytes matched) 3328/971776
        (total drops/bytes drops) 0/0

    Class-map: Corporate (match-all)
      2375 packets, 757332 bytes
      30 second offered rate 34000 bps, drop rate 0 bps
      Match: access-group name Corporate
      Queueing
        Output Queue: Conversation 43
        Bandwidth 30 (%)
        Bandwidth 76 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 2407/768620
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      830 packets, 711028 bytes
      30 second offered rate 81000 bps, drop rate 46000 bps
```

```
    Match: any
    Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 32
      (total queued/total drops/no-buffer drops) 0/349/0
       exponential weight: 9

 class    Transmitted      Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes       pkts/bytes       pkts/bytes    thresh  thresh  prob
     0     480/409418         56/48384       293/253152       20      40  1/10
     1       0/0                0/0              0/0          22      40  1/10
     2       0/0                0/0              0/0          24      40  1/10
     3       0/0                0/0              0/0          26      40  1/10
     4       0/0                0/0              0/0          28      40  1/10
     5       0/0                0/0              0/0          30      40  1/10
     6       0/0                0/0              0/0          32      40  1/10
     7       0/0                0/0              0/0          34      40  1/10
  rsvp       0/0                0/0              0/0          36      40  1/10
```

```
beta837-vpn#sh ver | inc image
System image file is "flash:c837-k9o3sy6-mz.122-11.YV.bin"
```

Note Without QoS provided by the ISP, the only way to eliminate or minimize down link congestion is adopt and asymmetrical broadband service. In this case the DSL connection is 256 Kbps/1.4 Mbps.

IP Security

In this section IPSec issues specific to SOHO/teleworker implementations are discussed. Topics include:

Multiple Peer Statements, IKE Keepalive and Dead Peer Detection

This design guide is based on a deployment model that uses multiple peer statements in the remote router's crypto map and dynamic crypto maps on the head-end routers. The remote router is configured for IKE keepalive/DPD to verify the selected head-end peer's availability, and to optionally select an alternate peer in the event the head-end router does not respond to IKE keepalive messages. Up to 40 peers can be defined, however typically two are sufficient. This deployment model is referred to as an *IPSec-only* configuration—meaning there is only an IPSec tunnel and no associated GRE tunnel to the head-end.

The advantage of this configuration for the SOHO deployment is scalability. Configuring GRE and a routing protocol limits the number of remote routers that can be supported by the head-end IPSec/GRE routers to the capability of the routing protocol. The practical maximum number of neighbors, either EIGRP or OSPF, is 500. A more conservative number of neighbors ranges from 200 to 300. As the numbers of neighbors increases toward the upper limit and the network encounters some instability (a link flap that can simultaneously disable hundreds of neighbors), a network might be unable to re-converge. The following symptom process would observed:

1. Neighbors come up.
2. The router's CPU approaches 100 percent bringing up additional neighbors.
3. The established neighbors are lost due to missed hello/keepalive.
4. The process restarts.

An IPSec-only configuration can scale higher for several reasons.

1. IKE keepalives are not always periodic. This is the behavior introduced by DPD. If there is traffic flowing over the IPSec tunnel, no IKE keepalive messages must be sent. Presence of packets being decrypted in the tunnel is an assurance the peer is functioning.
2. There is no additional overhead of a routing protocol to each peer. The IKE processing to establish IPSec tunnels is required even with GRE and a routing protocol—so the routing protocol overhead is additional.
3. GRE and a routing protocol together build and maintain IPSec tunnels. All the tunnels will come up and become active once the router reloads. Without a routing protocol, IKE and IPSec tunnels are only built if there is interesting traffic to send.
4. The presence of GRE tunnels and GRE encapsulation consumes extra CPU processing cycles.

The primary *disadvantage* of an IPSec-only configuration is the inability to support IP multicast. However for the teleworker environment, this is a minor issue. The primary advantage of IP multicast is bandwidth savings. IP multicast eliminates multiple flows between client and server and consolidates them to a single flow per source/sink. If you have ten users at a remote site, rather than have ten separate unicast flows for the same content (streaming video perhaps) you have one flow of data for that content. While this is an advantage for a small office, the advantage is lost for the teleworker deployment, as there is typically only one person on the broadband connection.

There is additional information on sample configurations in the "Head-end Redundancy for Remote Peers" section on page 7-32 as well as in *Voice and Video Enabled IPSec VPN (V³PN) SRND Guide*.

X.509 Certificates

As part of the Cisco Enterprise Solutions Engineering lab testing and Cisco internal trials, a Microsoft Certificate Server was deployed.

Head-end Topology

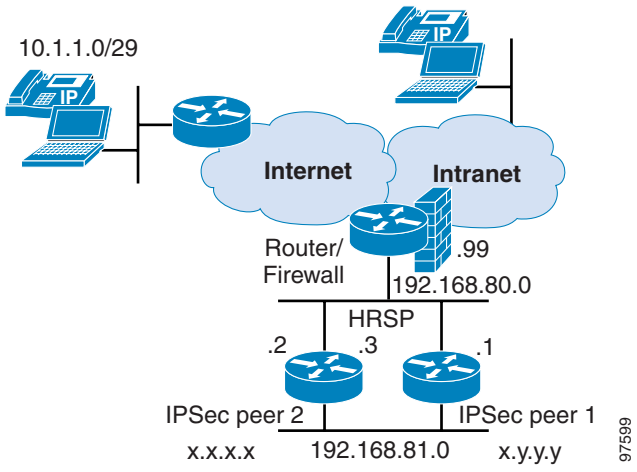
This section illustrates suggested head-end topologies for this solution. An issue relating to route injection by the IPSec head-end routers is also discussed.

Topology topics addressed in this section:

Sample Topology—Router-on-a-Stick

The *Voice and Video Enabled IPSec VPN (V³PN) SRND Guide* provides a detailed look at the *router-on-a-stick* configuration deployed in Cisco internal trials. The topology's basic configuration appears in Figure 7-13.

Figure 7-13 Head-end Topology—Router on a Stick



The above configuration as documented was very stable for more than a year in deployment. The only enhancement was to include a summary route to avoid looping packets between the IPSec head-ends and the router/firewall during periods of instability of remote routers. Hosts and IP Phones in the Intranet can send packets to the remote subnet after the IKE Keepalive/DPD logic has removed the remote subnet from the routing table. In this topology the router/firewall is configured as shown below.

```
ip route x.x.x.x 255.255.255.255 192.168.80.2
ip route x.y.y.y 255.255.255.255 192.168.80.1
ip route 10.1.0.0 255.255.0.0  192.168.80.3
!
#  10.1.0.0/16 is advertised into the Intranet
#  x.x.x.x and x.y.y.y are Internet routable addresses
```

Addresses x.x.x.x and x.y.y.y are the Internet routable addresses of the IPSec head-ends configured as loopback addresses on each IPSec peer and referenced in the remote router's crypto map as **set peer x.x.x.x** and **set peer x.y.y.y.** Additionally the router/firewall has one static route to 10.1.0.0/16, which covers all the remote router's subnets. This route points to the HSRP address shared by the two IPSec head-ends.

Since the IPSec head-ends are both *routers-on-a-stick*, they each only need a default route to the router/firewall address in order to route. For example:

```
!
ip route 0.0.0.0 0.0.0.0 192.168.80.99
!
```

The RRI routes injected into the routing table (and re-distributed by EIGRP between the two IPSec head-ends) allow the HSRP active router to do one of the following:

- Forward the unencrypted packet over the 192.168.81.0 network to the second IPSec peer for encryption.
- Encrypt the packet itself and forward following the RRI route from its own routing table.

If there are packets received from the Intranet for remote subnets, for example, 10.1.1.0/29, and no active IPSec tunnel exists on either IPSec peer, the HSRP router forwards these packets unencrypted back to the router/firewall, following the default route. The router/firewall again forwards the packet back to the HSRP router and the packets loops between these two routers until the time-to-live (TTL) expires on the packet. To eliminate this behavior, both IPSec head-end peer routers should have a summary route to the null interface in their routing table for the entire address range of all the remote routers. For example:

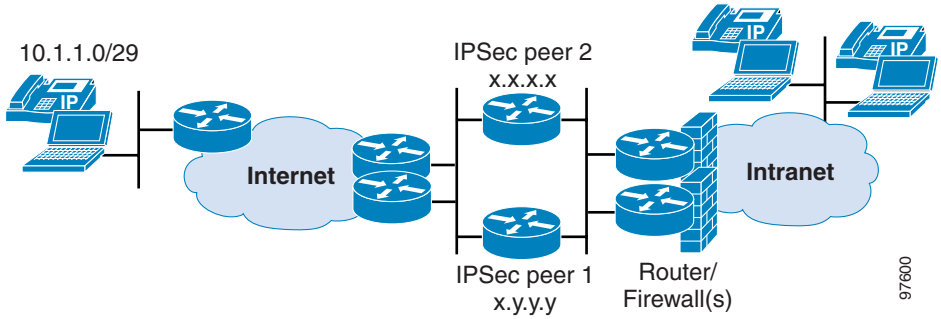
```
!

ip route 10.1.0.0 255.255.0.0 Null0
!
```

This discards the packet since no more specific route exists in the routing table.

Sample Topology—Routers In-line

An alternative approach to router-on-a-stick is to place the IPSec peers in-line. An example of this topology is summarized in Figure 7-14. In this topology, the router/firewall(s) are configured as EIGRP neighbors to the IPSec head-end peers and should advertise a summary route into the intranet (per **ip summary-address eigrp 44 10.1.0.0 255.255.0.0 5**). The IPSec head-end routers are configured for RRI and re-distribute the remote subnets to the router/firewalls via EIGRP.

Figure 7-14 Routers In-Line Head-end Topology



The IPSec head-end peers have configurations similar to the following example:

```
!
crypto dynamic-map dmap 10
 set transform-set FOO
 reverse-route
!
router eigrp 44
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 passive-interface FastEthernet0/0      # This is the Outside interface - toward the
Internet
 network 192.168.81.0                   # This is the Inside interface - toward the
Intranet
 no auto-summary
 eigrp log-neighbor-changes
!
ip route 0.0.0.0 0.0.0.0 10.81.0.1      # A HSRP address for the Internet WAN routers
ip route 10.1.0.0 255.255.0.0 Null0     # To avoid looping packets
!
access-list 1 permit 10.1.0.0 0.0.255.255
access-list 1 deny   any
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!
```

In this example the IPSec peers and the router/firewalls share a common network: 192.168.81/0. The IPSec peers connect to the Internet WAN aggregation routers over their FastEthernet0/0 interface on the 10.81.0.0 subnet. The IPSec peers either learn a default route from the Internet WAN aggregation routers via a dynamic routing protocol or by a static default route as shown in the configuration. If there is more than one WAN aggregation router—and no dynamic routing protocol is used—the target IP address should be a HSRP address.

Either the router-on-a-stick or the in-line topology is sufficient for most enterprise deployments. Firewall placement in relation to the IPSec peers depends on the organization's security requirements, as well as the use of Intrusion detection systems or other monitoring tools. Additionally, if the remote subnets are RFC 1918-compliant (private address space) and split tunneling is configured on the remote routers, NAT must be configured on the remote routers—otherwise NAT is required at the head-end topology for access to the Internet from the remote routers.

Head-end Redundancy for Remote Peers

In a deployment model featuring IPSec, IKE keepalive/DPD and RRI at the head-end, multiple **set peer [***ipaddress***]** statements are defined in the remote router's crypto map. Up to 40 peers can be defined, but in practice only 2-to-4 peers are necessary for most deployments.

```
!
crypto isakmp keepalive 10
!
crypto ipsec transform-set FOO esp-3des esp-sha-hmac
!
crypto map test 1 ipsec-isakmp
 set peer x.x.x.x
 set peer x.y.y.y
 set transform-set FOO
 match address 101
 qos pre-classify
```

As *interesting traffic* requires encryption, an IKE tunnel is attempted to the first peer in the list. If that process is successful, the IKE and IPSec tunnels retain an affinity to that peer. No IKE keepalives are sent as long as traffic is being decrypted from the peer router for the duration of the IKE keepalive interval (this is true from both the head-end and remote perspective). When there is no traffic in the IPSec tunnel, IKE keepalives are sent to the remote peer and if no acknowledgements are received—after the dead interval—a new IKE tunnel is attempted to the next peer in the list. This is a summary of the DPD and IKE logic. Output from a **debug crypto isa** is shown:

```
Jan 16 12:56:51 : ISAKMP (0:1): more than 10 seconds since last inbound data. Sending DPD.
Jan 16 12:56:51 : ISAKMP (0:1): DPD Sequence number 0x704EABCB
Jan 16 12:56:51 : ISAKMP (0:1): sending packet to 141.158.245.134 (R) QM_IDLE
Jan 16 12:56:51 : ISAKMP (0:1): received packet from 141.158.245.134 (R) QM_IDLE
Jan 16 12:56:51 : ISAKMP (0:1): processing HASH payload. message ID = -1667280517
Jan 16 12:56:51 : ISAKMP (0:1): processing NOTIFY R_U_THERE_ACK protocol 1 spi 0, message
ID = -1667280517, sa = 82D66828
Jan 16 12:56:51 : ISAKMP (0:1): DPD/R_U_THERE_ACK received from peer 141.158.245.134,
sequence ….
```

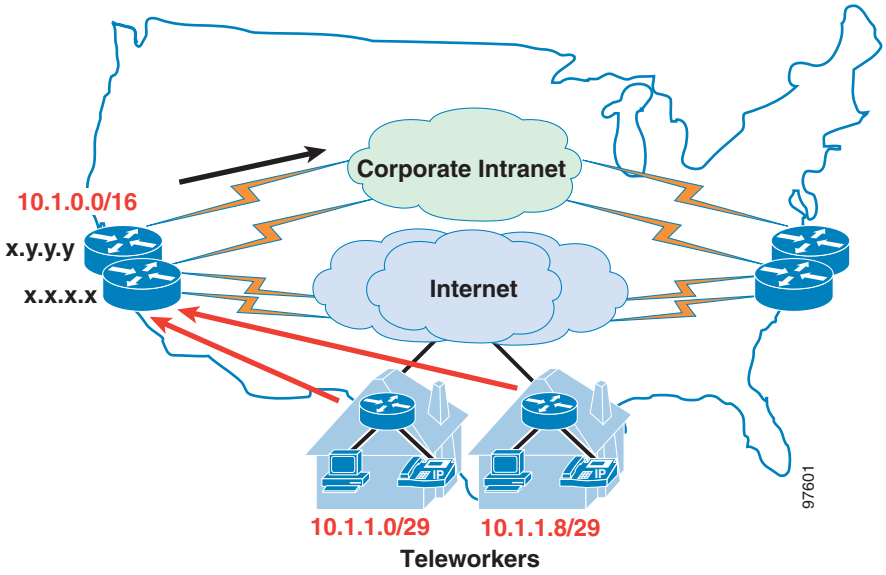
This process continues through the list, beginning again at the top, until tunnels are successfully established. During Cisco internal trials, the number of remote peers with IKE/IPSec tunnels to each head-end router was approximately equal.

Understanding this behavior influences the head-end placement in two ways.

- First, it means that load sharing of the head-ends is a natural occurrence when the peers' traffic must cross an ISP or other network that might encounter short service disruptions throughout the course of the day. In the Internet and in Frame Relay networks, it is not uncommon to see some short connectivity failures in a 24-hour period. Anyone who has run a Frame Relay network and executes a **syslog** command to a central server from all the Frame Relay WAN aggregation routers, will see in the log link up/down messages from some percentage of the Frame Relay sites. The same is true of the Internet. But with the Internet, you do not have a point-to-point link between the central site and the remote site—rather there is a logical link. Think of this as a *logical link flap* as opposed to a *physical link flap*. In this guide any references to a link flap include this concept of *logical* link flaps.
- The second design consideration relates to protecting the organization's intranet core from routing instability due to these logical link flaps. From a routing protocol design perspective, protecting the core routers from instability is the most important aspect of maintaining a stable core network. The tool to accomplish this is summarization. The network manager should summarize routes injected into the core network in order to hide individual link flaps from the core network.

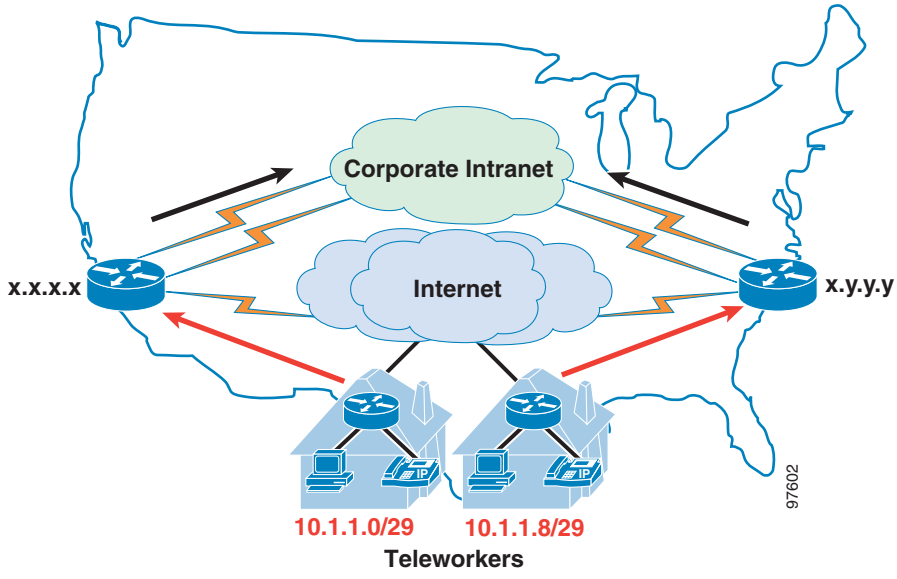
Given the configuration sample shown earlier, assume addresses 10.1.1.0/29 and 10.1.1.8/29 are allocated to two remote teleworker routers. The **set peer** addresses are x.y.y.y and x.x.x.x and both these peers are located in San Jose, California. Both these remote addresses can be advertised into the core corporate intranet as a route to 10.1.0.0/16 and no connectivity failures at the remote locations will be seen in the core. An example is illustrated in Figure 7-15.

Figure 7-15 Summary Route for RRI Subnets



The alternative is having one of the head-end peers in California and the second peer in North Carolina. In this case, the RRI injected routes must be advertised into the core corporate intranet from at least one of the locations for the return traffic to reach the IPSec head-end that has the active tunnels. As links flap—perhaps due to a power outage at the home—this instability will be seen by the core routing protocol. Refer to Figure 7-16.

Figure 7-16 No Summarization of RRI Routes



The number of head-end routers—and their placement in relation to the Internet connection point as well as the core of the corporate intranet—must be balanced with the geographic location of the end-users. Another consideration is *administrative distance* in terms of the number of hops and length of time (in regards to the delay or latency budget for voice calls) the packets spend on the Internet. Since the ISP consumes a large portion of the delay budget, minimizing the Internet exposure helps decrease delay and jitter of the voice calls.

Service Provider

This section explains the techniques used to simulate a service provider's network in the Cisco Enterprise Solutions Engineering lab testing. It also verifies the impact of cable plant congestion on voice drops, latency and jitter. Three specific considerations are addressed in this section:

- Cisco Powered Network References, page 7-34
- Testing Methods for Simulating an Internet Service Provider, page 7-34
- Testing Methods for Simulating a Congested Cable Plant, page 7-35

Cisco Powered Network References

For a more detailed explanation of the Cisco Powered Network Service Providers, please refer to the *Voice and Video Enabled IPSec VPN (V^3PN) SRND Guide*.

To search for available VPN/IP Multi-service providers, please use this link:

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

There are few if any service providers offering QoS on broadband links or SLAs for voice today. The primary focus of this publication is to address what enterprises can do today over existing broadband networks. In the future, as service providers begin offering DOCSIS 1.1 enabled services, the goal is to encourage them to become part of the Cisco Powered Network program so enterprise network planners have visibility to their service offerings.

Testing Methods for Simulating an Internet Service Provider

To simulate ISP latency and jitter of the voice stream, an Empirix Packet Sphere Model 200 is attached to the head-end Cisco 65xx switch via Gigabit Ethernet interfaces. Including the Packet Sphere was a means to validate voice quality with those values in the lab network, because the Cisco Powered Network SLA specifies a service provider-specific latency value of less than 60 msec, jitter of less than 20 msec, and drop rate of less than five percent.

The goal is to produce performance metrics of the platforms under test with little or no service provider latency, jitter and drops and then run the same tests with the Cisco Powered Network's SLA values included in the test to validate voice quality at the upper bounds of the SLA.

Testing with the Packet Sphere demonstrated two performance characteristics that were not anticipated:

- First, including a packet loss value in the Packet Sphere configuration actually reduced the reported jitter values as reported by Chariot. The explanation of this appears to be related to the fact that lost packets are excluded from the jitter calculation. For this reason, no packet loss was configured in the Packet Sphere. As we believe high jitter values degrade voice quality more than packet loss (in the case where packet loss is spread evenly across a 10-minute test call), the goal was to attempt to induce a high jitter value.

- Second, the Packet Sphere has no specific knob to create jitter. Inducing random amounts of delay creates jitter. However there was no way to create a jitter value approaching the upper limit of the Cisco Powered Network SLA (jitter equal to 20 msec), without configuring unrealistically high delay values. The Chariot tool's default value for the jitter buffer is 40 msec. This can be manually changed, but it is not dynamically elastic. The jitter buffer of an IP Phone is elastic and adapts to jitter by increasing or decreasing its size based on the jitter seen in the voice stream. In future testing, Chariot's jitter buffer will be increased and a Cisco internal delay tool will be also used to introduce delay and jitter.

For this test phase, the latency option was configured using a random distribution to cause Packet Sphere to delay or add jitter to packets as they traversed the system. The option specified was the reverse sawtooth distribution with 1.6-second repetition cycles. The range was 0-to-60 msec. With this option, added associated jitter was in the 2-to-3 msec range.

Performance charts that include the Packet Sphere are shown in the "Voice Quality Comparison" section on page 7-4.

Testing Methods for Simulating a Congested Cable Plant

With DSL using ATM as the underlying link-layer, an individual subscriber has a dedicated link from the DSL (bridge) modem to the DSLAM/IP DSL router. Any congestion in the network is upstream of that ATM PVC. With cable, the media is shared across subscribers on a particular Cisco uBR 7111 cable I/0 interface. To a degree, network use by a subscriber's neighbors might have some bearing in the congestion of the cable plant and overall voice quality.

To understand this issue, an internal script was installed in the test bed and was run to generated background traffic. The goal was to generate sufficient traffic via the script to bring the utilization of the cable1/0 interface on the Cisco uBR 7111 to approximately 50 percent utilization. In addition to that sustained load, the Cisco Enterprise Solutions Engineering teleworker voice and data traffic profile is applied while drops, latency and jitter are reported. Table 7-5 summarizes the results of these tests.

Table 7-5 Cable Script Test Results

		CMTS C1/0		Chariot		
		TX Load (Percent)	RX Load (Percent	Drops (Percent)	Jitter (msec)	Latency (msec)
1	Branch to Head		1.5	less than 0.04	7	23
	Head to Branch	5		less than 0.04	2.1	6.5
2	Branch to Head		3	less than 0.04	7.1	24
	Head to Branch	10		less than 0.04	2	6.4
3	Branch to Head		4	less than 0.04	7.7	25
	Head to Branch	15		less than 0.04	2.3	6.3
4	Branch to Head		6	less than 0.04	8.1	28
	Head to Branch	20		less than 0.04	2.2	6.3
	Branch to Head		16	less than 0.04	11.1	57
	Head to Branch	49		less than 0.04	2.4	6.4

In the test, the TX and RX load of the cable input/output interface was reported with the script running without the Chariot data traffic, so that the actual percentage of load is a few percent higher including the test stream. The 1-to-4 and 4+ rows in the table represent the number of cable modems running during the test. Each cable modem has four traffic flows running, so it represents four neighboring households with four power users each. The row identified by 4+ was four cable modems generating all large packets; the other rows are using a mix of packet sizes.

The Chariot drops are all represented by less the 0.04 percent. The worst drop rate of all the tests in either direction was 0.04 percent, which is insignificant. The results are posted in both the upstream and downstream direction (branch to head is upstream, head to branch is downstream) as these are asymmetrical speeds and the latency and jitter vary accordingly. The data rate for the device under test (Cisco 831) was 256 Kbps/1024 Kbps.

In all tests with a script traffic mix that included various packet sizes, the latency and jitter values were well within the “good” 8-to-10 msec range for jitter and less than 50 msec of latency. It was only when all large packets sizes were introduced into the mix that the Chariot reported values exceeding the criteria. Without changing the traffic profile to include all large packets, it was difficult to bring the interface load up to the 50 percent target. The traffic profile includes TCP applications that were decreasing their repetitive arrival rates due to the congestion of the cable plant.

While this test does not mimic the real world implementation in terms of the actual number of households on the shared media, it does provide some insight that utilization of the cable interface might not be as much of an issue for degrading voice quality as is often suggested.

Design Checklist

Table 7-6 presents a design checklist to facilitate the pre-implementation planning and the decision process.

Table 7-6 V³PN Design Checklist

Design Step	Publication/ Section References
Identify physical locations for the sites which will be supported by this design.	Customer specific
Determine IP addressing requirements of branch routers and manual or auto summary scheme.	Customer specific
Based on the number of remote sites and bandwidth requirements, determine head-end router requirements.	*Voice and Video Enabled IPSec VPN (V³PN) Design Guide*
Decide on location of head-end routers. Will they be in the same rack or across a continent? Goal for head-end placement is to minimize service provider delay.	Head-end Redundancy for Remote Peers, page 7-32
Plan for certificate authority servers.	X.509 Certificates, page 7-29
Plan for NTP server deployment.	NTP Servers, page 10-11
Identify any core network RFC 1918 issues.	RFC 1918 Addresses, page 10-12
Review broadband link speed requirements.	Recommended Broadband Link Speeds, page 7-3
Determine what classes of traffic will be required in remote router's policy-map.	Bandwidth Provisioning for WAN Edge QoS, page 7-8
Determine split tunneling requirements.	Split Tunneling—Prioritizing Enterprise Traffic over Spouse-and-Children Traffic, page 7-23
Review the issues of personal firewalls.	Personal Firewalls, page 6-4
Create policy on how special requests will be handled.	Special Requests, page 10-12
Create a procedure for replacing failed or damaged remote routers.	Hardware Failures, page 10-12
Determine the level of access the employee will have to the remote router.	Enable Secret Passwords, page 10-11
Select appropriate branch site product.	Product Selection, page 9-6
Determine requirements to limit the amount of priority traffic.	Limiting High Priority Traffic, page 7-21
Consider service provider selection process, consult CCO for Cisco Powered Network designated providers.	Cisco Powered Network References, page 7-34
Select and minimize the number of deployment models	Teleworker Deployment Model, page 7-1
Conduct trial deployments with selected service providers	Determining Available Uplink Bandwidth, page 7-18
Review existing emergency services plans.	*Voice and Video Enabled IPSec VPN (V³PN) SRND Guide*
Review supporting design guides.	*Voice and Video Enabled IPSec VPN (V³PN) SNRD Guide*

V3PN for Business Ready Teleworker Implementation and Configuration

This chapter is intended to provide step-by-step examples of the SOHO router tested in the Cisco Enterprise Solutions Engineering lab or deployed in the Cisco internal trials. Specific topics covered in this chapter include:

The recommended approach to using this chapter is to read through each section. For topics or concepts that are unclear, consult the associated design guides or documentation on www.cisco.com for more details. Then approach the first configuration with the checklist and refer back to specific sections for examples.

Switching Path

The packet switching path used during testing and Cisco internal trials is discussed in this section. Configuration topics include:

IP Cisco Express Forwarding

In both Cisco Enterprise Solutions Engineering lab testing and Cisco internal trials, Cisco Express Forwarding (CEF) is enabled on the SOHO router. To enable CEF switching, verify or configure:

