
Lesson 1: What is a VPN?

At a Glance



As a company becomes more and more dependent on networking to increase office communications, cooperative work, and productivity, it is forced to spend more and more money on increasing its network infrastructure. Increasing the network infrastructure requires the addition of expensive equipment, leased lines, and people power to maintain the growing network. In today's world, there is a significant increase in the number of remote employees needing access to their company's network from multiple locations.

As the Internet matured and became faster and more reliable, companies began to look at it as an alternative to the traditional networking model. They began to wonder if somehow the power of the Internet could be used to reduce their networking costs.

A virtual private network harnesses the power of the Internet by using it as the transport media for connecting multiple corporate locations, mobile employees, telecommuters, customers, suppliers, and business partners together.

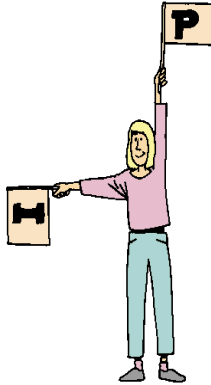
What You Will Learn

After completing this lesson, you will be able to do the following:

- Identify key features of a traditional WAN
- Identify key features of a virtual private network
- Compare the advantages and disadvantages of traditional WAN and VPN solutions
- Identify key features of PPTP, L2F, L2TP tunneling protocols and IPSec
- Develop of a Statement of Work for a network design proposal

Student Notes:

Tech Talk



- **Channel**—A data stream or path through which information passes between two networked devices.
- **Digital Signature**—A secret encryption code used for signing electronic documents. This signature can be used to ensure that no one is impersonating an authorized user.
- **Encryption**—The process of encoding data to prevent access by unauthorized individuals during transmission.
- **Extranet**—An extension to an organization's intranet, which allows limited access to the organization's intranet by individuals outside the organization, such as a company's suppliers and customers.
- **Internet Service Provider (ISP)**—A company that sells access to the Internet through their network backbone.
- **Intranet**—A network that is accessible only within a single organization and is used for specific applications important to the organization, such as document sharing, internal training, and access to the organization's databases.
- **Multilink PPP**—A modification of PPP that permits the combination of multiple PPP connections, thus increasing available bandwidth.
- **Point-to-Point Protocol (PPP)**—A data link protocol used for establishing telephone dial-up connections, such as between a computer and the Internet.
- **POP**—Point of Presence. A physical location where an individual can access the Internet through the services of an ISP.
- **Redundancy**—The state of having excess routes via multiple routers through which a packet may travel to its destination.
- **Tunneling**—Putting packets from one protocol inside of packets of another, which then travel across the path or tunnel of a shared network.
- **Virtual**—Simulated or performing the functions of something that is not present.

Traditional Wide Area Networks

Traditionally, smaller companies use analog connections over standard telephone circuits to network different locations into a WAN. The modems used to support data transfers across standard voice lines provide transfer rates up to 56 Kbps, which is usually adequate for a small company.

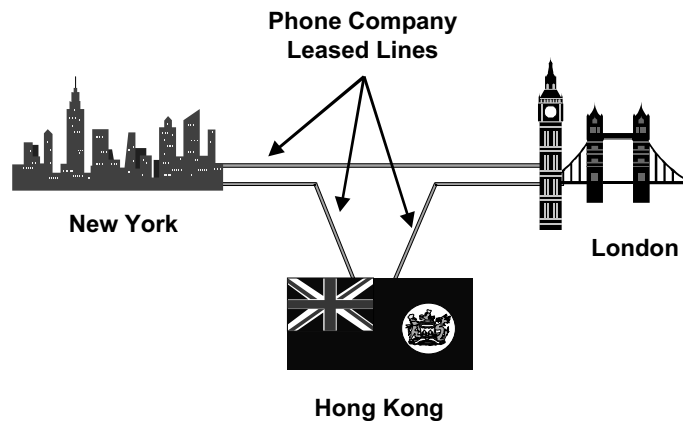
Although this solution is inexpensive, it does not scale well. In other words, as the number of users increase, more modems and telephone lines are needed. Increasing the number of modems and telephone lines increases the networking costs to the company. To reduce these costs, the company may increase the number of users accessing a port into the network, which will decrease the accessibility of the user to the network. Employees are not typically very happy when they are not able to connect to their company's network due to network congestion.

