IP Tunneling and VPNs

Overview

The purpose of this module is to explain Virtual Private Network (VPN) concepts and to overview various L2 and L3 tunneling techniques that allow for implementation of VPNs. The access VPN features in Cisco IOS Release 12.1 are explained along with Layer 2 and Layer 3 tunneling mechanisms.

Objectives

Upon completion of this module, you will be able to perform the following tasks:

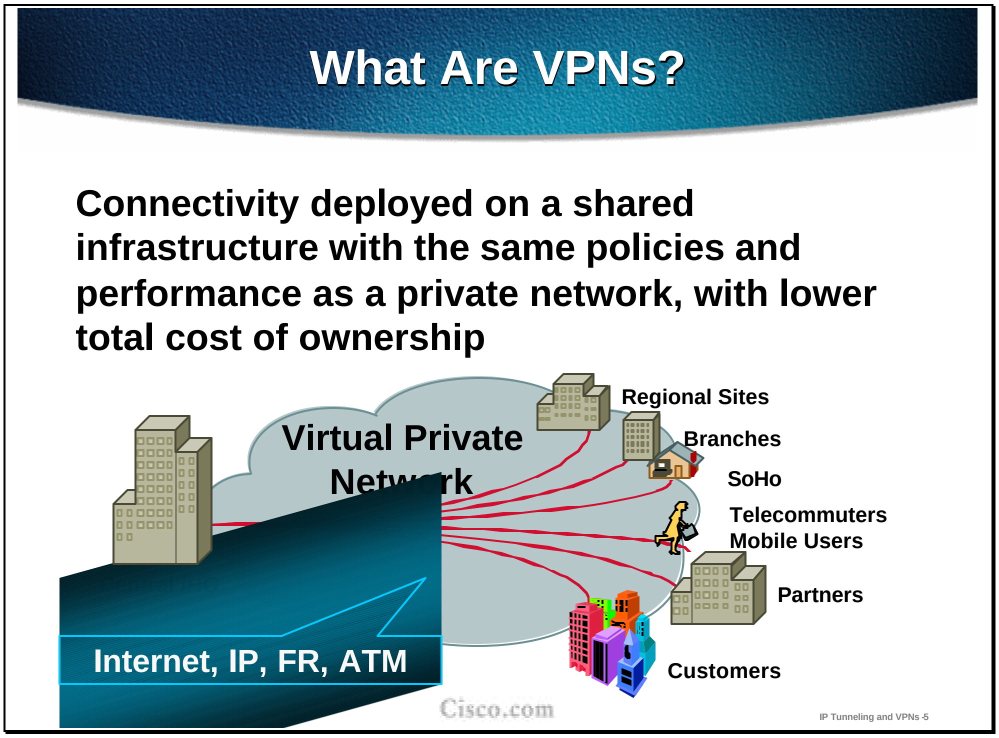
- Explain Virtual Private Network concepts and possibilities
- Describe Layer-2 tunneling features
- Configure support for Microsoft Point-to-Point Tunneling Protocol (PPTP) and Encryption (MPPE)
- Configure L2TP Dial-in and Virtual Private Dial-up Network (VPDN) for dial-in
- Describe and configure GRE Layer-3 tunneling

Introduction to IP VPNs

Objectives

Upon completion of this module, you will be able to perform the following tasks:

- Define a Virtual Private Network (VPN) and its benefits
- Describe the various types of VPNs:
  - Access, intranet, extranet
  - Layer 2 versus Layer 3
  - Carrier-provided versus not



What Are VPNs?

Connectivity deployed on a shared infrastructure with the same policies and performance as a private network, with lower total cost of ownership

Virtual Private Network

Internet, IP, FR, ATM

Regional Sites

Branches

SoHo

Telecommuters
Mobile Users

Partners

Customers

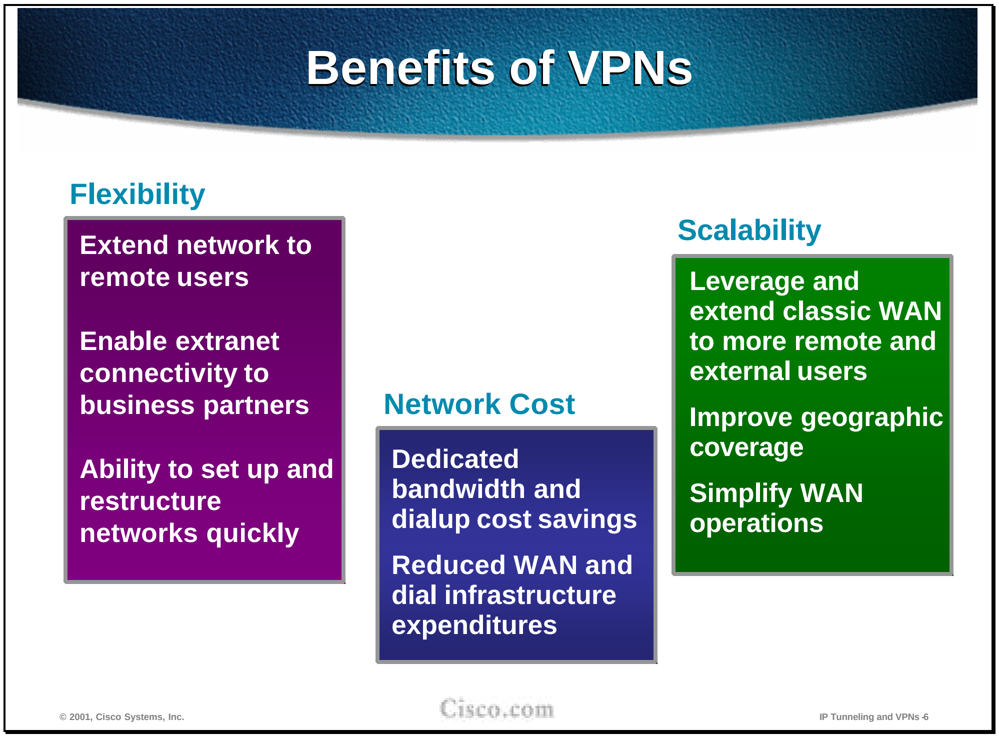
Cisco.com

IP Tunneling and VPNs -5

We will start by defining a VPN.

An academic definition of a VPN is “connectivity deployed on a shared infrastructure with the same policies and performance as a private network, with lower total cost of ownership.”

The infrastructure is public, and can be either the Internet, an IP infrastructure, a Frame Relay network, or an Asynchronous Transfer Mode (ATM) WAN. Our focus today is on the big “I,” the public Internet and IP VPNs, to the exclusion of Frame Relay and ATM.



Benefits of VPNs

Flexibility

Extend network to remote users

Enable extranet connectivity to business partners

Ability to set up and restructure networks quickly

Network Cost

Dedicated bandwidth and dialup cost savings

Reduced WAN and dial infrastructure expenditures

Scalability

Leverage and extend classic WAN to more remote and external users

Improve geographic coverage

Simplify WAN operations

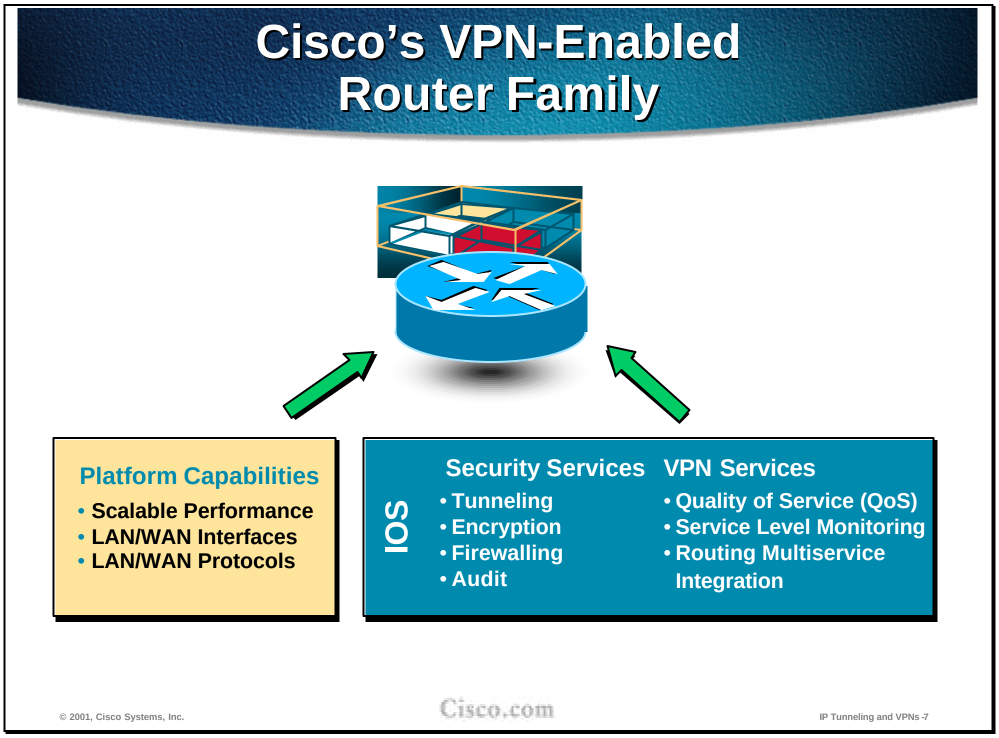
© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-6

The slide lists some of the benefits of VPNs, which are primarily flexibility, scalability, and lowered cost of communication.

VPNs offer flexiblity as site-to-site and remote-access connections can be set up quickly and over existing infrastructure. A variety of security policies can be provisioned in a VPN, enabling flexible interconnection of different security domains.

VPNs also offer scalability over large areas, as IP transport is universally available. This in turn reduces the number of physical connections and simplifies the underlying structure of a customer WAN.

Lower cost is one of the main reasons for migrating from traditional connectivity options to a VPN connection, as customers may reuse existing links and take advantage of statistical packet multiplexing features of IP networks, used as a VPN transport.



Cisco's VPN-Enabled Router Family

Platform Capabilities

- Scalable Performance
- LAN/WAN Interfaces
- LAN/WAN Protocols

IOS

Security Services

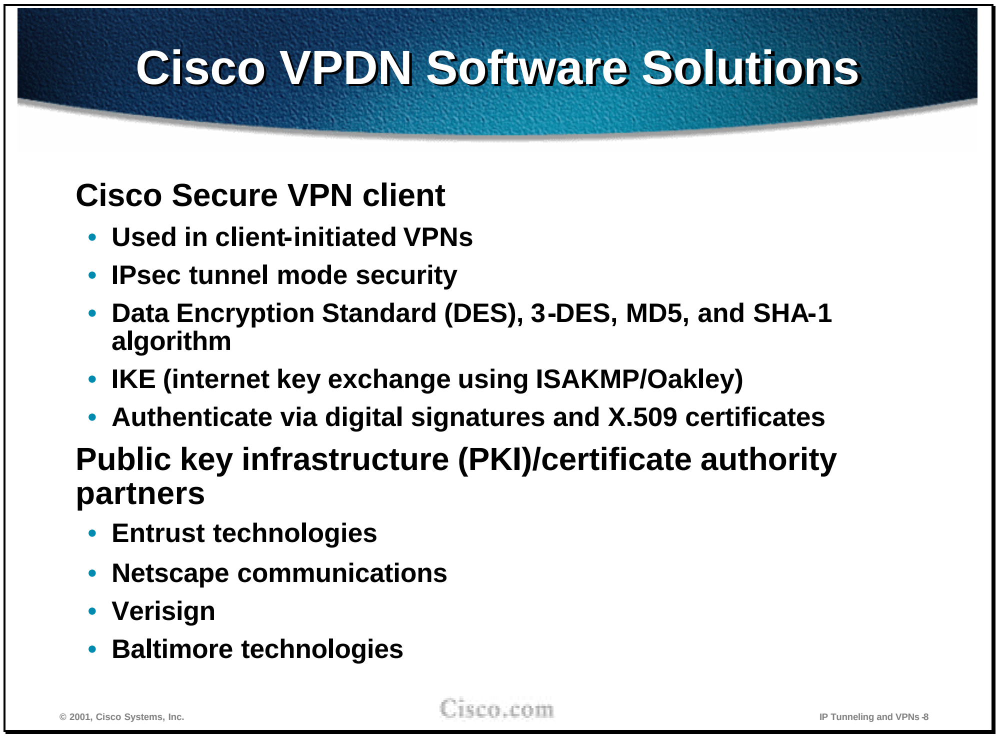
- Tunneling
- Encryption
- Firewalling
- Audit

VPN Services

- Quality of Service (QoS)
- Service Level Monitoring
- Routing Multiservice Integration

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs -7

The Cisco hardware and Cisco IOS software provide a full set of VPN tools, not only for just VPNs but for security, management, and all related needs.



Cisco VPDN Software Solutions

Cisco Secure VPN client

- Used in client-initiated VPNs
- IPsec tunnel mode security
- Data Encryption Standard (DES), 3-DES, MD5, and SHA-1 algorithm
- IKE (internet key exchange using ISAKMP/Oakley)
- Authenticate via digital signatures and X.509 certificates

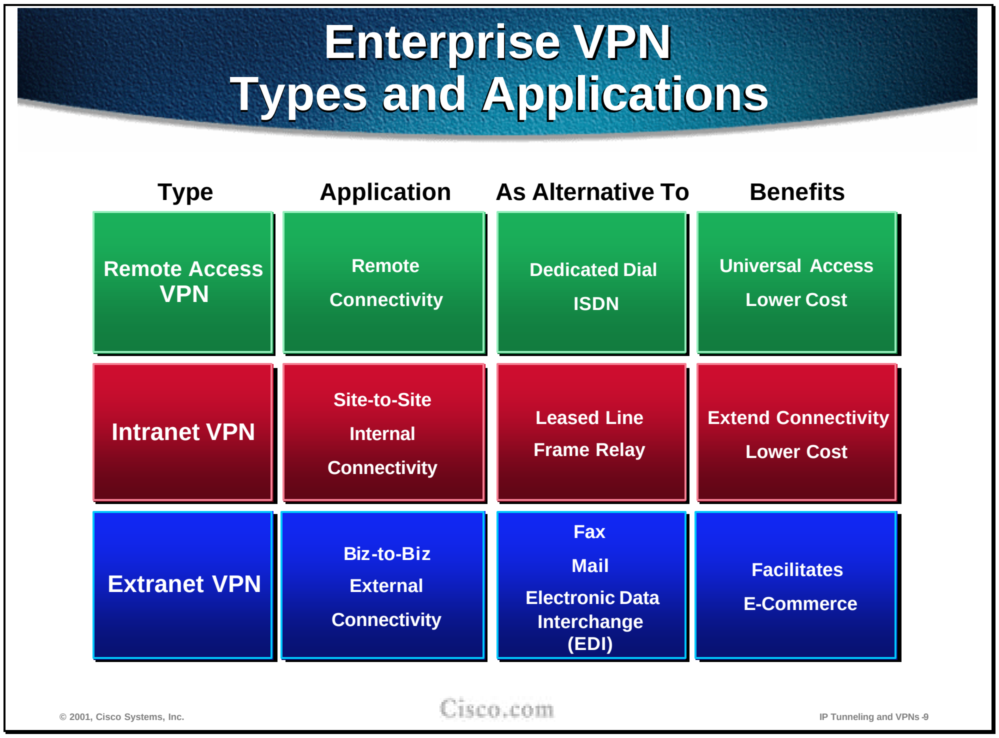
Public key infrastructure (PKI)/certificate authority partners

- Entrust technologies
- Netscape communications
- Verisign
- Baltimore technologies

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-8

The Cisco remote access line of routers is compatible with the Cisco Secure VPN Client PC client software. The slide lists some of the IPSec capabilities one would expect (and find) in such a client. Some of these will be covered in more detail in the next module on IPSec-based VPNs.

With client IPSec encryption, a public Internet connection can be used as part of a virtual private dial-up network (VPDN) solution.



Enterprise VPN Types and Applications

Type	Application	As Alternative To	Benefits
Remote Access VPN	Remote Connectivity	Dedicated Dial ISDN	Universal Access Lower Cost
Intranet VPN	Site-to-Site Internal Connectivity	Leased Line Frame Relay	Extend Connectivity Lower Cost
Extranet VPN	Biz-to-Biz External Connectivity	Fax Mail Electronic Data Interchange (EDI)	Facilitates E-Commerce

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs -9

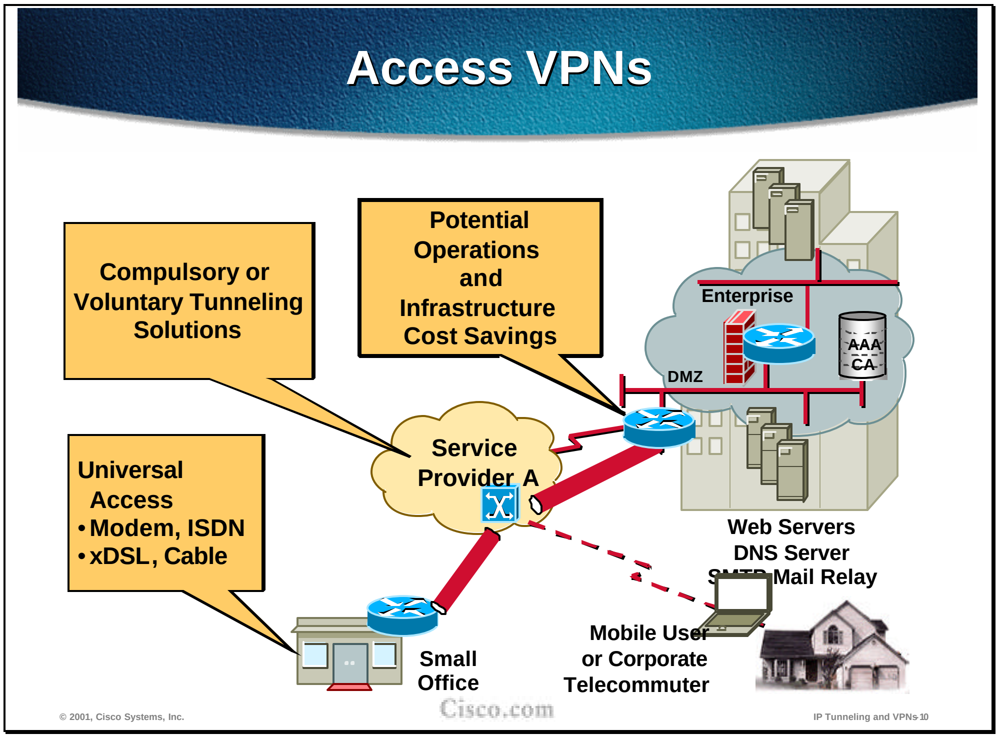
VPNs come in a number of flavors.

VPNs are designed based on one of two architectural options—client-initiated or network access server (NAS)-initiated VPNs.

Client-initiated VPNs—Users establish a tunnel across the Internet service provider (ISP) shared network to the customer network. The customer manages the client software that initiates the tunnel. The main advantage of client-initiated VPNs is that they secure the connection between the client and ISP. However, client-initiated VPNs are not as scalable and are more complex than NAS-initiated VPNs.

NAS-initiated VPNs—Users dial in to the ISP NAS, which establishes a tunnel to the private network. Network access server (NAS)-initiated VPNs are more robust than client-initiated VPNs and do not require the client to maintain the tunnel-creating software. NAS-initiated VPNs do not encrypt the connection between the client and the ISP, but this is not a concern for most customers because the Public Switched Telephone Network (PSTN) is much more secure than the Internet.

VPNs can also run from a remote client PC or remote office router across the Internet or an IP service provider network to one or more corporate gateway routers. VPNs between a company's offices are a company intranet. VPNs to external business partners are extranets.



Access VPNs

Compulsory or Voluntary Tunneling Solutions

Potential Operations and Infrastructure Cost Savings

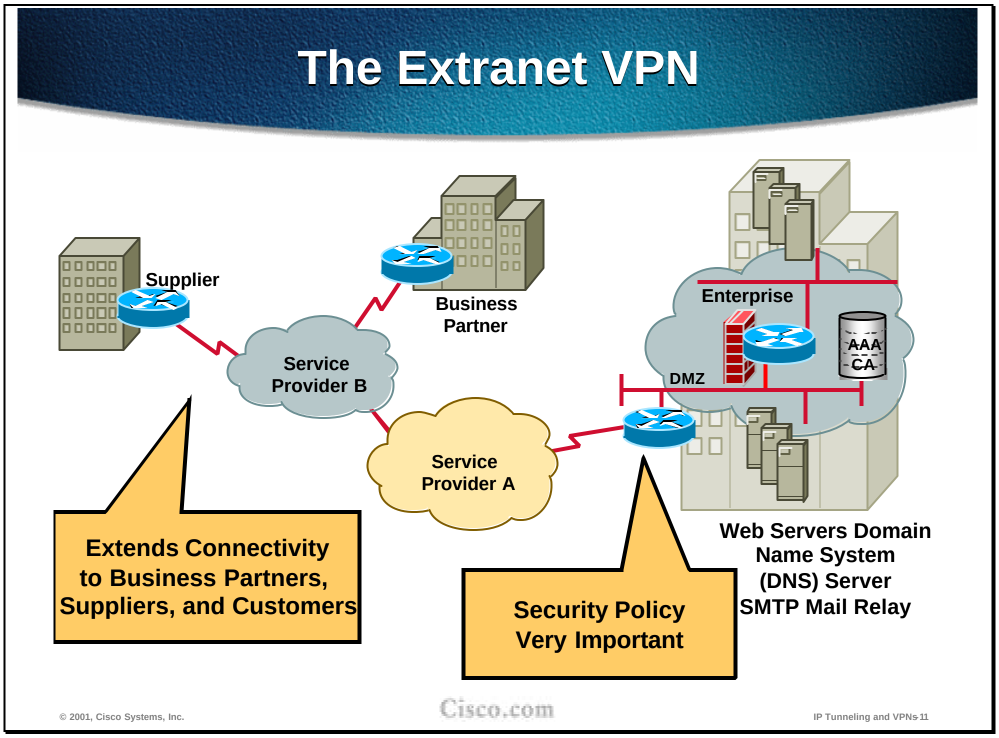
Universal Access
- Modem, ISDN
- xDSL, Cable

IP Tunneling and VPNs-10

Voluntary tunnels are those initiated by the client PC. Voluntary tunnels are ones where the client voluntarily starts up the tunnel. Compulsory tunnels take service provider participation and awareness. Compulsory tunnels leave the client no choice.

The slide shows some of the features of (remote) access VPNs. They can be used with whatever access is available, and ubiquity is important. This means they should work with modem, Integrated Service Digital Network (ISDN), xDSL, or cable. They provide potential operations and infrastructure cost savings because a company can outsource its dial plant, getting out of the remote access server business.

It is best if VPDN and access VPN connectivity involves only a single ISP. With more than one ISP involved, no service level agreements are possible.



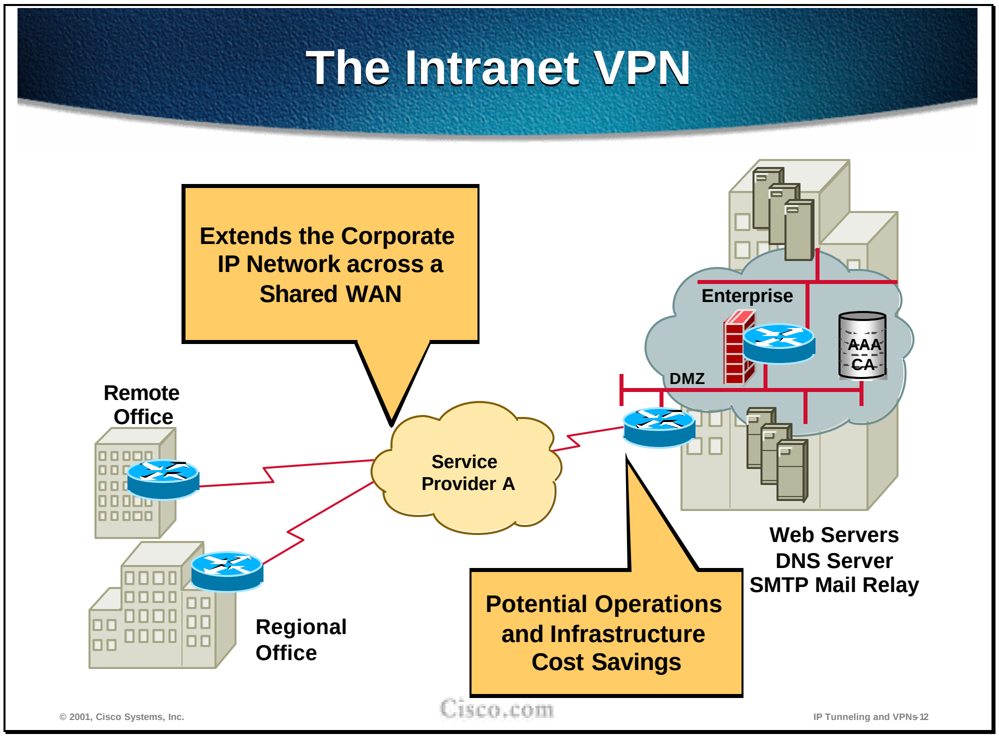
The Extranet VPN

Extends Connectivity to Business Partners, Suppliers, and Customers

Security Policy Very Important

Web Servers Domain Name System (DNS) Server SMTP Mail Relay

An extranet is where you also use the Internet or one or two SPs to connect to business partners. Security policy becomes very important at this point, because you would hate for a hacker to spoof an order for 1 million widgets from a business partner.