```
!
ip cef
!
```

Among other advantages, CEF does not require a fast-switching cache entry to be first built by a packet that is process-switched to the destination. The fast switching cache can only build entries with one prefix length for any particular destination within the routing table. CEF does not have this limitation.

NetFlow

NetFlow switching was used extensively on routers in Cisco internal trials—specifically on Cisco 72xx, Cisco 37xx, Cisco 26xx, Cisco 17xx and Cisco 83x series routers to aid in troubleshooting and data collection. To enable NetFlow switching, configure the **ip route-cache flow** command on each interface intended to collect flow statistics for packets received on that interface. For example, the configuration might be as follows for an Ethernet-to-FastEthernet router:

```
interface Ethernet0/0
 description Outside
 ip address dhcp
 ip route-cache flow
!
interface FastEthernet0/0
 description Inside
 ip address 10.1.2.1 255.255.255.248
 ip route-cache flow
```

For routers with a DSL WIC, enable **ip route-cache flow** on the physical interface

```
interface ATM1/0
 no ip address
 ip route-cache flow
```

Please consult the appropriate documentation for additional information on NetFlow. One example of how NetFlow was used in the Cisco internal trial was to identify IP Phones deployed. The head-end routers were set to export the raw flow records to a PC capturing the flows and writing out the parsed data to a flat file. A Perl script then parsed the raw data file and searched for TCP connections on ports 2000 to 2002 (well-known ports for SCCP). With the source IP address of the IP Phone known, the web server of the phone can be queried either from the Perl program or a web browser to determine the phone's specific information, such as directory number, MAC address, serial number, and Message Waiting indicator status. An additional application of NetFlow in this environment includes determining the number of concurrent active phone calls of all teleworkers for each head-end router (for capacity planning). Cisco internal trials recorded one active call for every 10 deployed routers—a ratio of 10:1.

QoS Configuration

The QoS configuration for the SOHO WAN edge router is outlined in this section. Configuration topics covered include:

Configure QoS Class Map

The purpose of the class map is to define the association between packets and their respective classes. While each enterprise is different in the type and nature of implemented applications, the following map was used during Cisco Enterprise Solutions Engineering lab testing. In the Cisco internal trial, the transactional-data class was not included, because there are no applications within Cisco that are marked as such. Transactional data is included in the Cisco Enterprise Solutions Engineering lab tests, because the Chariot test tool provides response time statistics on these applications. These statistics are used to validate test results. Class-mapping example:

```
!
class-map match-all VOICE
  match ip dscp ef
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
```

The access-control list to identify IKE traffic is included in these sections as it is referenced in the internetwork-control class. Defining the access list at the time of creating the class-map avoids it being overlooked later.

QoS Policy Map Configuration

The *policy map* defines the bandwidth allocations for the various classes of voice and data. Call setup of two percent and internetwork control of five percent have been demonstrated to be sufficient in both lab testing and internal trial testing. They can be adjusted upward if required to eliminate drops in these classes.

```
policy-map llq-branch
  class CALL-SETUP
   bandwidth percent 2
  class TRANSACTIONAL-DATA
   bandwidth percent 22
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
    priority 128
  class class-default
   fair-queue
   random-detect
```

The voice class priority or LLQ is shown at 128 Kbps. This value is recommended for production implementations to avoid voice drops in the event the codec for the user is inadvertently configured for G.711 rather than G.729. Additionally, if Cisco SAA or Cisco IPM is used to generate simulated voice packets for performance monitoring, bandwidth must be allocated in the priority or LLQ class to accommodate the codec in use—as well as the additional traffic generated by Cisco SAA.

The transactional-data class allocation of 22 percent is an arbitrary number and can be adjusted or the class eliminated as required.

The default class (**class-default**) has WRED enabled. This class was used in both lab testing and internal trials. Random drops were observed in both environments demonstrating the feature is working at intended. Enabling WRED is also beneficial for troubleshooting as is illustrated in the "Verifying Packet Classification" section on page 10-16.

Configure the Shaper

For Ethernet-to-Ethernet/FastEthernet routers, such as the Cisco 831 behind a cable modem or DSL bridge—a *shaper* is configured to provide congestion feedback. This is required since the output 10-Mbps interface will not be congested. The shaper policy map references the service policy previously configured. This HCBWFQ reflects the parent policy-map shapes and the child policy-map queues within the shaped rate.

```
policy-map shaper
  class class-default
   shape average mean-rate burst-size
   service-policy llq-branch
!
```

For the *mean-rate* and *burst-size*, substitute the values shown in Table 8-1 based on the upstream link rate.

Table 8-1 Shaper Parameters

Upstream Link Rate (Kbps)	Cable		DSL	
	Mean Rate	Burst Size	Mean Rate	Burst Size
128	122,000	1,220	91,200	1,000
160	152,000	1,520	114,000	1,140
256	243,200	2,432	182,400	1,824
384	384,800	3,648	273,600	2,736

To clarify the rates shown Table 8-1, note that 160 Kbps is the minimum value that can be expected to provide suitable voice quality and 256 Kbps or above is strongly recommended. The minimum burst-size that can be configured is 1000, which is the reason the 128 Kbps DSL value uses 1000 rather than one percent of the mean-rate value (or 912 bytes). Also, the policy-map shown in the"QoS Policy Map Configuration" section on page 8-3 cannot be associated with an upstream rate of 128 Kbps unless the voice priority queue is set to 64 and the transactional-data class is reduced to at least eight percent —or eliminated entirely.

The mean-rate values are calculated as

- Cable upstream link rate = upstream link rate * 0.95
- DSL upstream link rate = (DSL trained rate * 0.75) * 0.95

The DSL rates are lower to account for the larger amount of overhead associated with DSL verses cable. In the Cisco internal trial, values as low (conservative) as 160,000 for the mean-rate were used assuming a minimum upstream rate deployed of 256 Kbps on either DSL or cable with good results.

Attach the Service Policy to the Interface

To associate the service policy with the interface, use the following configuration:

```
interface Ethernet1
 description Outside
…
 service-policy output shaper
!
```

In the case of an Cisco 837 with a DSL interface, the service policy and interface configuration would be as follows:

```
interface ATM0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl power-cutback 0
!
interface ATM0.35 point-to-point
 description Outside
 bandwidth 256
 pvc dsl 0/35
  vbr-nrt 256 256
  tx-ring-limit 3
  pppoe max-sessions 5
  service-policy output llq-branch
  pppoe-client dial-pool-number 1
 !
```

Note In this configuration the **vbr-nrt** burst and sustained rates are set to the trained rate and the **tx-ring-limit** is set to 3. Generally, the lowest configurable **tx-ring-limit** value results in lowest jitter values. Most DSL providers use the VCI/VPI values of 0/35 or 8/35. As an example, a carrier might use 8/35 for DSL customers that use the carrier's ISP services and 0/35 if the circuit is provisioned by the carrier but the customer uses another ISP.

Configure TCP Adjust-MSS

To reduce the size of TCP packets (to minimize the impact of having no Layer-2 fragmentation technique on DOCSIS 1.0 cable and PPPoE with DSL), configure the following features:

```
!
interface Ethernet0
 description Inside
 …
 ip tcp adjust-mss 542

interface Ethernet1
 description Outside
 ipaddress dhcp
 ip tcp adjust-mss 542
!
```

When PPPoE is terminated on the router use this configuration:

```
!
```

```
interface Dialer1
 description Outside
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 ip tcp adjust-mss 542
!
```

Adjust the MSS value on the dialer interface rather than on the outside Ethernet or ATM interface. Include the command on the inside Ethernet interface as shown above. Also set the MTU value on the dialer interface to 1492 to account for the PPPoE header.

PPPoE Configuration

An example PPPoE configuration used in lab testing and internal trials follows:

```
!
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
!
```

Note Using **vpdn** commands are not required for PPPoE configurations in later releases of Cisco IOS. For example, Cisco IOS 12.2(13)ZH does not require the above commands.

The outside interface will either be an Ethernet (Ethernet 1 for an Cisco 831), as follows:

```
!
interface Ethernet1
 description Outside Interface
 bandwidth 256
 no ip address
 load-interval 30
 pppoe enable
 service-policy output shaper
 pppoe-client dial-pool-number 1
!
```

As an example, if using a Cisco 1751 with a DSL WIC, a Cisco 837 would be similarly configured except for the port and slot designations on the interface:

```
!
interface ATM1/0
 no ip address
 ip route-cache flow
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
 hold-queue 224 in
!
interface ATM1/0.35 point-to-point
 description Outside Interface
 pvc dsl 0/35
  vbr-nrt 256 256
  tx-ring-limit 3
  service-policy output llq-branch
  pppoe-client dial-pool-number 1
 !
```

```
 crypto map test
!
```

Regardless of the outside physical interface, a dialer interface must be configured. For example:

```
!
interface Dialer1
 description Outside
 bandwidth 256
 ip address negotiated
 ip access-group 102 in
 ip mtu 1492
 encapsulation ppp
 ip tcp adjust-mss 542
 load-interval 30
 dialer pool 1
 dialer-group 1
 no cdp enable
!               BellSouth FastAccess uses chap
 ppp authentication chap callin
 ppp chap hostname hostname@domain_name.com
 ppp chap password 7 xxxxxxxx
!               Mindspring/Earthlink uses pap
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username user@other_domain.com password xxxxxx

 ppp ipcp dns request
 ppp ipcp wins request
 crypto map test
!
!
ip route 0.0.0.0 0.0.0.0 Dialer1
!
dialer-list 1 protocol ip permit
!
end
```

The service provider will use either PAP or CHAP, an example of each is shown in the configuration above. A default route to the dialer interface is required.

For more detailed information on PPPoE, please refer to the appropriate documentation on http://www.cisco.com/.

Hold Queue

In the version of code tested on the Cisco 83x routers, the default value for the output hold queue (100) on the Ethernet 0 interface differs from other Cisco IOS routers. To be consistent with other platforms, a value of 40 was specified on all tested configurations.

```
interface Ethernet0
 description Inside interface
 hold-queue 40 out
!
```

IKE and IPSec Configuration

The IKE and IPSec configuration is similar to that used in the *Voice and Video Enabled IPSec VPN (V^{3}PN) SRND Guide*. Please refer to that guide for baseline information. Configuration topics covered in this section:

Configure X.509 Digital Certificate

To properly configure the certificate, the router must have the correct time, hostname and domain name configured and attached to the network, and the router must be able to reach the certificate server. An example configuration follows:

```
!
hostname host
!
ip domain name domain_name.com
!
clock timezone est -5
clock summer-time edt recurring
!
interface Ethernet0
 ip address dhcp
 no shutdown
!
ntp server 10.81.254.202
!
end
```

Prior to starting the certificate configuration, verify that the time is correct and that the router is on the network as follows:

```
host#show clock
13:34:46.919 edt Tue May 27 2003

host#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0                  172.26.156.24   YES DHCP   up                    up

host#show ip route | begin 0.0.0.0/0
S*   0.0.0.0/0 [254/0] via 172.26.156.1
```

Generate the key for the router; SSH will be enabled by default once the key is generated. An example follows of using the **crypto key generate rsa** command to do this:

```
host(config)#crypto key generate rsa
The name for the keys will be: host.domain_name.com
Choose the size of the key modulus in the range of 360 to 2048 for your
```

```
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]

host(config)#
May 27 13:41:28.591 edt: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

The trustpoint must be configured. An example follows. The actual configuration depends on the deployment and certificate server in use. The following was used with a Microsoft CA Server:

```
crypto ca trustpoint ese-vpn-cert
 enrollment mode ra
 enrollment url http://10.81.0.18:80/certsrv/mscep/mscep.dll
 crl optional
 auto-enroll 70
!
```

Enter the enrollment command:

```
host(config)#cry ca authenticate ese-vpn-cert
Certificate has the following attributes:
Fingerprint: 56E41DD0 C495CF01 B08BCC7C 61C6E348
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
host(config)#
```

Start the certificate enrollment process.

```
host(config)#cry ca enroll ese-vpn-cert
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be: host.domain_name.com
% The subject name in the certificate will be: host.domain_name.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

host(config)#    Fingerprint:  472852A5 1322C58A 12209C27 457E2A14

May 27 16:59:19.987 edt: %CRYPTO-6-CERTRET: Certificate received from Certificate
Authority
host(config)#
```

Configure the **source interface** command for the trustpoint. If the certificate server is only reachable via the IPSec tunnel, future enrollment requests must be sourced from the inside interface IP address so the request is encrypted in the tunnel itself. Previously, auto-enrollment was configured, but not the source interface because the IPSec configuration was not completed yet. In the following example, the inside interface is Ethernet 0:

```
crypto ca trustpoint ese-vpn-cert
```

```
 source interface ethernet 0
end
```

At this point, save the configuration to NVRAM using the **copy run start** command before completing the following configuration steps.

Configure IKE (ISAKMP) Policy

Configure the IKE policy and keepalive value:

```
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
```

Configure IPSec Transform-Set

The IPSec transform-set used includes 3DES as the encryption algorithm and SHA-1 for authentication and message integrity. An example follows:

```
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
```

Configure the Crypto Map

An example crypto map and associated access-control list configuration follows:

```
!
crypto map test 10 ipsec-isakmp
 description This calls the dynamic map on the crypto agg box(es)
 set peer 192.168.252.1
 set peer 192.168.252.2
 set transform-set vpn-test
 match address 103
!
access-list 103 remark --------Crypto Map ACL----------------
access-list 103 permit ip 10.112.22.0 0.0.0.255 10.0.0.0 0.255.255.255
!
```

Two **set peer** statements are included to provide fail-over and recovery in the event a head-end router fails.

Note The command **qos pre-classify** is not available in the Cisco IOS release tested in the Cisco Enterprise Solutions Engineering lab. If this feature is available in the release being used, include the command under the **crypto map**.

Apply Crypto Map to Interface

Apply the crypto map to the outside interface. Apply it to the Ethernet 1 interface for a Cisco 831 using DHCP or to the dialer interface for a Cisco 837/Cisco 1700 series using PPPoE. An example configuration follows:

```
! 831
interface Ethernet1
 description Outside

crypto map test


! 837 or 17xx
interface Dialer1
 description Outside

crypto map test
```

Configure an Inbound Access List

Split tunneling was not evaluated during this phase of Cisco Enterprise Solutions Engineering lab testing or in the Cisco internal trial. As such, NAT and CBAC are not included in the configuration. However, for performance test reasons, an inbound access-control list was included on the outside interfaces for all testing (to simulate a minimal configuration that an enterprise might implement). The following configuration was used:

```
!
access-list 102 remark --------Inbound interface ACL----------------
access-list 102 permit esp host 192.168.252.1 any
access-list 102 permit esp host 192.168.252.2 any
access-list 102 permit ip 10.0.0.0 0.255.255.255 10.112.22.0 0.0.0.255
access-list 102 permit udp any eq isakmp any eq isakmp
access-list 102 permit ip host 192.168.252.6 any
access-list 102 permit ip host 192.168.200.1 any
access-list 102 permit ip host 10.113.1.1 any
access-list 102 permit icmp any 192.168.200.0 0.0.0.255
access-list 102 deny   ip any any log

interface Ethernet1
 …
 ip access-group 102 in
```

In the next phase of Cisco Enterprise Solutions Engineering lab testing, split tunneling will be evaluated and performance results for NAT and CBAC will be included in future revisions of this guide.

Configure Context-Based Access Control

In an IPSec-only configuration, an input access-control list on an interface with a crypto map is evaluated twice, prior to decryption and then the un-encrypted packet is checked against the access-control list again. In the access-control list shown in the example of the previous section, the CBAC firewall feature was not configured in the Cisco Enterprise Solutions Engineering test lab because the inbound access-control list permits IP packets originated from the 10.0.0.0 network. This network includes all the Chariot workstations that are sources and sinks of data in the testing.

In a live deployment, the enterprise might also require allowing Internet access through the IPSec tunnel. The remote routers must also be configured to permit specified TCP and UDP traffic through the inbound access-control list when the connection is initiated from within the remote router's subnet. To accomplish this, a configuration such as the following should be deployed:

```
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
!
interface FastEthernet0/0
 description Inside
 ip inspect CBAC in
```

For more information on how to configure traffic inspection to create temporary openings in the firewall's access-control lists (to allow return traffic and additional data connections for permissible sessions), please refer to the appropriate documentation on http://www.cisco.com/.