Larger companies typically use even more expensive solutions to create their WANs. Instead of using analog telephone lines, the company will use T1 or ISDN lines. T1 lines provide 24 channels, each offering 64 Kbps for a total of 1.544 Mbps bandwidth. ISDN-BRI offers two B channels for data transfer, each offering 64kbps. Using the Multilink Point-to-Point Protocol (PPP), an ISDN connection can have up to 128 Kbps transmission rate by combining the two channels per connection session. ISDN-PRI offers 23 B channels for data transfer, offering a maximum bandwidth of 1.52 Mbps. These solutions eliminate the need for large modem banks and large numbers of telephone lines. With multiple channels available, multiple users may use the line simultaneously.

Although, initially it would seem that using T1 or ISDN lines is a suitable solution, these lines can be expensive. As the number of users increases, the configuration, re-configuration, and maintenance of the network becomes cumbersome and expensive.

The costs of using these leased lines are dependent on both the bandwidth provided and the distance required to link offices. Many companies feel they cannot afford to link their smaller offices to the central office network. Companies are faced with balancing the costs of extending their corporate network and providing network access to their remote offices and users.

Traditional Wide Area Networks



Features of the Traditional WAN

Traditional WAN solutions provide features that are important components of any network.

- **Security**—Today's networks carry very sensitive and confidential information. For example, a student's grades may be transmitted from the teacher's desk to the administrator's office. Using leased lines, the network is private, and therefore it is secure. Privacy refers to preventing unauthorized people from gaining access to the information.
- **Availability**—High end leased lines, T1 and ISDN, have a high rate of availability. This is important, since users may be inconvenienced when the network is not accessible for any reason. The inability to access the network usually means lost productivity by the user.
- **Dedicated bandwidth**—Since leased lines are private and dedicated, the network's speed (transmission rate) is predictable. If additional speed is required, additional bandwidth can be added (i.e., upgrading the lines or adding more lines).

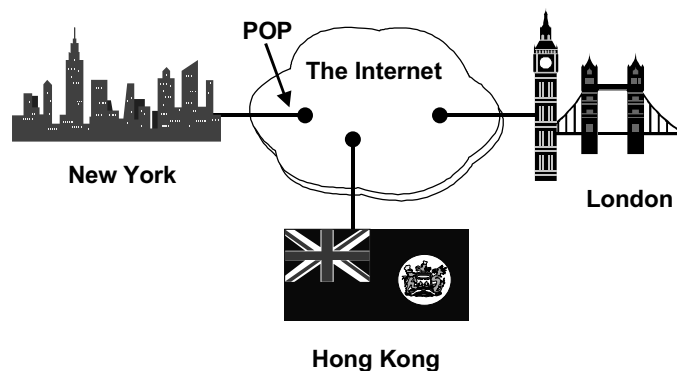
What is a Virtual Private Network?

Virtual private networks transmit private communications over either a shared or public channel, e.g., the Internet, using the Internet Protocol. They connect a company's multiple locations, mobile employees, telecommuters, customers, suppliers, and business partners through a connection between the company's network and an Internet Service Provider's point of presence (POP). A POP is a physical location where an individual can access the Internet through the services of an ISP.

The word "virtual" implies simulated or performing the functions of something that is not present. In the case of a VPN, the word "virtual" implies that a direct dedicated connection between intranets is not present. There is not a cable, either owned or leased by the company, that is directly interconnecting the company's various office locations. In fact, a VPN uses public or shared network connections, providing the illusion of a direct connection to the user.

A VPN also can be used to create an extranet. An extranet is an extension to an organization's intranet, which allows limited access to the organization's intranet by individuals outside the organization, such as a company's suppliers and customers.