The Intranet VPN

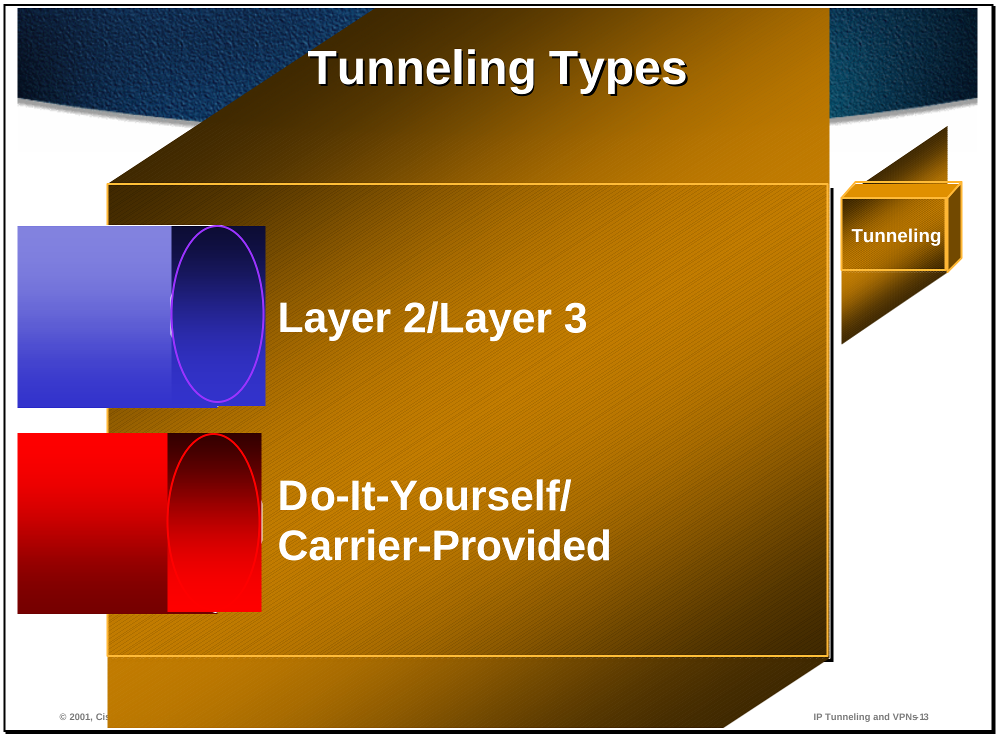
Extends the Corporate IP Network across a Shared WAN

Potential Operations and Infrastructure Cost Savings

Intranet VPNs extend the basic remote access VPN to other corporate offices with connectivity across the Internet or across the SP IP backbone. Service levels are likely to be maintained and enforced within a single SP. With VPNs across the Internet, there are no performance guarantees—no one is in charge of the Internet.

The main attractions of intranet VPNs are reduced WAN infrastructure needs, lower ongoing leased line or Frame Relay charges, and operational savings.

Security on shared media (the Internet or SP backbone) is important too.



Tunneling Types

Layer 2/Layer 3

Do-It-Yourself/ Carrier-Provided

© 2001, Ci

IP Tunneling and VPNs-13

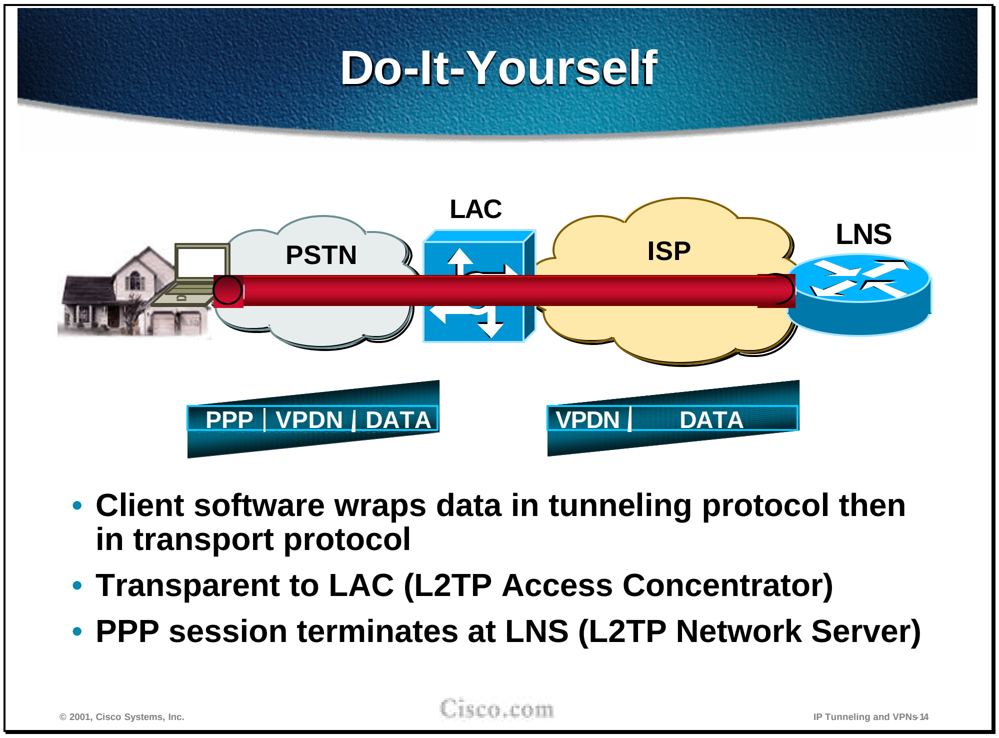
Most VPNs are really tunnels, whereby Point-to-Point Protocol (PPP) frames or IP packets are tunneled inside some other protocol.

Microsoft Point-to-Point Tunneling Protocol (PPTP) (see the Layer 2 module) is a Layer 2 technique, where IP is used to encapsulate and transport PPP and IP packets to a corporate gateway or server.

Cisco Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP) are also Layer 2 techniques. They simulate PPP connectivity directly from a client PC to a corporate gateway router or server.

Multiprotocol Label Switching (MPLS) (see the module), generic routing encapsulation (GRE), and IPSec are, however, Layer 3 tunnels, where Layer 3 information is transported directly inside another Layer 3 header across the intervening SP network.

The terms Layer 2 and Layer 3 may be imprecise when applied to VPNs. Some people consider Frame Relay and ATM to be Layer 2 VPNs. Others consider that to be an out-of-date usage of the term “VPN.”



Do-It-Yourself

- Client software wraps data in tunneling protocol then in transport protocol
- Transparent to LAC (L2TP Access Concentrator)
- PPP session terminates at LNS (L2TP Network Server)

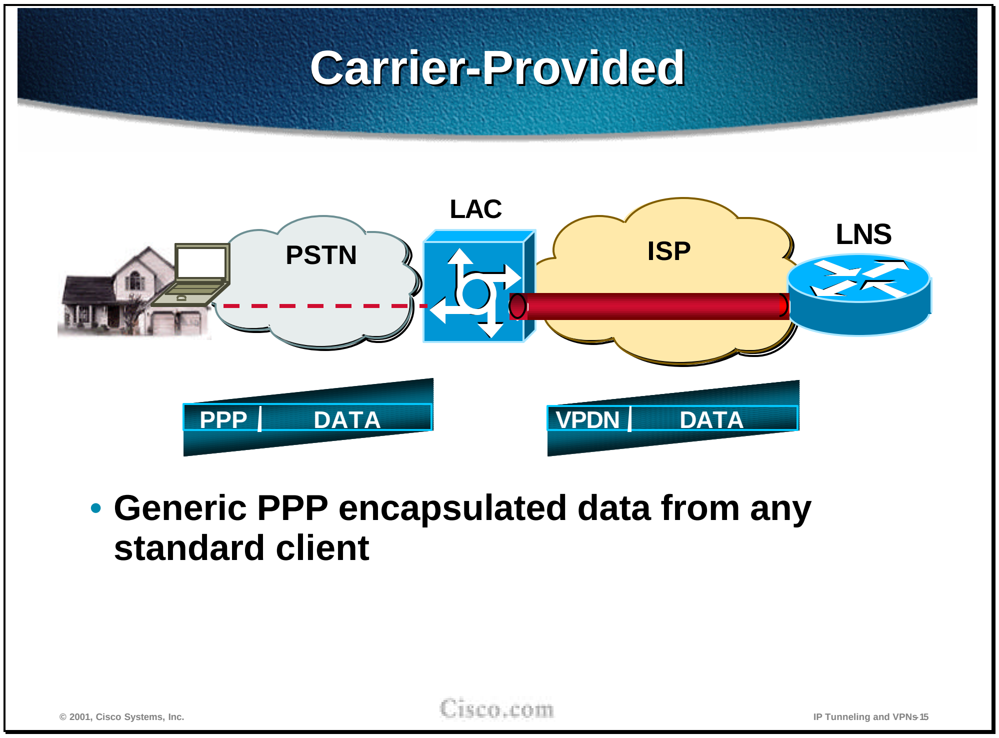
© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-14

Do-it-yourself or voluntary tunnels are those using techniques such as PPTP or IPSec where the tunnel extends from the client PC all the way across the SP network to the corporate gateway.

The actual overhead depends on what client software is in use. Generally, PPP + IP encapsulate the VPDN header (which might be another PPP and IP header) and payload data being sent to the L2TP Access Concentrator (LAC). The LAC strips off the outer PPP and IP routing transports the IP header, VPDN header, and payload to the corporate gateway.

Terminology:

- VPDN—virtual private dial-up network
- Voluntary tunnel—client-initiated



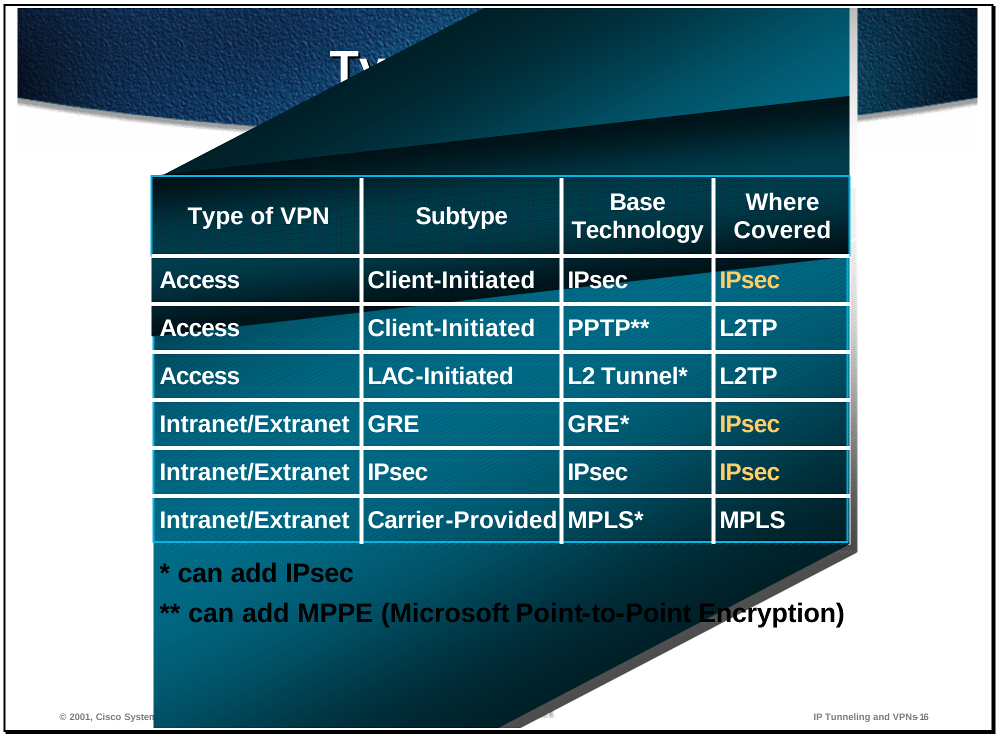
Carrier-Provided

- Generic PPP encapsulated data from any standard client

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs 15

Carrier-Provided tunnels are where the Carrier or service provider does the work. The main advantage is that the corporate IT staff does not have to install and maintain client PC software on large numbers of client PCs. These are also known as compulsory tunnels—the end-user has no choice in the matter.

Generally, the client sends PPP, IP header, and payload data to the LAC. The LAC may tunnel all of this, as with L2TP, or it may strip off the PPP header and use IP routing to deliver the data.



Ty

Type of VPN	Subtype	Base Technology	Where Covered
Access	Client-Initiated	IPsec	IPsec
Access	Client-Initiated	PPTP**	L2TP
Access	LAC-Initiated	L2 Tunnel*	L2TP
Intranet/Extranet	GRE	GRE*	IPsec
Intranet/Extranet	IPsec	IPsec	IPsec
Intranet/Extranet	Carrier-Provided	MPLS*	MPLS

* can add IPsec

** can add MPPE (Microsoft Point-to-Point Encryption)

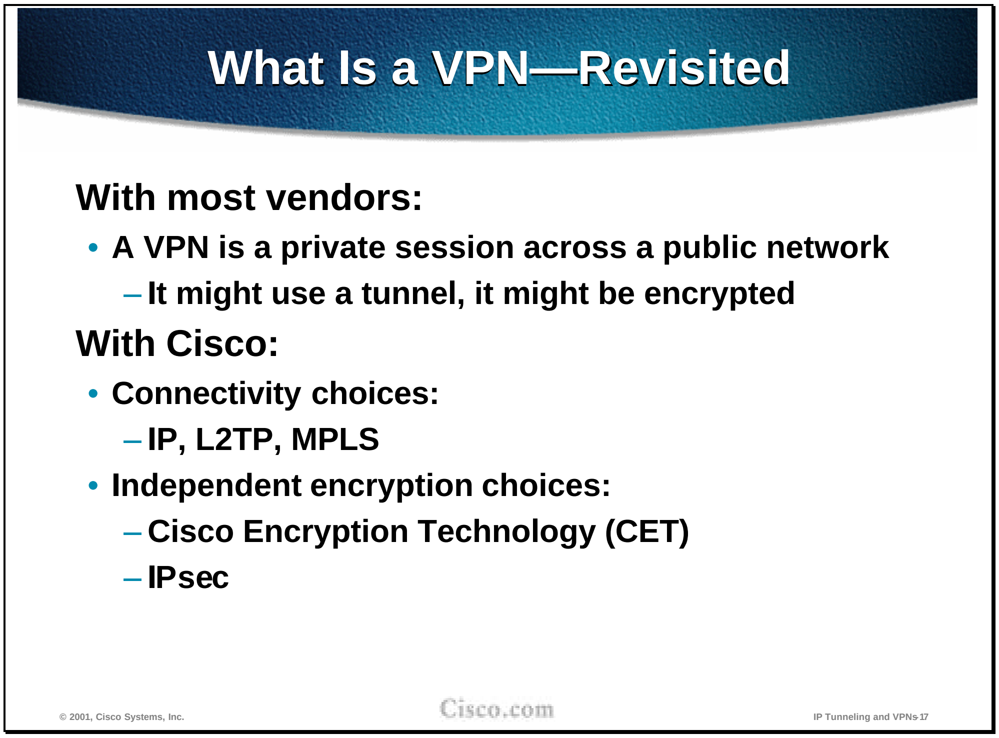
© 2001, Cisco Systen

IP Tunneling and VPNs-16

The chart in the slide breaks out various VPN tunneling and other technologies covered in the following modules. Note that IPSec can be added for IP security even on top of other IP tunneling technologies.

The protocols used to transport Layer 2 frames and Layer-3 packets are:

- L2TP —Layer 2 Tunneling Protocol
- GRE – Generic Route Encapsulation
- PPTP – Point-to-Point Tunneling Protocol
- IPsec – IP security protocols
- MPLS – Multi Protocol Label Switching



What Is a VPN—Revisited

With most vendors:

- **A VPN is a private session across a public network**
  - **It might use a tunnel, it might be encrypted**

With Cisco:

- **Connectivity choices:**
  - **IP, L2TP, MPLS**
- **Independent encryption choices:**
  - **Cisco Encryption Technology (CET)**
  - **IPsec**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-17

We will also see a small pattern in what follows. With Cisco VPNs, there are two somewhat unrelated emphases. First, you must establish connectivity. Then you independently may elect to use some form of encryption for security and data privacy.

Summary

- A VPN is connectivity deployed on a shared infrastructure with the same policies and performance as a private network, with lower total cost of ownership.
- A VPN has more flexibility, is more scalable, and more cost-effective than traditional dedicated links or dial connections
- Access VPNs enable remote client access over a shared infrastructure. An extranet VPN is where you also use the Internet or one or more SPs to connect to business partners. Intranet VPNs extend the basic remote access VPN to other corporate offices with connectivity across the Internet or across the SP IP backbone.
- VPNs can be Layer-2, where a Layer-2 protocol (usually PPP) is tunneled over a Layer-3 (usually IP) network, or Layer-3, where a routed protocol (IP, IPX, DECnet, etc.) is tunneled over a Layer-3 network (usually IP).
- VPNs can be provisioned by the service provider or by the end-user

Lesson Review

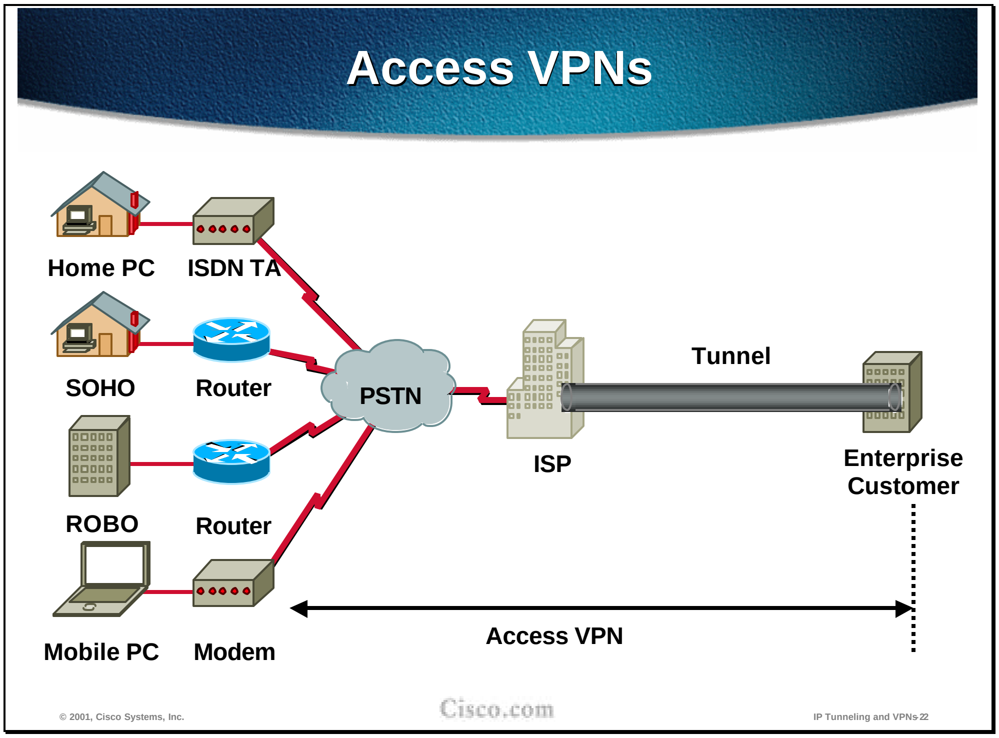
1. What is a VPN?
2. What are the three main benefits of using a VPN?
3. What are the three main VPN deployment scenarios?
4. Which different tunneling philosophies can be used in a VPN?

IP Layer 2 Tunneling

Objectives

After completing this module, you should be able to perform the following tasks:

- Define Layer-2 Access VPNs
- Describe Layer-2 Access VPN technology
- Configure AAA security and virtual dial-in interfaces

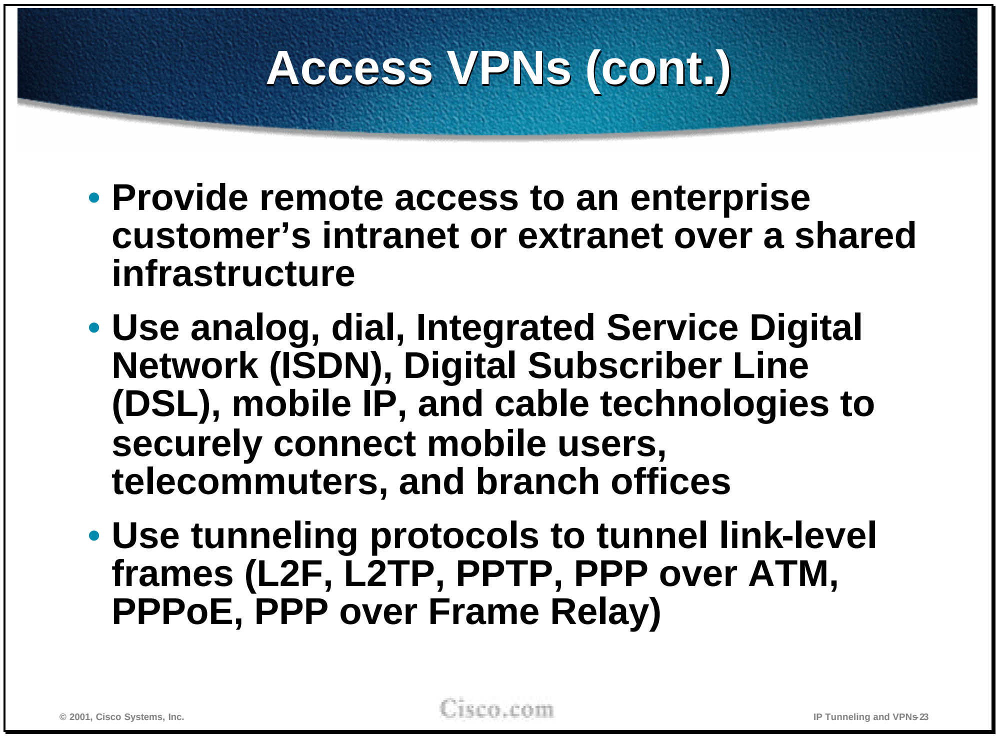


Access VPNs

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-22

Access VPNs utilize access technologies to allow remote users to become part of a corporate VPN.

This usually involves the use of the Point-to-Point Protocol (PPP) and tunnels that extend the PPP connection from the access server to the corporate network. With Microsoft Point-to-Point Tunneling Protocol (PPTP), it also extends the tunnel from the access server out to the end-user PC.



Access VPNs (cont.)

- Provide remote access to an enterprise customer’s intranet or extranet over a shared infrastructure
- Use analog, dial, Integrated Service Digital Network (ISDN), Digital Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, and branch offices
- Use tunneling protocols to tunnel link-level frames (L2F, L2TP, PPTP, PPP over ATM, PPPoE, PPP over Frame Relay)

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-23

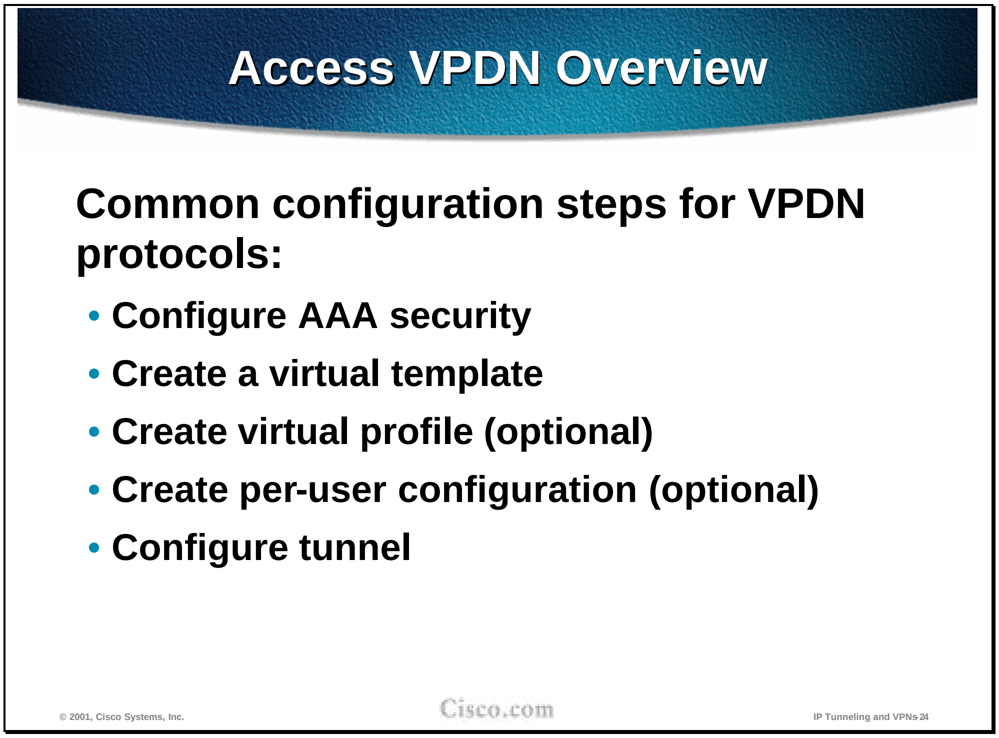
Virtual private dial-up networking (VPDN) enables users to configure secure networks that rely upon Internet service providers (ISPs) to tunnel a company’s remote access traffic through their ISP cloud.

Remote offices or mobile users can connect to their corporate network using local dialup services of third parties. The dialup service provider agrees to forward the company’s traffic from the ISP’s point of presence (POP) to a company-run home gateway. Network configuration and security remains in the control of the client. The dialup service provider provides a virtual pipe between the company’s sites.

Access VPNs extend the advantages of VPNs to access technologies. This increases scalability, accessibility, and security and reduces management complexity. Corporations can outsource their access network to further reduce their efforts and costs.