Implementation and Configuration Checklist

Table 8-2 presents a checklist to help organize the implementation process. It is targeted to the remote router. Head-end router configuration is addressed in the planning section of this guide as well as in the *Voice and Video Enabled IPSec VPN (V^{3}PN) SRND Guide*. It is assumed the head-end routers are configured and awaiting connection from the remote routers.

Table 8-2 Implementation and Configuration Checklist

Implementation/Configuration Step	Section References
Load appropriate Cisco IOS on router.	Software Releases Evaluated, page 9-9
Configure NTP on the router to provide for accurate time.	NTP Servers, page 10-11
Configure hostname and domain name of remote router, prerequisite for digital certificate.	Enterprise specific
Generate RSA keys, and configure, authenticate and enroll digital certificate.	Configure X.509 Digital Certificate, page 8-8
Configure switching path.	Switching Path, page 8-1
Configure QoS class map based on enterprise network requirements.	Configure QoS Class Map, page 8-3
Configure appropriate QoS policy map based in enterprise traffic requirements and need for split-tunneling.	QoS Policy Map Configuration, page 8-3
Configure shaper (if required) according to the uplink bandwidth.	Configure the Shaper, page 8-4
Implement the QoS policy.	Attach the Service Policy to the Interface, page 8-5
Configure TCP adjust-mss.	Configure TCP Adjust-MSS, page 8-5
Configure PPPoE (if required).	PPPoE Configuration, page 8-6
Verify (and optionally override) output hold queue value.	Hold Queue, page 8-7
Configure IKE.	Configure IKE (ISAKMP) Policy, page 8-10
Configure appropriate IPSec transform set per head-end configuration.	Configure IPSec Transform-Set, page 8-10
Configure the IPSec crypto map and access-control list.	Configure the Crypto Map, page 8-10
Apply crypto map to output interface.	Apply Crypto Map to Interface, page 8-11
Protect the router's outside interface.	Configure an Inbound Access List, page 8-11
Configure traffic inspection (firewall features).	Configure Context-Based Access Control, page 8-11
Configure DHCP server (if required).	Enterprise specific
Encrypt packets generated by the router.	Source Interface, page 10-19
Configure SAA for troubleshooting and debugging assistance.	Service Assurance Agent, page 10-1

V3PN for Business Ready Teleworker Product and Performance Data

This chapter addresses Cisco internal V3PN scalability and performance evaluation. It provides product performance results, recommendations and conclusions that can be used for design parameters when planning and implementing a V3PN deployment over broadband. Topics covered include:

Scalability Test Methodology

The Cisco Enterprise Solutions Engineering VPN performance and scalability lab uses test tools to generate data traffic simulating actual end-to-end applications running on Solaris and Red Hat Linux TCP/IP stacks. The traffic generated incorporates flow control inherent to a TCP implementation. The tools create a network environment that is fairly realistic in terms of predicting how a comparable real-world network will perform.

NetIQ's Chariot test tool is used to generate network traffic. As NetIQ endpoints, SUN NETRA and Penguin Red Hat Linux servers are deployed. The Linux servers generate the simulated voice traffic; the SUN NETRA servers generate the data traffic.

More information on NetIQ Chariot can be found on the following NetIQ website:

http://www.netiq.com/products/chr/default.asp

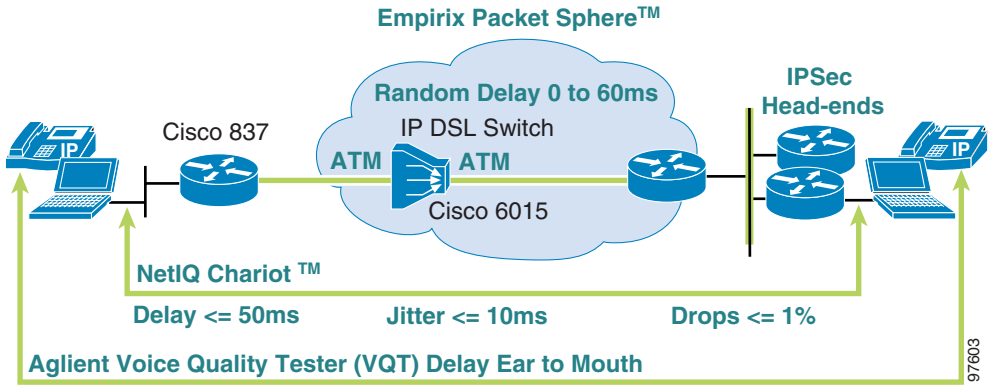
In addition to the Chariot test tool, Cisco SAA was also configured for some tests. The changes in the traffic profile to accommodate this additional simulated voice traffic were simply to provision for a second G.729 call during those tests.

Cisco 7960 IP Phones and analog phones were used during the wave file captures.

Test Tool Topology

The Cisco Enterprise Solutions Engineering lab utilized three non-Cisco devices to simulate, generate, or capture data as part of the testing effort. They are the Empirix Packet Sphere Model 200, NetIQ Chariot and the Agilent Telegra VQT. How these three tools fit in the lab topology is shown in Figure 9-1.

Figure 9-1 Test Tool Topology Diagram



The Empirix Packet Sphere simulates the delay and jitter introduced by a service provider and can be enabled or disabled depending on the testing requirements.

The NetIQ Chariot endpoints are used in all testing, providing simulated voice and data traffic and the resulting performance statistics for voice delay, jitter and loss—as well as response time statistics for some classes of data. Chariot does not include the delay associated with coder or adaptive jitter buffers; it measures LAN-to-LAN as shown in Figure 9-1.

The Agilent Telegra VQT is used to generate audio through the handset connection of an analog or IP Phone and to report ear-to-mouth delay, which includes coder and jitter buffer. It is also used to produce the wave files referenced in this document.

Cisco SAA was configured as a point of reference; it is built-in component of Cisco IOS (not a separate product). It measures delay and jitter LAN-to-LAN.

Traffic Profiles

The traffic profile used for the teleworker testing is similar to the profile used in the *Voice and Video Enabled IPSec VPN (V^{3}PN) SRND Guide*. There are several minor differences:

- Chariot scripts mark the ToS byte as DSCP rather than IP Precedence.
- One voice call is provisioned, regardless of WAN speed.
- A Call Control script was included.
- The DNS script data rate was reduced to simulate one user rather than what might be encountered from a branch with several users.

The details of the scripts are documented in Table 9-1. IP Precedence values are shown as a reference.

Table 9-1 Summary of Traffic Profile Scripts

Application	QoS	Frequency Factor	Transaction Profile (sizes are Pre-crypto/PPPoE/ATM Encapsulations.)
VoIP G.729	IP Precedence 5 or DSCP EF	Constant	50 pps; 20 byte payload
FTPput	IP Precedence 0 or DSCP 0	Constant	FTP file transfer request of 240,000 byte file
HTTP	IP Precedence 0 or DSCP 0	Random Sleep 10-to-30 seconds	300 byte request followed by 1,000 byte response
HTTP-Transactional HTTP	IP Precedence 2 or DCSP AF21	Random Sleep 10-to-30 seconds	Same as above.
POP3	IP Precedence 0 or DSCP 0	Random Sleep 30-to-60 seconds	20 byte request; 20 byte response and final 2000 byte reply
Call Control (Script named: vpn-CC-D2DT-1calls; reflects the time from off hook to dial tone)	IP Precedence 3 or DCSP AF31	Random Sleep 29-to-30 seconds	Total bytes requested: 1860+4+16 = 1880 bytes Total bytes reply: 120+4+16+16+20+48+20+8+12 = 264 bytes
TN3270	IP Precedence 0 or DSCP 0	Random Sleep 30-to-60 seconds	100 byte request; 1000 byte response
TN3270-Transactional TN3270	IP Precedence 2 or DCSP AF21	Random Sleep 30-to-60 seconds	Same as above.
DNS	IP Precedence 0 or DSCP 0	1 call per second Rate limit to 0.5 Kbps	100 byte request; 100 byte response

To illustrate the traffic mix, a NetFlow export of a 10-minute test was conducted and the flows were charted (test used a Cisco 831/Cisco 837 setup featuring a 256 Kbps/1.4 Mbps DSL configuration in an Integrated Unit + Access Device model). This was similar to the traffic mix used for the *Voice and Video Enabled IPSec VPN (V^3PN) SRND Guide*

This test used the traffic profile presented in Table 9-2, with the exception of Call Control. At the time of this test, the profile for that class of data was 1,000 bytes in each direction with 30-to-60 seconds between initiations. In this test the TCP MSS size was set by the router (**ip tcp adjust-mss 536**) at 536 bytes.

The NetFlow derived summary data for this test is provided in Table 9-2 and Table 9-3.

Table 9-2 Branch to Head-end Data

NetFlow-derived Parameter	Value
Total bytes	8,296,311
Total packets	72,122
Total flows	743
Average packets size	115 bytes

Table 9-3 Head-end to Branch Data

NetFlow-derived Parameter	Value
Total bytes	39,848,930
Total packets	106,005
Total flows	702
Average packet size	376 bytes

Figure 9-2 presents a NetFlow graph of the traffic profile described in this section.

Figure 9-2 NetFlow Graph of Traffic Profile

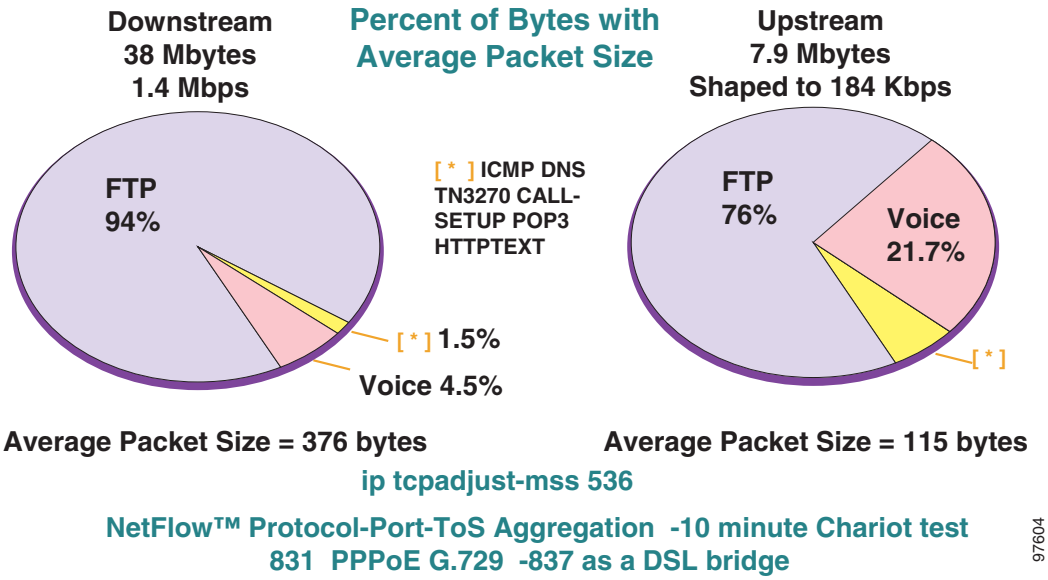


Table 9-4 presents the data graphed in Figure 9-2 broken down by number of packets and the traffic profile/protocol/application/DSCP value.

Table 9-4 Number of Packets by Protocol/Application/DSCP

Protocol/Application/DSCP	Downstream (in Packets)	Upstream (in Packets)
UDP (Voice-EF)	30,003	30,006
TCP (Call-Setup-AF31)	52	74
UDP (DNS-0)	687	525
TCP (TN3270-0)	686	636
TCP (HTTP text-0)	255	211
TCP (POP3-0)	323	225
TCP (FTP Put-0)	73,571	40,103
TCP (HTTP/TN3270-AF21)	427	340

This traffic profile can be considered a worst-case situation for the teleworker. From an end-user standpoint, this teleworker is simultaneously on a G.729 call, sending and receiving large files (the FTP mimics sending and receiving E-mail attachments and GIF and JPEG images from a web browser), using a TN3270 application (with both transactional and best effort transactions), running a web browser, and using an E-mail client. This is a very busy user.

Rarely is a teleworker in the normal course of the day doing all these jobs at one time; however, in most cases, voice quality over broadband services sounds much better during periods of little or no data traffic, but degrades rapidly during periods of congestion. The intent of this testing was to provide performance results based on the worst case.

Note From the charts and table, the asymmetric nature of the DSL connection is obvious; during the test the downstream direction transmitted substantially more data in the downstream direction. Since the teleworker represents only one concurrent voice call, the percentage of voice to data and average packet size is influenced by these differing rates. The packet sizes reported in this chapter are as displayed by NetFlow and are Layer-3 sizes without any IPSec headers or trailers.

Product Selection

Topics presented in this section include:

Performance Results by Link Speed

Performance tests were run on both cable and DSL connections. The results are shown in the Table 9-5.

Table 9-5 Performance Results by Link Speed

Product	VPN HW Accelerator	Number of G.729 Calls	Line Rate (Kbps) Down/Up	Service	Bi-directional Data (Kbps)	Latency (msec)		Jitter (msec)		Total CPU (percent)
						Branch to Head	Head to Branch	Branch to Head	Head to Branch	
Cisco 831	HIFN79XX	1	1536/384	Cable	974	21	13	5.8	3.8	53
Cisco 831	HIFN79XX	1	1024/256	Cable	974	22	6	6.5	2.2	45
Cisco 831	HIFN79XX	1	1536/384	ADSL	648	50	33	5.0	5.4	40
Cisco 837	HIFN79XX	1	1536/384	ADSL	764	**57**	35	8.6	6.0	53
Cisco 831	HIFN79XX	1	1408/256	ADSL	373	**62**	24	**10.1**	2.5	29
Cisco 831	HIFN79XX	1	864/160	ADSL	206	**82**	26	**10.2**	2.3	24

Items to note when interpreting this data:

- **Latency**—The average values for latency are directly related to link speed and type of service, cable or DSL. This is not a single box test of latency for the platform; it represents latency from Chariot end-point to Chariot end-point. It does not include any component of service provider simulated latency unless noted. In all testing, DSL services demonstrate higher latency values than a comparable cable service due to ATM cell tax and overhead associated with AAL5 padding and encapsulation.
- **Jitter**—The average values for jitter are Chariot calculated and based on the RFC 1889 guidelines. Table 9-5 reports jitter as an average value of the jitter observation from the uplink and downlink values. For asymmetrical services of both cable and DSL, with no QoS on downlink, the jitter values on the uplink are higher—sometimes by a factor of 3:1-to-4:1.
- **Data Traffic**—These tests were run with the traffic profile described previously. It must be understood that the values reported are the *worst-case scenario*. Rarely does a typical user generate the volume and continuous stream of data traffic as is represented by the Chariot scripts.

- **QoS**—In all cases, except with the Cisco 837, the uplink QoS was accomplished by HCBWFQ—prioritizing traffic within a shaped rate. For the Cisco 837, the QoS service policy was applied to the output ATM subinterface.

Performance results for Cisco 1700 series routers were not tested over broadband services; however, they were tested in a HDLC and Frame Relay configuration and are documented in the *Voice and Video Enabled IPSec VPN (V^{3}PN) SRND Guide*. The Cisco 1700 series router was widely deployed in internal Cisco trial deployments and can be expected to perform at or above what was documented for the Cisco 831 and Cisco 837. Experience in both a FastEthernet/Ethernet as well as FastEthernet/DSL WIC has been favorable.

There are two key observations regarding voice quality to emphasize from Table 9-5.

- More bandwidth is better
- Everything else being equal, cable is preferable to DSL

In all of the testing, voice loss due to dropped packets is rarely an issue, unless it is service provider induced loss. Typically when a service provider drops packets, it is all packets over several seconds as opposed to a few packets spread across several minutes. Dropped packets were not performance related in deployments tests; they are normally attributed to link or other hardware failures.

Delay can be managed to a greater extent. The two key components are broadband link speed and service provider delay. Minimizing the amount of time spent (in terms of *hops*) on the Internet provides the biggest gain in reducing delay, as does purchasing higher broadband data rates.

Jitter can be managed by using the QoS techniques detailed in this document, but from a performance standpoint, more bandwidth helps minimize jitter. Given an equal amount of bandwidth available to the user, cable exhibits less jitter than DSL.

Issues with Cisco PIX 501 and Cisco VPN 3002

Both the Cisco PIX 501 and Cisco VPN 3002 are desirable as SOHO devices. They are relatively low cost, easy to configure and manage, and successful products. They lack two features that are required for supporting VoIP on broadband service offerings: QoS and hardware encryption acceleration. Before examining the performance results for these platforms, review a baseline performance chart for Cisco 831 (Table 9-6) with both hardware encryption acceleration and HCBWFQ on a DSL circuit (256 Kbps/1.4 Mbps). There is no added service provider delay. Table 9-6 and Table 9-7 represent adjusting the TCP MSS size to 542 bytes.

Table 9-6 Cisco 831 Baseline Performance

	Call Leg	Chariot Voice Drops (percent)	Chariot RFC 1988 Jitter (msec)	Chariot One-Way Delay (msec
Cisco 831	Branch to Head	0	10.1	61
	Head to Branch	0.03	2.5	24
	Average	0.015	6.3	43

Lab testing criteria was held to less than one percent voice drops, average jitter below 10 msec and average one-way delay less than 50 msec. While the averages met these criteria, the branch to head call leg actually exceeded these parameters slightly.

Now compare this baseline with performance results for a Cisco PIX 501, Cisco VPN 3002 and an Cisco 831 that has hardware encryption acceleration disabled and no QoS configured on the uplink.

Table 9-7 Cisco PIX 501 and Cisco VPN 3002 Performance Comparisons

	Call Leg	Chariot Voice Drops (percent)	Chariot RFC 1988 Jitter (msec)	Chariot One-Way Delay (msec)
Cisco PIX 501	Branch to Head	2.0	13.9	304
	Head to Branch	0.0	4.1	28
Cisco VPN 3002	Branch to Head	2.3	19.7	328
	Head to Branch	0.043	2.8	32
Cisco 831 (No QoS and No Hardware Encryption)	Branch to Head	3.2	14.8	345
	Head to Branch	0.0	8.1	43

In the upstream call leg, all delay values are more than 300 msec. Recall that the lab test criteria goal is less than 50 msec. There is a detailed discussion on the voice delay budget in the *Voice and Video Enabled IPSec VPN (V^{3}PN) SRND Guide*. Recall the ITU recommendation of ear-to-mouth, one-way delay less than 150 msec. While 250 msec can be acceptable, the values reported in Table 9-7 do not include coder, jitter buffer and service provider/WAN component of the delay budget.

The jitter values are also unacceptable. In the upstream call leg, jitter values are 50 percent and approaching 100 percent higher than the 10 msec target. Voice drops as well are two to three times the target rate of one percent.

The Cisco 831 was included in this testing as a comparison. Essentially the *dumbed down* Cisco 831 was included to illustrate that an Cisco 831 without the required features of QoS and hardware encryption acceleration exhibits similar performance to other platforms—Cisco and other vendor's equipment—that do not include these features.

Caution Cisco PIX 501 and Cisco VPN 3002 *are not recommended* for V^{3}PN teleworker deployments in the Integrated Unit + Access Device model.

Software Releases Evaluated

The primary software evaluated in this phase of testing is the Cisco 831/Cisco 837 with 12.2(11)YV, releases of software for the other components are listed Table 9-8:

Table 9-8 Summary of Product and Software Mapping

Product	Software Version
Cisco 837	c837-k9o3sy6-mz.122-11.YV
Cisco 831	c831-k9o3sy6-mz.122-11.YV
IPSec Head-end (Cisco 7200)	c7200-ik9o3s-mz.122-13.2.S1
IPSec Head-end (for Cisco SAA/Cisco VPN 3002)	c7200-ik9o3s-mz.122-13.T1
PPPoE Termination (Cisco 7200)	c7200-ik9o3s-mz.122-13.T1
IP DSL Switch (Cisco 6015)	ni2-dsl-mz.121-7.DA2
Cable CMTS (Cisco uBR 7111)	ubr7100-ik1st-mz.121-7.EC
Cable Modem (Cisco uBR 925)	ubr925-k9o3sy5-mz.122-8.YJ
Cable Router/MODEM (Cisco uBR 925)	ubr925-k9o3sv9y5-mz.122-12.14.T1
Voice Gateway (Cisco 26xx with FXS)	c2600-ik9o3s-mz.122-11.T2
Cisco 65xx switch	c6sup12-jk2sv-mz.121-11b.E1

For the Cisco SAA and Cisco VPN 3002 testing, the Cisco 7200 IPSec head-ends were loaded with 12.2(13)T1 to gain access to features required for this testing which were not available in 12.2(1s3.2)S1.

Performance Results—Additional Features and Higher Bandwidth

Following initial Cisco Enterprise Solutions Engineering lab tests, additional tests were performed to assess the performance impact of other features enterprise customers might deploy.

The additional features tested included:

- Input access-control list configured on the inside Ethernet interface to support an auth-proxy configuration
- NAT/pNAT configured to support split tunneling
- CBAC configured to support split tunneling and/or Internet access through the IPSec tunnel
- Cisco IOS-IDS enabled on the remote (branch) router
- Additional traffic flows to simulate split-tunneling traffic
- Inclusion of QoS Pre-classify in Cisco IOS releases under test

Higher data rates, two voice streams and the Cisco 1751 have been incorporated into testing, in order to provide design and performance guidance as deployments move from the single teleworker deployment to the small office environment.

For the purposes of lab testing, it is not practical to enter a username/password in response to an auth-proxy (**ip auth-proxy** command) configuration. As the device under test is monitored, configured and controlled by automated scripts. Test traffic is generated by NetIQ Chariot software rather than an actual user. An input access-control list was configured to force a check for packets entering the inside interface similar to an auth-proxy configuration.