A VPN creates the appearance that a company's intranets and extranets are part of a single network, operating in the same manner as a traditional WAN.



Internet-Based Virtual Private Networks

Features of a Virtual Private Network

- **Security**—Using specialized network protocols, a VPN permits secret or private communication between two devices. The network addressing used for the VPN is separate from the underlying shared network, which prevents others using the shared network to view communications not their own. Tunneling protocols are implemented that allow the encapsulation of the original packets inside a new IP packet. This allows the original addresses to be protected from view as they pass over the public or shared network. This encapsulation process also allows non-IP packets, such as Internet Packet Exchange (IPX) packets, to be tunneled across the network. Security is also maintained with the use of encryption of the data and user authentication through digital signatures and passwords. Encryption is the process of encoding data to prevent access by unauthorized individuals during transmission. Digital signatures are secret encryption codes used for signing electronic documents. These signatures can be used to ensure that no one is impersonating an authorized user.
- **Availability**—When using leased or purchased dedicated lines, packets sent over the network travel directly from the source to the destination with few detours, with the exception of a few hops through the network of routers. Although most WANs have some built in redundancy (multiple possible paths for transmission), it is possible that when a specific line is not functioning, the packet will not be transmitted. In a VPN, specifically using the Internet as its media for transmittals, the level of redundancy is much higher than with leased lines. There is no single connection from the source to the destination. The Internet offers a web of connections in which a packet can take any of thousands of paths to its destination. Perhaps the transmission will at times take longer, but the transmission will be successful.
- **Dedicated Bandwidth**—Adding extra lines in a traditional WAN is a very expensive solution to increasing bandwidth and access to the network. Mobile users, those who travel from city to city, typically will not have access to the WAN since it is nearly impossible for a company to provide leased lines in every location across the world. However, using a VPN, the solution to increasing bandwidth and access is in the addition of another POP account with an Internet service provider (ISP). A POP is a point of presence or physical location where an individual can access the Internet through the services of an ISP. Although there are fees associated with the creation and access rights of a POP, the fees are significantly less than the addition of leased or purchased lines. The cost of maintaining the backbone lines of the ISP is spread over many users of the ISP.

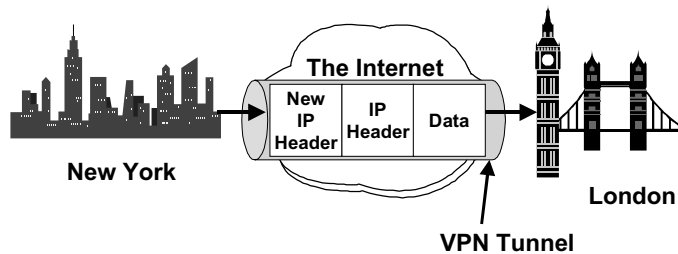
Check Your Understanding

- ◆ Compare the advantages and disadvantages of traditional WANs and VPNs.

Tunneling Protocols

Tunneling protocols create a path or tunnel through the Internet or shared public network to connect two private networks as a VPN. Tunneling allows packets from one protocol to be placed inside of packets of another protocol. If the original packets were IP packets, then this process is called IP-in-IP encapsulation.

IP-in-IP Encapsulation

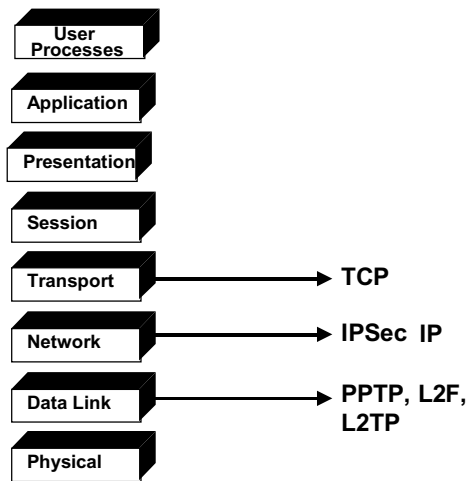


There are several types of tunneling protocols used to establish a virtual private network. Three will be discussed in this lesson.