Terminology:

- ATM—Asynchronous Transfer Mode
- L2F—Layer 2 Forwarding
- L2TP—Layer 2 Tunneling Protocol
- PPP—Point-to-Point Protocol
- PPoE—PPP over Ethernet
- PPTP—Point-to-Point Tunneling Protocol



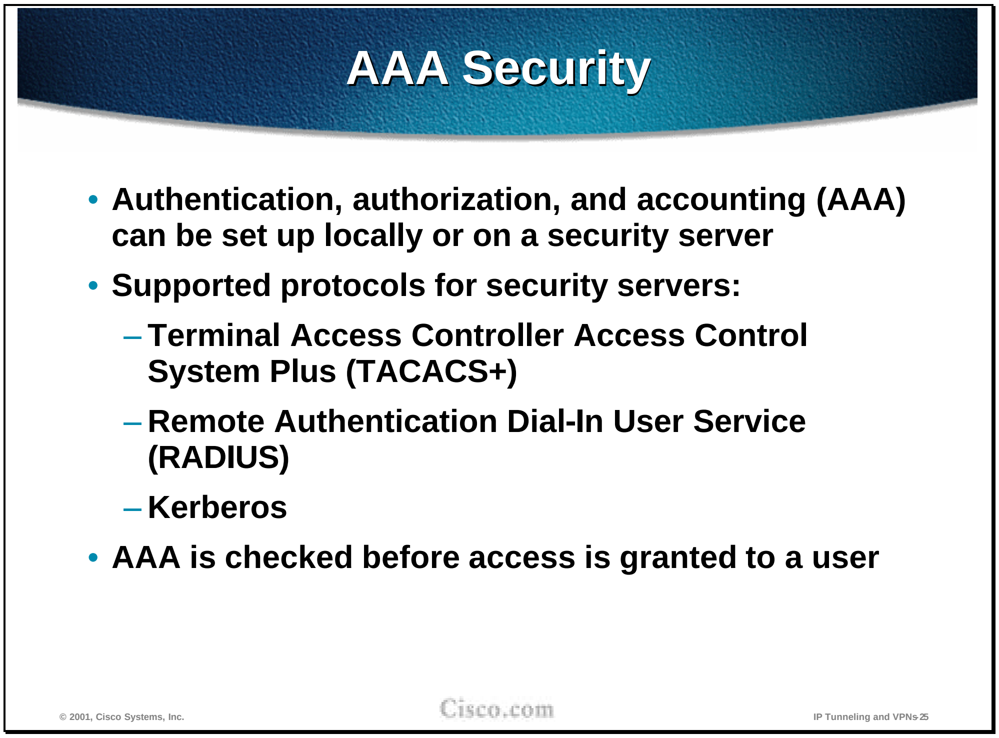
Access VPDN Overview

Common configuration steps for VPDN protocols:

- **Configure AAA security**
- **Create a virtual template**
- **Create virtual profile (optional)**
- **Create per-user configuration (optional)**
- **Configure tunnel**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-24

Several protocols support access VPDNs, but they share a common generic configuration. We will quickly review these configuration steps so that we can focus on the specifics for each protocol when we get to them.



AAA Security

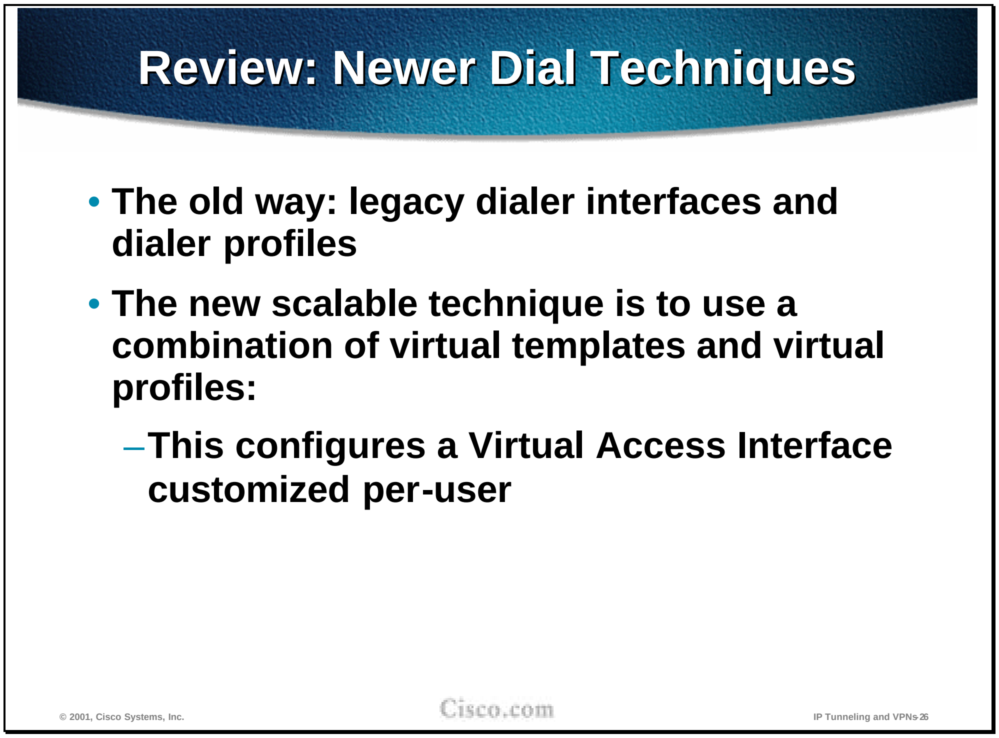
- Authentication, authorization, and accounting (AAA) can be set up locally or on a security server
- Supported protocols for security servers:
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - Remote Authentication Dial-In User Service (RADIUS)
  - Kerberos
- AAA is checked before access is granted to a user

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-25

Setting up authentication, authorization, and accounting (AAA) is the first step in configuring access VPNs. The functions of AAA are critical to providing a secure access solution. In addition, AAA provides support for the dynamic configuration of tunnels. We will look more closely at these features in the VPDN per-user module.

Terminology:

- Kerberos—Kerberos is the developing standard for authenticating network users. Kerberos offers two key benefits: it functions in a multivendor network, and it does not transmit passwords over the network.



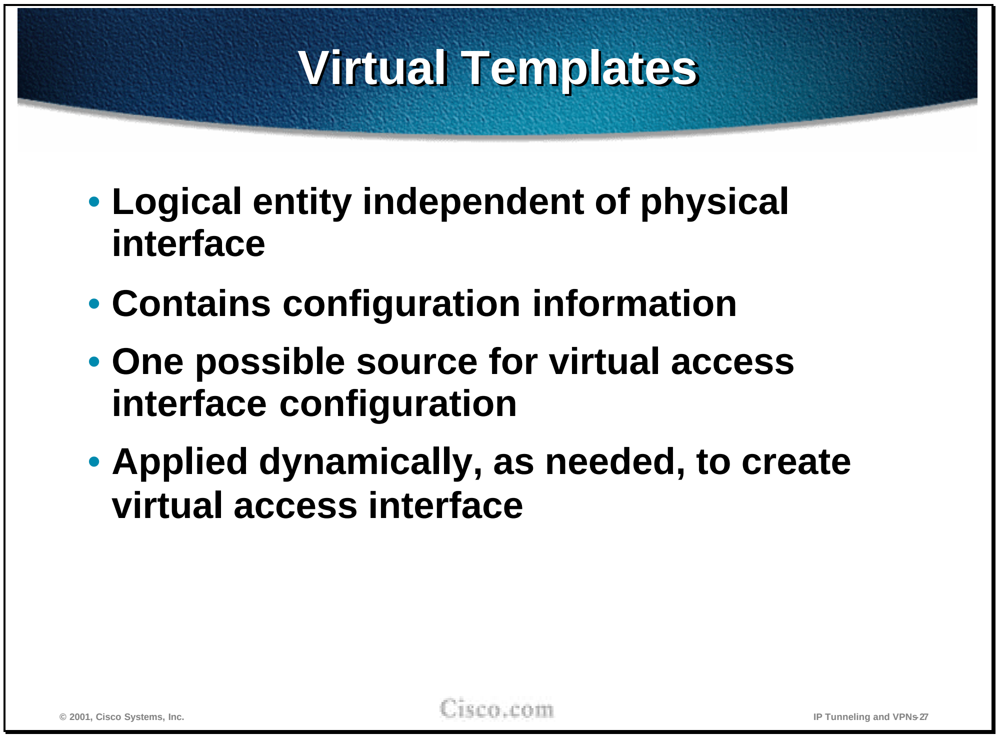
Review: Newer Dial Techniques

- The old way: legacy dialer interfaces and dialer profiles
- The new scalable technique is to use a combination of virtual templates and virtual profiles:
  - This configures a Virtual Access Interface customized per-user

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-26

The old way to configure dial and dial on demand routing (DDR) was using dialer interfaces and “legacy dialer profiles,” or “legacy DDR” as it is now referred to in the documentation. This approach can be simple and efficient but does not scale to the needs of service providers and Large Enterprises.

The newer approach is to use a combination of virtual templates and virtual profiles, which dynamically combine to produce a virtual access interface customized per-user. We will look briefly at these two techniques in the next slides as a review, since we will need to refer to these techniques as we discuss new VPN-related dial features.



Virtual Templates

- Logical entity independent of physical interface
- Contains configuration information
- One possible source for virtual access interface configuration
- Applied dynamically, as needed, to create virtual access interface

© 2001, Cisco Systems, Inc.

Cisco.com

IP Tunneling and VPNs-27

Virtual templates provide a flexible and scalable generic service that can be used to apply predefined interface configurations to dynamically created virtual access interfaces.

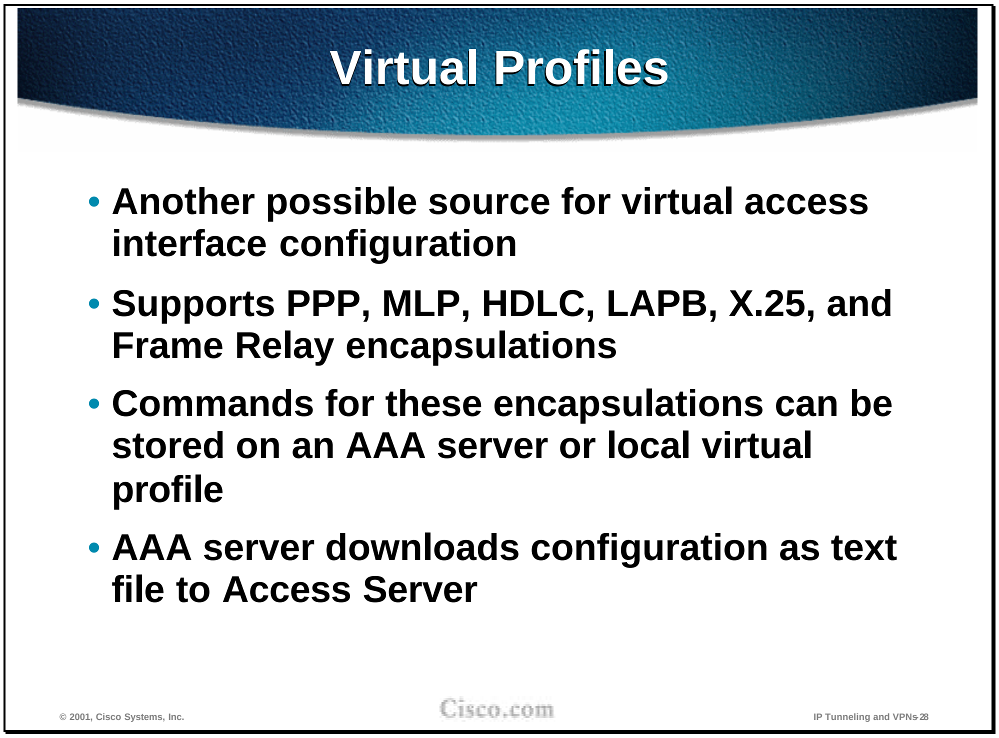
Virtual template interfaces can be configured independently of any physical interface and applied dynamically, as needed, to create virtual access interfaces, which are the actual IOS interfaces used to terminate a (virtual) Layer-2 dial-up session. When a user dials in, a predefined configuration template is used to configure a virtual access interface; when the user is done, the virtual access interface goes down and the resources are freed for other dial-in uses.

A virtual template interface is a logical entity—a configuration for a serial interface but not tied to a physical interface—that can be applied dynamically as needed. Virtual access interfaces are virtual interfaces that are created, configured dynamically (for example, by cloning a virtual template interface), used, and then freed when no longer needed.

Virtual template interfaces are one possible source of configuration information for a virtual access interface. Virtual interface templates provide no direct value to users; they must be applied to or associated with a virtual access feature by use of a command with the **virtual-template** keyword. For example, the **interface virtual-template** command creates the **virtual template interface** and the **multilink virtual-template** command applies the virtual template to a multilink stack group. The **virtual-profile virtual-template** command specifies that a virtual template interface will be used as a source of configuration information for virtual profiles.

Limitations:

- Although a system can have as many as 25 virtual template interfaces, one template for each virtual access application is a more realistic limit.
- When in use, each virtual access interface cloned from a template requires the same amount of memory as a serial interface. Cisco routers support a maximum of 300 virtual interfaces.
- Virtual access interfaces are not directly configurable by users, except by configuring a virtual template interface or including the configuration information of the user (through virtual profiles or per-user configuration) on an AAA server. However, information about an in-use virtual access interface can be displayed and the virtual access interface can be cleared.
- Virtual interface templates provide no direct value to users; they must be applied to or associated with a virtual access feature by use of a command with the **virtual-template** keyword.
- For example, the **interface virtual-template** command creates the virtual template interface and the **multilink virtual-template** command applies the virtual template to a multilink stack group. The **virtual-profile virtual-template** command specifies that a virtual template interface will be used as a source of configuration information for virtual profiles.



Virtual Profiles

- Another possible source for virtual access interface configuration
- Supports PPP, MLP, HDLC, LAPB, X.25, and Frame Relay encapsulations
- Commands for these encapsulations can be stored on an AAA server or local virtual profile
- AAA server downloads configuration as text file to Access Server

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-28

A virtual profile is a unique configuration that can create and configure a virtual access interface dynamically when a dial-in call is received, and tear down the interface dynamically when the call ends. Virtual profiles support these encapsulation methods: PPP; Multilink Point-to-Point Protocol (MLP); High-Level Data Link Control (HDLC); Link Access Procedure, Balanced (LAPB); X.25; and Frame Relay

Any commands for these encapsulations that can be configured under a serial interface can be configured under a virtual profile stored in a user file on an AAA server and a virtual profile virtual template configured locally. The AAA server daemon downloads them as text to the network access server (NAS), and is able to handle multiple download attempts.

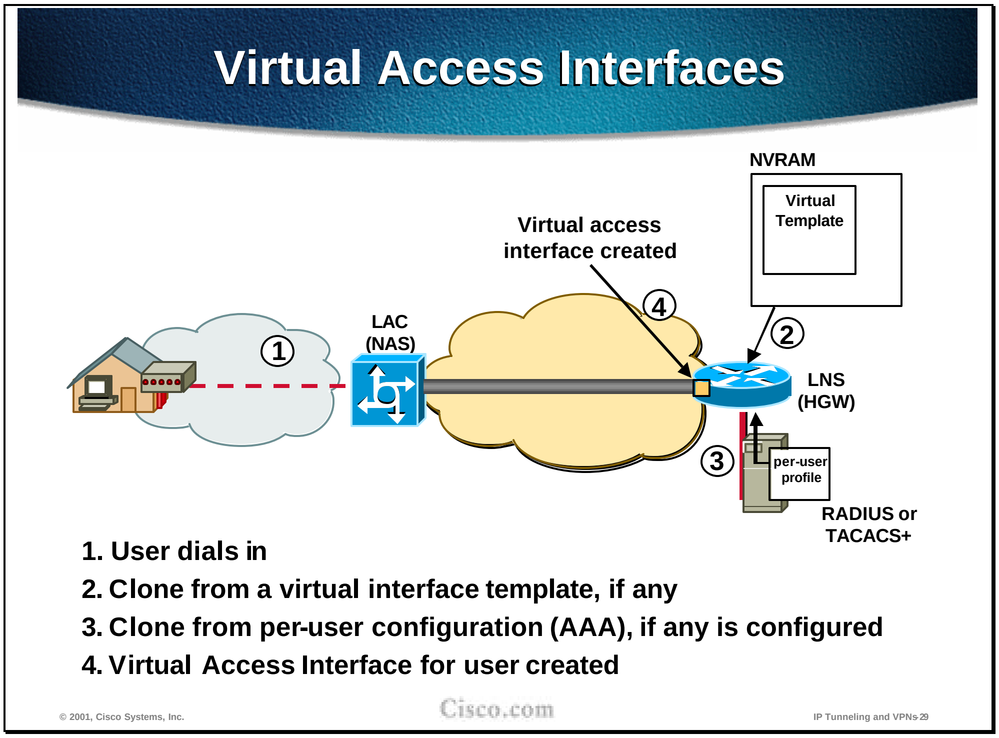
The configuration information for a virtual profiles virtual access interface can come from a virtual template interface, or from user-specific configuration stored on an AAA server, or both.

Virtual profiles separate configuration information into two logical parts:

- Generic—Common configuration for dial-in users plus other router-dependent configuration. This common and router-dependent information can define a virtual template interface stored locally on the router. The generic virtual template interface is independent of and can override the configuration of the physical interface on which a user dialed in.
- User-specific interface information—Interface configuration stored in a user file on an AAA server; for example, the authentication requirements and specific interface settings for a specific user. The settings are sent to the router in the response to the request from the router to authenticate the user, and the settings can override the generic configuration.

Two rules govern virtual access interface configuration by virtual profiles virtual template interfaces and AAA configurations:

- Each virtual access application can have at most one template to clone from but can have multiple AAA configurations to clone from (virtual profiles AAA information and AAA per-user configuration, which in turn might include configuration for multiple protocols).
- When virtual profiles are configured by virtual template, its template has higher priority than any other virtual template.



Virtual Access Interfaces

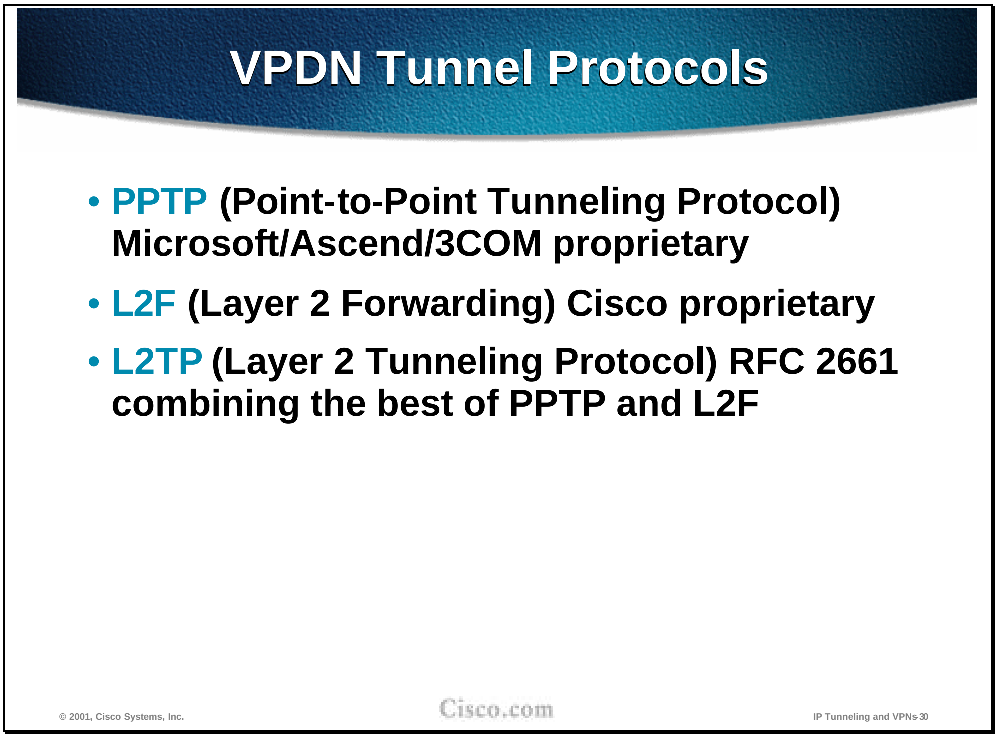
1. User dials in
2. Clone from a virtual interface template, if any
3. Clone from per-user configuration (AAA), if any is configured
4. Virtual Access Interface for user created

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-29

Virtual template interfaces are one possible source of configuration information for a virtual access interface. Virtual profiles are another.

Each virtual access interface can clone from only one template. But some applications can take configuration information from multiple sources; for example, virtual profiles can take configuration information from a virtual template interface, or from interface-specific configuration information stored from a user on a AAA server, or from network protocol configuration from a user stored on a AAA server, or all three. The result of using template and AAA configuration sources is a virtual access interface uniquely configured for a specific dial-in user.

A router can create a virtual access interface by first using the information from a virtual template interface (if any is defined for the application) and then using the information in a per-user configuration (if AAA is configured on the router and virtual profiles or per-user configuration or both are defined for the specific user).



VPDN Tunnel Protocols

- PPTP (Point-to-Point Tunneling Protocol) Microsoft/Ascend/3COM proprietary
- L2F (Layer 2 Forwarding) Cisco proprietary
- L2TP (Layer 2 Tunneling Protocol) RFC 2661 combining the best of PPTP and L2F

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-30

PPTP is a Layer 3 generic routing encapsulation (GRE)-like tunnel that crosses the Internet service provider (ISP) network. We put it in this module because it seemed to belong with the rest of our PPP coverage.

L2F and L2TP are the means to provide Layer 2 tunneling to encapsulate PPP frames and move them across a network where they can be “dropped” back into a home network.

There are other technologies that can provide Layer 3 tunnels such as GRE, IP Security (IPSec), and Multiprotocol Label Switching (MPLS). These were discussed in the other modules of this section on VPNs.

Summary

- Layer-2 access VPNs or Virtual Private Dial-up Networks (VPDN) enable users to configure secure networks that take advantage of Internet service providers (ISPs) to tunnel the company's remote access traffic through the ISP cloud.
- Layer-2 access VPNs work by tunneling Layer-2 frames over a public (Internet) or SP-provided Layer-3 backbone, usually based on IP
- Layer-2 VPNs are configured by configuring Cisco IOS AAA parameters and virtual dial interfaces

Lesson Review

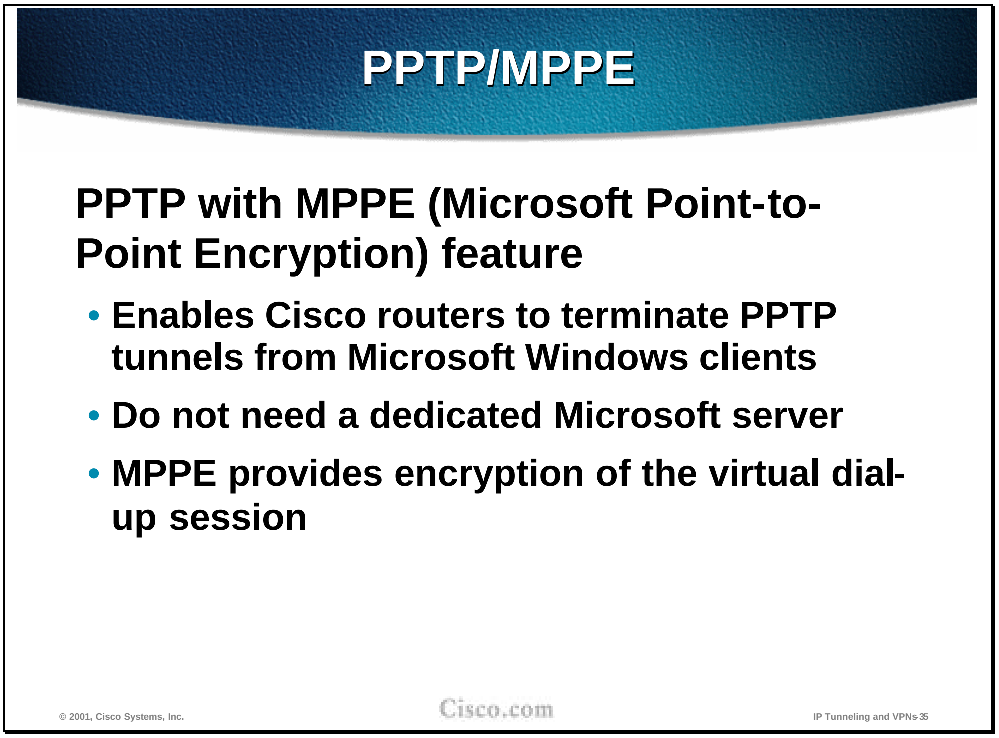
1. What is an Access VPN?
2. What AAA parameters need to be configured for dial-in VP(D)Ns?
3. What is a Cisco IOS virtual template interface?
4. What is a Cisco IOS virtual profile interface?
5. What is a Cisco IOS virtual access interface?

Point-to-Point Tunneling Protocol (PPTP)

Objectives

After completing this module, you should be able to perform the following tasks:

- Describe the PPTP Layer-2 tunneling protocol
- Configure Cisco IOS to accept PPTP dial-in sessions



PPTP/MPPE

PPTP with MPPE (Microsoft Point-to-Point Encryption) feature

- Enables Cisco routers to terminate PPTP tunnels from Microsoft Windows clients
- Do not need a dedicated Microsoft server
- MPPE provides encryption of the virtual dial-up session

© 2001, Cisco Systems, Inc.

Cisco.com

IP Tunneling and VPNs-35

PPTP is a tunneling and encryption protocol developed by Microsoft as a VPN technology. It is included with Windows 95/98, NT 4.0, and Windows 2000 and does not require any additional client software. This makes it a very attractive solution for setting up VPNs with Microsoft networks. MPPE is a sub-feature of Microsoft Point-to-Point Compression (MPPC) that provides confidentiality through encryption.