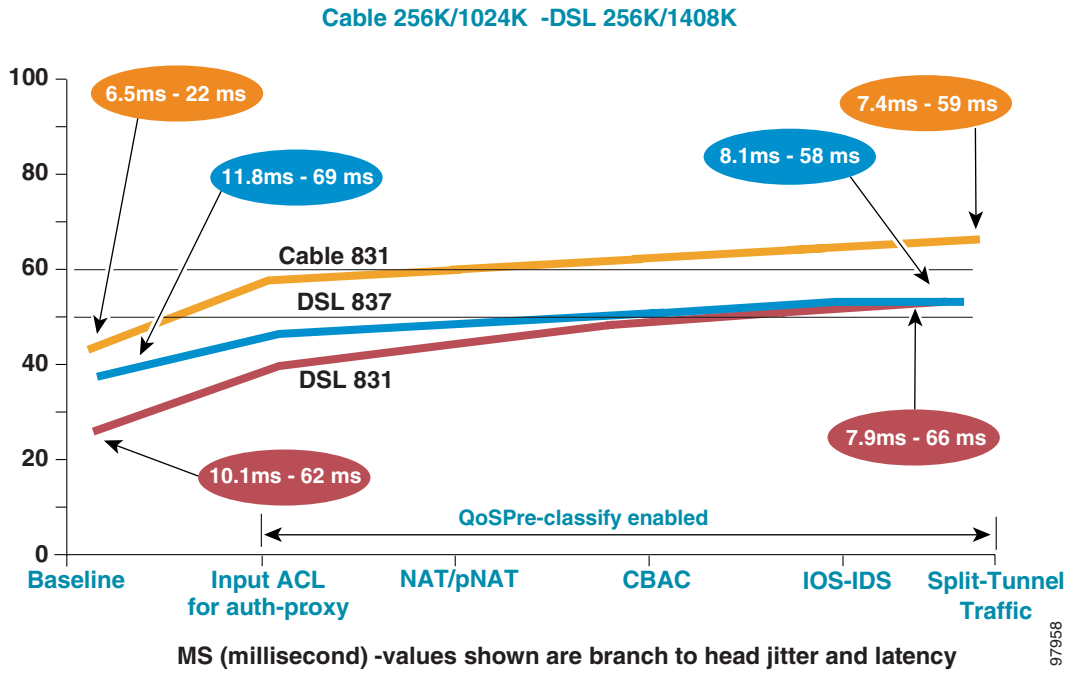
In addition, in an IPSec-only configuration with split tunneling, unencrypted packets from the Internet are checked only once by the outside interface input access-control list. Encrypted packets from the head-end IPSec peer are checked twice: once while encapsulated in the IPSec (ESP) tunnel; and, then a second time following decryption.

The Cisco IOS-IDS configuration was used to check all packets to the inside interface, to log events to the router's logging buffer, and to syslog to a head-end campus syslog server for analysis. The configuration did not drop or shun packets. The test traffic profile did not include any simulated attacks.

CPU Utilization by Feature

To gauge the impact of implementing additional features, a series of tests were run on both cable (256 Kbps/1024 Kbps) and DSL (256 Kbps/1408 Kbps) with the Cisco 831 and Cisco 837 routers. Figure 9-3 illustrates CPU utilization by feature.

Figure 9-3 CPU Utilization by Feature



The features annotated on the X-axis in Figure 9-3 are as follows.

- Baseline—Represents what is illustrated in Chapter 8, "V3PN for Business Ready Teleworker Implementation and Configuration." QoS Pre-classify was not available in the tested release—Cisco IOS 12.2(11)YV.

- Input Access-Control List for Auth-Proxy—Included an inbound access-control list on the inside Ethernet interface implementing auth-proxy. QoS Pre-classify is available in this test phase and all subsequent phases. Cisco IOS 12.2(13)ZH was used in tests. NAT transparency is available by default in the release, but was disabled for testing.
- NAT/pNAT—Allows for split tunneling; however, a split tunnel traffic profile is only enabled in the last test. All traffic continues through the IPSec tunnel.
- CBAC—Supports split tunneling or access to the Internet via the IPSec tunnel in configurations that have an inbound access-control list on the outside interface that only permits connections from the enterprise address space. All traffic continues through the IPSec tunnel.
- Cisco IOS-IDS—Enabled, but with signatures 1107, 2000 and 2001 disabled[1]. These signatures were triggered by false positives in the lab environment. All traffic continues through the IPSec tunnel.
- Split Tunnel Traffic—Last data point includes all features, but the traffic profile includes HTTP and RealMedia traffic simulating downloads from the Internet in addition to the traffic profile going through the IPSec tunnel.

The associated configuration samples for these features are shown in Appendix C, "Additional Performance Data Configuration Examples."

There can be several observations made regarding the results documented in this section. The largest single jump in CPU utilization was between the baseline and the Cisco IOS upgrade that included QoS Pre-classify and the input access list for auth-proxy. Additional tests were conducted to determine which feature had the greatest impact. First, the input access-control list for auth-proxy was enabled, then a re-test was conducted adding QoS Pre-classify. The input access-control list increased the CPU utilization by approximately 1-to-2 percent. QoS Pre-classify increased the CPU utilization by approximately 13 percent. However, the total data bit rate increased in one instance to over 100 percent of the rate without QoS Pre-classify. In addition, the voice delay from branch to head-end was about the same to slightly lower, while the branch-to-head end voice jitter decreased by more than two milliseconds in at least one case.

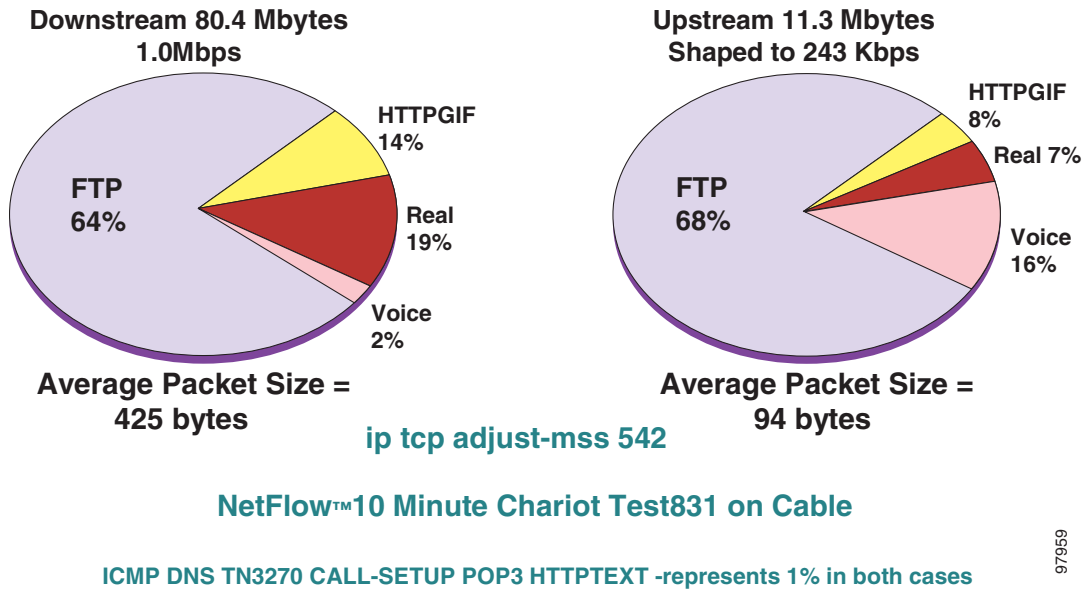
From this it was determined that QoS Pre-classify is a desirable feature because it increased data throughput substantially without sacrificing the characteristics of the voice stream.

Split Tunnel Traffic Profile

Additional Chariot streams were added to represent traffic being downloaded from the Internet that would not be encrypted. This was done to simulate data traffic in a split tunnel environment—in addition to the baseline traffic profile. These streams were a RealMedia stream (TCP) and a HTTP GET of GIF and text files. A second DNS stream was added in the IPsec tunnel to represent a spouse's PC DNS traffic. To illustrate the relationship of the test traffic, a 10-minute test was run over a 256 Kbps/1024 Kbps cable configuration using an Cisco 831. NetFlow was enabled on the remote router to export the flows to a Unix server. Figure 9-4 illustrates the resulting data captured.

1. 1107=RFC 1918 Addresses Seen; 2000=ICMP Echo Reply; 2001=ICMP Host Unreachable

Figure 9-4 Split Tunnel Traffic Profile



The percentage values shown in Figure 9-4 are stated as the percent of bytes as reported by NetFlow (Layer 3-sized packets excluding IPSec headers and trailers). The average packet size on the upstream (branch to head) direction is only 94 bytes. This is influenced by the G.729 voice packets (60 bytes) and also small packets for the HTTP and RealMedia TCP sessions. These packets are TCP acknowledgements for the downstream HTTP and RealMedia flows. The downstream average packet size is limited by the **ip tcp adjust-mss 542** command. Without that command the average packet size would be substantially higher since the voice and other application traffic make up only three percent of the downstream flows. FTP, HTTP and RealMedia make up 97 percent of the downstream flows. Note that this traffic profile was run on an Cisco 831 router behind a cable modem simulating a 256 Kbps/1 Mbps cable subscriber.

Higher Bandwidth for Small Office Deployments

Given the availability of business class broadband data rates—and increasing interest in DSL and cable to support small offices—additional testing was completed at uplink data rates above 384 Kbps. The Cisco 1751 has also been included in this test phase. The Cisco 1700 series was not included in the original baseline teleworker testing. As the Cisco 1700 series supports voice modules and VLANS, it may be implemented by customers for small office deployments at business class data rates.

These tests were conducted with the split tunnel traffic profile described in the "Split Tunnel Traffic Profile" section on page 9-11.

Latency values that exceed the average one-way target of 50 msec and average jitter exceeding 10 msec are highlighted. These values are used as a goal for Cisco Enterprise Solutions Engineering lab testing in a controlled environment with no simulated service-provider delay or jitter. Latency and jitter values above the threshold might not impact voice quality or usability of an IP phone with this traffic profile in a production deployment; however, it does suggest that the ISP allocation for delay and jitter should be closely controlled. As one component introduces more delay or jitter, other components must be more stringent in terms of managing delay and jitter. In all cases, voice packet drops are rarely an issue with the appropriate QoS techniques and hardware encryption acceleration.

The total CPU utilization exceeded 75 percent in many tests and has also been noted accordingly. The high CPU utilization values generally do not negatively impact the average jitter, but do produce higher latency. Most enterprise customers should deploy a router platform that will average less than 50 percent total CPU utilization over the course of a typical 24-hour period.

Note The cumulative data rate of a 512 Kbps/2048 Kbps broadband connection approaches the bit per second rate of a full T1 and 768 Kbps/3072 Kbps exceeds a full T1 data rate.

Business Class Bandwidth Rates—DSL

Table 9-9 illustrates the DSL-based business-class bandwidth rates observed in Cisco Enterprise Solutions Engineering lab tests.

Table 9-9 Business Class Bandwidth Rates (DSL)[1]

Link Rate (Kbps) Up/Down	Platform	Number of G.729 Calls	MSS Value	Jitter (msec)		Latency (msec)		Mbps Data	Total CPU (percent)
				Branch to Head	Head to Branch	Branch to Head	Head to Branch		
256/1408	Cisco 831	1	542	8.0	7.2	**67**	37	0.9	54
	Cisco 1751	1	542	7.6	7.1	**66**	37	0.9	36
384/1536	Cisco 831	1	542	6.7	9.0	**54**	**74**	1.2	67
	Cisco 1751	1	542	6.7	9.7	**54**	**72**	1.2	46
512/2048	Cisco 831	1	542	5.1	5.8	**71**	**52**	1.6	**81**
	Cisco 1751	1	542	5.1	5.7	**80**	49	1.6	56
768/3072	Cisco 831	1	542	3.7	5.1	**51**	**64**	2.1	**92**
	Cisco 1751	1	542	3.8	3.6	**86**	28	2.1	70
768/3072	Cisco 831	1	1360[2]	8.8	7.9	**53**	38	2.3	73
	Cisco 1751	1	1360[3]	8.4	7.6	**54**	37	2.3	50

1. Voice drops not shown; less than 0.5 percent in all cases.
2. Workstation MTU set to 1400.
3. Workstation MTU set to 1400.

This testing was conducted with a PPPoE configuration using the dynamic IP addressing common with residential DSL service—but at data rates common for business class services.

At the 786 Kbps/3072 Kbps data rate tests were conducted with and without using the **ip tcp adjust-mss** command. A data rate of 768 Kbps is generally the threshold where Layer-2 fragmentation and interleaving (FRF.12 / LFI) are no longer required. While saving approximately 5 msec of branch-to-head jitter with the smaller TCP packets, the CPU utilization and latency were higher. Smaller packets translates into more packets. As a result, a higher packet per second rate will equate to a higher CPU utilization.

Business Class Bandwidth Rates – Cable

Table 9-10 illustrates the cable-based business-class bandwidth rates observed in Cisco Enterprise Solutions Engineering lab tests.

Table 9-10 Business Class Bandwidth Rates (Cable)[1]

Link Rate (Kbps) Up/Down	Platform	Number of G.729 Calls	MSS Value	Jitter (msec)		Latency (msec)		Mbps Data	Total CPU (percent)
				Branch to Head	Head to Branch	Branch to Head	Head to Branch		
256/1408	Cisco 831	1	542	**14.0**	6.4	**64**	9.8	1.4	68
	Cisco 1751	1	542	**12.1**	1.6	48	4.0	1.4	42
384/1536	Cisco 831	1	542	9.0	7.4	42	4.5	2.2	**90**
	Cisco 1751	1	542	8.7	1.9	33	4.9	2.2	62
512/2048	Cisco 831	1	542	6.3	6.5	35	**61**	2.3	**94**
	Cisco 1751	1	542	**10.1**	2.7	38	6.1	2.5	68
768/3072	Cisco 831	1	542	6.8	7.0	37	**74**	2.3	**97**
	Cisco 1751	1	542	**11.1**	3.4	42	7.2	2.7	72
768/3072	Cisco 831	1	1360[2]	5.4	5.0	32	18	3.3	**89**
	Cisco 1751	1	1360[3]	7.6	2.6	34	5.6	3.8	67

1. Voice drops not shown; less than 0.5 percent in all cases.
2. Workstation MTU set to 1400.
3. Workstation MTU set to 1400.

This testing was conducted using DOCSIS 1.0, but at data rates that are typical of business class cable services.

With the cable tests, observe that *Mbps Data* is much higher than with the corresponding link speed of DSL. Cable has substantially less Layer-2 overhead than DSL and the net effect is higher application throughput.

While the CPU utilization on both platforms is very high, the reader should not assume it is impractical to deploy an Cisco 831 or Cisco 1751 for a small office or teleworker on a 768 Kbps/3072 Kbps link. The following section illustrates the CPU utilization characteristics from an actual deployment.

Teleworker Deployment 768 Kbps/3072 Kbps

In a Cisco internal teleworker trial deployment, there was a software developer with a Cisco 831 deployed behind a Linksys personal firewall and cable modem with 768 Kbps/3072 Kbps data rate.

A script was run from a Unix workstation every 15 minutes throughout the day to capture the output of several **show** commands, including a **show proc cpu history**. The following display encompasses a period where the engineer was using his IP phone.

```
33223323333332333111112111121112111111222122211113111221 11
     44961244324504423546492288927722523257122804146582867321 16
 100
  90
  80
  70
  60
  50
  40            *
  30 ****** ****** ***                                    *
  20 **####**#*##*#**##* * ** ****** **   ********* *********  *
  10 ####################************************#******#********
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
                CPU% per minute (last 60 minutes)
                * = maximum CPU%   # = average CPU%

      1 11 111  1  1 1111  1 11 1  11 1  1 1 1 1  1  1 1111 11111 11111 1
    46090090009707806000073080070970070990608080970570900009000009000009061
    49020000006202406000030030060390090270801030120290500009000007000005051
 100   * ** **** *  * ****  * ** *  ** * ** * * * *  *  ********************
  90   ********* *  * ****  * ** ** ** **** * * ** *  ********************
  80   ********* * ** ****  *************** ****** * *********************
  70  ********************** ************************ ***********************
  60  ********************** ************************ ***********************
  50  ********************** ************************************************
  40 ********************** ************************************************
  30 *************************************************************************
  20 *************************************************************************
  10 ##########################################################################
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
              0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                   * = maximum CPU%   # = average CPU%
```

Note The average CPU utilization percentage—as represented by the value in the previous display—was less than or equal 10 percent over the last 72 hours.

Based on observations of the log file, this display is from the only voice call made that day by the teleworker and there was very little data transfer this day. Note the CPU busy over the course of the last 20 minutes is in the 24-to-35 percent range. However, in this time period there were less than five packets per second of data traffic other than the voice call.

It is important to take the performance results and CPU data of the previous sections in perspective; the Cisco Enterprise Solutions Engineering lab test results would be representative of a very busy teleworker and may not be indicative of every deployment. Testing is done to simulate worst case situations. Interface load and CPU utilization in actual deployments might be much lower.

Small Office—Two Concurrent Voice Calls

Enterprise organizations are increasingly interested in replacing existing Frame Relay WAN links with broadband connections. The motivation is reduced monthly expenses—often accompanied by an increase in available bandwidth. In many cases these offices may support two-to-five workers, in which case two concurrent voice calls are required.

Table 9-11 summarizes the results of tests performed at 768 Kbps/3072 Kbps with QoS Pre-classify, input access list for auth-proxy, NAT/pNAT, CBAC, IOS-IDS and the split tunnel traffic profile.

Table 9-11 Small Office—Two Concurrent Voice Calls[1]

Link Rate (Kbps) Up/Down	Platform	Number of G.729 Calls	MSS Value	Jitter (msec)		Latency (msec)		Mbps Data	Total CPU (percent)	Media
				Branch to Head	Head to Branch	Branch to Head	Head to Branch			
768/3072	Cisco 831	2	542	7.9	7.0	42	**73**	1.9	**97**	Cable
	Cisco 1751	2	542	**11.5**	3.4	45	7.3	2.5	72	Cable
768/3072	Cisco 831	2	542	4.1	5.2	**72**	**74**	1.9	**94**	DSL
	Cisco 1751	2	542	4.6	3.4	**104**	32	1.8	71	DSL
768/3072	Cisco 837	2	542	6.5	4.2	45	37	1.7	**92**	DSL

1. Voice drops not shown; less than 0.5 percent in all cases.

As described in the "Split Tunnel Traffic Profile" section on page 9-11, the test scripts—particularly the FTP-DATA script—will consume all available bandwidth. While the total CPU utilization for the Cisco 800 series is very high, the voice jitter and latency values are respectable, considering that the total bandwidth for these tests exceeded a full T1.

When assessing performance tradeoffs, consider the small office originally provisioned with a 56 Kbps Frame Relay CIR and a 128 Kbps port speed. Internet access via the link to the corporate headquarters might consume considerably more bandwidth after provisioning with direct Internet access at 768 Kbps/3072 Kbps. Not only will multiple voice calls be possible, better response time to corporate servers can facilitate greater use of both corporate and Internet applications.

CHAPTER 10

V3PN for Business Ready Teleworker Verification and Troubleshooting

Verification and troubleshooting sections presented in this chapter:

Service Assurance Agent

One of the challenges network managers face in implementing this solution is determining whether or not a deployment can provide acceptable voice quality. To resolve that issue, a Cisco SAA configuration was included in the test bed to provide a point of reference to the lab environment and tools—namely Chariot. Please refer to www.cisco.com/go/saa for more information.

Cisco SAA verification and troubleshooting topics addressed include:

Configuration to Measure Jitter

In the "Voice Quality Comparison" section on page 7-4, jitter values were calculated for Cisco SAA and documented along with the Chariot reported RFC 1889 jitter. With the cost associated with Chariot, hardware, licensing, and training time, many network managers with small deployments are reluctant to implement this tool for site surveys and troubleshooting. Chariot is an excellent tool. The goal is to provide a quick and inexpensive means of conducting site surveys and troubleshooting. Cisco SAA fits that requirement nicely. It is a component of Cisco IOS and can be run on the Cisco 83x and Cisco 17xx platforms, which are commonly deployed in the SOHO location.

The configuration used during the voice quality comparison tests is as follows:

```
rtr 12
 type jitter dest-ipaddr 10.3.16.20 dest-port 9 source-ipaddr 10.112.12.1 source-port 9
num-packets 200

 tos 184
 frequency 30
rtr schedule 12 start-time now life forever
```

This configuration generates a simulated voice stream of 200 UDP packets, 20 msec apart, setting the ToS byte to hex 184 or DSCP value of EF. The elapsed time is 4 seconds. It runs every 30 seconds until removed from the configuration. The priority queue value was increased from 64 to 128 during these tests to accommodate the additional *simulated* voice stream. Not shown in the configuration is the default value of 32 bytes for the packet size. A value of **request-data-size 32**, when UDP and IP headers are added to this value (8 bytes for UDP, 20 bytes for IP), results in a Layer-3 size of 60 bytes and simulates a G.729 call. To simulate a G.711 call use **request-data-size 172** in the Cisco SAA configuration.

The receiving router's configuration should include the **rtr responder** command for the above configuration to produce the expected results.

Note If this sample configuration is used in a production network provisioned for one G.729 call, and the IP phone is in use when the Cisco SAA jitter operation executes, the voice quality of the IP Phone call will suffer.

Figure 10-1 illustrates a NetFlow capture of a Cisco SAA jitter operation on a teleworker router (a Cisco 1751 in this example) configured to emulate a G.711 call.