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding Protocol (L2F)
- Layer 2 Tunneling Protocol (L2TP)

PPTP, L2F, and L2TP are Layer 2 tunneling protocols that are used to tunnel Point-to-Point Protocol (PPP) packets through the Internet. IPSec is a network layer security protocol used to provide authentication and encryption for IP packets travelling through a VPN tunnel. Authentication is a process that validates that a specific user is permitted access to the network or that packets transmitted are from an authorized user.

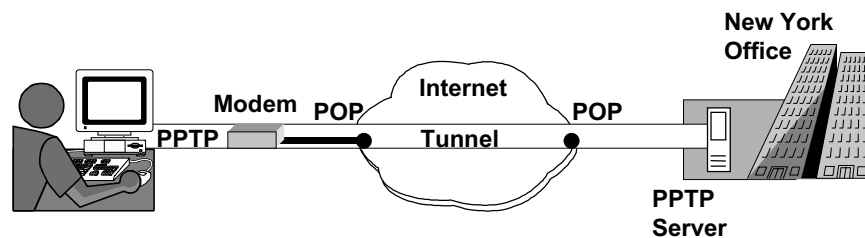
VPN Protocols and the OSI Model



Point-to-Point Tunneling Protocol (PPTP)

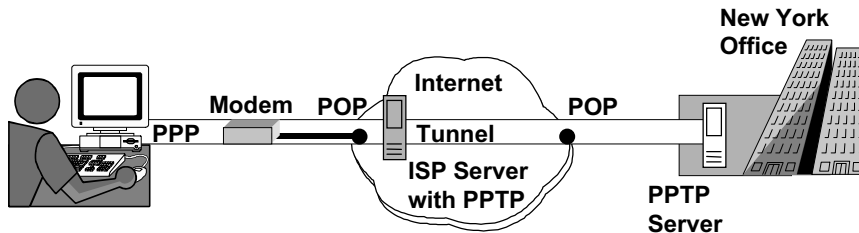
PPTP was initially developed by Ascend and later adopted by Microsoft as part of its Windows NT 4.0 Server package. It is also available with the Microsoft's Windows 98 operating system and also as an add-on to the Windows 95 operating system. It is an extension of the Point-to-Point Protocol (PPP), a data-link protocol for dial-up connections to the Internet.

PPTP Client-to-LAN Tunnel



The PPTP-enabled client (the client has the PPTP software installed) makes a dial-up connection to the Internet and a connection is then established through the VPN tunnel to the PPTP server on the private LAN. Data is sent over the PPTP tunnel using encapsulation. The new IP header contains the source address assigned to the client by the ISP, and the destination address of the switch on the public network. When the destination switch receives the packet, it removes the new IP header and forwards the packet to the appropriate private network, where the packet ultimately arrives at its destination node.

PPTP ISP-to-LAN Tunnel



It is not always necessary for the client to be PPTP enabled. If the ISP network server is equipped with PPTP, then PPP will run between the client and the ISP and the PPTP tunnel is established between the ISP and the LAN.

PPTP can also encapsulate IPX (from NetWare) and AppleTalk packets even though these are not IP packets. This allows PPTP to be used to establish VPNs using non-IP network operating systems.

There are some drawbacks to using PPTP as the VPN protocol. PPTP does not provide address authentication or data encryption.

Layer 2 Forwarding Protocol (L2F)

L2F is a VPN protocol that was developed by Cisco. As with PPTP, L2F does not provide for data encryption. It does, however, provide some authentication using the Password Authentication Protocol, which identifies a user attempting to log on to a PPP server, such as an ISP. L2F states that all authorization and address management should be done by the home network instead of by the ISP.