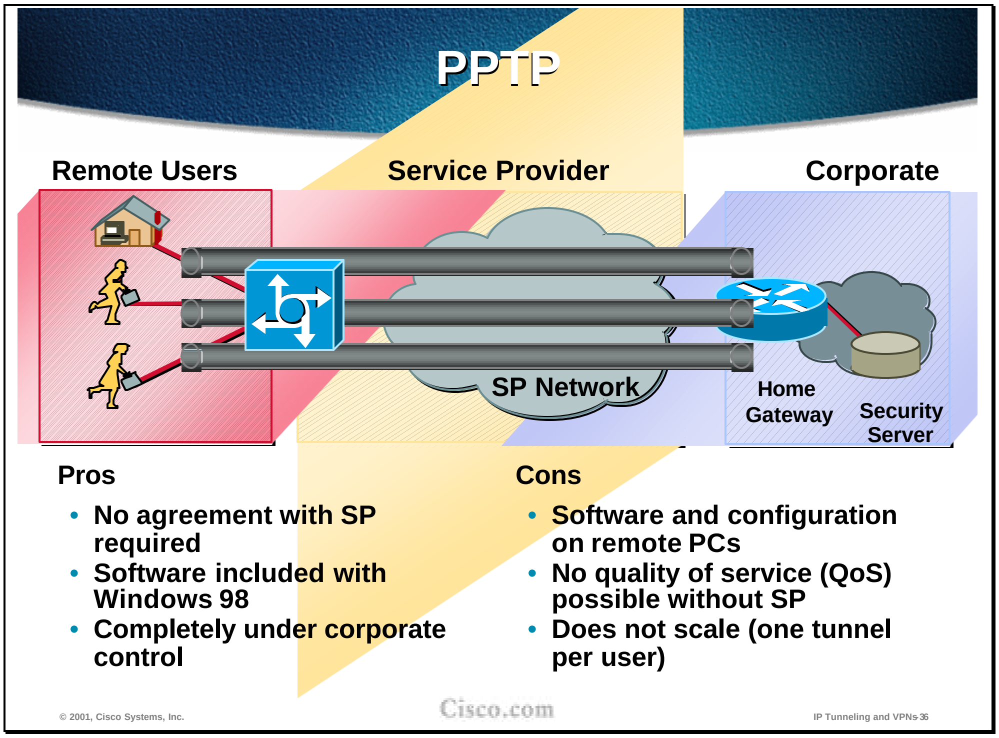
Restrictions:

- Only Cisco Express Forwarding (CEF) and process switching are supported. Regular fast switching is not supported.
- PPTP must be initiated by end user, not service provider.
- PPTP will not support multilink.
- VPDN multihop is not supported TCP.

Because all PPTP signaling is over Transmission Control Protocol (TCP), configurations will affect PPTP performance in large-scale environments.

Supported platforms:

- Cisco 7100 and 7200 series



PPTP

Pros

- No agreement with SP required
- Software included with Windows 98
- Completely under corporate control

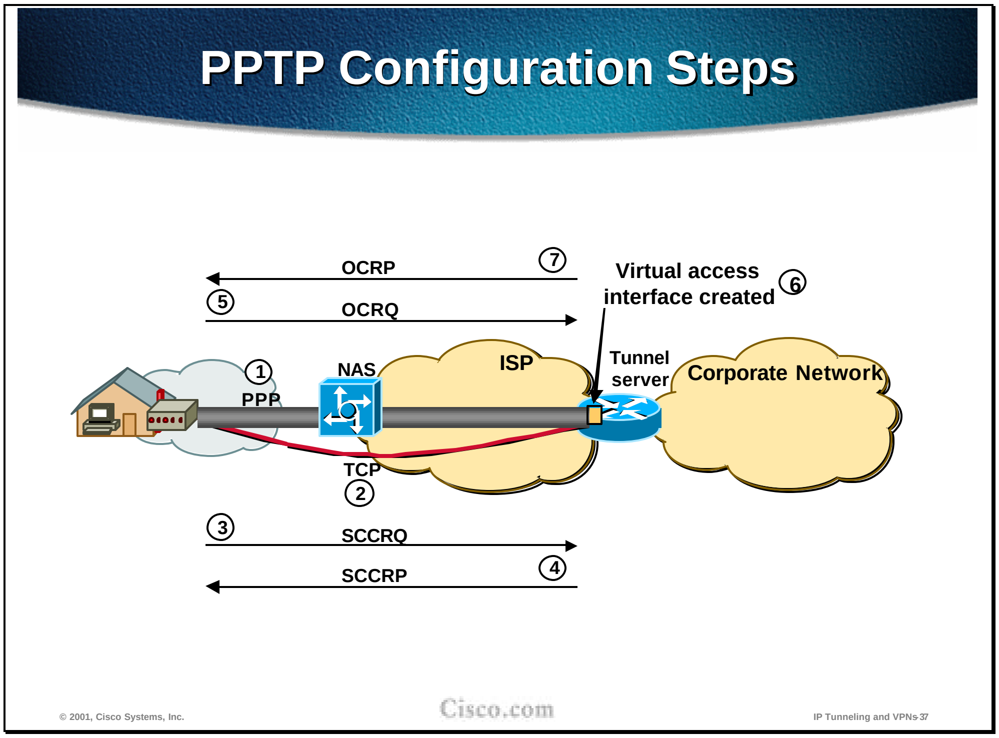
Cons

- Software and configuration on remote PCs
- No quality of service (QoS) possible without SP
- Does not scale (one tunnel per user)

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-36

The slide notes the pros and cons of PPTP. Note that the tunnels extend from the user PC to the corporate gateway router (or inside it, to a Microsoft server acting as tunnel endpoint). This is not a scalable model for business to business communications.

Initially setting up PPTP involves creating a second dial adapter on the PC, one that tunnels PPP over the actual dial adapter that connects to the ISP.



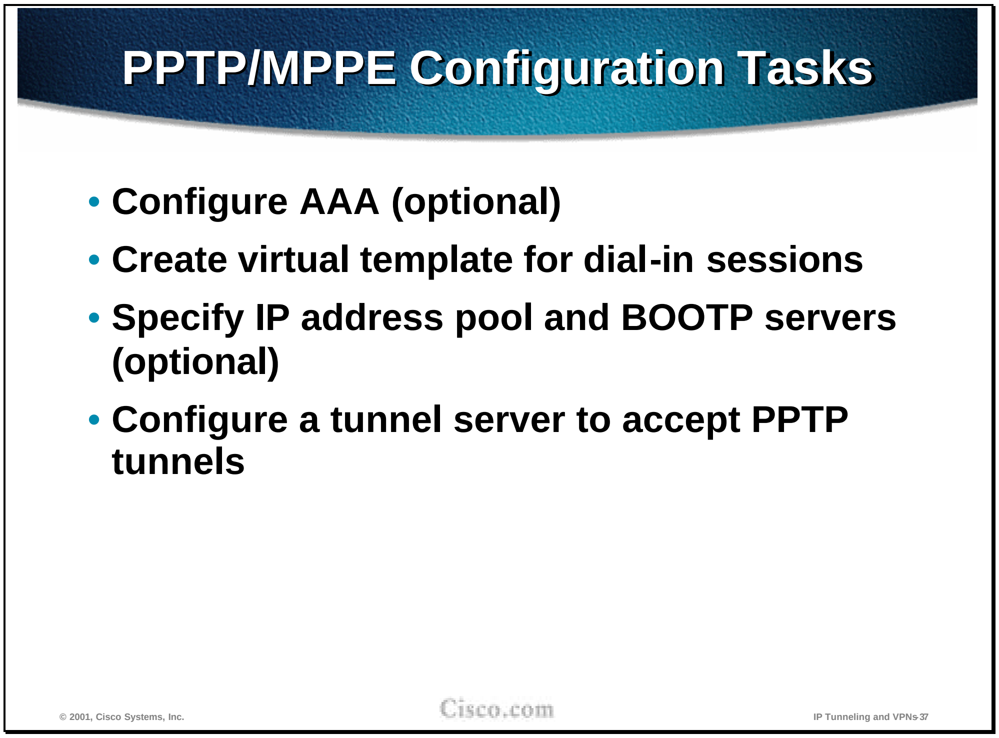
PPTP Configuration Steps

OCRP 7
5 OCRQ
Virtual access interface created 6
1 PPP
NAS
ISP
Tunnel server
Corporate Network
TCP 2
3 SCCRQ
SCCRP 4

Cisco.com
IP Tunneling and VPNs-37

The following steps are needed in in establishing a PPTP tunnel:

- The client dials in to the ISP and establishes a PPP session.
- The client establishes a TCP connection with the tunnel server.
- The tunnel server accepts the TCP connection.
- The client sends a PPTP Start Control Connection Request (SCCRQ) message to the tunnel server.
- The tunnel server establishes a new PPTP tunnel and replies with an Start Control Connection Reply (SCCRP) message.
- The client initiates the session by sending an Outgoing Call Request (OCRQ) message to the tunnel server.
- The tunnel server creates a virtual-access interface.
- The tunnel server replies with an Outgoing Call Reply (OCRP) message.

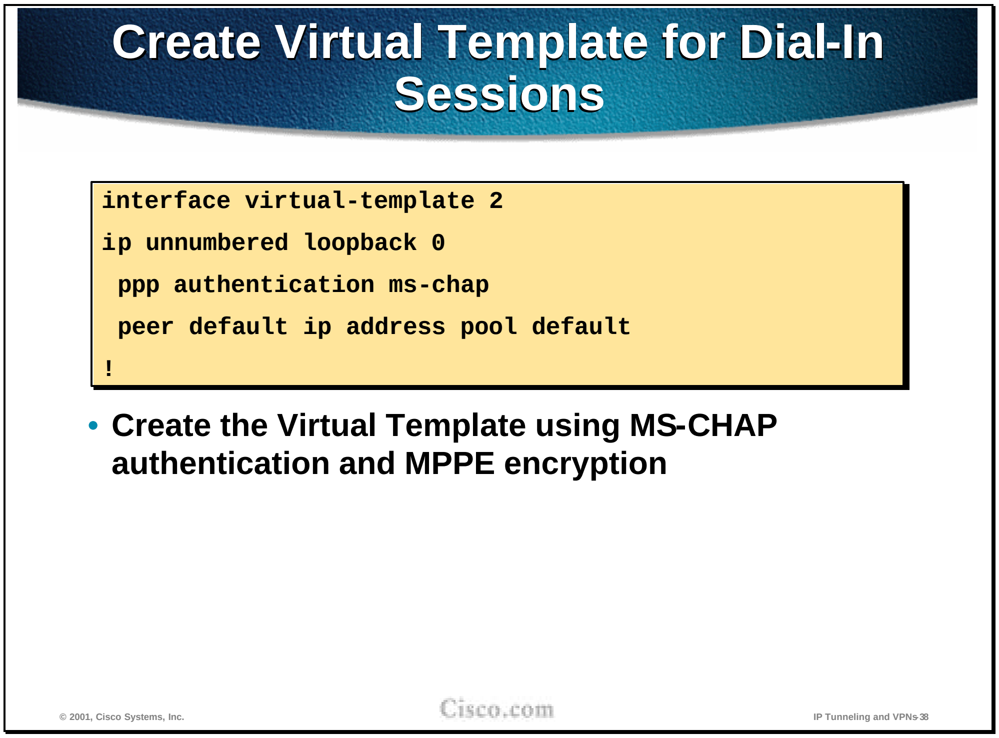


PPTP/MPPE Configuration Tasks

- Configure AAA (optional)
- Create virtual template for dial-in sessions
- Specify IP address pool and BOOTP servers (optional)
- Configure a tunnel server to accept PPTP tunnels

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-37

Configuration for PPTP/MPPE follows the generic VPDN connection configuration outline. As with any dial session, configuration of AAA parameters enforces an access security polic y. The configured virtual templates provide configuration information from which Cisco IOS creates virtual access interfaces. Optionally, Cisco IOS can configure the remote end IP address using a locally or remotely configured address pool. Finally, using the Cisco IOS VPDN group configuration mechanism, the router is configured to act as a PPTP tunnel server, accepting incoming PPTP sessions.



Create Virtual Template for Dial-In Sessions

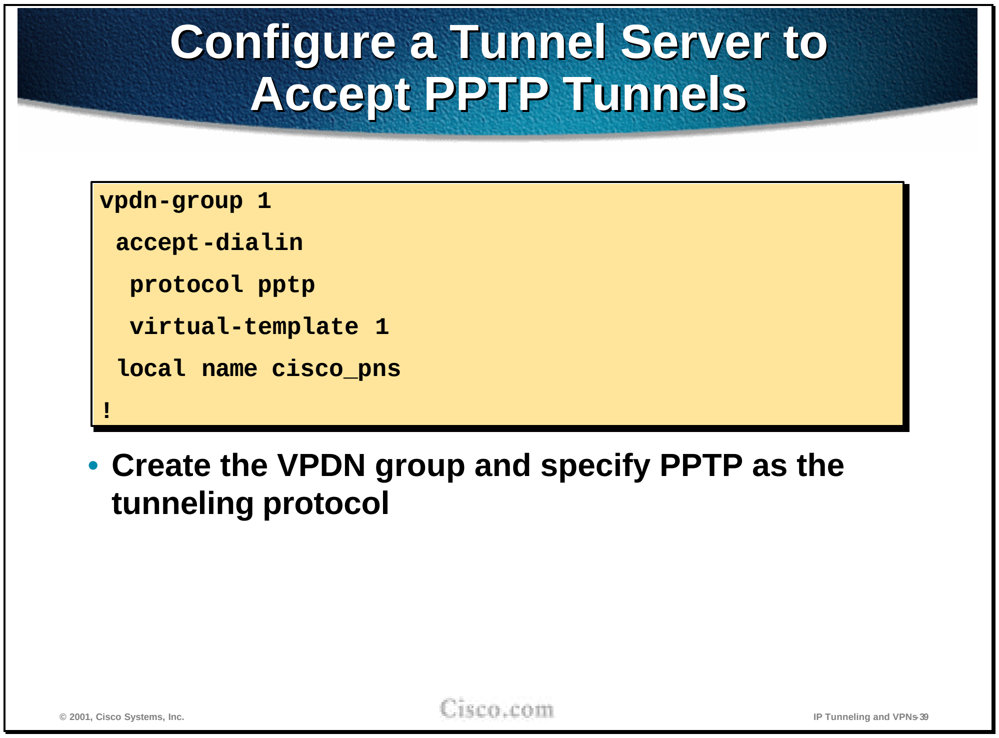
```
interface virtual-template 2
ip unnumbered loopback 0
 ppp authentication ms-chap
 peer default ip address pool default
!
```

- **Create the Virtual Template using MS-CHAP authentication and MPPE encryption**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-38

The slide illustrates a virtual template for the dial-in sessions. We use MS-CHAP as the PPP authentication type and set the options for MPPE encryption. MPPE uses RC-4 encryption with either 40- or 128-bit keys. All keys are derived from the clear text authentication password of the user. The Cisco implementation of MPPE is fully interoperable with the Microsoft implementation.

With MPPE, the stateful mode provides the best performance, but is adversely affected by high packet loss. The **stateful** option with the **ppp encrypt mppe** command means that MPPE will only accept a stateful connection. The default is to offer a stateless and accept a stateful if offered.



Configure a Tunnel Server to Accept PPTP Tunnels

```
vpdn-group 1
 accept-dialin
  protocol pptp
  virtual-template 1
 local name cisco_pns
!
```

- Create the VPDN group and specify PPTP as the tunneling protocol

© 2001, Cisco Systems, Inc.

Cisco.com

IP Tunneling and VPNs-39

The example shown in the slide uses the new modularized group command syntax. We will look at more detailed examples of this later in this module.

To configure a tunnel server to accept PPTP tunnels we create a VPDN group and set the protocol to be PPTP. The virtual template is the same one we configured to use MS-Challenge Handshake Authentication Protocol (CHAP) authentication and MPPE encryption. The local name is optional and specifies that the tunnel server will identify itself with this local name. If no local name is specified, the tunnel server will identify itself with its host name.

Summary

- Cisco IOS supports the Microsoft Point-to-Point Tunneling Protocol (PPTP) Layer-2 tunneling method, using native Microsoft Point-to-Point Encryption
- The PPTP method is configured almost like a dial-up session, with the help of Cisco IOS vpdn-group CLI functionality

Lesson Review

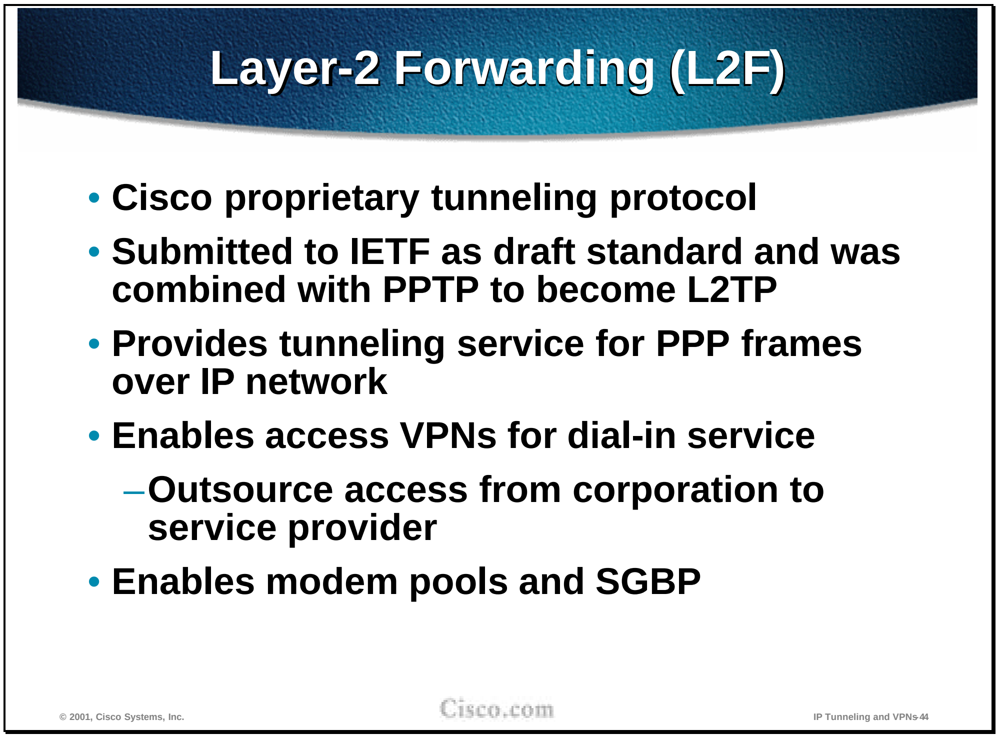
1. What protocol is tunneled within PPTP?
2. Which Cisco IOS configuration mechanism is used to bind PPTP sessions to virtual interfaces?

Layer-2 Tunneling Protocol (L2TP)

Objectives

After completing this module, you should be able to perform the following tasks:

- Describe the L2TP Layer-2 tunneling protocol
- Configure Cisco IOS to accept L2TP dial-in sessions
- Describe the Stack Group Bidding Protocol and its benefits



Layer-2 Forwarding (L2F)

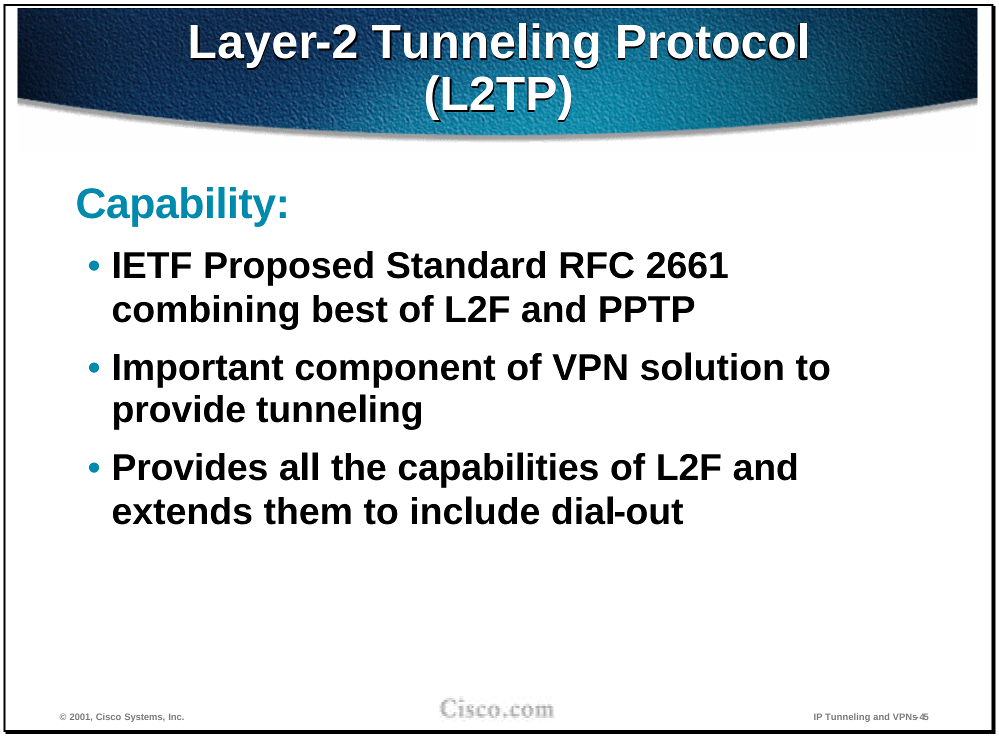
- Cisco proprietary tunneling protocol
- Submitted to IETF as draft standard and was combined with PPTP to become L2TP
- Provides tunneling service for PPP frames over IP network
- Enables access VPNs for dial-in service
  - Outsource access from corporation to service provider
- Enables modem pools and SGBP

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-44

L2F was developed by Cisco as solution for tunneling PPP frames over an IP network. This allows the creation of Access VPNs. PPP frames from remote users are forwarded by the NAS to the Home Gateway (HGW) over an intermediate IP network cloud. L2F provided support for Stacking Home Gateways and L2F Multihop. These features increased the scalability of the L2F solution.

Cisco submitted L2F to the Internet Engineering Task Force (IETF) where it was combined with PPTP to become L2TP.

L2F is also used with Stack Group Bidding Protocol (SGBP) to allow stacked access servers to cooperate to handle multi-link PPP calls from users. This is a form of investment protection, since dial ports on different hardware can be used together to provide one large modem pool.



Layer-2 Tunneling Protocol (L2TP)

Capability:

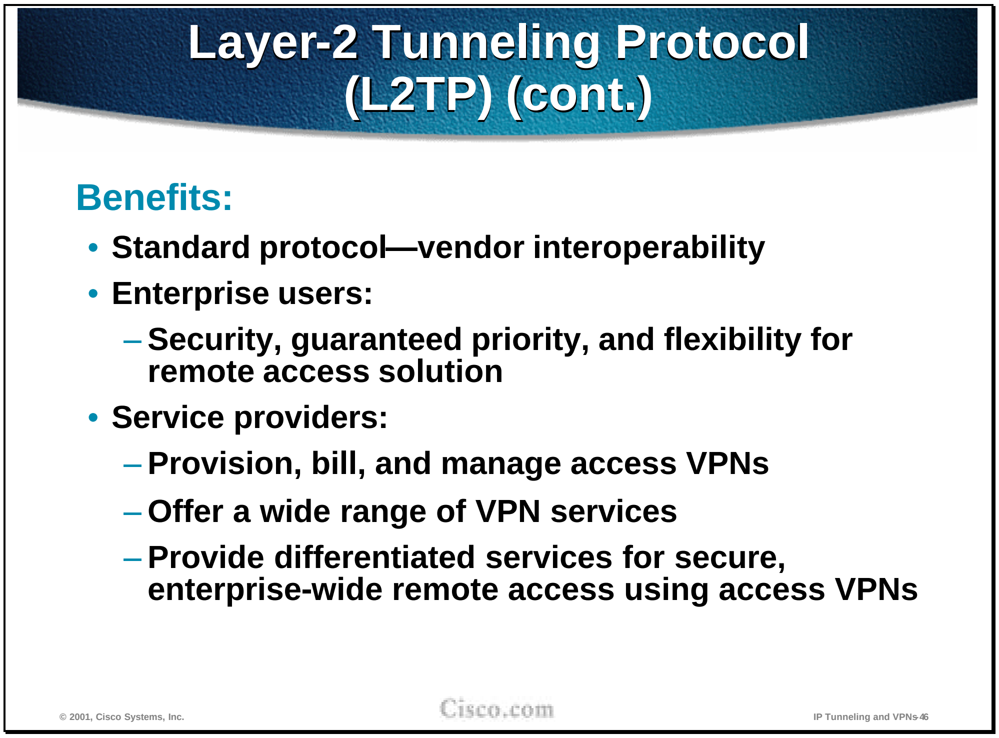
- IETF Proposed Standard RFC 2661 combining best of L2F and PPTP
- Important component of VPN solution to provide tunneling
- Provides all the capabilities of L2F and extends them to include dial-out

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-45

L2TP is a key building block for access VPNs. Access VPN support includes VPDNs for modem and ISDN users, and VPNs for cable and digital subscriber line (DSL) users. L2TP is an extension to the Point-to-Point Protocol (PPP). L2TP merges the best features of two other tunneling protocols: L2F from Cisco Systems and PPTP from Microsoft. L2TP is an IETF proposed standard, currently under codevelopment and endorsed by Cisco Systems, Microsoft, Ascend, 3Com, and other networking industry leaders.

Platforms and considerations:

- L2TP is supported on the Cisco 1600, 160x, 25xx, 26xx, 36xx, 4000/m, 4x00/m, UAC 64xx, 72xx, and 75xx, routers, the AS52xx, AS5300 assay servers, and platform AS5800 in Cisco IOS Software 12.0(1)T.
- First appearance in a Cisco IOS software T release was12.0(1)T.