Figure 10-1 Netflow Display of Cisco SAA Jitter Probe

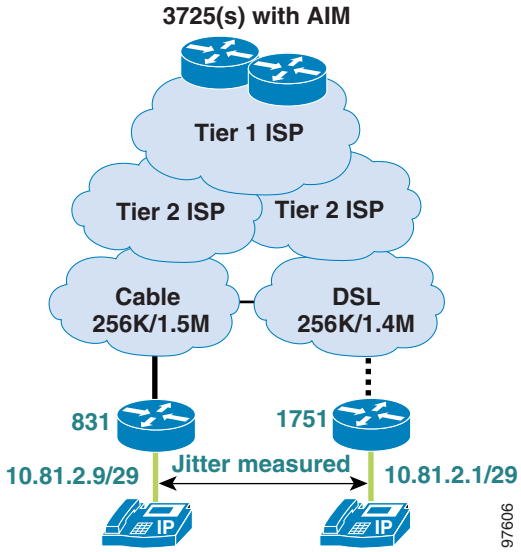
```
joeking-vpn#show ip cache verb flow
IP packet size distribution (1325939 total packets):
...
Protocol      Total   Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------      Flows    /Sec    /Flow  /Pkt    /Sec    /Flow    /Flow
TCP-Telnet      174     0.0       66    45     0.0     25.8     12.9
TCP-WWW         642     0.0       13   322     0.0      1.9      3.9
TCP-other     82850     0.1        2   112     0.2      0.1     15.4
UDP-DNS          55     0.0        1    66     0.0      0.5     15.4
...
IP-other      23360     0.0       23   233     0.6     12.2     15.4
Total:       183895     0.2        7   194     1.6      1.7     15.4

SrcIf       SrcIPaddress    DstIf       DstIPaddress    Pr TOSFlgs  Pkts
Port Msk AS                 Port Msk AS    NextHop         B/Pk   Active
This illustrates how to use Netflow to verify  the  UDP Jitter probe
Protocol = 0x11  UDP ToS=0xB8 DSCP=EF 200 packets in the flow
Active for 4 seconds  and the layer 3 size was 200 bytes
Et0/0       xx.xxx.xxx.x    Local       192.168.1.102   32 00 10    301
D439 /0  0                  E999 /0  0    0.0.0.0          207    60.8
Et0/0       10.81.2.9       Local       10.81.2.1       11 B8 10    200
0009/0  0                   0009/29 0     0.0.0.0          200     4.0
```

97605

Spoke-to-Spoke Jitter Illustration

Figure 10-2 illustrates of the application of Cisco SAA jitter operation over a spoke-to-spoke (branch-to-branch) teleworker deployment via the Internet environment shown.

Figure 10-2 Teleworker Trial Topology



A Cisco SAA configuration simulates a G.729 call between the two teleworker router Ethernet interfaces. This is an actual deployment from a Cisco internal teleworker trial based out of the Research Triangle Park, NC campus. The broadband service providers tie into their respective Tier 2 ISPs which in turn connect to a Tier 1 ISP providing connectivity to the Research Triangle Park campus.

For this example, the following configuration was applied to a Cisco 1751 router (the only required configuration option on the Cisco 831 router is **rtr responder**):

```
rtr responder
rtr 18
 type jitter dest-ipaddr 10.81.2.9 dest-port 9 source-ipaddr 10.81.2.1 source-port 9
num-packets 200
 tos 184
 frequency 30
rtr schedule 18 start-time now life forever
```

This setup involved no other background voice or data traffic between the two teleworkers (both were in the central site office during the capture) other than normal SCCP keepalives of the configured IP Phones. The collection statistics are as follows:

```
1751-vpn#show rtr collection-statistics 18
Entry number: 18
Start Time Index: 14:53:43.823 edt Tue Apr 29 2003
Number of successful operations: 5
Number of operations over threshold: 0
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
RTT Values:
```

```
NumOfRTT: 1000  RTTAvg: 91      RTTMin: 83      RTTMax: 125
RTTSum: 91009   RTTSum2: 8299261
Packet Loss Values:
PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
InternalError: 0        Busies: 0
Jitter Values:
MinOfPositivesSD: 1     MaxOfPositivesSD: 35
NumOfPositivesSD: 288   SumOfPositivesSD: 1460  Sum2PositivesSD: 14368
MinOfNegativesSD: 1     MaxOfNegativesSD: 20
NumOfNegativesSD: 316   SumOfNegativesSD: 1454  Sum2NegativesSD: 12438
MinOfPositivesDS: 1     MaxOfPositivesDS: 26
NumOfPositivesDS: 414   SumOfPositivesDS: 1684  Sum2PositivesDS: 15016
MinOfNegativesDS: 1     MaxOfNegativesDS: 23
NumOfNegativesDS: 394   SumOfNegativesDS: 1681  Sum2NegativesDS: 13583
Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
NumOfOW: 1000
OWMinSD: 41     OWMaxSD: 86     OWSumSD: 49814  OWSum2SD: 2497682
OWMinDS: 37     OWMaxDS: 65     OWSumDS: 41195  OWSum2DS: 1712979
```

Five iterations completed in the preceding example display output—each configured for 200 packets (for a total of 1000 packets, as shown by the **NumOfRTT** value). Adding the **SumOfPositivesSD** and **SumOfNegativesSD** jitter values and dividing by the total number of packets yields 2.9 msec jitter from source to destination. The same calculation for the destination to source return path yields 3.4 msec. The **MaxOfPositives** and **MaxOfNegatives** represent the extreme jitter values.

There were no packets lost, packets out-of-sequence, or packets lost-without-knowledge-of-direction. The average round trip time was 91 msec (a one-way value of 45.5 msec). The **RTTMin** and **RTTMax** values should be viewed with an eye to the consistency of latency.

Generally spoke-to-spoke calls in this illustration provide acceptable voice quality. Recall from the topology diagram, that the data path represents four encrypt/decrypt cycles and the call leg traversing four ISPs. These jitter and latency statistics are with minimal data traffic present during the capture.

ICMP Echo

One other Cisco SAA tool deployed in Cisco internal trials was ICMP Echo. This probe provides two benefits in deployments:

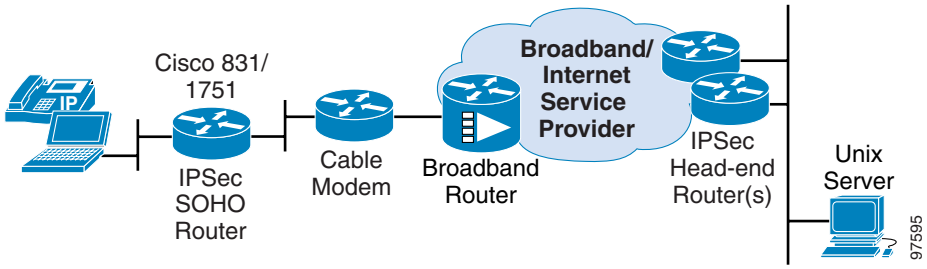
- ICMP Echo maintains the IPSec tunnels to the head-ends. This is important when using dynamic crypto maps that require the remote node's traffic to generate interesting packets to establish the tunnels. With Cisco 7960 IP Phones, the SCCP keepalives to the call manager establish these tunnels, but with no phone present or SIP phones, Cisco SAA is an effective means to maintain IPSec tunnels.
- This ICMP Echo configuration is used for troubleshooting. The probe is configured to maintain 60 buckets of history, allowing the network manager visibility into the last 60 iterations. This is used as a troubleshooting tool to monitor recent latency values and to identify potential jitter issues. Additionally, packet loss is recorded and is an indication of network connectivity problems.

The standard configuration deployed on all teleworker routers is:

```
rtr 12
 type echo protocol ipIcmpEcho 172.26.129.252 source-ipaddr 10.81.2.1
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time now life forever
```

The destination address is a Unix server at a central site lab location. The ToS values of these packets are decimal 192 or IP Precedence 6 (internetwork control). The packet size is an arbitrary value. The size of ICMP packets influences round trip times—smaller packet sizes have a lower trip time than do larger packets. The value of 164 results in a 200 bytes Layer-3 sized packet. Figure 10-3 provides a reference for the above configuration.

Figure 10-3 Cisco SAA ICMP Probe Setup



Viewing the history log for this probe provides insight into this connection.

```
test-vpn#show rtr history
        Point by point History
Entry    = Entry number
LifeI    = Life index
BucketI  = Bucket index
SampleI  = Sample index
SampleT  = Sample start time
CompT    = Round Trip Time (RTT) (milliseconds)
Sense    = Response return code

Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense      TargetAddr
12    1          18186      1          163649201  52         1          172.26.129.252
12    1          18187      1          163658201  52         1          172.26.129.252
12    1          18188      1          163667201  52         1          172.26.129.252
12    1          18189      1          163676201  52         1          172.26.129.252
12    1          18190      1          163685201  52         1          172.26.129.252
12    1          18191      1          163694201  52         1          172.26.129.252
12    1          18192      1          163703201  52         1          172.26.129.252
12    1          18193      1          163712201  52         1          172.26.129.252
[repetition  removed]
12    1          18202      1          163793201  52         1          172.26.129.252
12    1          18203      1          163802201  52         1          172.26.129.252
12    1          18204      1          163811201  52         1          172.26.129.252
12    1          18205      1          163820201  52         1          172.26.129.252
[repetition removed]
12    1          18242      1          164153201  52         1          172.26.129.252
12    1          18243      1          164162211  144        1          172.26.129.252
12    1          18244      1          164171201  56         1          172.26.129.252
12    1          18245      1          164180201  52         1          172.26.129.252
```

In this example there are very consistent round trip times of 52 msec, or 26 msec one-way delay to the head-end Unix server. This path traverses three ISP connections and six or more routers within the corporate network. These are very good round trip times. However notice that one iteration the round trip time jumped to 144 msec and the subsequent iteration was 56 msec. Generally a few such fluctuations are to be expected over the Internet and are not a cause for concern. Fluctuations that persist—or normally solid connections that demonstrate changes from day-to-day or week-to-week—are an indication of network problems. The sense code of 1 is a successful iteration.

The command **show rtr history full** provides detailed information for every iteration and can be used for further analysis.

Comparison of Broadband Internet Connectivity

This example illustrates two teleworker routers deployed in the Cisco internal trial, one with good Internet connectivity and the second with connectivity problems. Symptoms of the location with connectivity problems include:

- SSH sessions resetting due to CRC errors
- Voice calls ringing the remote phone but with no media stream present (an indication of call control packets being lost)
- Generally poor data throughput.

Both routers are configured similarly, as follows:

```
rtr 12
 type echo protocol ipIcmpEcho 172.26.129.252 source-ipaddr router_inside_ip_address
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time now life forever
```

The history of the router with good connectivity is shown. Note the **CompT** value is a very consistent 52 msec for all but one sample—26 msec one-way latency to the head-end. The **Sense** code is all 1, meaning successful.

```
test-vpn> sh rtr history
        Point by point History
Entry    = Entry number
LifeI    = Life index
BucketI  = Bucket index
SampleI  = Sample index
SampleT  = Sample start time
CompT    = RTT (milliseconds)
Sense    = Response return code

Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense      TargetAddr
12    1          7338       1          66081917   52         1          172.26.129.252
12    1          7339       1          66090917   52         1          172.26.129.252
12    1          7340       1          66099917   52         1          172.26.129.252
12    1          7341       1          66108917   52         1          172.26.129.252
12    1          7342       1          66117917   52         1          172.26.129.252
12    1          7343       1          66126917   52         1          172.26.129.252
12    1          7344       1          66135917   52         1          172.26.129.252
12    1          7345       1          66144917   52         1          172.26.129.252
12    1          7346       1          66153917   52         1          172.26.129.252
12    1          7347       1          66162917   52         1          172.26.129.252
```

```
12    1          7348       1          66171917   52         1          172.26.129.252
12    1          7349       1          66180917   52         1          172.26.129.252
12    1          7350       1          66189917   52         1          172.26.129.252
12    1          7351       1          66198917   52         1          172.26.129.252
12    1          7352       1          66207917   52         1          172.26.129.252
12    1          7353       1          66216917   52         1          172.26.129.252
12    1          7354       1          66225917   52         1          172.26.129.252
12    1          7355       1          66234917   52         1          172.26.129.252
12    1          7356       1          66243917   52         1          172.26.129.252
12    1          7357       1          66252917   52         1          172.26.129.252
12    1          7358       1          66261917   52         1          172.26.129.252
12    1          7359       1          66270917   52         1          172.26.129.252
12    1          7360       1          66279917   52         1          172.26.129.252
12    1          7361       1          66288917   52         1          172.26.129.252
12    1          7362       1          66297917   52         1          172.26.129.252
12    1          7363       1          66306917   52         1          172.26.129.252
12    1          7364       1          66315917   52         1          172.26.129.252
12    1          7365       1          66324917   52         1          172.26.129.252
12    1          7366       1          66333917   52         1          172.26.129.252
12    1          7367       1          66342917   52         1          172.26.129.252
12    1          7368       1          66351917   52         1          172.26.129.252
12    1          7369       1          66360917   52         1          172.26.129.252
12    1          7370       1          66369917   52         1          172.26.129.252
12    1          7371       1          66378917   52         1          172.26.129.252
12    1          7372       1          66387917   52         1          172.26.129.252
12    1          7373       1          66396917   52         1          172.26.129.252
12    1          7374       1          66405917   52         1          172.26.129.252
12    1          7375       1          66414917   52         1          172.26.129.252
12    1          7376       1          66423917   52         1          172.26.129.252
12    1          7377       1          66432917   52         1          172.26.129.252
12    1          7378       1          66441917   52         1          172.26.129.252
12    1          7379       1          66450917   52         1          172.26.129.252
12    1          7380       1          66459917   52         1          172.26.129.252
12    1          7381       1          66468917   52         1          172.26.129.252
12    1          7382       1          66477917   52         1          172.26.129.252
12    1          7383       1          66486917   52         1          172.26.129.252
12    1          7384       1          66495917   52         1          172.26.129.252
12    1          7385       1          66504917   52         1          172.26.129.252
12    1          7386       1          66513917   52         1          172.26.129.252
12    1          7387       1          66522917   52         1          172.26.129.252
12    1          7388       1          66531917   52         1          172.26.129.252
12    1          7389       1          66540917   52         1          172.26.129.252
12    1          7390       1          66549917   52         1          172.26.129.252
12    1          7391       1          66558917   52         1          172.26.129.252
12    1          7392       1          66567917   52         1          172.26.129.252
12    1          7393       1          66576917   52         1          172.26.129.252
12    1          7394       1          66585917   52         1          172.26.129.252
12    1          7395       1          66594917   64         1          172.26.129.252
12    1          7396       1          66603917   52         1          172.26.129.252
12    1          7397       1          66612917   52         1          172.26.129.252
```

Now compare this to a router that is experiencing an issue with the upstream cable modem. Note the **`Sense`** code of 4 indicates no ICMP reply was received. For those that were received, the **`CompT`** values range from a low value of 48 msec to a high value of 104 msec.

```
Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense      TargetAddr
12    1          399        1          35855820   48         1          172.26.129.252
12    1          400        1          35945819   0          4          172.26.129.252
12    1          401        1          36035819   48         1          172.26.129.252
12    1          402        1          36125818   52         1          172.26.129.252
12    1          403        1          36215818   52         1          172.26.129.252
12    1          404        1          36305821   60         1          172.26.129.252
12    1          405        1          36395821   40         1          172.26.129.252
12    1          406        1          36485820   40         1          172.26.129.252
```

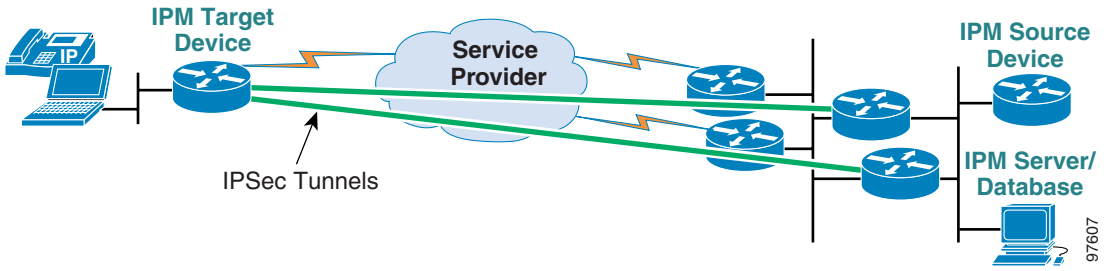
12	1	407	1	36575820	0	4	172.26.129.252
12	1	408	1	36665819	48	1	172.26.129.252
12	1	409	1	36755819	40	1	172.26.129.252
12	1	410	1	36845818	0	4	172.26.129.252
12	1	411	1	36935818	48	1	172.26.129.252
12	1	412	1	37025818	0	4	172.26.129.252
12	1	413	1	37115821	48	1	172.26.129.252
12	1	414	1	37205821	48	1	172.26.129.252
12	1	415	1	37295820	48	1	172.26.129.252
12	1	416	1	37385820	56	1	172.26.129.252
12	1	417	1	37475819	48	1	172.26.129.252
12	1	418	1	37565819	48	1	172.26.129.252
12	1	419	1	37655818	0	4	172.26.129.252
12	1	420	1	37745818	56	1	172.26.129.252
12	1	421	1	37835821	53	1	172.26.129.252
12	1	422	1	37925821	52	1	172.26.129.252
12	1	423	1	38015821	48	1	172.26.129.252
12	1	424	1	38105820	44	1	172.26.129.252
12	1	425	1	38195820	52	1	172.26.129.252
12	1	426	1	38285819	48	1	172.26.129.252
12	1	427	1	38375819	48	1	172.26.129.252
12	1	428	1	38465818	48	1	172.26.129.252
12	1	429	1	38555818	56	1	172.26.129.252
12	1	430	1	38645821	48	1	172.26.129.252
12	1	431	1	38735821	0	4	172.26.129.252
12	1	432	1	38825820	56	1	172.26.129.252
12	1	433	1	38915820	104	1	172.26.129.252
12	1	434	1	39005819	49	1	172.26.129.252
12	1	435	1	39095819	48	1	172.26.129.252
12	1	436	1	39185819	48	1	172.26.129.252
12	1	437	1	39275818	48	1	172.26.129.252
12	1	438	1	39365817	0	4	172.26.129.252
12	1	439	1	39455821	80	1	172.26.129.252
12	1	440	1	39545821	52	1	172.26.129.252
12	1	441	1	39635820	40	1	172.26.129.252
12	1	442	1	39725820	48	1	172.26.129.252
12	1	443	1	39815819	48	1	172.26.129.252
12	1	444	1	39905819	48	1	172.26.129.252
12	1	445	1	39995818	61	1	172.26.129.252
12	1	446	1	40085818	52	1	172.26.129.252
12	1	447	1	40175822	48	1	172.26.129.252
12	1	448	1	40265821	0	4	172.26.129.252
12	1	449	1	40355821	48	1	172.26.129.252
12	1	450	1	40445820	48	1	172.26.129.252
12	1	451	1	40535820	0	4	172.26.129.252
12	1	452	1	40625819	40	1	172.26.129.252
12	1	453	1	40715819	40	1	172.26.129.252
12	1	454	1	40805818	60	1	172.26.129.252
12	1	455	1	40895818	40	1	172.26.129.252
12	1	456	1	40985821	40	1	172.26.129.252
12	1	457	1	41075821	40	1	172.26.129.252
12	1	458	1	41165820	0	4	172.26.129.252

This illustration is provided to help show how connectivity issues can affect both voice quality and data connectivity issues.

Internetwork Performance Monitor

As part of the Cisco internal teleworker trial, several remote teleworker routers were enabled as CiscoWorks Internetwork Performance Monitor (IPM) target devices. In a network management lab at the head-end location, an IPM source device (router) and IPM server/client/database workstation are installed. See Figure 10-4.

Figure 10-4 IPM Topology Diagram



IPM measures latency, availability, jitter, packet loss, and errors by configuring source devices to initiate Cisco SAA probes in a similar manner as illustrated in the "Service Assurance Agent" section on page 10-1. Manually configuring Cisco SAA via the router's CLI is simple and quick. It can be quickly implemented to conduct spot checks or to troubleshoot problems in the network. By comparison, IPM is a fully functional network management application with a database that can store the performance history over weeks and months. IPM is useful for ongoing support and trend analysis.

Implementing IPM is strongly encouraged for an enterprises that intend to roll out V^3PN over broadband services. The latency, jitter and loss associated with the service provider is the most critical aspect of the teleworker voice quality. Configuring IPM to analyze this portion of the network is extremely helpful in working through service provider issues. The IPSec tunnels appear as one hop which traverse the ISP network. By placing an IPM source router in the topology *close* to the IPSec head-end routers and using the remote router as the IPM target, the ISP latency, jitter and drops can be determined.

Note If you are configuring IPM (or Cisco SAA) to generate simulated voice traffic as illustrated in the previous chapter (or through the IPM pre-configured operations, such as the **`Default60ByteVoice),`** provision QoS service policy with sufficient bandwidth in the priority queue (LLQ), otherwise voice quality suffers if Cisco SAA runs during a phone call.

For this reason, all combined Cisco SAA and Chariot testing the priority (LLQ) queue was provisioned for two G.729 calls.

For more information on IPM, please refer to the documentation section at:

- http://www.cisco.com/go/ipm

Common Deployment Issues

This section contains a list of issues encountered during deployments of V^{3}PN for teleworkers. Deployment issues addressed here include:

Codec Changes

In the Cisco Enterprise Solutions Engineering lab tests, the configuration used for testing provisioned 64 Kbps for voice given that Chariot generates a G.729 call. In the Cisco internal deployment, the priority (LLQ) is always provisioned for G.711 (128 Kbps), even though it is recommended that the second (home) IP Phone be configured in a G.729 region.

This is a safe approach for deployment. In the Cisco internal trial, employees were responsible for requesting/creating a tracking case to add the second phone to the appropriate call manager. In Cisco's case, an employee's call manager might be in one of a number of campus locations, depending on the person's geographical location. Since the deployment of the router and the implementation of the second line are different processes, the safe approach is to assume everyone is using G.711, but to recommend G.729. The higher bandwidth requirements provisioned for G.711 are not wasted if the person is using a G.729 codec.

There have been examples in which employees were to be provisioned for 64 Kbps—as they were using an IDSL connection (144 Kbps/144 Kbps)—but the call manager administrator changed them from G.729 to G.711 due to resource limitations on the call manager. In these situations, calls are of marginal cell phone quality. This type of issue is further justification of a minimum recommendation of no less than 256 Kbps uplink for V^{3}PN teleworker deployments. It gives sufficient bandwidth to adequately provisioned G.711 without additional trouble calls or voice quality problems if users must be switched or run G.711.