Layer-2 Tunneling Protocol (L2TP) (cont.)

Benefits:

- **Standard protocol—vendor interoperability**
- **Enterprise users:**
  - **Security, guaranteed priority, and flexibility for remote access solution**
- **Service providers:**
  - **Provision, bill, and manage access VPNs**
  - **Offer a wide range of VPN services**
  - **Provide differentiated services for secure, enterprise-wide remote access using access VPNs**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-46

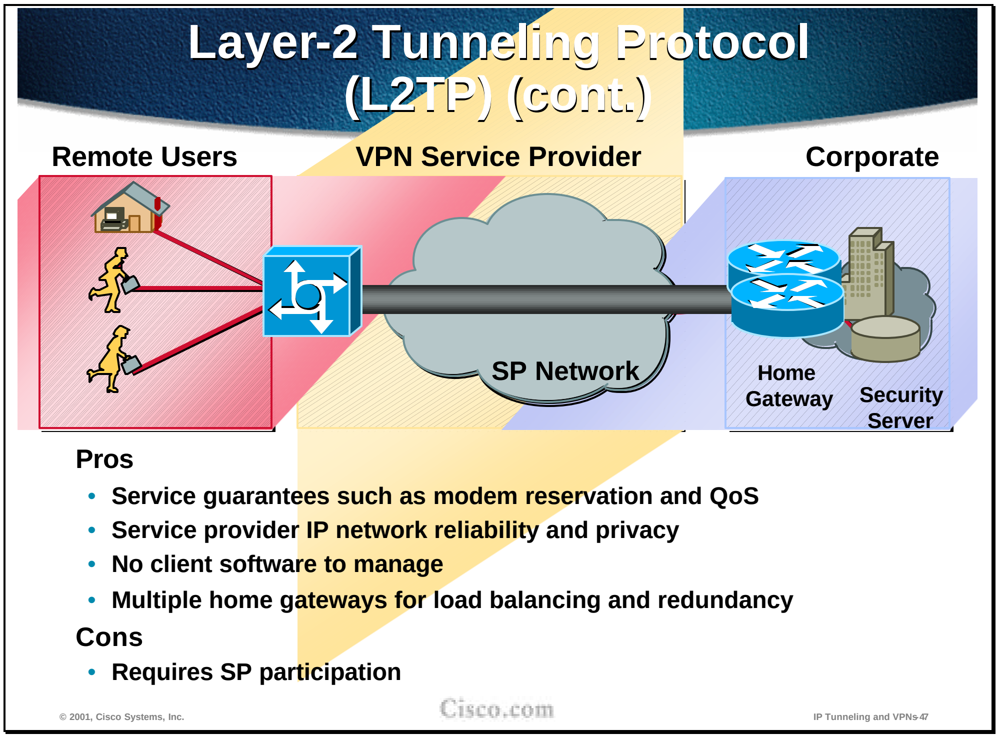
Because L2TP is a standard protocol, all customers—service providers and corporate network managers alike—can enjoy a wide range of service offerings available from multiple vendors. Interoperability among the vendors will help ensure rapid global deployment of a standard access VPN service.

The Cisco L2TP solution brings a long list of benefits to enterprise users:

- Security and guaranteed priority for their most mission-critical applications
- Improved connectivity, reduced costs, and freedom to refocus resources on core competencies
- Flexible, scalable remote network access environment without compromising corporate security or endangering mission-critical applications

Service providers derive the following benefits from access VPNs built on a foundation of the following Cisco IOS software L2TP features:

- Ability to provision, bill, and manage access VPNs that provide a competitive advantage, minimize customer turnover, and increase profitability
- Flexibility to offer a wide range of VPN services across many different architectures, using Cisco's L2TP in concert with robust Cisco IOS software features
- Capability to provide differentiated services for secure, enterprise-wide remote access using access VPNs over the public Internet or service providers' backbone



Layer-2 Tunneling Protocol (L2TP) (cont.)

Pros

- Service guarantees such as modem reservation and QoS
- Service provider IP network reliability and privacy
- No client software to manage
- Multiple home gateways for load balancing and redundancy

Cons

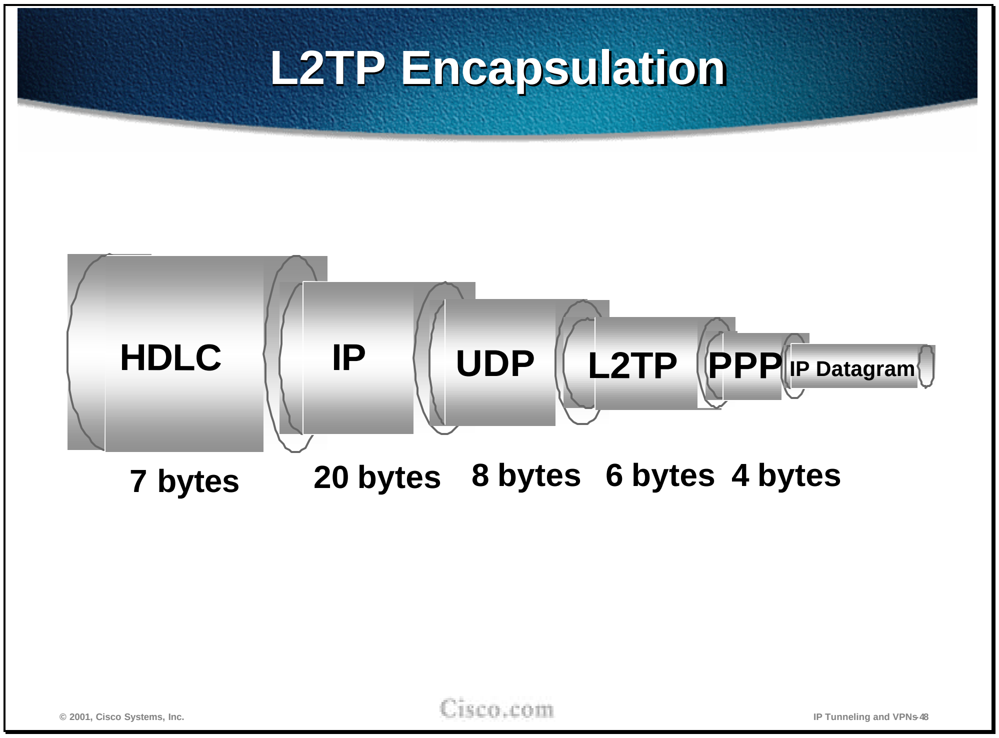
- Requires SP participation

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-47

VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources.

L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet.

It also allows enterprise customers to outsource dial-out support, thus reducing overhead for hardware maintenance costs and 800 number fees, and allows them to concentrate corporate gateway resources. Outsourcing also reduces support costs. Employees make local calls to access the corporate network. This is a much more efficient use of resources.



L2TP Encapsulation

© 2001, Cisco Systems, Inc.

Cisco.com

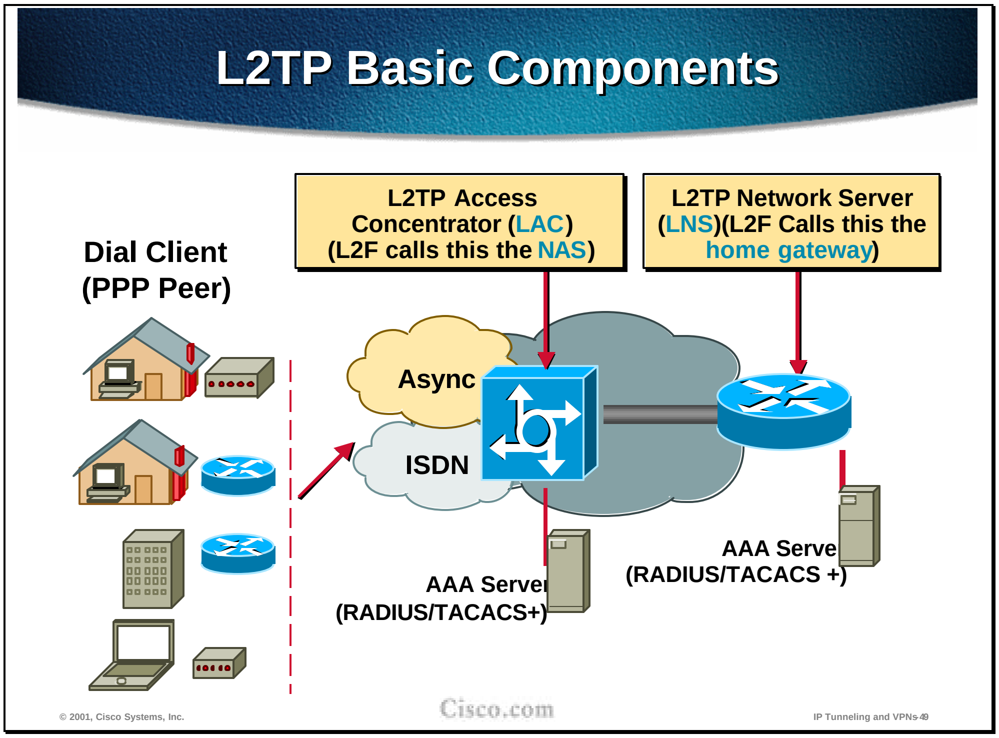
IP Tunneling and VPNs-48

L2TP encapsulates PPP frames to tunnel them across an IP network. The L2TP packets must be encapsulated as well for transmission.

Here we see the result if we were to use an HDLC encapsulation on a serial link for a total of 45 bytes of header on the original IP datagram. On Fast Ethernet, the overhead would be 38 bytes.

Other possible concerns:

- Fragmentation issues
- IPSec—adds its own header



L2TP Basic Components

Dial Client
(PPP Peer)

L2TP Access Concentrator (LAC) (L2F calls this the NAS)

L2TP Network Server (LNS)(L2F Calls this the home gateway)

Async

ISDN

AAA Server
(RADIUS/TACACS+)

AAA Serve
(RADIUS/TACACS +)

© 2001, Cisco Systems, Inc.

Cisco.com

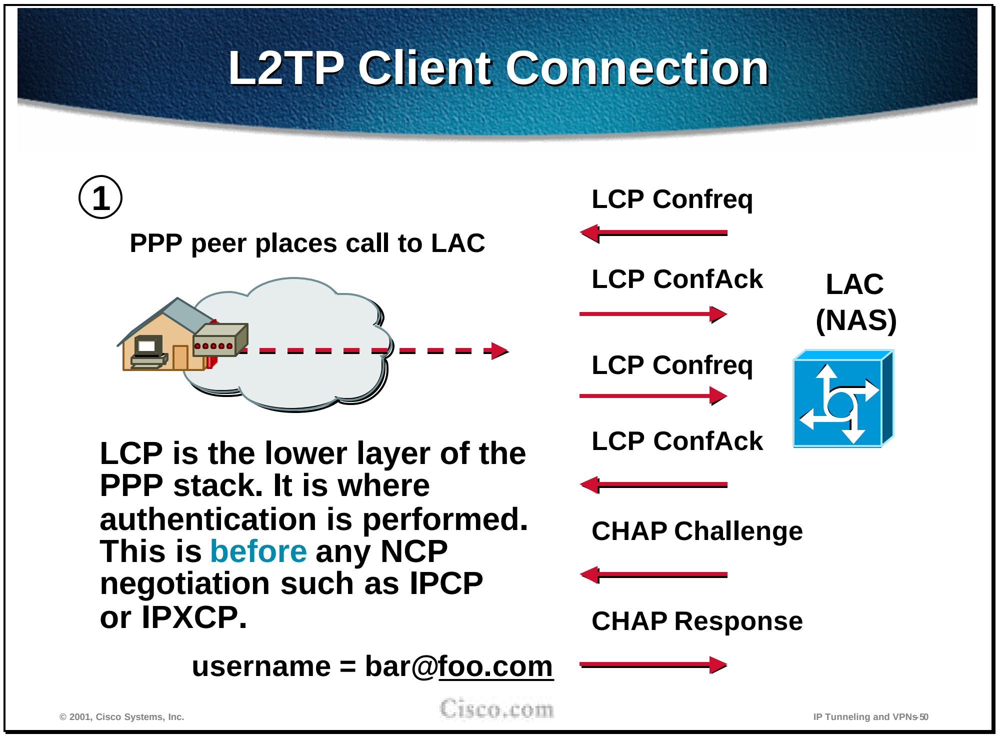
IP Tunneling and VPNs-49

The L2TP Access Concentrator (LAC) located at the ISP’s point of presence (POP) exchanges PPP messages with remote users and communicates by way of L2TP requests and responses with the customer’s L2TP network server (LNS) to set up tunnels.

L2TP passes PPP packets through the IP tunnel between end points of a point-to-point connection.

Frames from remote users are accepted by the ISP’s POP, stripped of any linked framing or transparency bytes, encapsulated in L2TP, and forwarded over the appropriate tunnel. The customer’s home gateway accepts these L2TP frames, strips the L2TP encapsulation, and processes the incoming frames as PPP delivered directly to the appropriate interface.

Tunnel peers are basic components of L2TP.



L2TP Client Connection

1

PPP peer places call to LAC

LCP Confreq

LCP ConfAck

LCP Confreq

LCP ConfAck

CHAP Challenge

CHAP Response

LAC (NAS)

LCP is the lower layer of the PPP stack. It is where authentication is performed. This is before any NCP negotiation such as IPCP or IPXCP.

username = bar@foo.com

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-50

The slide shows the initial connection between the remote-user and the LAC. The LAC performs authentication to identify the user and get information to set up the tunnel. This information will be forwarded to the LNS later on in the process.

The LAC physically terminates the incoming call; it does not terminate the PPP session, though. The PPP session is terminated at the LNS. Some PPP LCP negotiation is performed between the remote user and the LAC, where the LAC identifies the user to determine the VPDN customer to which the remote user belongs.

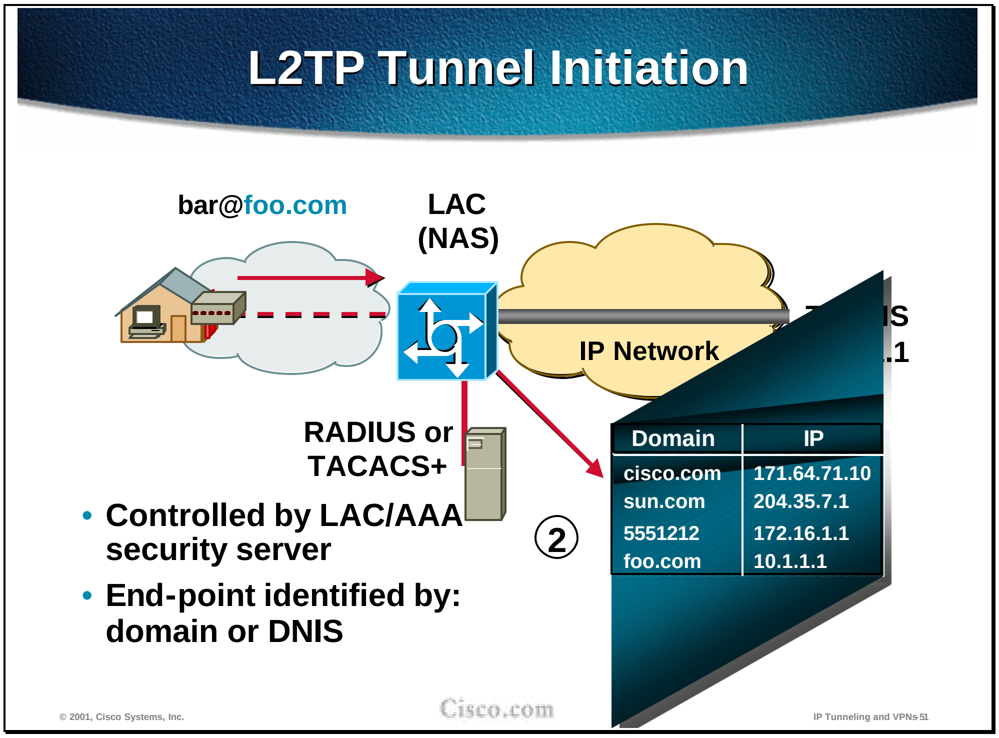
To diagnose problems at this phase, you can use the following **debug** commands:

```
debug PPP negotiation
```

```
debug PPP authentication
```

Terminology:

- IPCP—IP Control Protocol
- IPXCP—Internetwork Packet Exchange (IPX) Control Protocol
- LCP—Link control protocol
- NCP—Network Control Program

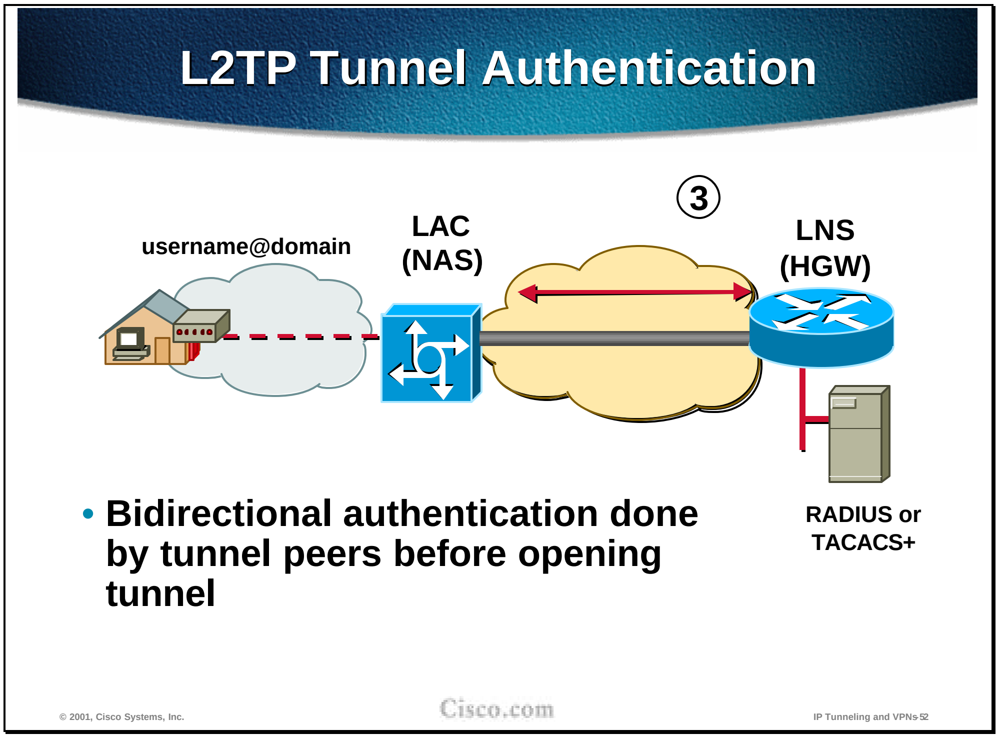


L2TP Tunnel Initiation

- Controlled by LAC/AAA security server
- End-point identified by: domain or DNIS

Domain	IP
cisco.com	171.64.71.10
sun.com	204.35.7.1
5551212	172.16.1.1
foo.com	10.1.1.1

The LAC initiates the establishment of the tunnel to the remote LNS. The LNS end point can be identified by the remote-user’s domain or Dialed Number Identification Service (DNIS). The mapping of domain or DNIS can be maintained locally on the LAC or on an AAA security server run by the service provider.



L2TP Tunnel Authentication

3

username@domain

LAC
(NAS)

LNS
(HGW)

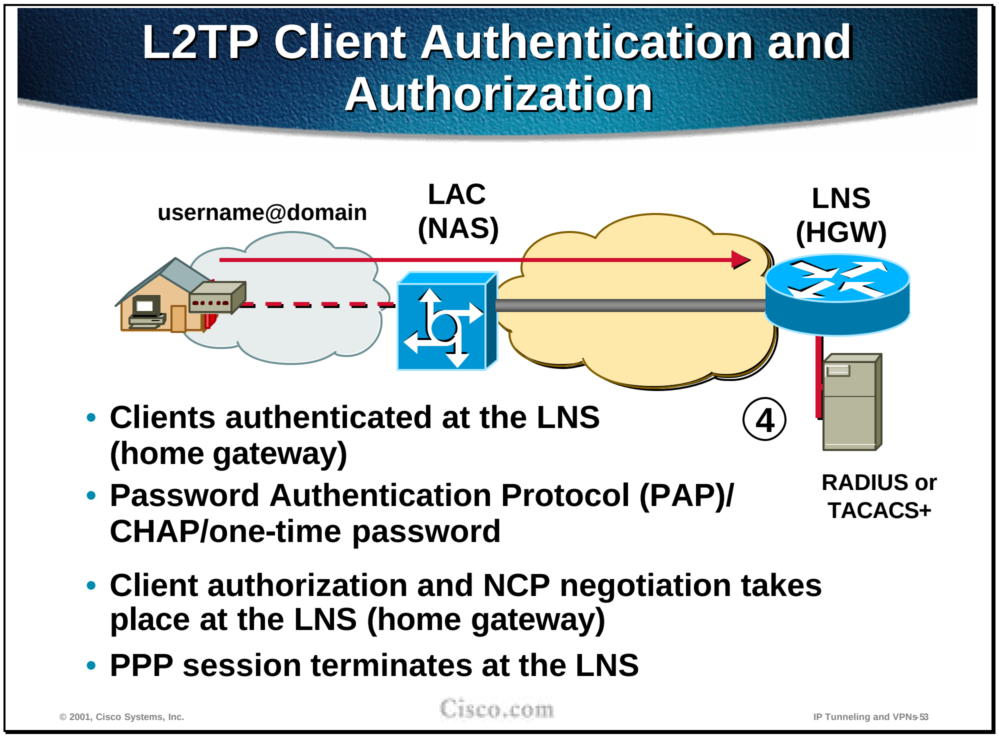
RADIUS or
TACACS+

- Bidirectional authentication done by tunnel peers before opening tunnel

Cisco.com

IP Tunneling and VPNs-52

Once the LAC contacts the LNS, they authenticate each other before any sessions are attempted within the tunnel. Alternately the LNS can accept tunnel creation without any tunnel authentication of the LAC. The purpose of LAC-to-LNS authentication is to prevent L2TP session spoofing.



L2TP Client Authentication and Authorization

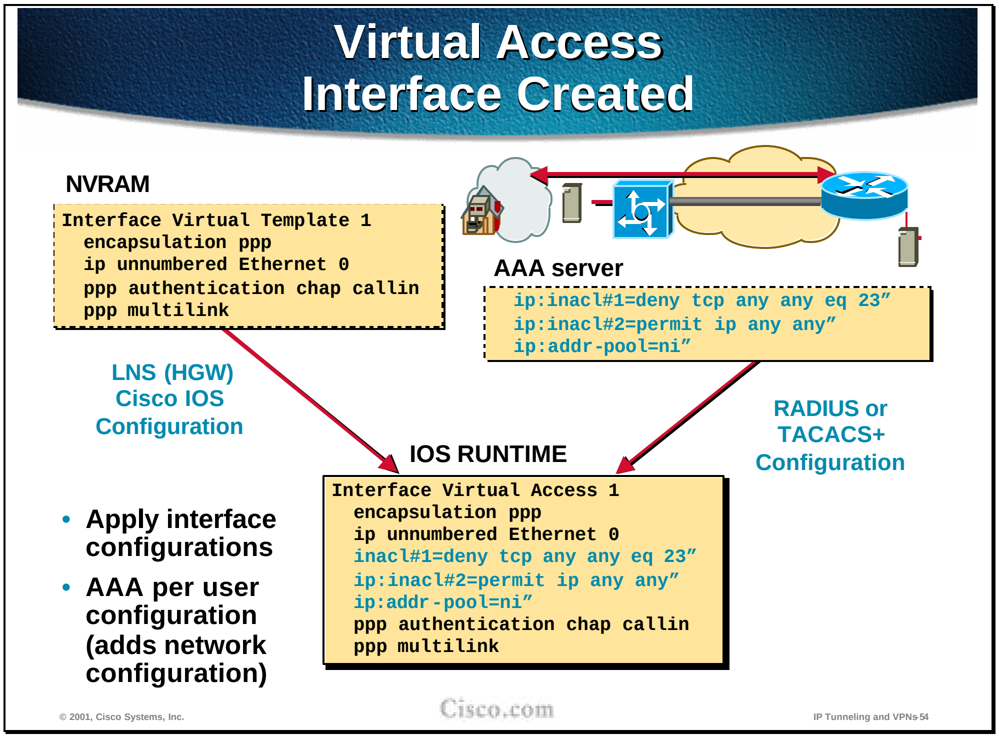
- Clients authenticated at the LNS (home gateway)
- Password Authentication Protocol (PAP)/ CHAP/one-time password
- Client authorization and NCP negotiation takes place at the LNS (home gateway)
- PPP session terminates at the LNS

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-53

The LAC forwards the NCP negotiation and CHAP response from the remote user to the LNS, which attempts to authenticate the remote user, using its own authentication methods and user database.

Once the remote user is authenticated on the LNS, the LNS creates a new virtual access interface to terminate the PPP session. Here the LNS is authenticating the user against the corporate AAA server. If you compare with the first authentication step, this means that the SP needs only to identify the DNIS or corporate identity, and that true user authentication is done by the LNS (the corporation). In other words, the SP does not have to track who is currently employed by the corporation, a considerable labor saving.

The corporation can also assign an address from a corporate network space or address pool to the dial client. This preserves SP address space. And since the dial user’s subnet is known (as opposed to whatever address the SP might issue), implementing security and other access policies is simpler for the corporation.



Virtual Access Interface Created

NVRAM

```
Interface Virtual Template 1
  encapsulation ppp
  ip unnumbered Ethernet 0
  ppp authentication chap callin
  ppp multilink
```

AAA server

```
  ip:inacl#1=deny tcp any any eq 23”
  ip:inacl#2=permit ip any any”
  ip:addr-pool=ni”
```

LNS (HGW)
Cisco IOS
Configuration

RADIUS or
TACACS+
Configuration

IOS RUNTIME

```
Interface Virtual Access 1
  encapsulation ppp
  ip unnumbered Ethernet 0
  inacl#1=deny tcp any any eq 23”
  ip:inacl#2=permit ip any any”
  ip:addr-pool=ni”
  ppp authentication chap callin
  ppp multilink
```

- Apply interface configurations
- AAA per user configuration (adds network configuration)

© 2001, Cisco Systems, Inc.

Cisco.com

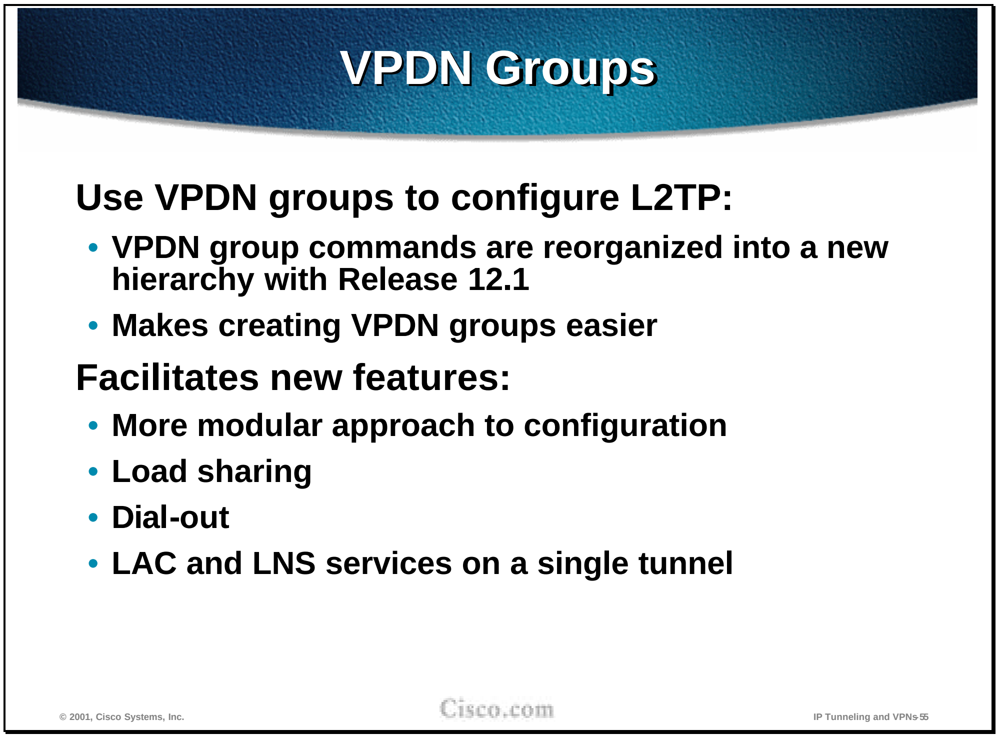
IP Tunneling and VPNs-54

The LNS creates a virtual access interface using negotiated options and authentication information.

If options on the virtual template do not match the options negotiated with the LAC, the connection will fail and a disconnect is sent to the LAC.

After creating the virtual access interface, the LNS then installs a static route to the interface in the routing table.

The address issued can come from the AAA server, out of the corporate address space.



VPDN Groups

Use VPDN groups to configure L2TP:

- **VPDN group commands are reorganized into a new hierarchy with Release 12.1**
- **Makes creating VPDN groups easier**

Facilitates new features:

- **More modular approach to configuration**
- **Load sharing**
- **Dial-out**
- **LAC and LNS services on a single tunnel**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-55

VPDN groups are used to configure L2TP. We will need to sidetrack briefly to understand how the VPDN group commands work, before looking at them in use in real configuration examples.

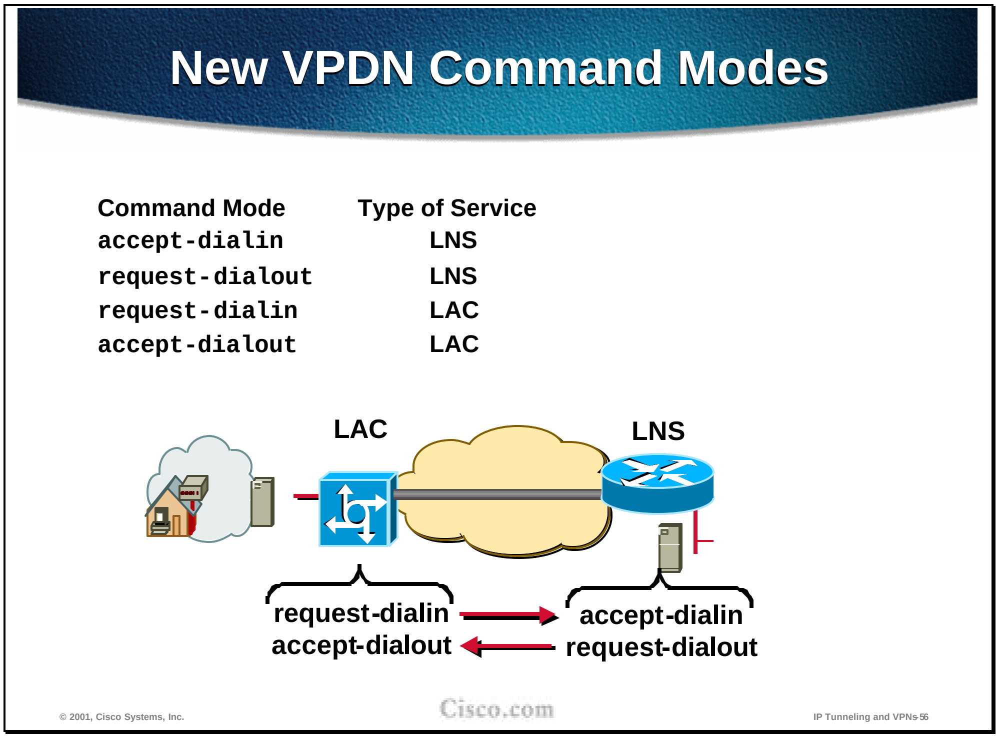
The VPDN Group Reorganization feature in Cisco IOS Release 12.1 organizes the VPDN group commands into a new hierarchy. As we'll see, VPDN groups can now support:

- LNS VPDN services:
  - Accept dial-in
  - Request dial-out
- LAC VPDN services:
  - Request dial-in
  - Accept dial-out
- One of the four VPDN services

This feature helps facilitate the following new features and protocol flexibility:

- Load sharing
- Dial-out
- LAC and LNS services on a single tunnel

This feature enables individual VPDN groups to tunnel both dial-in and dial-out calls using the same tunnel.



New VPDN Command Modes

Command Mode	Type of Service
`accept-dialin`	LNS
`request-dialout`	LNS
`request-dialin`	LAC
`accept-dialout`	LAC

Cisco.com

IP Tunneling and VPNs-56

We will see what these configuration commands actually do in more detail later. These refer to modes or roles a router will be playing in a VPDN design.

The keywords and arguments for the existing **accept-dialin** and **request-dialin** commands are now independent **accept-dialin** mode and **request-dialin** mode commands. The previous syntax is still supported, but when you display the configuration, the commands will be converted to appear in the new format.

That is, the old style commands took many keywords and arguments in a long command. The options are now entered separately within a mode. For example, to configure a LAC to request dial-in, you could use the old command:

```
request dialin l2tp ip 10.1.2.3 domain jgb.com
```

When you view the configuration, the keywords and arguments are displayed in the new format as individual commands:

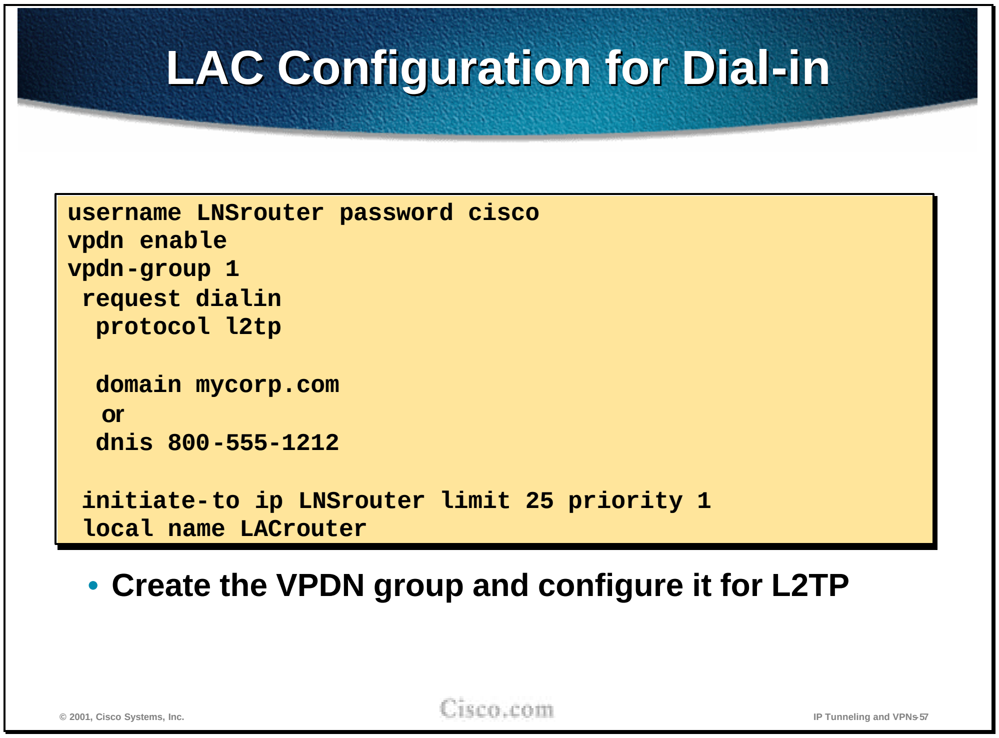
```
request dialin

protocol l2tp

domain jgb.com

initiate-to ip 10.1.2.3
```

Similarly, the new **accept-dialout** and **request-dialout** commands have subgroup commands that are used to specify such information as the tunneling protocol and dialer resource.

LNS VPDN groups can be configured for **accept-dialin** or **request-dialout**. These are the roles an LNS would be playing in a network—it would accept incoming dialin tunnels and request a tunnel for dialout.

LAC VPDN groups can be configured for **accept-dialout** or **request-dialin**. These are the roles the LAC would be playing in the network: it would accept a tunnel connection from an LNS for dialout, and if a call comes into the LAC, it will need to request a tunnel for dial-in purposes.

Within one of the VPDN modes you can then configure various subgroup commands, as appropriate for that setting. We will see these in actual configurations in a few slides, where all this will come together for you (we trust and hope).



LAC Configuration for Dial-in

```
username LNSrouter password cisco
vpdn enable
vpdn-group 1
 request dialin
  protocol l2tp

  domain mycorp.com
   or
  dnis 800-555-1212

 initiate-to ip LNSrouter limit 25 priority 1
 local name LACrouter
```

- Create the VPDN group and configure it for L2TP

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-57

L2TP configuration also follows the access VPN process, so we will focus on the tunnel configuration.

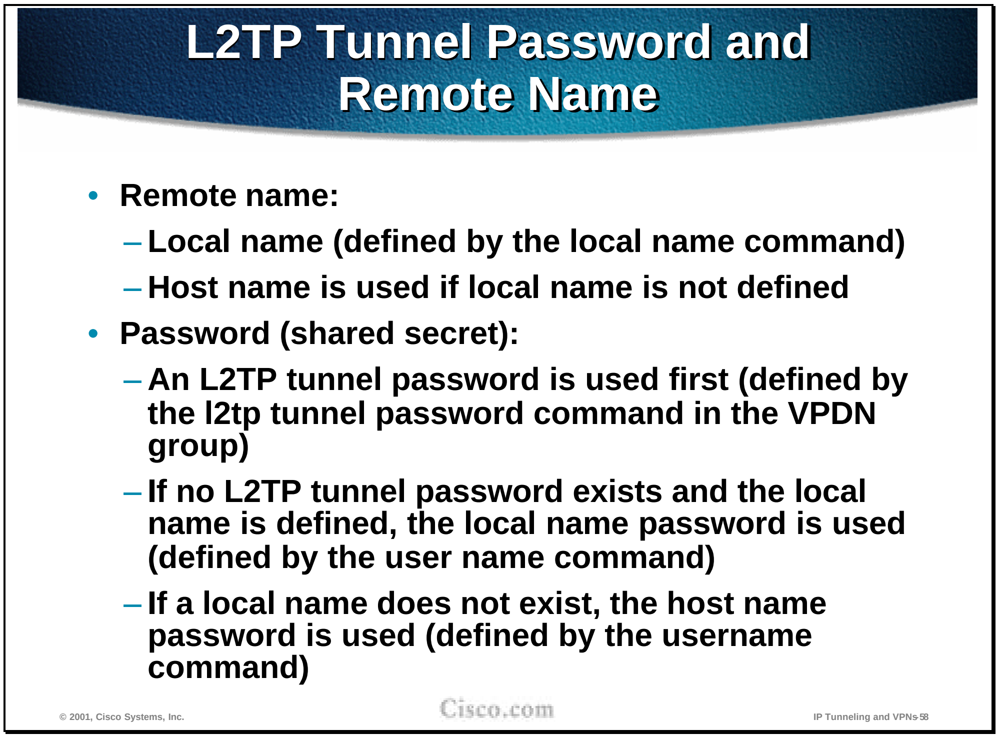
The configuration starts with a local username, which is the name of the router this router will tunnel to. Authentication is CHAP style, with a shared secret.

To configure the LAC for dial-in after having configured AAA, enable VPDN and create the VPDN group that will have all the VPDN atttributes.

Set the protocol to L2TP and specify the domain name or DNIS of the users that are to be tunneled by this VPDN group. (There is one VPDN group per DNIS or customer domain name.)

The **initiate-to ip-address** is the address of the LNS for the far end of the tunnel. If local name is defined, then a matching username must be defined at the LNS. The limit is how many sessions may pass through the tunnel at one time, and is optional. Priority is also an optional keyword, specifying priority for this tunnel peer. One (1) is the highest priority.

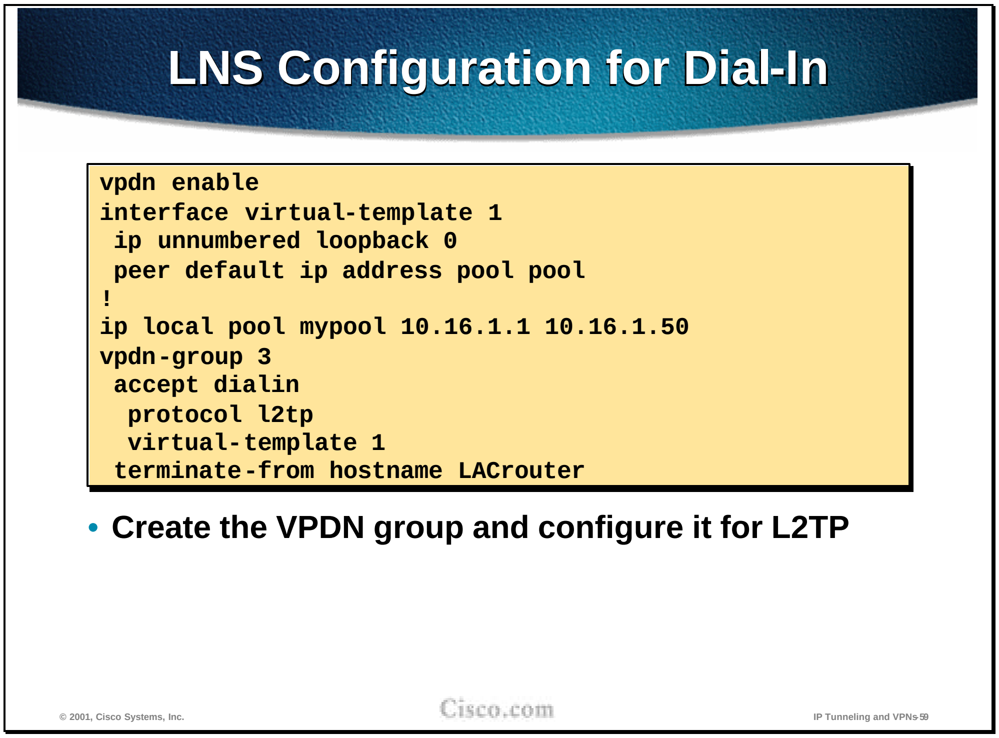
Note Note the new syntax of the **vpdn-group** command.



L2TP Tunnel Password and Remote Name

- Remote name:
  - Local name (defined by the local name command)
  - Host name is used if local name is not defined
- Password (shared secret):
  - An L2TP tunnel password is used first (defined by the l2tp tunnel password command in the VPDN group)
  - If no L2TP tunnel password exists and the local name is defined, the local name password is used (defined by the user name command)
  - If a local name does not exist, the host name password is used (defined by the username command)

The L2TP tunnel password and remote name is used when the LAC and LNS authenticate each other prior to activating the tunnel.



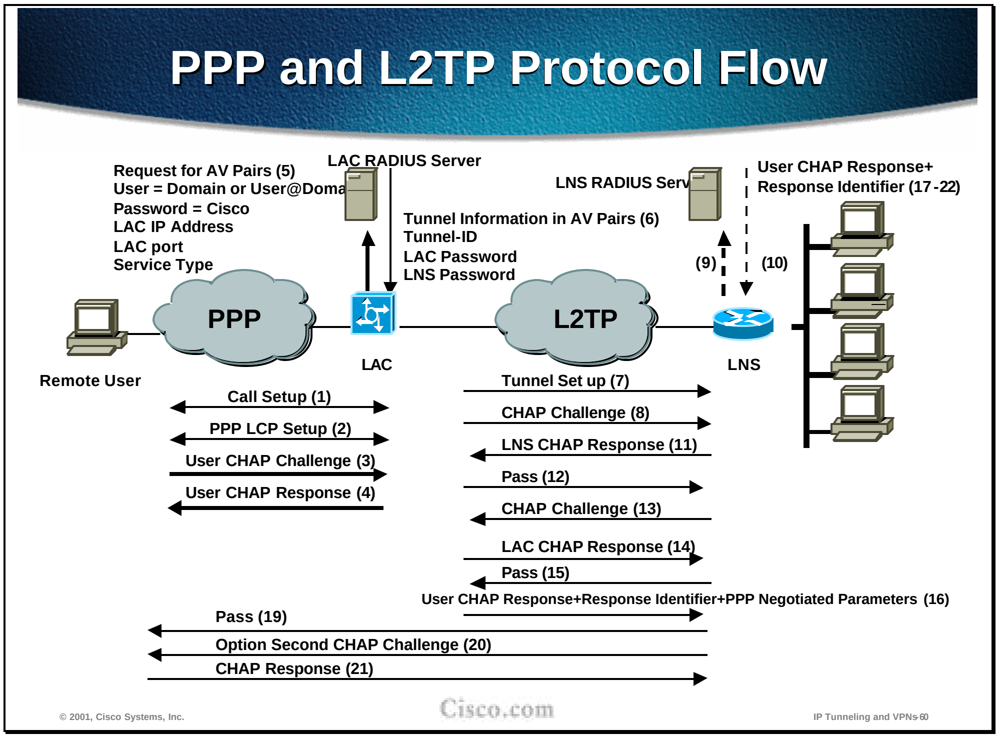
LNS Configuration for Dial-In

```
vpdn enable
interface virtual-template 1
 ip unnumbered loopback 0
 peer default ip address pool pool
!
ip local pool mypool 10.16.1.1 10.16.1.50
vpdn-group 3
 accept dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname LACrouter
```

- **Create the VPDN group and configure it for L2TP**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-59

To configure the LNS for dial-in, create a virtual template and VPDN Group that will be cloned to create the virtual access interface. The **terminate-from hostname** command tells the LNS to accept tunnels from hosts that have this configured as the local name. We will look at the configuration for dial-out later on in this module.



PPP and L2TP Protocol Flow

Request for AV Pairs (5)
User = Domain or User@Doma
Password = Cisco
LAC IP Address
LAC port
Service Type

LAC RADIUS Server

LNS RADIUS Serv

User CHAP Response+
Response Identifier (17-22)

Tunnel Information in AV Pairs (6)
Tunnel-ID
LAC Password
LNS Password

(9)

(10)

PPP

L2TP

Remote User

LAC

LNS

Call Setup (1)

PPP LCP Setup (2)

User CHAP Challenge (3)

User CHAP Response (4)

Tunnel Set up (7)

CHAP Challenge (8)

LNS CHAP Response (11)

Pass (12)

CHAP Challenge (13)

LAC CHAP Response (14)

Pass (15)

User CHAP Response+Response Identifier+PPP Negotiated Parameters (16)

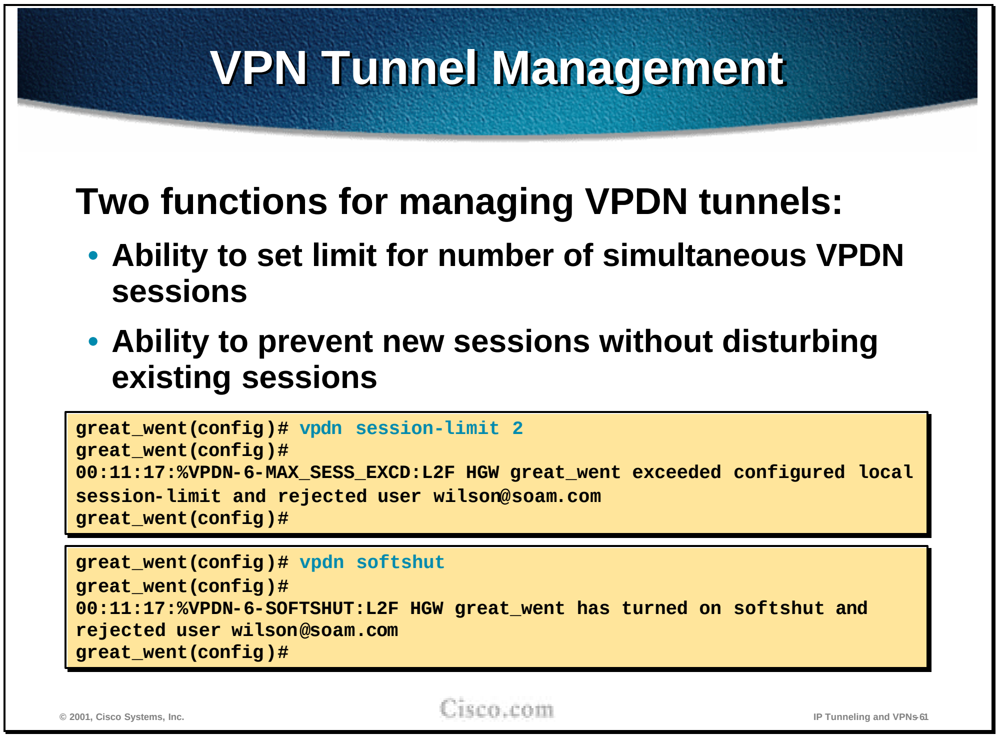
Pass (19)

Option Second CHAP Challenge (20)

CHAP Response (21)

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-60

This diagram shows the end-to-end protocol flow and is useful for debugging connection issues. Use debugging commands to trace and isolate where the problem is occurring.



VPN Tunnel Management

Two functions for managing VPDN tunnels:

- **Ability to set limit for number of simultaneous VPDN sessions**
- **Ability to prevent new sessions without disturbing existing sessions**

```
great_went(config)# vpdn session-limit 2
great_went(config)#
00:11:17:%VPDN-6-MAX_SESS_EXCD:L2F HGW great_went exceeded configured local
session-limit and rejected user wilson@soam.com
great_went(config)#
```

```
great_went(config)# vpdn softshut
great_went(config)#
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW great_went has turned on softshut and
rejected user wilson@soam.com
great_went(config)#
```

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs 61

The VPN Tunnel Management feature provides network administrators with two new functions for managing VPN tunnels:

- The ability to set a limit for the maximum number of allowed simultaneous VPN sessions
- The ability to prevent new sessions from being established on a VPN tunnel without disturbing the service of existing sessions (this function is called VPN tunnel soft shutdown)

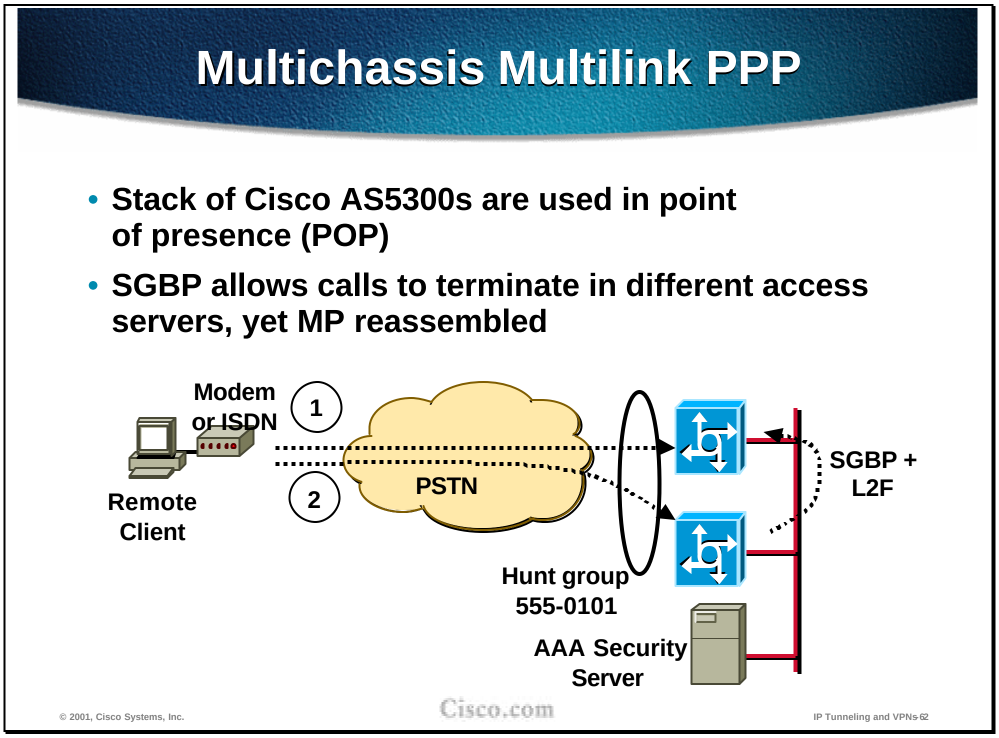
To limit the number of simultaneous VPN sessions that can be established on a router, use the **vpdn session-limit** command. To allow an unlimited number of simultaneous VPN sessions, use the **no** form of this command.