NTP Servers

As part of this solution's deployment, the enterprise should operate NTP Stratum 1 servers at the Internet access points accessible from intranet and the Internet. X.509 certificates require accurate time on the routers.

Cisco IOS images that do not incorporate CSCdz87526 require an accurate time source to establish the IPSec tunnel. By using public NTP servers as the only time source for a remote router, the enterprise is exposed to possible denial-of-service attack should these servers be compromised or taken off-line.

Enable Secret Passwords

Many organizations choose to block teleworkers from changing a remote router's configuration and to prevent these users from having the **enable secret** password. This presents a troubleshooting and support challenge to the network administrator. One method of allowing local access is to generate a separate **enable secret** password for each remote router, and maintain that information in a database—limiting access to only the IT support staff. If the enable secret password is to be given to a remote user, it should be unique to the assigned router and changed whenever a troubleshooting session is complete.

Configuring the remote router to allow only SSH in via the VTY ports also provides a means for central staff to access the router without the IPSec tunnels being active; however, if routers are attached to the network behind IPSec pass-through devices, the outside IP address is a RFC 1918 private address—which is not routable over the Internet. A static NAT entry must be configured on the IPSec pass-through device and this might prove difficult for non-technical staff.

Remote users doing a password recovery and changing the configuration is also an issue. Polling the running configuration and comparing it to a copy stored on a central TFTP/FTP server is one means of addressing the end-user changing the configuration and perhaps violating the enterprise security policy.

Certificate Server

Configuring the certificate server to permit auto-enrollment of certificates greatly facilitates the build/deploy process of remote routers and allows deployed routers to re-enroll the certificate as it reaches its end date. The **crypto ca trustpoint** subcommands **source interface** and **auto-enroll** are applicable to this type of configuration.

To prevent unauthorized users from configuring a router and enrolling it with the certificate server, access to the server should be limited (by an access-control list on the router supporting the subnet). The result is that only the remote user's inside address space and certain internal trusted subnets have permission to reach the CA server. If auto-enrollment is permitted from the home user's internal subnet, that user can configure and enroll routers for others by attaching those routers behind any router that has a functioning IPSec tunnel and then issuing the appropriate commands (such as **crypto ca authenticate** and **crypto ca enroll**) and configuration.

Testing and verification of the certificate server's ability to revoke certificates and recover the database prior to deployment is strongly recommended.

Special Requests

With a router in the user's home, expect requests for additional or non-standard configurations. Accommodating these requests consumes time of the central support technicians. These include troubleshooting home networks, but also include requests such as additional IP address allocation and configuration changes to exclude addresses from the remote router's DHCP server. Considerable thought should be given to these kinds of potential issues prior to deployment. For example, a /29 or /28 network prefix length is commonly deployed, but a /29 prefix might not be sufficient if teleworkers are deploying test or lab equipment in the home office. Making changes after deployment is time consuming.

Home Topology

Minimum requirements should be defined prior to deployment. Examples of setup requirements that should be articulated include: minimum supported uplink bandwidth (for example 256 Kbps); use of personal firewalls (and if permitted, what models are supported); and, whether wireless access points are permitted behind the IPSec tunnel.

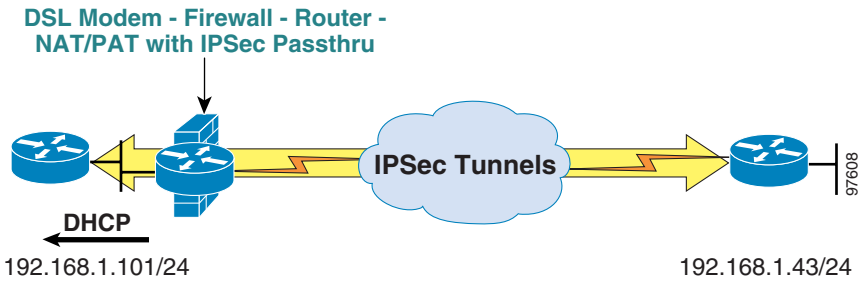
Hardware Failures

Since digital certificates authenticate a device (the router) rather than a user, replacement of a router due to hardware failure might require additional deployment steps and re-configuration from a back-up copy. Additionally, the end-user might not be knowledgeable enough to attach a console connection to the remote router and cut and paste the old configuration information into a new router. In the planning process, understanding the steps needed to replace defective hardware should be examined before deployments begin.

RFC 1918 Addresses

Most personal firewalls include a DHCP server which is configured to allocate a RFC 1918 private IP address to the hosts on the inside interface. Commonly used is 192.168.1.0/24, although other addresses might be in use. Refer to Figure 10-5.

Figure 10-5 Example RFC 1918 Address Usage



In Figure 10-5, the enterprise network manager allocated an address/subnet in the 192.168.1.0/24 address space somewhere else in the network and this address is not being handled by NAT. In the above topology example, the IPSec router is not able to encrypt and forward packets to host 192.168.1.43,

because that address appears to be local to the IPSec router's outside interface and the connection fails. Network managers must plan for this and verify personal firewalls do not overlap with existing RFC 1918 address space in use.

Identifying Remote Link Flaps

In the "Head-end Redundancy for Remote Peers" section on page 7-32, the concept of logical verses physical link flaps was discussed in regards to routing protocol summarization and the importance to network core stability. These logical link flaps can be used as a diagnostic tool to identify user connectivity problems. Assume there are two remote users with complaints of service disruption. In this example their remote subnets are 10.81.2.208./29 and 10.81.4.64/29. From a head-end router, configure a standard access list with these subnets:

```
access-list 99 permit 10.81.2.208 0.0.0.7
access-list 99 permit 10.81.4.64 0.0.0.7
```

Use the **debug ip routing** command on one of the head-end routers that re-distribute RRI injected routes:

```
gw2#debug ip routing 99
IP routing debugging is on for access list 99
```

For log destinations with debugging level, the network manager is able to identify the data and time the head-end routers lost connectivity with the remote routers and removed the subnets from the routing table. To illustrate:

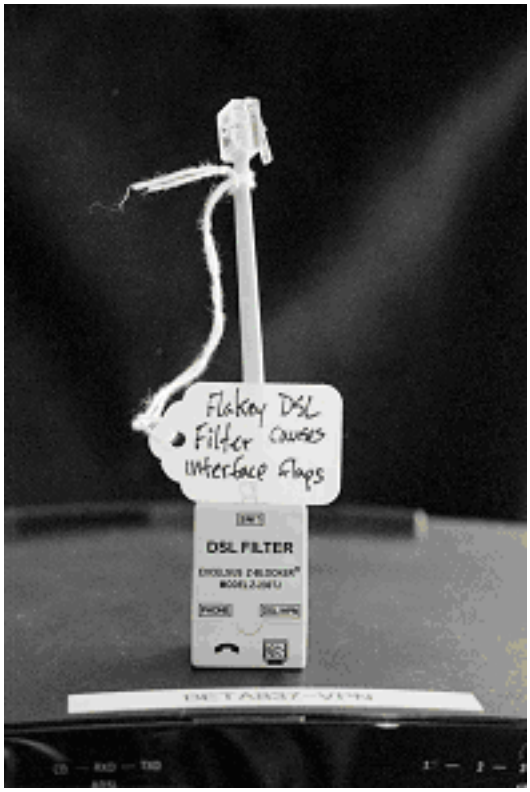
```
Mar 21 10:03:38 est: RT: del 10.81.4.64/29 via 0.0.0.0, static metric [1/0]
Mar 21 10:03:38 est: RT: delete subnet route to 10.81.4.64/29
Mar 21 10:04:02 est: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid
spi for destaddr=xx.218.223.4, prot=50, spi=0x3C62D0CC(1013108940), srcaddr=xx.40.46.1
Mar 21 10:04:21 est: RT: add 10.81.4.64/29 via 192.168.81.3, eigrp metric [170/2588160]
```

This provides information to identify whether the connectivity problem is associated with events at the head-end location—affecting all users or only a few users—and can be a tool for isolating specific user service provider issues.

Troubleshoot the Basics

Often troubleshooting becomes more involved and complicated than needed to solve the problem. Before working to isolate upper-layer issues, verify the physical layer and link layer are working properly. Figure 10-6 illustrates a DSL filter.

Figure 10-6 DSL Filter



This filter was attached to an Cisco 837 router. The router was functioning normally, but was moved to a separate room in the house to accommodate some family members. Shortly following the move, the ATM interface on the Cisco 837 router became inactive for approximately 30 seconds and then came back up for a half hour, then would flap again every 30-to-60 minutes. While the router had been functioning before the move, the existing DSL filter was not moved with the router and the new filter was faulty. Replacing the DSL filter resolved the problem. Not installing DSL filters on all phone jacks can also cause interface flaps and should be investigated. Installing a filter at the NTU and then branching out all internal home phone lines off the one filtered connection can be a simpler solution to installing filters on all RJ-11 jacks in the home or office.

Many problems can be resolved with a **show log** and **show interface** command from the remote router. An incorrect time on the remote router, no IP address from the upstream DHCP or PPPoE server, duplex mismatches, or CRC/Errors on interfaces can cause the teleworker problems. Most of the common problems can be detected with these two simple **show** commands. Other common problems relate to wiring. Family members (and pets) sometimes re-cable equipment. Cross-over verses straight-through Category-5 cables can cause physical-level problems. Personal firewalls also account for a considerable amount of connectivity problems. Reload any home networking equipment before performing additional troubleshooting.

Cable, DHCP and MAC Addresses

Some cable providers restrict end user to a specific MAC address. In some cases the subscriber must provide this information at installation time—usually the MAC address of the PC or personal firewall. Replacing the existing topology with a Cisco 831 router also requires changing the MAC address registered with the cable provider. These types of problems can usually be diagnosed by requesting the

end-user supply a **show log** and a **show ip interface** from the console connection of the router. Failure of the router to obtain an IP address via DHCP and failure of the router clock to be set properly via NTP are common problems.

Certificate Expiration

Digital certificates have a validity date associated with the certificate. This date range can be seen by entering the **show crypto ca certificates** command, for example:

```
test-vpn#show crypto ca certificates  | begin Validity
  Validity Date:
    start date: 16:59:38 est Nov 26 2002
    end   date: 17:09:38 est Nov 26 2003
    renew date: 06:06:38 edt Aug 9 2003
  Associated Trustpoints: BETA-CA
```

If the auto-enrollment feature is not enabled on the remote routers, the remote user cannot establish an IKE/IPSec tunnel to the head-end routers at the expiration date of the certificate. The only indication of this problem is a message on the head-end router's console as follows:

```
%CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from xxx.xxx.xxx.xxx was not encrypted and it
should've been.
```

On the remote router a message similar to the following will be displayed:

```
% CA Cert not yet valid or is expired -
    start date: 14:40:10 edt May 16 2002
    end   date: 14:50:10 edt May 16 2003
```

However, since the IPSec tunnel is not up, the only way for central site technical support staff to see these messages is for the remote user to provide the console log *out-of-band* or to provide SSH access to the router. This presents some difficulty in troubleshooting. As a best practice, use of the certificate auto-enrollment feature is desirable if it meets the security requirements of the organization. Also, sourcing the certificate enrollment off the inside interface is desirable, which requires a Cisco IOS image which supports CSCdw41126.

Windows Kerberos Authentication

There is a software defect in Windows 2000 that causes the PC to hang or boot very slowly when connected behind the V^{3}PN teleworker router. It relates to fragmented Kerberos UDP packets. The link for more information is as follows:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q244474

Powering the Cisco 7960 IP Phone

With in-line power widely deployed in enterprise campus environments, users sometimes forget the fact that IP Phones require power.

For deployments where there is no switch to supply power, order the following:

- CP-PWR-CUBE: IP Phone power transformer for Cisco 7900 series phones
- CP-PWR-CORD-NA: Cisco 7900 Series transformer power cord, North Americal

Category-5 Cables

The Cisco 831 and Cisco 837 routers include a built-in switch and can use a straight-through Category-5 cable between the IP Phone and the router. Some Cisco 1700 series routers do not include a switch port and a Category-5 cross-over cable is needed between the router and the IP Phone.

Duplicate IP Subnet

In any large network, inevitably the same IP subnet will be assigned to two different routers, thereby creating a duplicate network. These are commonly caused by typographical errors or oversight. In a traditional WAN network, issuing a **show ip route** command for the network being deployed prior to configuring the router is one means of verifying this mistake is not made. However, with RRI and dynamic crypto maps, you cannot be sure the remote router is on-line. The teleworker's router might be powered off for fairly long periods of time, for example, during a vacation or holiday. Detecting a duplicate subnet might be difficult to detect. It also might exist for days or weeks without a trouble call from the affected parties. This situation existed in the Cisco internal trial deployment for almost a month without notice. The users experienced intermittent connectivity loss and the IP Phone would loose connectivity to the call manager and reset frequently. A Telnet session from the enterprise core to the duplicated subnet would allow login, but then the connection would be lost after a few seconds and could then be re-established.

To avoid these mistakes, saving all remote router configuration files to a central FTP/TFTP server and scanning for duplications via a Perl or shell script is highly recommended.

Verifying Packet Classification

One common problem that can affect voice quality is improper packet classification. In the "Internetwork Performance Monitor" section on page 10-9, the importance of provisioning for IPM simulated voice traffic was emphasized—in addition to provisioning for the voice call in the LLQ. The following **show** output example illustrates how to identify and investigate applications that are incorrectly setting the ToS byte—DSCP or IP Precedence. In troubleshooting voice quality issues, it is important to become familiar with the **show policy-map interface** command.

```
test-vpn#show policy-map interface ethernet 0/0
 Ethernet0/0

  Service-policy output: Shaper

    Class-map: class-default (match-any)
      3131051 packets, 833150952 bytes
      30 second offered rate 3000 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
           182400/182400    456    1824      1824      10        228

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         3129958   832807370 861837    353148296 no
```

In the shaper portion of the **policy-map** (this is a HCBWFQ configuration on a dual Ethernet/FastEthernet router) note the interval value is 10 msec. This is the correct value; it is derived from the shaped rate value and the sustained bits per interval value. For voice this interval should be 10 msec to minimize the latency of voice packets because the shaper can delay them.

The current Queue Depth value is zero and there are no packets queued by the shaper; however, during periods of heavy traffic (which exceeds the shaped rate), there are packets queued by the shaper. This is usually the case when running a Chariot test in the lab.

Note The shaper is not active since packet arrival rate is less than the shaped rate.

From the following output, note that the IP Phone in this example is using DSCP values of AF31 rather than CS3, as there are no packets matched under the CS3 entry. Verify there are no drops in this class. Dropping call control packets affects an IP Phone's ability to place calls or use DMTF tones for voice mail systems.

```
Service-policy : VoIP_IPSec
      Class-map: CALL-SETUP (match-any)
          126901 packets, 14549454 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af31
            126901 packets, 14549454 bytes
            30 second rate 0 bps
          Match: ip dscp cs3
            0 packets, 0 bytes
            30 second rate 0 bps
          Queueing
            Output Queue: Conversation 41
            Bandwidth 2 (%)
            Bandwidth 3 (kbps) Max Threshold 64 (packets)
            (pkts matched/bytes matched) 1390/160108
        (depth/total drops/no-buffer drops) 0/0/0

Class-map: TRANSACTIONAL-DATA (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af21
          Queueing
            Output Queue: Conversation 42
            Bandwidth 8 (%)
            Bandwidth 14 (kbps) Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
```

In the INTERNETWORK-CONTROL class packets are matching the IKE access-control list and there is also CS6 or IP Precedence 6 traffic being matched. Recall that NTP packets are marked CS6 and this router is configured for several NTP servers.

```
Class-map: INTERNETWORK-CONTROL (match-any)
          39243 packets, 8148366 bytes
          30 second offered rate 3000 bps, drop rate 0 bps
          Match: ip dscp cs6
            32026 packets, 6744796 bytes
            30 second rate 3000 bps
          Match: access-group name IKE
            7217 packets, 1403570 bytes
            30 second rate 0 bps
          Queueing
            Output Queue: Conversation 43
            Bandwidth 5 (%)
```

```
     Bandwidth 9 (kbps) Max Threshold 64 (packets)
     (pkts matched/bytes matched) 725/190414
  (depth/total drops/no-buffer drops) 0/0/0
```

In the "Internetwork Performance Monitor" section on page 10-9, the importance of provisioning for IPM simulated voice traffic—in addition to the voice call in the LLQ—was emphasized. If IPM and voice are running simultaneously, the voice class must be provisioned and (accordingly) drops will occur (as illustrated in the following output example). To alleviate this potential problem, provision sufficient bandwidth to handle more than one call (the planned phone call plus any IPM traffic).

```
Class-map: VOICE (match-all)
  791569 packets, 205538430 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp ef
  Queueing
    Strict Priority
    Output Queue: Conversation 40
    Bandwidth 128 (kbps) Burst 3200 (Bytes)
    (pkts matched/bytes matched) 202498/54672132
    (total drops/bytes drops) 819/221130
```

In the preceding voice class output example, there were drops since the last time the router was reloaded or the interface counters were cleared. This should be addressed as it can affect voice quality. In this case, it was only 4/10 of one percent. Note the bandwidth is configured for 128 Kbps and the IP Phone on this connection is using G.711 rather than the recommended G.729. One way of addressing dropped voice packets is to increase the burst size. For example, the following configuration can be used to eliminate drops in this case.

```
policy-map VoIP_IPSec
 class VOICE
 priority 128 6400
```

In the following display output, **class-default class** has 185 total drops, which can be expected, as this is where the best-effort traffic falls. Since WRED is configured in this class, and WRED is by default IP Precedence aware, the columns show the packets and bytes transmitted, random dropped and tail dropped. Note that of the IP Packets that were dropped, 185 in total, all were random drops as opposed to tail drops. This is ideal behavior, as it means WRED is working properly by decreasing the arrival rate of application packets (to minimize tail drops).

```
Class-map: class-default (match-any)
          2173338 packets, 604914702 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: any
          Queueing
            Flow Based Fair Queueing
            Maximum Number of Hashed Queues 32
        (total queued/total drops/no-buffer drops) 0/185/0
             exponential weight: 9

  class    Transmitted      Random drop      Tail drop    Minimum Maximum  Mark
           pkts/bytes       pkts/bytes       pkts/bytes    thresh  thresh  prob
      0  213393/15744836      185/113846         0/0           20      40  1/10
      1       0/0               0/0              0/0           22      40  1/10
      2       0/0               0/0              0/0           24      40  1/10
      3       0/0               0/0              0/0           26      40  1/10
      4       0/0               0/0              0/0           28      40  1/10
      5   67058/16105684        0/0              0/0           30      40  1/10
      6       0/0               0/0              0/0           32      40  1/10
      7       0/0               0/0              0/0           34      40  1/10
   rsvp       0/0               0/0              0/0
```

In the preceding display output, there are packets matching in the class 5 row (IP Precedence 5). Normally, IP precedence 5 is used for voice, or by default DLSw. The nature or source of these packets should be investigated as obviously the administrator responsible for this application intended that they receive preferential treatment on the network. NetFlow is running on this router so use that tool to gather information about the application in question.

From the following output, the sender's IP address can be identified by determining which flows have a ToS value of 0xA0 (equates to IP Precedence 5). Appendix B, "ToS Byte Reference Chart" provides the conversion from hex. From this information, the system administrator can be contacted to make any changes necessary. This is not a voice application; therefore, including this traffic in the priority queue is not required. However, network administrators have in the past coded voice gateways to use IP Precedence 5 (CS5) to identify voice packets. In the case where this IP Phone might be in a call with a phone on the PSTN, the voice gateway might be setting the call leg from the gateway to the IP Phone as DSCP CS5 and the phone to the gateway might be DSCP EF. These configuration mismatches should be identified and addressed.

```
host-vpn#show ip cache verb flow | begin SrcIf
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop             B/Pk  Active
Et0/0          172.18.86.112   Local          10.81.2.1       11 A0  10      10
E633 /0  0                     4010 /29 0     0.0.0.0               188     0.1
```

Source Interface

It is a recommended standard implementation practice to *source* packets generated by the router off an interface that causes packets to match the crypto map (and to be encrypted and sent through the IPSec tunnel). Assume the inside interface to be configured as follows:

```
interface FastEthernet0/0
 description Inside
 ip address 10.81.2.1 255.255.255.248
```

Some services that might be considered to source off the inside and to be encrypted in the tunnel are as follows:

```
ip telnet source-interface FastEthernet0/0
ip tftp source-interface FastEthernet0/0
ip ftp source-interface FastEthernet0/0
snmp-server trap-source FastEthernet0/0
ntp server 10.81.254.202 source FastEthernet0/0
logging source-interface  FastEthernet0/0
!
rtr 12
 type echo protocol ipIcmpEcho xxx.26.129.252 source-ipaddr 10.81.2.1
```

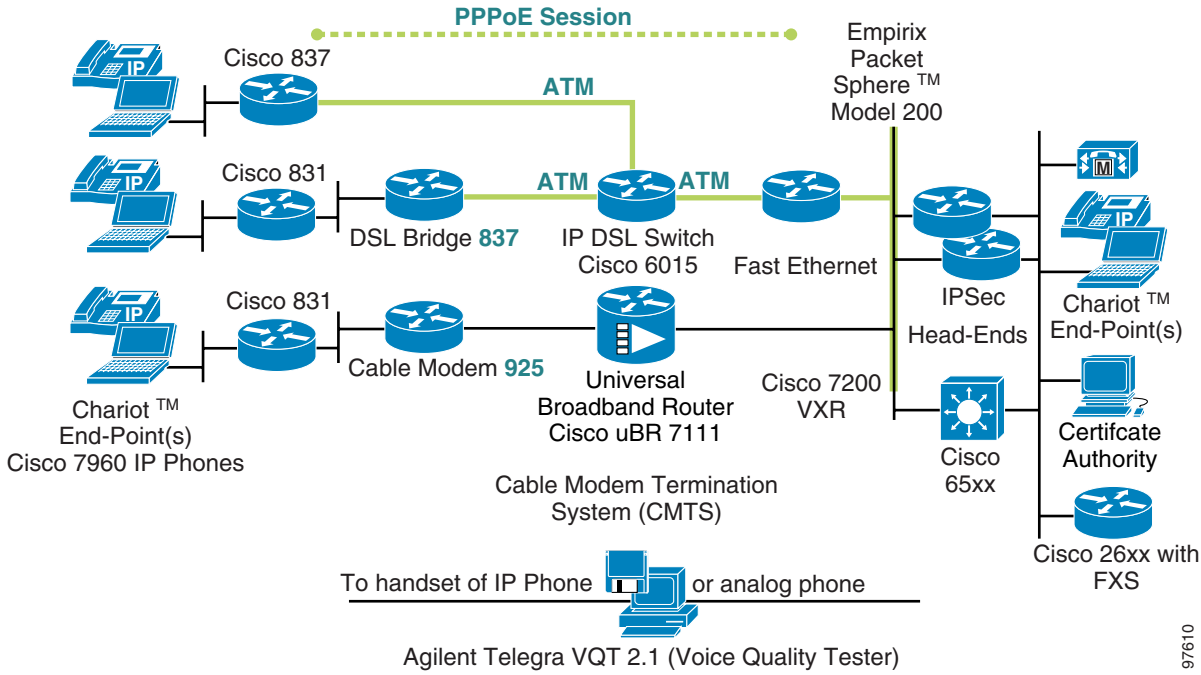
Other services can also benefit, depending on implementation requirements.