The **vpdn softshut** command prevents new sessions from being established on a VPN tunnel without disturbing existing sessions.

These functions can be used on either end of a VPN tunnel—the NAS or on the tunnel server.

When this feature is enabled, Multichassis Multilink PPP (MMP) L2F tunnels can still be created and established.

The VPN Tunnel Management feature gives network administrators greater flexibility in managing VPN traffic. It enables network administrators to prevent a VPN tunnel from becoming congested without affecting previously established sessions.



Multichassis Multilink PPP

- Stack of Cisco AS5300s are used in point of presence (POP)
- SGBP allows calls to terminate in different access servers, yet MP reassembled

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-62

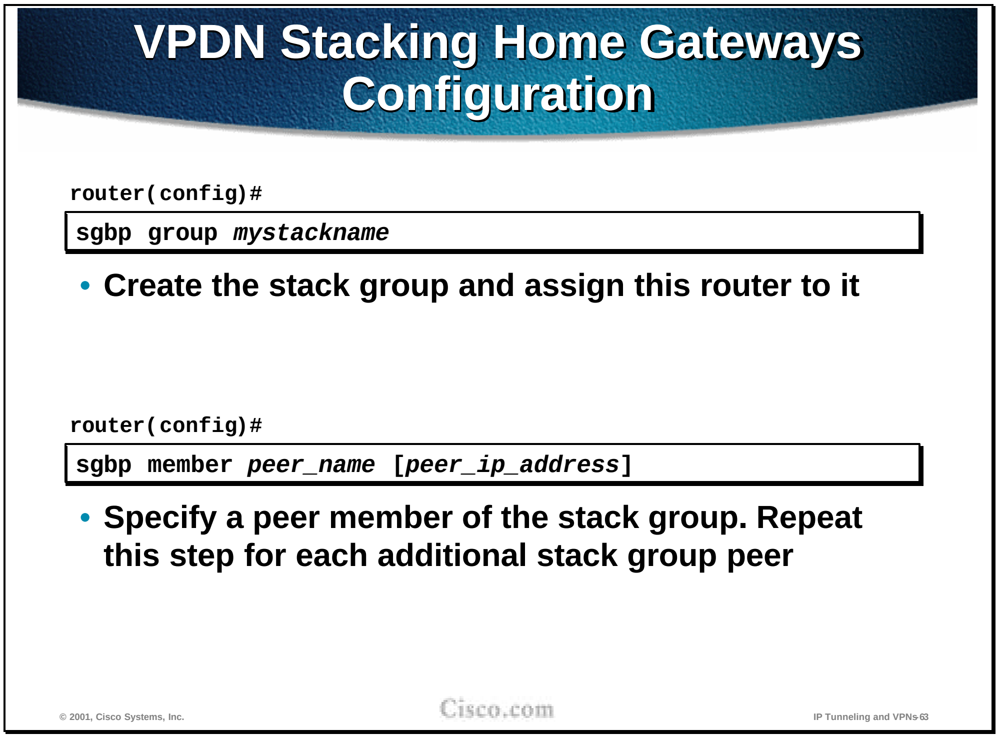
VPDN Stacking Home Gateways are designed to support large scale POPs. They use MLP, MMP, SGBP and tunneling (L2F or L2TP).

What is new here is the support for L2TP (see multi-hop). MMP itself has been available for a while with direct dial-in.

We will now review how MMP works. The idea is that two calls may not end up on the same physical device. This could be a big problem for a service provider if their customer wants to run MLP. The answer is for the second access server called to create an L2F tunnel to the first, and for that access server to re-assemble the MLP fragments.

The SGBP provides investment protection by allowing a bidding process, so you can steer the reassembly to the best device, possibly a dedicated MMP offload router. (The Cisco 3600 and 7200 particle buffer memory architecture lends itself particularly well to this task.)

Note MMP is **not** Cisco proprietary, in the sense that the user is doing standard MP and should be completely unaware that anything special is happening at the other end of their connection.



VPDN Stacking Home Gateways Configuration

```
router(config)#
sgbp group mystackname
```

- **Create the stack group and assign this router to it**

```
router(config)#
sgbp member peer_name [peer_ip_address]
```

- **Specify a peer member of the stack group. Repeat this step for each additional stack group peer**

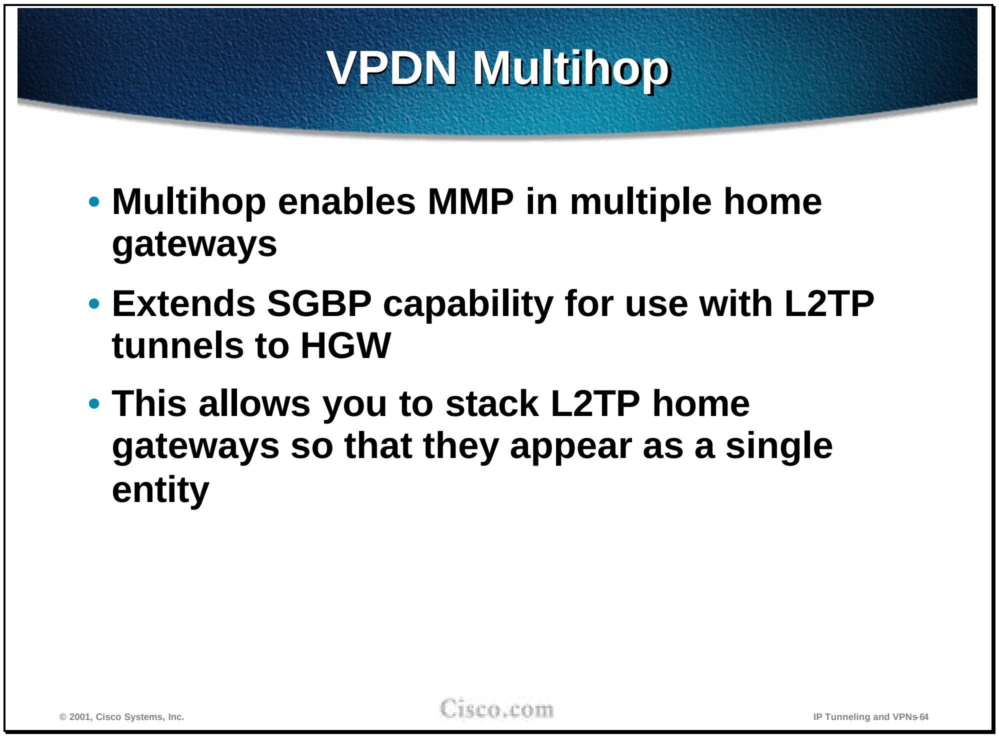
© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-63

To configure SGBP, configure access VPNs then add the configuration shown.

Just create the SGBP group and assign peer IP addresses on the LNSs.

To define a named stack group and make this router a member of that stack group, use the **sgbp group** command in global configuration mode.

To specify the host name and IP address (optional) of a router or access server that is a peer member of a stack group, use the **sgbp member** command in global configuration mode. (The command is shown in the slide.)



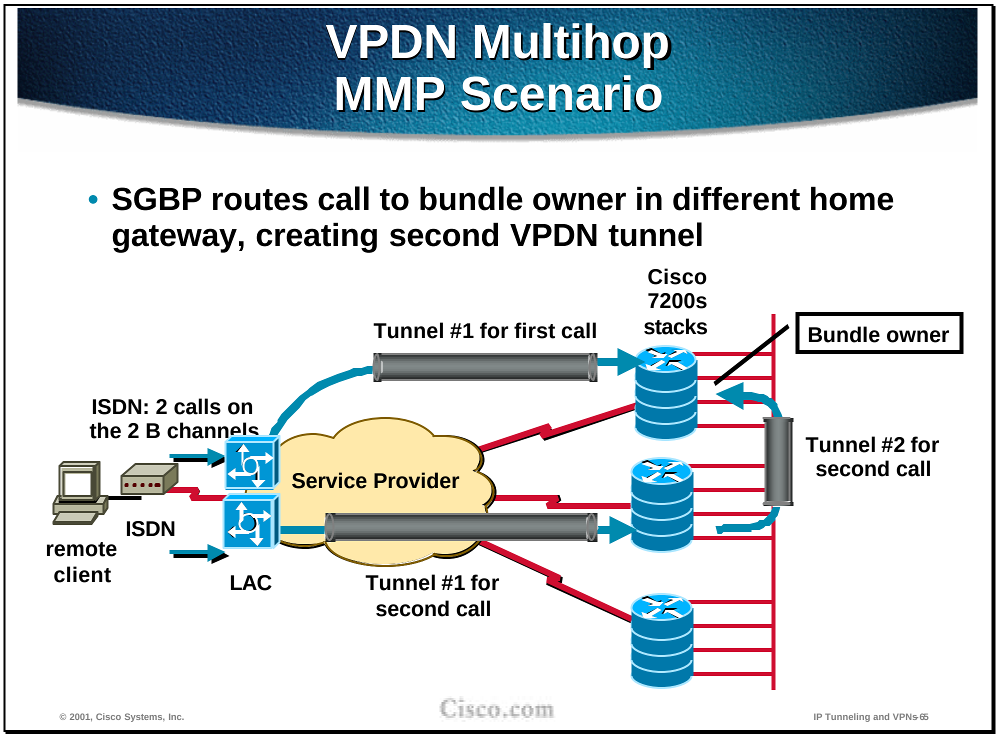
VPDN Multihop

- Multihop enables MMP in multiple home gateways
- Extends SGBP capability for use with L2TP tunnels to HGW
- This allows you to stack L2TP home gateways so that they appear as a single entity

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-64

With multihop VPDN, packets generated from a remote host can traverse more than one tunnel. Ordinarily, packets cannot hop through more than one tunnel. Packets received by different home gateways in a multiple home gateway stack must be recombined and resequenced on the bundle owner. Some instances require packets to be rerouted to the bundle owner in another home gateway, traversing more than two tunnels. Before even reaching the corporate network, the packets have already crossed a tunnel created by the VPDN, connecting the NAS to the corporate network. Once they arrive at the corporate network, the packets may need to traverse more than another tunnel, crossing home gateways to arrive at the bundle owner. This number of tunnel crossings would violate the multiple-tunnel rule, preventing the packets from successfully arriving at the bundle owner.

Multihop VPDN allows packets to pass through multiple tunnels using both L2F and L2TP protocols in a VPDN environment.



VPDN Multihop MMP Scenario

- SGBP routes call to bundle owner in different home gateway, creating second VPDN tunnel

© 2001, Cisco Systems, Inc.

Cisco.com

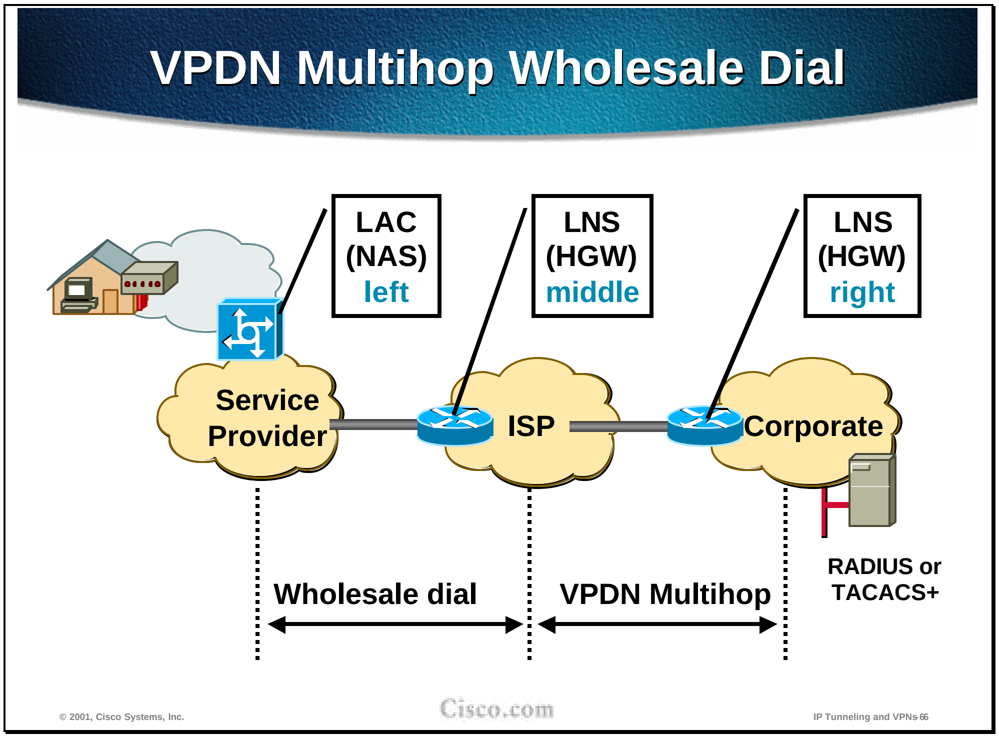
IP Tunneling and VPNs-65

There are two scenarios for VPDN multihop: MMP and wholesale dial.

For the MMP scenario, the corporate location has configured stacking LNSs for scalability using the SGBP. This is sometimes known as stacking home gateways.

The client using ISDN to connect to the LAC has established one tunnel to the first corporate LNS. When the client needs more bandwidth than a single B-Channel can provide, it can use MLP to dial up an additional B-channel. If the call is received on the same LAC as the first B-Channel, the existing tunnel will be used.

However, if the call terminates in another LAC, the LAC will try to create its own tunnel to the stack group (if one does not already exist). If the tunnel is not received on the first LNS, which by default will be the bundle owner, the LNS that receives the call will use SGBP to find the bundle owner. It will then create a third L2TP tunnel to the bundle owner and forward packets to it for reassembly.



VPDN Multihop Wholesale Dial

LAC (NAS) left

LNS (HGW) middle

LNS (HGW) right

Service Provider

ISP

Corporate

RADIUS or TACACS+

Wholesale dial

VPDN Multihop

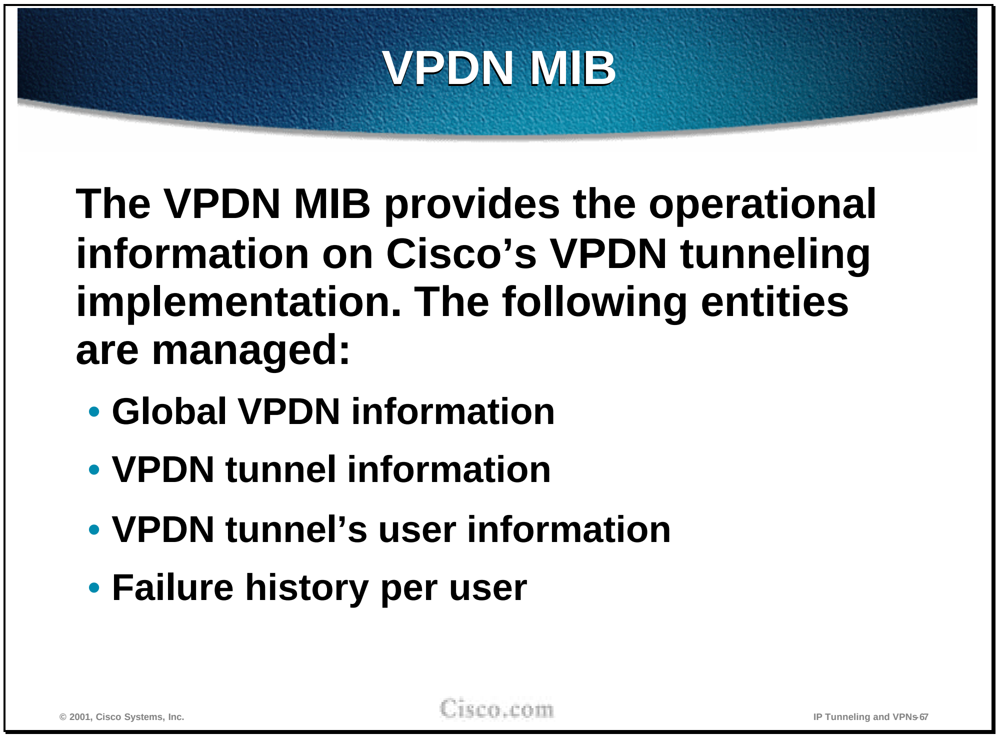
© 2001, Cisco Systems, Inc.

Cisco.com

IP Tunneling and VPNs-66

The second scenario for VPDN multihop is wholesale dial. In this case an ISP would like to provide dial access to its customers without actually owning any equipment with physical dial-in capability. An ISP can sign a wholesale dial contract with another service provides with dial access capability, and use the service provider's access servers at the last mile. The service provider then forwards dial sessions over IP to the ISP, which may in turn offer its own VPDN service to its customers, creating another Layer-2 tunneling session between the ISP "middle gateway" and the customer LNS.

Each end-to-end connection will traverse two L2TP tunnels: the first tunnel providing virtual dial access to the ISP, and the second providing VPDN functionality to the customers of the ISP.



VPDN MIB

The VPDN MIB provides the operational information on Cisco's VPDN tunneling implementation. The following entities are managed:

- **Global VPDN information**
- **VPDN tunnel information**
- **VPDN tunnel's user information**
- **Failure history per user**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-67

The VPDN MIB includes four groups of objects:

- System-wide information and statistics regarding VPDN:
  - cvpdnSystemInfo
- Information and statistics regarding active VPDN tunnels:
  - cvpdnTunnelInfo
- Information and statistics regarding active user sessions in active VPDN tunnels:
  - cvpdnTunnelUserInfo
- Information regarding failure history per user name:
  - cvpdnUserToFailHistInfo

The names of the relevant SNMP MIBs are:

- SNMP Ver 1 MIB—CISCO-VPDN-MGMT-MIB -V1SMI.my
- SNMP ver 2 MIB—CISCO-VPDN-MGMT-MIB.my

Summary

- Cisco IOS supports the standardized L2TP Layer-2 tunneling method
- The L2TP method is configured almost like a dial-up session, with the help of Cisco IOS vpdn-group CLI functionality
- The Stack Group Bidding Protocol enables multiple access servers to terminate multilink dial connections, and maintain consistency by terminating the Layer-2 (PPP) session on one access server only. This enables a SP to scale its dial pools by simply adding additional access servers and still maintain multilink functionality.

Lesson Review

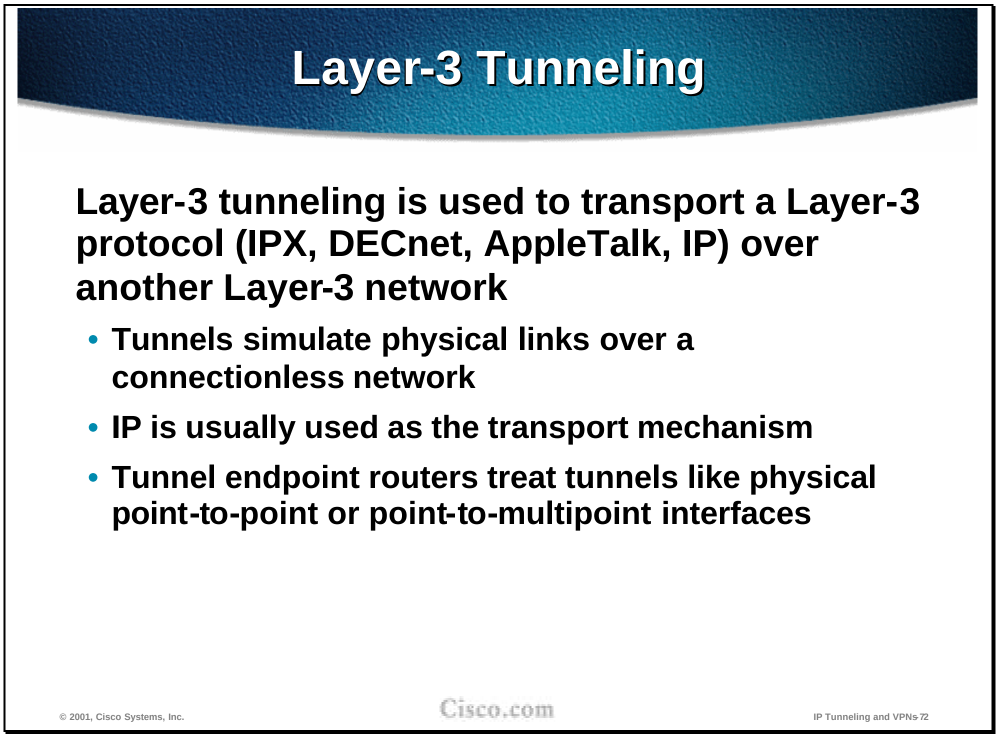
1. What protocol is tunneled within L2TP?
2. How does L2TP differ from PPTP?
3. Which Cisco IOS configuration mechanism is used to bind L2TP sessions to virtual interfaces?
4. How is the AAA functionality distributed between the LAC and the LNS?
5. How does the Multichassis Multilink PPP feature use L2TP functionality?

Layer-3 Tunneling

Objectives

Upon completion of this module, you will be able to perform the following tasks:

- Describe Layer-3 tunneling
- Describe the GRE tunneling method
- Configure and troubleshoot GRE tunneling



Layer-3 Tunneling

Layer-3 tunneling is used to transport a Layer-3 protocol (IPX, DECnet, AppleTalk, IP) over another Layer-3 network

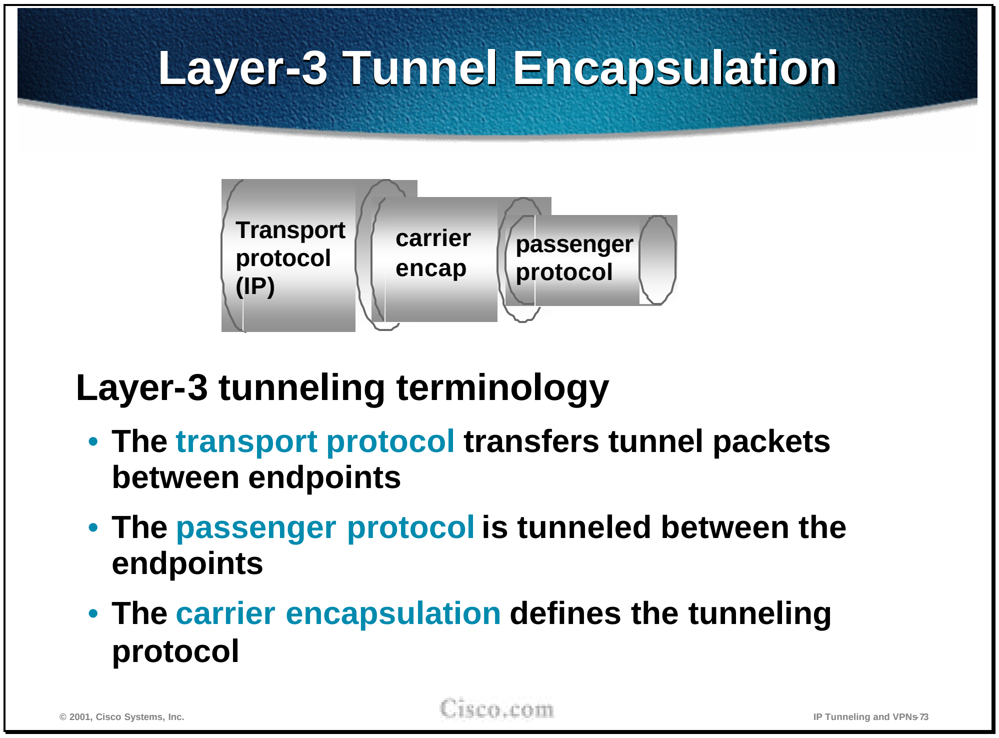
- **Tunnels simulate physical links over a connectionless network**
- **IP is usually used as the transport mechanism**
- **Tunnel endpoint routers treat tunnels like physical point-to-point or point-to-multipoint interfaces**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-72

Layer-3 tunneling is used to transport a Layer-3 protocol over another Layer-3 network. Usually, Layer-3 tunneling is used either to connect two discontiguous parts of a non-IP network over an IP network, or to connect two IP networks over a backbone IP network, possibly hiding IP addressing details of the two networks from the backbone IP network.

To understand the process of Layer-3 tunnelling, consider connecting two AppleTalk networks with a non-AppleTalk backbone, such as IP. Tunnelling AppleTalk through a foreign protocol, such as IP, can solve this problem. Tunnelling encapsulates an AppleTalk packet inside the foreign protocol packet, which is then sent across the backbone to a destination router. The destination router then removes the foreign protocol encapsulation from the AppleTalk packet and, if necessary, routes the packet to a normal AppleTalk network. While in transit over the backbone, the encapsulated packet benefits from any features normally enjoyed by IP packets, including QoS, flexible routing, and load balancing. The backbone network is unaware of the tunneled passenger protocol, because it routes traffic only based on the outer, IP header.

Layer-3 tunnels can be point-to-point or point-to-multipoint associations of routers or hosts. Point-to-point tunnels are used to emulate physical links between pairs of sites, while point-to-multipoint tunnels are usually used to simplify a hub-and-spoke tunnel configuration among many routers.


Transport
protocol
(IP)
carrier
encap
passenger
protocol

Layer-3 Tunnel Encapsulation

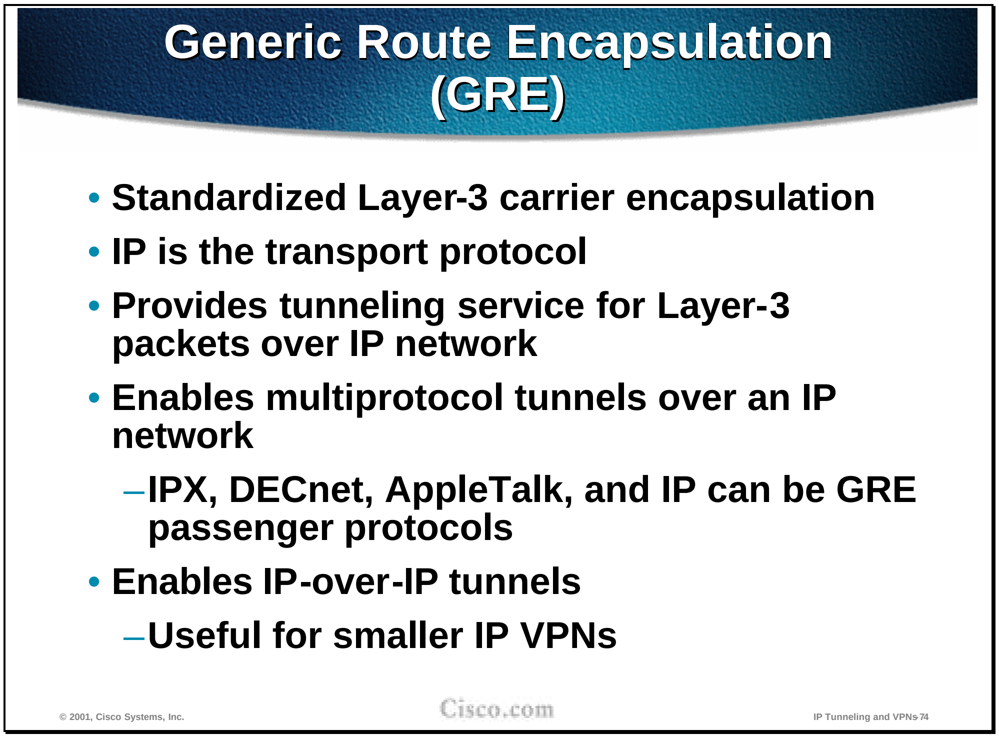
Layer-3 tunneling terminology

- The transport protocol transfers tunnel packets between endpoints
- The passenger protocol is tunneled between the endpoints
- The carrier encapsulation defines the tunneling protocol

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-73

When discussing Layer-3 tunneling, the following terms are used

- The transport protocol is the protocol used to transport tunneled packets between tunnel endpoints. With IP tunnels, the transport protocol is IP.
- The passenger protocol is the protocol carried inside the tunnel, invisible to the transport network. The transport network does not have to support the passenger protocol.
- The carrier encapsulation is used as a shim encapsulation, describing the passenger protocol to the tunnel endpoints, where the passenger protocol is encapsulated and decapsulated.



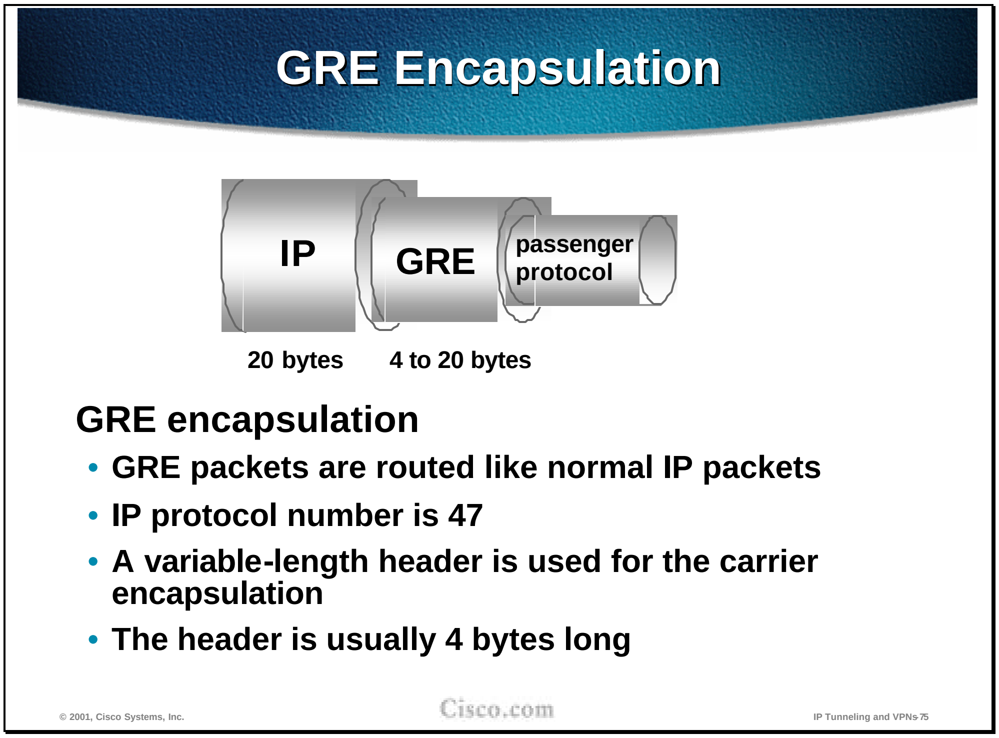
Generic Route Encapsulation (GRE)

- Standardized Layer-3 carrier encapsulation
- IP is the transport protocol
- Provides tunneling service for Layer-3 packets over IP network
- Enables multiprotocol tunnels over an IP network
  - IPX, DECnet, AppleTalk, and IP can be GRE passenger protocols
- Enables IP-over-IP tunnels
  - Useful for smaller IP VPNs

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-74

The Generic Route Encapsulation (GRE) is a standardized Layer-3 carrier encapsulation, designed for generic tunneling of protocols. GRE is described in RFC 1701, and RFC 1702 defines how GRE uses IP as the transport protocol (GRE IP).

In Cisco IOS, GRE tunneling is used to tunnel multiple protocols (IPX, DECnet, AppleTalk, and others) over an IP network. Also, GRE IP can tunnel IP over IP, which is useful when building small-scale IP VPN network, which do not require substantial security. GRE has no built-in security mechanisms built, but can be secured by additional mechanisms, such as IPsec traffic protection, of the Cisco Encryption Technology protection.



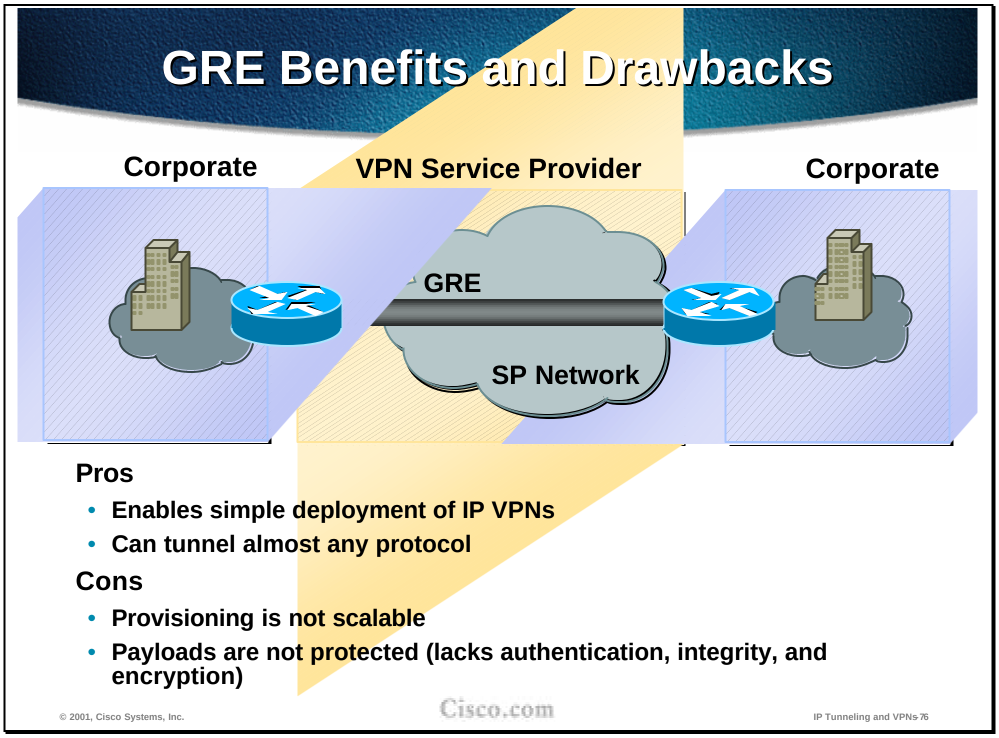
GRE Encapsulation

GRE encapsulation

- GRE packets are routed like normal IP packets
- IP protocol number is 47
- A variable-length header is used for the carrier encapsulation
- The header is usually 4 bytes long

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-75

The GRE protocol is an IP protocol with the protocol number of 47. The GRE header is of variable length, and at the minimum defines the passenger protocol carried in a GRE packet. The header is from 4 to 20 bytes long, depending on the GRE options (such as optional sequencing) used within each packet.



GRE Benefits and Drawbacks

Pros

- **Enables simple deployment of IP VPNs**
- **Can tunnel almost any protocol**

Cons

- **Provisioning is not scalable**
- **Payloads are not protected (lacks authentication, integrity, and encryption)**

© 2001, Cisco Systems, Inc. Cisco.com IP Tunneling and VPNs-76

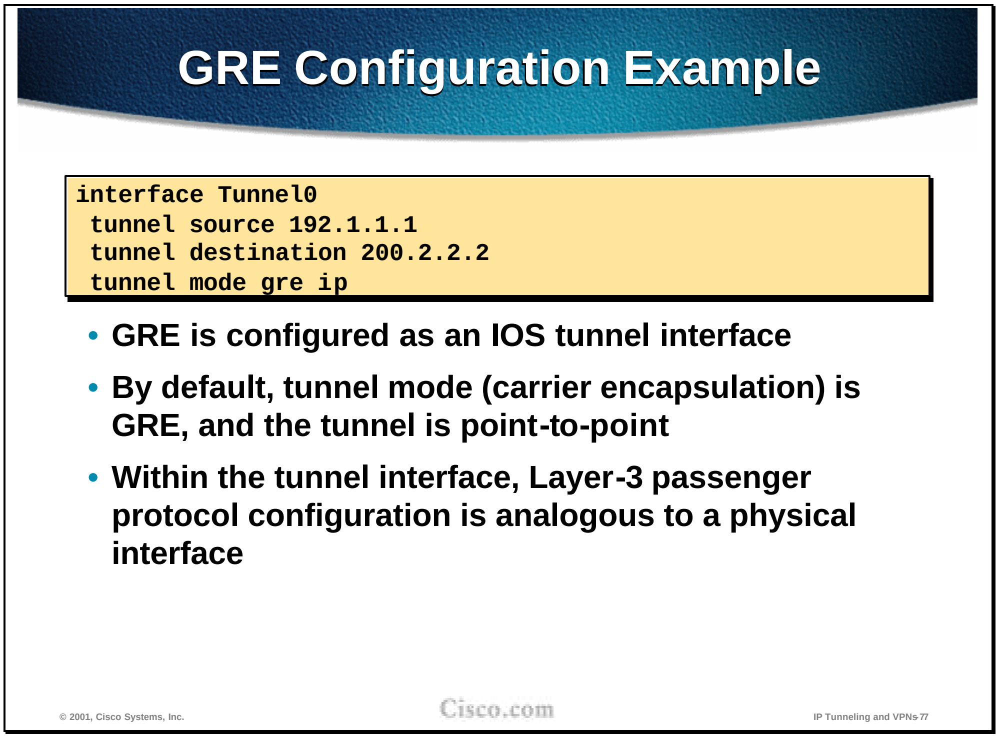
The figure shows two discontiguous networks, connected over a point-to-point logical link implemented over an IP network using a GRE IP tunnel. Such a tunnel is implemented on both border routers, and is visible in Cisco IOS as an interface.

The benefits of GRE IP tunneling are

- GRE enables simple and flexible deployment of basic IP VPNs.
- In Cisco IOS, GRE IP can tunnel almost any Layer-3 protocol.

GRE IP tunneling also has some drawbacks

- Provisioning of tunnels is not very scalable in a full-mesh network (every point-to-point association has to be defined separately; the Next-Hop Routing Protocol (NHRP) can be used to achieve some configuration scalability, and point-to-multipoint tunnels can be used as a remedy in strictly hub-and-spoke networks).
- Packet payload is not protected against snooping and unauthorized changes, and there is no authentication of sender. IPsec provides all those functions, and can be combined with GRE IP.



GRE Configuration Example

```
interface Tunnel0
 tunnel source 192.1.1.1
 tunnel destination 200.2.2.2
 tunnel mode gre ip
```

- GRE is configured as an IOS tunnel interface
- By default, tunnel mode (carrier encapsulation) is GRE, and the tunnel is point-to-point
- Within the tunnel interface, Layer-3 passenger protocol configuration is analogous to a physical interface

© 2001, Cisco Systems, Inc.

Cisco.com

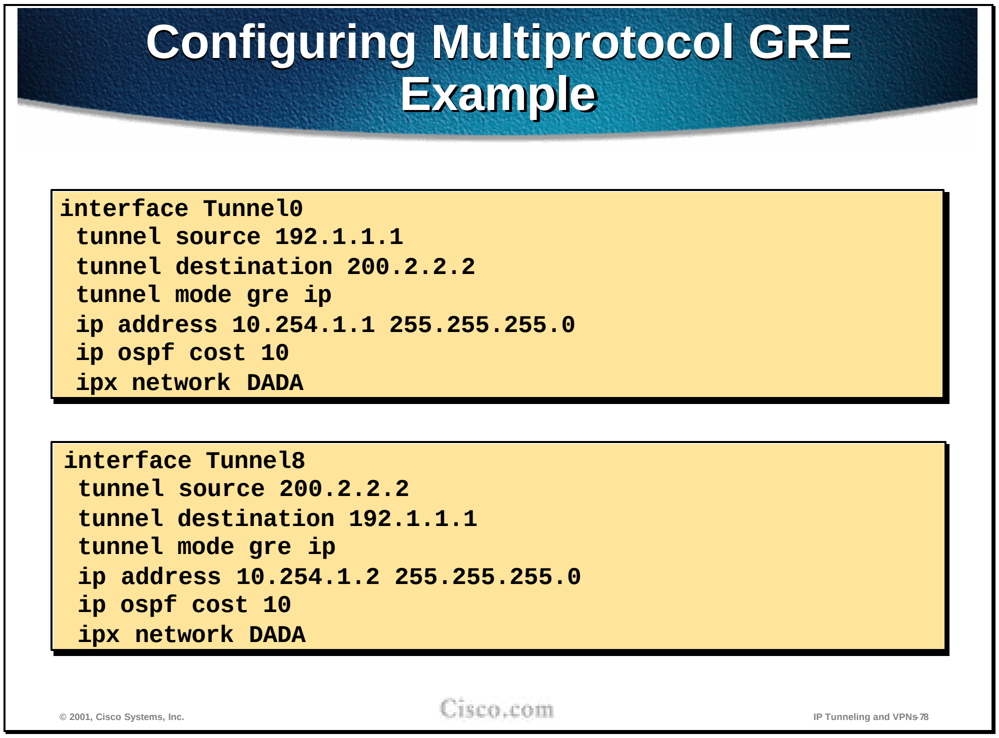
IP Tunneling and VPNs 77

Tunneling provides a way to encapsulate arbitrary packets inside a transport protocol. This feature is implemented as a virtual interface to provide a simple interface for configuration. The tunnel interface is not tied to specific "passenger" or "transport" protocols, but rather, it is an architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. Because tunnels are point-to-point links, you must configure a separate tunnel for each link.

Within the tunnel interface, the **tunnel source** and **tunnel destination** commands configure the tunnel endpoints. The tunnel source must be a local routers interface address, such as, for example, a loopback address. The other peer's tunnel source and destination must exactly mirror the local peer's configuration, that is, the tunnel must be defined between the same IP addresses in both peers' configuration. The **tunnel mode gre ip** command specifies that GRE should be used as the tunnel carrier encapsulation.

The tunnel interface can be in almost all cases treated like a physical interface. Within the tunnel, Layer-3 parameters of the point-to-point link are defined (such as the Layer-3 address and routing protocol information), and most Layer-3 interface commands can be applied to the tunnel.

The Distributed GRE Tunneling Support feature allows Cisco IOS software to switch packets into and out of the generic routing encapsulation (GRE) tunnels using distributed Cisco Express Forwarding (dCEF). If dCEF is enabled, GRE packets will be dCEF-switched on distributed platforms.



Configuring Multiprotocol GRE Example

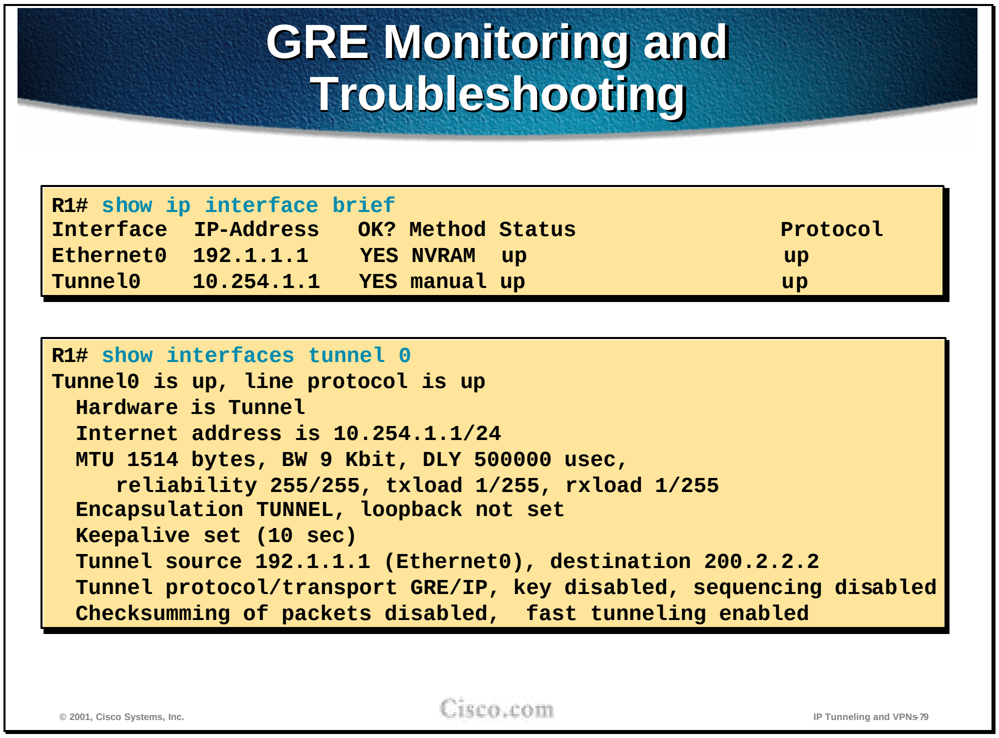
```
interface Tunnel0
 tunnel source 192.1.1.1
 tunnel destination 200.2.2.2
 tunnel mode gre ip
 ip address 10.254.1.1 255.255.255.0
 ip ospf cost 10
 ipx network DADA
```

```
interface Tunnel8
 tunnel source 200.2.2.2
 tunnel destination 192.1.1.1
 tunnel mode gre ip
 ip address 10.254.1.2 255.255.255.0
 ip ospf cost 10
 ipx network DADA
```

Cisco.com

IP Tunneling and VPNs-78

The figure shows the configurations of two routers configured for GRE tunneling. Note the symmetric configuration of tunnel source and destination. IP and IPX are enabled over the tunnel link, and OSPF provides routing over the tunnel, treating it like a point-to-point link.



GRE Monitoring and Troubleshooting

```
R1# show ip interface brief
Interface  IP-Address   OK? Method Status                Protocol
Ethernet0  192.1.1.1    YES NVRAM  up                    up
Tunnel0    10.254.1.1   YES manual up                    up
```

```
R1# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.254.1.1/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (10 sec)
  Tunnel source 192.1.1.1 (Ethernet0), destination 200.2.2.2
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Checksumming of packets disabled,  fast tunneling enabled
```

The **show ip interface brief** command can be used to quickly determine the status of the tunnel interface. The **show interface** command shows the configured tunnel parameters and the interface traffic statistics.

Summary

- Layer-3 tunneling transports Layer-3 packets of a routed protocol over another Layer-3 protocol, usually IP
- The GRE tunneling method is a RFC standard and can be used as a virtual point-to-point link transporting most Layer-3 protocols
- GRE point-to-point and point-to-multipoint tunnels are configured as Cisco IOS tunnel interfaces

Lesson Review

1. What is the usual transport protocol used by GRE?
2. What protocols can be tunneled within GRE?
3. Which Cisco IOS configuration mechanism is used to bind GRE sessions to interfaces?
4. How do routing protocols treat a GRE tunnel?

Summary

- A VPN is connectivity deployed on a shared infrastructure with the same policies and performance as a private network, with lower total cost of ownership.
- Layer-2 tunneling transports frames of a Layer-2 protocol over a routed, Layer-3 network. In a VPDN context, the tunneled protocol is usually the Point-to-Point Protocol (PPP).
- Cisco IOS supports the Microsoft Point-to-Point Tunneling Protocol (PPTP) Layer-2 tunneling method
- Cisco IOS supports the standardized L2TP Layer-2 tunneling method, which is configured almost like a dial-up session
- The GRE Layer-3 tunneling method is a RFC standard and can be used as a virtual point-to-point link transporting most Layer-3 protocols. GRE point-to-point and point-to-multipoint tunnels are configured as Cisco IOS tunnel interfaces

Appendix: Answers to Review Questions

Introduction to IP VPNs

1. What is a VPN?

A VPN is a connectivity option, which provides private connectivity over a public (shared network).

2. What are the three main benefits of using a VPN?

The three main benefits of a VPN are flexibility, scalability, and lower costs.

3. What are the three main VPN deployment scenarios?

The three main deployment scenarios are an Access VPN, an Intranet VPN, and an Extranet VPN.

4. Which different tunneling philosophies can be used in a VPN?

Based on the tunnelling philosophies, VPNs can be divided into Layer-2 versus Layer-3 tunnelling VPNs, or “do-it-yourself” versus carrier-provided VPNs.

IP Layer 2 Tunneling

1. What is an Access VPN?

Access VPNs combine VPNs with access technologies to allow remote users to be part of the corporate VPN.

2. What AAA parameters need to be configured for dial-in VP(D)Ns?

All the three AAA categories (authentication, authorization, and accounting) need to be configured in a VPDN.

3. What is a Cisco IOS virtual template interface?

A virtual template interface is a configuration template, which is usually applie d to many users’ sessions, and used ultimately to create a virtual access interface from it.

4. What is a Cisco IOS virtual profile?

A virtual profile is a per-used collection of settings, which can be applied when creating a virtual access interface.

5. What is a Cisco IOS virtual access interface?

A virtual access interface is a Cisco IOS interface, which is the final result of a setup of a virtual dial-up session. This is the interface, which terminates the virtual dial-up call and acts as the endpoint of the user’s layer-2 session.

Point-to-Point Tunneling Protocol (PPTP)/Microsoft Point-to-Point Encryption (MPPE)

1. What protocol is tunneled within PPTP?

The Point-to-Point Protocol (PPP) is tunneled within PPTP.

2. Which Cisco IOS configuration mechanism is used to bind PPTP sessions to virtual interfaces?

Cisco IOS uses **vpdn groups** to bind PPTP session to virtual interfaces.

Layer-2 Tunneling Protocol (L2TP)

1. What protocol is tunneled within L2TP?

The Point-to-Point Protocol (PPP) is tunneled within L2TP.

2. How does L2TP differ from PPTP?

L2TP is standardized, and allows both client-initiated or LAC-initiated VPNs over an IP transport network. L2TP has no native encryption and compression capabilities, but can reuse layer-3 mechanisms such as IPsec.

3. Which Cisco IOS configuration mechanism is used to bind L2TP sessions to virtual interfaces?

Cisco IOS uses **vpdn groups** to bind L2TP session to virtual interfaces.

4. How is the AAA functionality distributed between the LAC and the LNS?

Normally, the LAC only performs LCP negotiation, identifies the user, and forwards the PPP session to the appropriate LNS. The LNS performs NCP negotiation, authenticates the user, and terminates the PPP session. Therefore, most of the AAA functionality is performed at the LNS.

5. How does the Multichassis Multilink PPP feature use L2TP functionality?

MMP uses L2F as the forwarding mechanisms for multilink sessions between stack group members.

Layer-3 Tunneling

1. What is the usual transport protocol used by GRE?

GRE usually uses IP as the transport protocol.

2. What protocols can be tunneled within GRE?

Any layer-3 protocol can be tunneled within GRE.

3. Which Cisco IOS configuration mechanism is used to bind GRE sessions to interfaces?

Cisco IOS uses the **tunnel interface** as the configuration mechanism to establish GRE sessions.

4. How do routing protocols treat a GRE tunnel?

Routing protocols normally treat a GRE tunnel as a point-to-point link.