V³PN for Business Ready Teleworker Solution Testbed Network Diagram

Figure A-1 represents the Cisco Enterprise Solutions Engineering lab test topology for the performance results reported in this document. The Empirix Packet Sphere™ is Gigabit Ethernet-attached and can be enabled when conducting ISP simulated testing. The Agilent Telegra™ VQT connects to the phone handsets—an IP Phone or analog phone. The Cisco 26xx router with FXS ports is in the topology to conduct IP Phone-to-voice gateway testing. In this testing configuration, an IP Phone would be connected to one port of the Agilent Telegra™ and the analog phone's handset would be connected to the other port.

While two IPSec head-ends are deployed in the test topology, this testing is focusing on remote performance and traffic is sent though only one head-end during the tests—failover and redundant configurations are not part of this test plan.

Figure A-1 Solution Testbed Network Diagram



ToS Byte Reference Chart

Figure B-1 and Table B-1 illustrate the ToS Byte to assist in implementation and troubleshooting.

Figure B-1 ToS Byte

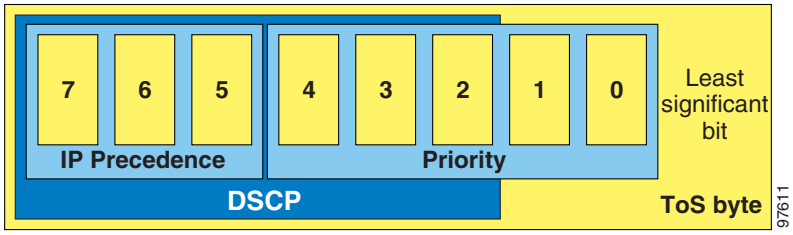


Table B-1 TOS Byte Reference Chart

TOS Hex	TOS Decimal	IP Precedence	Class-map Name	DSCP	Binary
E0	224	7 Network Control		CS7	11100000
C0	192	6 Internetwork Control	internetwork-control	CS6	11000000
B8	184		voice	EF	10111000
A0	160	5 Critical		CS5	10100000
80	128	4 Flash Override		CS4	10000000
68	104		call-setup	AF31	01101000
60	96	3 Flash	call-setup	CS3	01100000
48	72		transactional-data	AF21	01001000
40	64	2 Immediate		CS2	01000000
20	32	1 Priority		CS1	00100000
00	0	0 Routine		Default	00000000

The **class-map** configuration file entries illustrated and tested in this solution are provided below and are defined in Table B-1.

```
class-map match-all VOICE
  match ip dscp ef
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match  access-group name IKE
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
```

Additional Performance Data Configuration Examples

These configuration examples are the relevant portion of the base configurations that equate to the changes made for performance testing associated with the "CPU Utilization by Feature" section on page 9-10. Specific configuration descriptions provided include:

Global Configuration Changes

In the configuration examples shown in this appendix, NAT transparency was disabled and QoS Pre-classify was enabled as follows:

```
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto map test 10 ipsec-isakmp
 description This calls the dynamic map on the crypto agg box(es)
 set peer 192.168.252.1
 set peer 192.168.252.2
 set transform-set vpn-test
 match address CryptoMapACL
 qos pre-classify
!
```

The Cisco IOS images in use were:

- c831-k9o3sy6-mz.122-13.ZH
- c837-k9o3sy6-mz.122-13.ZH
- c1700-k9o3sv8y7-mz.122-13.T1

Input Access-Control Lists for Auth-Proxy

The following access-control list was configured to simulate the access-control list checks required for all packets transmitted into the remote router's inside LAN interface when using auth-proxy to support split tunneling:

```
interface Ethernet0
 description Inside interface
 ip address 10.112.22.1 255.255.255.0
 ip access-group SimulatedAuthproxyACL in
...

ip access-list extended SimulatedAuthproxyACL
 permit ip host 10.112.22.89 10.0.0.0 0.255.255.255
 permit ip host 10.112.22.89 any
 permit ip 10.112.22.0 0.0.0.255 10.0.0.0 0.255.255.255
 permit ip any any
 remark This ACL is a filter which simulated the amount of processing that would need
 remark to accrue if auth-proxy were already logging in on this branch.
 remark this is applied to the lan side interface e0
```

NAT/pNAT

The NAT/pNAT configuration used was as follows:

```
interface Ethernet0
 description Inside interface
 ip address 10.112.22.1 255.255.255.0
 ip access-group SimulatedAuthproxyACL in
 ip nat inside
...

interface Ethernet1
 description Outside interface
 ...
 ip nat outside

ip nat inside source list NoNatACL interface Ethernet1 overload

ip access-list extended NoNatACL
 deny   ip 10.112.22.0 0.0.0.255 10.0.0.0 0.255.255.255
 permit ip 10.112.22.0 0.0.0.255 any
 remark This ACL is a filter of which traffic is to be NAT/pNATed for the Internet
```

CBAC

For the CBAC portion of the performance testing, the following configuration was used:

```
ip inspect max-incomplete high 700
ip inspect one-minute high 700
ip inspect name fwout tcp
ip inspect name fwout udp
ip inspect name fwout ftp

interface Ethernet1
 description Outside interface
 ...
 ip inspect fwout out
```

Cisco IOS-IDS

For the Cisco IOS-IDS portion of the performance testing, the following configuration was used:

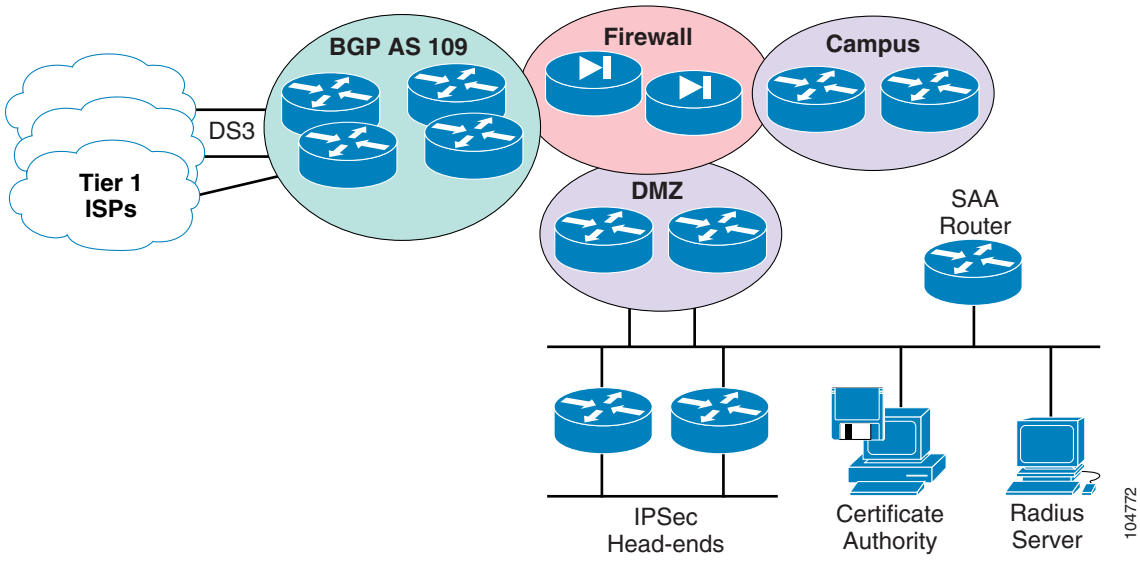
```
ip audit notify log
ip audit po max-events 100
ip audit po local hostid 55 orgid 123
ip audit smtp spam 25
ip audit signature 1107 disable
ip audit signature 2000 disable
ip audit signature 2001 disable
ip audit name AUDIT.1 info action alarm
ip audit name AUDIT.1 attack action alarm

interface Ethernet0
 description Inside interface
 ...
 ip audit AUDIT.1 out
```

Sample Deployment

The configuration examples in this appendix represent a typical environment in use within Cisco for an internal trial. Two of the remote router configurations are used at a Cisco employee home network. The third remote configuration includes a sample 802.1X configuration.

Head-end

Figure D-1 Sample Deployment—Head-end



Primary Head-end Configuration

```
! c3725-ik9o3s-mz.122-15.T9
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service tcp-small-servers
!
hostname XXX5-esevpn-gw4
```

```
!
boot system flash c3725-ik9o3s-mz.122-15.T9
boot system flash
logging queue-limit 100
logging buffered 100000 debugging
enable secret 5 [removed]
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
aaa new-model
!
!
aaa authentication login admin group tacacs+ enable
aaa session-id common
ip subnet-zero
no ip source-route
ip flow-cache timeout active 5
!
!
ip cef
ip tftp source-interface Loopback0
ip domain name cisco.com
ip host XXX5-esevpn-ca 10.1.0.18
ip name-server xxx.70.168.183
ip name-server xxx.68.226.120
ip name-server xxx.xxx.6.247
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 60
ip ssh authentication-retries 2
!
crypto ca trustpoint ese-vpn-cert
 enrollment mode ra
 enrollment url http://10.1.0.18:80/certsrv/mscep/mscep.dll
 auto-enroll 70
!
crypto ca certificate chain ese-vpn-cert
 certificate ca 36092145BAA631BF4763493E714CD857

[removed]


  quit
 certificate 610660B0000000000004

[removed]


  quit
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map dmap 10
 set transform-set t2
```

```
 reverse-route
!
!
crypto map test local-address Loopback0
crypto map test 1 ipsec-isakmp dynamic dmap
!
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
!
interface Loopback0
 description Public address
 ip address xx.xxx.223.24 255.255.255.255
!
interface FastEthernet0/0
 description VLAN 100 XXX5-Alpha-GW1
 ip address 10.1.0.24 255.255.255.240
 ip access-group DoS_Input_Queue_Wedge in
 no ip redirects
 ip route-cache same-interface
 ip route-cache flow
 speed 100
 full-duplex
 standby 1 ip 10.1.0.20
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication [removed]
 crypto map test
!
interface FastEthernet0/1
 description VLAN 101 XXX5-Alpha-GW1
 ip address 192.168.82.24 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 network 192.168.82.0
 no auto-summary
 no eigrp log-neighbor-warnings
!
no ip http server
no ip http secure-server
ip flow-export version 5
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.0.17
ip route 10.1.7.0 255.255.255.0 Null0
!
!
```

```
!
ip access-list extended DoS_Input_Queue_Wedge
 remark http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
 deny   53 any any
 deny   55 any any
 deny   77 any any
 deny   pim any any
 permit ip any any
!
logging source-interface FastEthernet0/0
logging xx.xx.168.186
access-list 1 remark Home user address pool(s)
access-list 1 remark 10.1.2.0 / 23
access-list 1 remark 10.1.4.0 / 22
access-list 1 remark ... but we are only allowing the last address block
access-list 1 permit 10.1.7.0 0.0.0.255
access-list 1 deny   any log
access-list 88 permit xx.xxx.18.178
access-list 88 permit xx.xxx.86.64 0.0.0.63
access-list 88 deny   any log
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!
tacacs-server host xx.xx.10.137
tacacs-server host xx.xx.11.123
tacacs-server timeout 15
tacacs-server directed-request
snmp-server community 2dollars RW 88
snmp-server trap-source Loopback0
snmp-server location [removed]
snmp-server contact fortran@cisco.com
snmp-server enable traps tty
!
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
!
rtr responder
rtr 12
 type echo protocol ipIcmpEcho xx.xx.129.252 source-ipaddr 10.1.0.24
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time now life forever
banner exec _
This router's configuration is backed up on  assembler.cisco.com.
 Any changes to this router need to be communicated outside
operational emergencies, in advance to
 fortran@cisco.com, basic@cisco.com
 Thank you.
```

```
_
banner motd _
   C i s c o S y s t e m s
      ||               ||
      ||               ||       Cisco Systems, Inc.
     ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                     + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.
_
alias exec scr show run | b crypto isakmp
alias exec wrnet copy run tftp://assembler/vpn/DIRECTORY/XXX5-esevpn-gw4-confg
!
line con 0
 exec-timeout 30 0
line aux 0
line vty 0 4
 login authentication admin
 transport input ssh
line vty 5 15
 login authentication admin
 transport input ssh
!
exception memory minimum 1048576
ntp clock-period 17180810
ntp server 10.1.254.202
ntp server 10.1.254.131
end
```

Secondary Head-end Configuration

```
! c3725-ik9o3s-mz.122-15.T9
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service tcp-small-servers
!
hostname XXX5-esevpn-gw5
!
boot system flash c3725-ik9o3s-mz.122-15.T9
boot system flash
logging queue-limit 100
logging buffered 65536 debugging
enable secret 5 [removed]
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
aaa new-model
!
!
aaa authentication login admin group tacacs+ enable
aaa session-id common
ip subnet-zero
no ip source-route
```

```
ip flow-cache timeout active 5
!
!
ip cef
ip tftp source-interface Loopback0
ip domain name cisco.com
ip host XXX5-esevpn-ca 10.1.0.18
ip name-server xxx.70.168.183
ip name-server xxx.68.226.120
ip name-server xx.xxx.6.247
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
!
crypto ca trustpoint ese-vpn-cert
 enrollment mode ra
 enrollment url http://10.1.0.18:80/certsrv/mscep/mscep.dll
 auto-enroll 70
!
crypto ca certificate chain ese-vpn-cert
 certificate ca 36092145BAA631BF4763493E714CD857

[removed]



  quit
 certificate 3A503D93000000000022

[removed]



  quit
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map dmap 10
 set transform-set t2
 reverse-route
!
!
crypto map test local-address Loopback0
crypto map test 1 ipsec-isakmp dynamic dmap
!
!
!
!
!
!
!
!
!
```

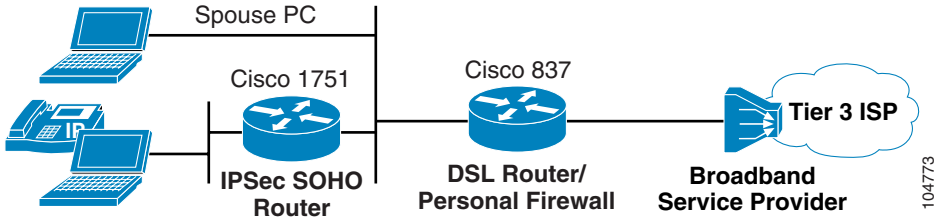
```
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
!
interface Loopback0
 description Public address
 ip address xx.xxx.223.25 255.255.255.255
!
interface FastEthernet0/0
 description Private
 ip address 10.1.0.25 255.255.255.240
 ip access-group DoS_Input_Queue_Wedge in
 no ip redirects
 ip route-cache same-interface
 ip route-cache flow
 speed 100
 full-duplex
 standby 1 ip 10.1.0.20
 standby 1 preempt
 standby 1 authentication [removed]
 crypto map test
!
interface FastEthernet0/1
 description VLAN 101 XXX5-Alpha-GW1
 ip address 192.168.82.25 255.255.255.0
 speed 100
 full-duplex
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 network 192.168.82.0
 no auto-summary
 no eigrp log-neighbor-changes
 no eigrp log-neighbor-warnings
!
no ip http server
no ip http secure-server
ip flow-export version 5
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.0.17
ip route 10.1.7.0 255.255.255.0 Null0
!
!
!
ip access-list extended DoS_Input_Queue_Wedge
 remark http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
 deny   53 any any
 deny   55 any any
 deny   77 any any
 deny   pim any any
 permit ip any any
!
logging source-interface FastEthernet0/0
logging xx.xx.168.186
access-list 1 remark Home user address pool(s)
access-list 1 remark 10.1.2.0 / 23
access-list 1 remark 10.1.4.0 / 22
```

```
access-list 1 remark ... but we are only allowing the last address block
access-list 1 permit 10.1.7.0 0.0.0.255
access-list 1 deny   any log
access-list 88 permit xx.xxx.18.178
access-list 88 permit xxx.xx.86.64 0.0.0.63
access-list 88 deny   any log
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!
tacacs-server host xx.xx.10.137
tacacs-server host xx.xx.11.123
tacacs-server timeout 15
tacacs-server directed-request
snmp-server community 2dollars RW 88
snmp-server trap-source Loopback0
snmp-server location [removed]
snmp-server contact fortran@cisco.com
snmp-server enable traps tty
!
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
!
rtr responder
rtr 12
 type echo protocol ipIcmpEcho xx.xx.129.252 source-ipaddr 10.1.0.25
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time now life forever
banner exec _
This router's configuration is backed up on  assembler.cisco.com.
 Any changes to this router need to be communicated outside
operational emergencies, in advance to
 fortran@cisco.com, basic@cisco.com
 Thank you.
_
banner motd _
   C i s c o S y s t e m s
     ||               ||
     ||               ||       Cisco Systems, Inc.
    ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                     + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.
_
```

```
alias exec scr show run | b crypto isakmp
alias exec wrnet copy run tftp://assembler/vpn/DIRECTORY/XXX5-esevpn-gw5-confg
!
line con 0
 exec-timeout 30 0
line aux 0
line vty 0 4
 login authentication admin
 transport input ssh
line vty 5 15
 login authentication admin
 transport input ssh
!
exception memory minimum 1048576
ntp clock-period 17180642
ntp server 10.1.254.202
ntp server 10.1.254.131
end
```

Remote—DSL Integrated Unit Plus Access

Figure D-2 Sample Deployment—DSL Integrated Unit Plus Access



IPSec SOHO Router

```
! c1700-k9o3sy7-mz.123-3
!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname fortran-vpn
!
boot-start-marker
boot-end-marker
!
logging count
logging buffered 65536 debugging
enable secret 5 [removed]
!
username fortran privilege 15 secret 5 [removed]
username COBOL privilege 15 secret 5 [removed]
memory-size iomem 25
clock timezone est -5
```

```
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
ip tcp path-mtu-discovery
ip telnet source-interface FastEthernet0/0
ip tftp source-interface FastEthernet0/0
ip ftp source-interface FastEthernet0/0
no ip domain lookup
ip domain name cisco.com
ip host assembler xx.xx.129.252
ip host XXX5-esevpn-ca 10.1.0.18
ip name-server xx.xxx.6.247
!
ip dhcp pool Client
   import all
   network 10.1.7.0 255.255.255.248
   default-router 10.1.7.1
   dns-server xx.xxx.6.247 xxx.68.226.120
   domain-name cisco.com
   option 150 ip xx.xxx.2.93
   netbios-name-server xxx.68.235.228 xxx.68.235.229
!
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto ca trustpoint ese-vpn-cert
 enrollment mode ra
 enrollment url http://10.1.0.18:80/certsrv/mscep/mscep.dll
 crl optional
 source interface FastEthernet0/0
 auto-enroll 70
!
crypto ca certificate chain ese-vpn-cert
 certificate 6102B21F000000000010

[removed]


  quit
 certificate ca 36092145BAA631BF4763493E714CD857

[removed]


  quit
!
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
```

```
crypto map RTP 1 ipsec-isakmp
 description RTP Business Ready Teleworker
 set peer xx.xxx.223.24
 set peer xx.xxx.223.25
 set transform-set REPLAY
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
!
!
 class-map match-all VOICE
  match ip dscp ef
 class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
 class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
!
!
 policy-map V3PN-teleworker
  description Note LLQ for ATM/DSL G.729=64K, G.711=128K
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
   priority 128
  class class-default
   fair-queue
   random-detect
 policy-map Shaper
  class class-default
   shape average 182400 1824
   service-policy V3PN-teleworker
!
!
!
interface Ethernet0/0
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 service-policy output Shaper
 ip route-cache flow
 ip tcp adjust-mss 542
 half-duplex
 no cdp enable
 crypto map RTP
!
interface FastEthernet0/0
 description Inside
 ip address 10.1.7.1 255.255.255.248
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 542
 speed auto
 hold-queue 40 out
!
```

Note The dialer and DSL interfaces (ATM1/0) are not in use in this topology and are administratively shutdown. The configuration is shown for reference only.

```
interface ATM1/0
 no ip address
 ip route-cache flow
 load-interval 30
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
 hold-queue 224 in
!
interface ATM1/0.35 point-to-point
 description DSL 256/1.4M
 pvc dsl 0/35
  vbr-nrt 256 256
  tx-ring-limit 3
  service-policy output V3PN-teleworker
  pppoe-client dial-pool-number 1
 !
 crypto map RTP
!
interface Dialer1
 bandwidth 256
 ip address negotiated
 ip access-group INPUT_ACL in
 ip mtu 1492
 ip inspect CBAC in
 encapsulation ppp
 ip tcp adjust-mss 542
 shutdown
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username pascal@clist.com password 7 [removed]
 crypto map RTP
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
ip flow-export version 5
!
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.1.7.0 0.0.0.7 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
 remark Allow IKE and ESP from the RTP headends
 permit udp xx.xxx.223.16 0.0.0.15 any eq isakmp
 permit udp xx.xxx.223.16 0.0.0.15 eq isakmp any
 permit esp xx.xxx.223.16 0.0.0.15 any
 remark Cisco Corporate Subnets (not complete)
 permit ip xxx.68.0.0 0.3.255.255 10.1.7.0 0.0.0.7
 permit ip 172.16.0.0 0.15.255.255 10.1.7.0 0.0.0.7
 permit ip 192.168.0.0 0.0.255.255 10.1.7.0 0.0.0.7
 permit ip 128.107.0.0 0.0.255.255 10.1.7.0 0.0.0.7
 permit ip 64.100.0.0 0.3.255.255 10.1.7.0 0.0.0.7
 permit ip 64.104.0.0 0.0.255.255 10.1.7.0 0.0.0.7
 permit ip 10.0.0.0 0.255.255.255 10.1.7.0 0.0.0.7
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp xxx.5.41.40 0.0.0.1 eq ntp any
```

```
 permit udp host xxx.210.169.40 eq ntp any
 remark SSH from RTP Ridge
 permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any
logging source-interface FastEthernet0/0
access-list 88 permit xx.xx.86.64 0.0.0.63
access-list 88 deny   any log
!
snmp-server community 2dollars RW 88
snmp-server trap-source FastEthernet0/0
snmp-server location fortran Home Office
snmp-server contact fortran@cisco.com
snmp-server enable traps tty
snmp-server host xx.xx.156.10 version 2c assembler
rtr responder
rtr 12
 type echo protocol ipIcmpEcho xx.xx.129.252 source-ipaddr 10.1.7.1
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time now life forever
banner motd _
   C i s c o S y s t e m s
     ||               ||
     ||               ||       Cisco Systems, Inc.
    ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                   + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.
_
alias exec wrnet copy run tftp://assembler/vpn/DIRECTORY/fortran-vpn-confg
alias exec scr show running | b crypto isakmp
alias exec cmf show running | begin voice-port
privilege exec level 0 show crypto isakmp sa
privilege exec level 0 show crypto isakmp
privilege exec level 0 show crypto ipsec sa
privilege exec level 0 show crypto ipsec
privilege exec level 0 show crypto engine connections active
privilege exec level 0 show crypto engine connections
privilege exec level 0 show crypto engine
privilege exec level 0 show crypto
privilege exec level 0 show ip inspect sessions
privilege exec level 0 show ip inspect
privilege exec level 0 show ip nat translations
privilege exec level 0 show ip nat
privilege exec level 0 show ip
privilege exec level 0 show
!
line con 0
 exec-timeout 300 0
 login local
 stopbits 1
line aux 0
 transport input all
 transport output all
 stopbits 1
```

```
line vty 0 4
 exec-timeout 300 0
 login local
 transport input ssh
!
exception memory minimum 786432
ntp clock-period 17180002
ntp server xxx.5.41.41
ntp server xxx.5.41.40
ntp server xxx.210.169.40
ntp server 10.1.254.202 source FastEthernet0/0
!
end
```

Remote—DSL Router / Personal Firewall (Access Router)

```
! Last configuration change at 21:24:12 est Mon Nov 17 2003
! NVRAM config last updated at 21:24:15 est Mon Nov 17 2003
!
! c837-k9o3sy6-mz.123-4.T
version 12.3
no parser cache
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname pascal-FW
!
boot-start-marker
boot-end-marker
!
enable secret 5 [removed]
!
username fortran privilege 15 secret 5 [removed]
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
ip domain lookup source-interface Dialer1
ip domain name pascal.org
!
ip dhcp pool HOME_NETWORK
   import all
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
!
!
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!
no crypto isakmp enable
```

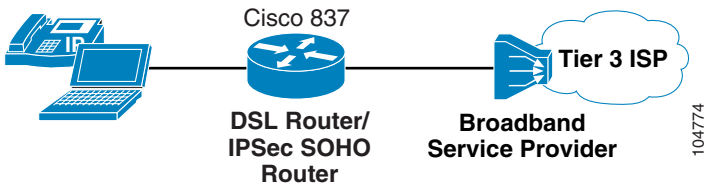
```
!
!
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match access-group name IKE
!
!
policy-map V3PN-teleworker
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 128 6400
 class class-default
  fair-queue
!
!
!
interface Ethernet0
 description Inside
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 hold-queue 40 out
!
interface ATM0
 no ip address
 ip route-cache flow
 no ip mroute-cache
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.35 point-to-point
 description DSL 256K/1.4M
 no ip mroute-cache
 pvc dsl 0/35
  vbr-nrt 256 256
  tx-ring-limit 3
  service-policy output V3PN-teleworker
  pppoe-client dial-pool-number 1
 !
!
interface ATM0.835 point-to-point
 shutdown
 pvc dslX 8/35
  vbr-nrt 256 256
  tx-ring-limit 3
  service-policy output V3PN-teleworker
  pppoe-client dial-pool-number 1
 !
!
interface Dialer1
```

```
 description Outside
 bandwidth 256
 ip address negotiated
 ip access-group INPUT_ACL in
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 ip route-cache flow
 dialer pool 1
 no cdp enable
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username pascal@clist.com password 7 [removed]
 ppp ipcp dns request accept
!
ip nat translation port-timeout udp 500 7200
ip nat inside source list NAT_THIS interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
!
!
ip access-list extended DoS_Input_Queue_Wedge
 remark http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
 deny   53 any any
 deny   55 any any
 deny   77 any any
 deny   pim any any
 permit ip any any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
 remark http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
 deny   53 any any
 deny   55 any any
 deny   77 any any
 deny   pim any any
 remark Allow IKE and ESP from the RTP headends
 permit udp xx.xxx.223.16 0.0.0.15 any eq isakmp
 permit udp xx.xxx.223.16 0.0.0.15 eq isakmp any
 permit esp xx.xxx.223.16 0.0.0.15 any
 remark Allow NTP
 permit udp any eq ntp any eq ntp
 permit udp any eq domain any eq domain
 remark SSH from campus
 permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any
ip access-list extended NAT_THIS
 permit ip 192.168.1.0 0.0.0.255 any
access-list 23 permit 10.10.10.0 0.0.0.255
snmp-server location A House Cary, NC
snmp-server enable traps tty
!
control-plane
!
banner exec ^CC

This is for a 837 running at my access device at home. It terminates
the DSL connection and support IPSec passthru. It includes the workaround
for the IKE re-key issue.

Date: 5 November 2003
```

```
^C
banner motd ^CCC

  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in criminal prosecution
 or death. Your mileage may vary. A pint is a pound the world
 around.

^C
!
line con 0
 exec-timeout 120 0
 no modem enable
 transport preferred all
 transport output all
 stopbits 1
line aux 0
 transport preferred all
 transport output all
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 login local
 transport preferred all
 transport input ssh
 transport output all
!
exception memory minimum 786432
scheduler max-task-time 5000
sntp server xxx.5.41.41
sntp server xxx.5.41.40
!
end
```

Remote—DSL Integrated Unit

Figure D-3 Sample Deployment—DSL Integrated Unit




```
!   c837-k9o3sy6-mz.123-4.T
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname beta837-vpn
!
boot-start-marker
```

```
boot-end-marker
!
memory-size iomem 5
logging buffered 65536 debugging
enable secret 5 [removed]
!
username fortran privilege 15 secret 5 [removed]
username COBOL privilege 15 secret 5 [removed]
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
ip telnet source-interface Ethernet0
ip tftp source-interface Ethernet0
no ip domain lookup
ip domain name cisco.com
ip host assembler xxx.xxx.129.252
ip host XXX5-esevpn-ca 10.1.0.18
ip name-server xxx.69.188.186
ip name-server xxx.69.188.185
ip name-server xxx.xxx.6.247
!
ip dhcp pool Client
   import all
   network 10.1.7.248 255.255.255.248
   default-router 10.1.7.249
   dns-server xx.xxx.6.247 xxx.68.235.229
   domain-name cisco.com
   option 150 ip xx.xxx.2.93
   netbios-name-server xxx.68.235.228 xxx.68.235.229
!
!
ip ftp source-interface Ethernet0
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip audit notify log
ip audit po max-events 100
ip ssh source-interface Ethernet0
no ftp-server write-enable
!
crypto ca trustpoint ese-vpn-cert
 enrollment mode ra
 enrollment url http://10.1.0.18:80/certsrv/mscep/mscep.dll
 revocation-check none
 source interface Ethernet0
 auto-enroll 70
!
!
crypto ca certificate chain ese-vpn-cert
 certificate 610C802200000000000C
 certificate ca 36092145BAA631BF4763493E714CD857
!
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
```

```
crypto map RTP 1 ipsec-isakmp
 description RTP Business Ready Teleworker
 set peer xx.xxx.223.24
 set peer xx.xxx.223.25
 set transform-set REPLAY
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
!
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match access-group name IKE
!
!
policy-map V3PN-teleworker
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 128 6400
 class class-default
  fair-queue
  random-detect
!
!
!
interface Ethernet0
 description Inside
 ip address 10.1.7.249 255.255.255.248
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 542
 no ip mroute-cache
 load-interval 30
 no cdp enable
 hold-queue 40 out
!
interface ATM0
 no ip address
 ip route-cache flow
 no ip mroute-cache
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.35 point-to-point
 description DSL 256K/1.4M
 no ip mroute-cache
 pvc dsl 0/35
  vbr-nrt 256 256
  tx-ring-limit 3
  service-policy output V3PN-teleworker
  pppoe-client dial-pool-number 1
 !
!
interface Dialer1
```

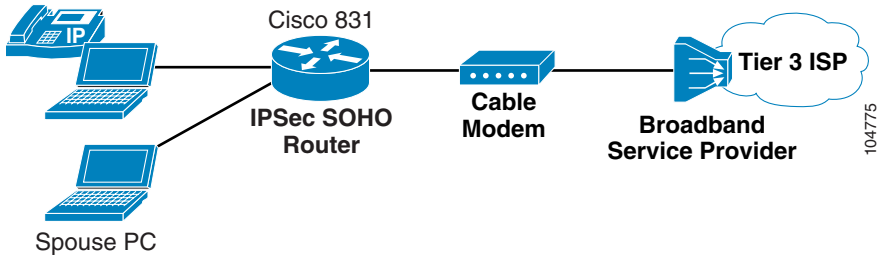
```
 description Outside
 bandwidth 256
 ip address negotiated
 ip access-group INPUT_ACL in
 ip mtu 1492
 encapsulation ppp
 ip tcp adjust-mss 542
 no ip mroute-cache
 load-interval 30
 dialer pool 1
 no cdp enable
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username pascal@clist.com password 7 [removed]
 crypto map RTP
 hold-queue 32 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
ip flow-export version 5
ip flow-export destination 10.1.7.251 7777
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.1.7.248 0.0.0.7 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
 remark Allow IKE and ESP from the RTP headends
 permit udp xx.xxx.223.16 0.0.0.15 any eq isakmp
 permit udp xx.xxx.223.16 0.0.0.15 eq isakmp any
 permit esp xx.xxx.223.16 0.0.0.15 any
 remark Cisco Corporate Subnets (not complete)
 permit ip xxx.68.0.0 0.3.255.255 10.1.7.248 0.0.0.7
 permit ip xxx.16.0.0 0.15.255.255 10.1.7.248 0.0.0.7
 permit ip xxx.168.0.0 0.0.255.255 10.1.7.248 0.0.0.7
 permit ip xxx.107.0.0 0.0.255.255 10.1.7.248 0.0.0.7
 permit ip xxx.100.0.0 0.3.255.255 10.1.7.248 0.0.0.7
 permit ip xxx.104.0.0 0.0.255.255 10.1.7.248 0.0.0.7
 permit ip 10.0.0.0 0.255.255.255 10.1.7.248 0.0.0.7
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp xxx.5.41.40 0.0.0.1 eq ntp any
 permit udp host xxx.210.169.40 eq ntp any
 remark SSH
 permit tcp xxx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any
logging source-interface Ethernet0
access-list 88 permit xxx.xxx.18.178
access-list 88 permit xxx.xxx.86.64 0.0.0.63
access-list 88 deny any log
snmp-server community 2dollars RW 88
snmp-server trap-source Ethernet0
snmp-server location beta837 Home Office
snmp-server contact beta837@cisco.com
snmp-server enable traps tty
no cdp run
!
control-plane
!
rtr responder
```

```
rtr 12
 type echo protocol ipIcmpEcho xx.xx.129.252 source-ipaddr 10.1.7.249
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 life forever start-time now
rtr 20
 type jitter dest-ipaddr xx.xxx.223.23 dest-port 2020 source-ipaddr 10.1.7.249 codec g729a
advantage-factor 5
 tos 184
rtr schedule 20 life forever start-time now
banner motd ^C
   C i s c o S y s t e m s
     ||               ||
     ||               ||       Cisco Systems, Inc.
    ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                   + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.
^C
alias exec xa crypto ipsec client ezvpn xauth
alias exec scr show running | b crypto isakmp
alias exec wrnet copy run tftp://assembler/vpn/DIRECTORY/beta837-vpn-confg
privilege exec level 0 show crypto isakmp sa
privilege exec level 0 show crypto isakmp
privilege exec level 0 show crypto ipsec sa
privilege exec level 0 show crypto ipsec
privilege exec level 0 show crypto engine connections active
privilege exec level 0 show crypto engine connections
privilege exec level 0 show crypto engine
privilege exec level 0 show crypto
privilege exec level 0 show ip inspect sessions
privilege exec level 0 show ip inspect
privilege exec level 0 show ip nat translations
privilege exec level 0 show ip nat
privilege exec level 0 show ip
privilege exec level 0 show
!
line con 0
 exec-timeout 0 0
 login local
 no modem enable
 transport preferred all
 transport output all
 stopbits 1
line aux 0
 transport preferred all
 transport output all
 stopbits 1
line vty 0 4
 exec-timeout 240 0
 login local
 transport preferred all
 transport input ssh
 transport output all
!
exception memory minimum 786432
```

```
scheduler max-task-time 5000
sntp server xxx.5.41.41
sntp server xxx.5.41.40
sntp server xxx.210.169.40
!
end
```

Remote—Cable Integrated Unit Plus Access with 802.1X

Figure D-4 Sample Deployment—Cable Integrated Unit Plus Access




```
!  c831-k9o3sy6-mz.123-2.XA
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname rexx-vpn
!
boot system flash c831-k9o3sy6-mz.123-2.XA
logging buffered 4096 debugging
enable secret 5 [removed]
!
username fortran privilege 15 secret 5 [removed]
username COBOL privilege 15 secret 5 [removed]
clock timezone est -5
clock summer-time edt recurring
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa session-id common
ip subnet-zero
ip telnet source-interface Ethernet0
ip tftp source-interface Ethernet0
no ip domain lookup
ip domain name cisco.com
ip host XXX5-esevpn-radius 10.1.0.19
ip host XXX5-esevpn-ca 10.1.0.18
ip host assembler xxx.xxx.129.252
ip name-server xxx.xxx.6.247
ip name-server xxx.69.188.185
!
ip dhcp pool Client
   import all
   network 10.1.7.96 255.255.255.248
   default-router 10.1.7.97
   dns-server xxx.xxx.6.247 xxx.68.226.120
   domain-name cisco.com
```

```
   option 150 ip xx.xxx.2.93
   netbios-name-server xxx.68.235.228 xxx.68.235.229
!
ip dhcp pool NONCORPUSER
   import all
   network 192.168.99.0 255.255.255.0
   default-router 192.168.99.1
   domain-name NONCORPUSER.org
!
!
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip audit notify log
ip audit po max-events 100
ip ssh source-interface Ethernet0
no ftp-server write-enable
!
template Virtual-Template1
!
!
crypto ca trustpoint ese-vpn-cert
 enrollment mode ra
 enrollment url http://10.1.0.18:80/certsrv/mscep/mscep.dll
 revocation-check none
 source interface Ethernet0
 auto-enroll 70
!
!
crypto ca certificate chain ese-vpn-cert
 certificate 6105C7AC000000000024

[removed]


  quit
 certificate ca 36092145BAA631BF4763493E714CD857

[removed]


  quit
!
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto map RTP 1 ipsec-isakmp
 description RTP Business Ready Teleworker
 set peer xxx.xxx.223.24
 set peer xxx.xxx.223.25
 set transform-set REPLAY
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
dot1x system-auth-control
identity profile default
```

```
 description 802.1x configuration
 template Virtual-Template1
 device authorize type cisco ip phone
!
!
 class-map match-all VOICE
  match ip dscp ef
 class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
 class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
!
!
 policy-map V3PN-teleworker
  description Note LLQ for ATM/DSL G.729=64K, G.711=128K
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
   priority 128
  class class-default
   fair-queue
   random-detect
 policy-map Shaper
  class class-default
   shape average 182400 1824
   service-policy V3PN-teleworker
!
!
!
interface Loopback0
 description NONCORPUSER inside interface
 ip address 192.168.99.1 255.255.255.0
!
interface Ethernet0
 description Inside
 ip address 10.1.7.97 255.255.255.248
 ip nat inside
 ip route-cache flow
 ip tcp adjust-mss 542
 dot1x port-control auto
 dot1x reauthentication
 hold-queue 40 out
!
interface Ethernet1
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 ip nat outside
 ip inspect CBAC out
 service-policy output Shaper
 ip route-cache flow
 ip tcp adjust-mss 542
 duplex auto
 no cdp enable
 crypto map RTP
!
interface Virtual-Template1
 description This will spawn a virtual-access for each non-authorized non-CORPUSER
 ip unnumbered Loopback0
 ip nat inside
```

```
 ip tcp adjust-mss 542
!
interface Dialer1
 no ip address
!
ip nat inside source list NoNatACL interface Ethernet1 overload
ip classless
no ip http server
no ip http secure-server
ip flow-export version 5
!
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.1.7.96 0.0.0.7 any
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
 remark Allow IKE and ESP from the RTP headends
 permit udp xxx.xxx.223.16 0.0.0.15 any eq isakmp
 permit udp xxx.xxx.223.16 0.0.0.15 eq isakmp any
 permit esp xxx.xxx.223.16 0.0.0.15 any
 permit ip xxx.68.0.0 0.3.255.255 10.1.7.96 0.0.0.7
 permit ip xxx.16.0.0 0.15.255.255 10.1.7.96 0.0.0.7
 permit ip xxx.168.0.0 0.0.255.255 10.1.7.96 0.0.0.7
 permit ip xxx.107.0.0 0.0.255.255 10.1.7.96 0.0.0.7
 permit ip xxx.100.0.0 0.3.255.255 10.1.7.96 0.0.0.7
 permit ip xxx.104.0.0 0.0.255.255 10.1.7.96 0.0.0.7
 permit ip xxx.0.0.0 0.255.255.255 10.1.7.96 0.0.0.7
 permit ip xxx.44.0.0 0.0.255.255 10.1.7.96 0.0.0.7
 permit udp any any eq bootpc
 remark NTP ACLs
 permit udp xxx.5.41.40 0.0.0.1 eq ntp any
 permit udp host xxx.210.169.40 eq ntp any
 remark SSH from RTP [removed]
 permit tcp xxx.xxx.87.0 0.0.0.255 any eq 22
 permit icmp any any
 deny   ip any any
ip access-list extended NoNatACL
 remark This ACL is a filter of which traffic is to be NAT/PATed for the Internet
 remark Only the Spouse will be allowed to the Internet directly, the employee
 remark will go to the HQ location to get Internet access.
 permit ip xxx.168.99.0 0.0.0.255 any
ip radius source-interface Ethernet0
logging source-interface Ethernet0
access-list 88 permit xx.xxx.18.178
access-list 88 permit xxx.xx.86.64 0.0.0.63
access-list 88 deny   any log
snmp-server community 2dollars RW 88
snmp-server trap-source Ethernet0
snmp-server location rexx Home Office
snmp-server contact rexx@cisco.com
snmp-server enable traps tty
radius-server host 10.1.0.19 auth-port 1645 acct-port 1646
radius-server key 7 [removed]
rtr responder
rtr 12
 type echo protocol ipIcmpEcho xxx.xxx.129.252 source-ipaddr 10.1.7.97
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time now life forever
```

```
banner exec _
 Commands for showing and debugging 802.1x connections:
 To show the current 802.1x clients:
    "show dot1x interface e0 details" - to show the 802.1x timers and user states
    "show arp"  - to show the MAC to IP mappings
 Clearing out the current 802.1x clients:
    "clear dot1x all" - to dump all authentications.
 Debugging
    "debug dot1x all" - verbose debug for all 802.1x related authentication communications
_
banner motd _
   C i s c o S y s t e m s
     ||               ||
     ||               ||       Cisco Systems, Inc.
    ||||             ||||      IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                     + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.
_
alias exec scr show running | b crypto isakmp
alias exec wrnet copy run tftp://assembler/vpn/DIRECTORY/rexx-vpn-confg
privilege exec level 0 show crypto isakmp sa
privilege exec level 0 show crypto isakmp
privilege exec level 0 show crypto ipsec sa
privilege exec level 0 show crypto ipsec
privilege exec level 0 show crypto engine connections active
privilege exec level 0 show crypto engine connections
privilege exec level 0 show crypto engine
privilege exec level 0 show crypto
privilege exec level 0 show ip inspect sessions
privilege exec level 0 show ip inspect
privilege exec level 0 show ip nat translations
privilege exec level 0 show ip nat
privilege exec level 0 show ip
privilege exec level 0 show
privilege exec level 0 clear dot1x all
privilege exec level 0 clear dot1x
privilege exec level 0 clear
!
line con 0
 no modem enable
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport input ssh
!
exception memory minimum 786432
scheduler max-task-time 5000
ntp clock-period 17180001
ntp server xxx.5.41.41
ntp server xxx.5.41.40
ntp server xxx.210.169.40
ntp server 10.1.254.202 source Ethernet0
!
end
```

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X