The client does not have to be L2F-enabled. The tunnel is established by the ISP, not by the client. The client is not aware of the tunnel and cannot directly perform encapsulation of the packet. The client sends a packet across a PPP connection to the ISP unchanged. At the ISP, a new IP header is added to encapsulate the packet. The packet is then forwarded on to the switch on the private network, where the new header is removed and the packet is sent to its destination.

L2F can also be used over frame relay, SONET, and ATM networks.

Layer 2 Tunneling Protocol (L2TP)

L2TP is the synthesis of PPTP and L2F. It combines features of both protocols. As with PPTP, the client makes a dial-up connection to the Internet and a connection is then established through the VPN tunnel to the PPTP server on the private LAN. The client is not L2TP-enabled, so the VPN tunnel is established by the ISP. L2TP requires user authentication, but does not provide data encryption.

L2TP can be used over frame relay, SONET, and ATM networks, and it supports the encapsulation of non-IP packets, i.e., IPX and AppleTalk.

Internet Protocol Security (IPSec)

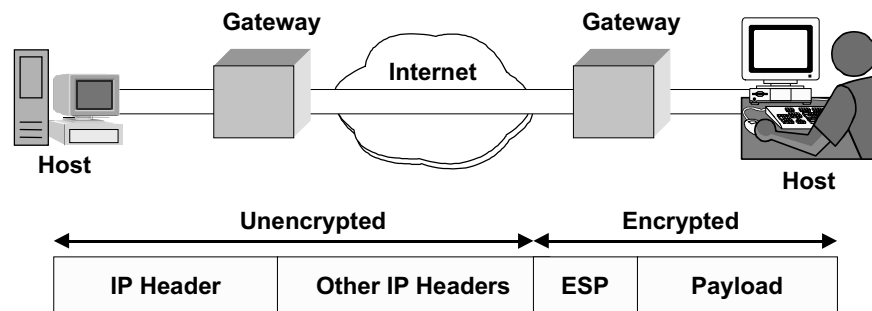
IPSec is a security protocol that addresses the secure use of the Internet. IPSec and L2TP can be used together to provide both tunneling and security for IP packets across a network. L2TP builds the tunnel and IPSec provides security.

Data is sent over the L2TP tunnel using IP-in-IP encapsulation. A new IP header is added to the IP packet that contains the source address of the client, assigned by the ISP, and the destination address of the switch on the public network.

IPSec can provide user authentication or encryption or both. An IPSec authentication header, added after the new IP header, verifies to the destination node that the data has arrived from the correct source and is unchanged.

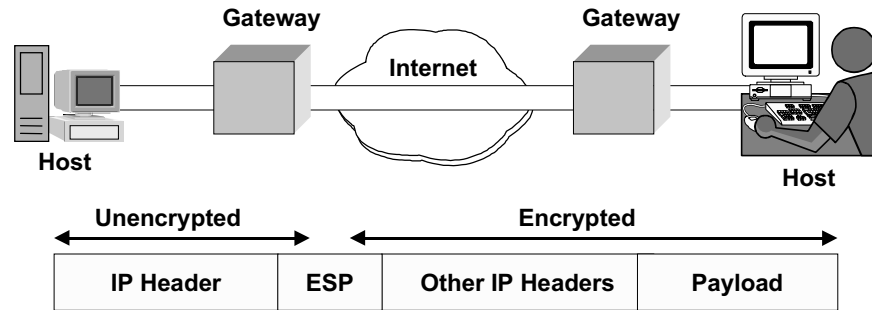
If encryption is necessary, an encapsulating security header is added that encrypts the data. IPSec operates in two different modes; transport mode and tunnel mode. The placement of the security header identifies the mode.

IPSec Tunnel Mode



In tunnel mode, the security header is added between the new IP header and the original header. This placement encrypts the original destination and source address. In this situation the packet is exchanged between security gateways (switch or router with encryption/decryption capability). The sending gateway encrypts the data and adds the new source and destination addresses of the security gateways. The receiving gateway processes the security header, decrypts the message, and restores the original destination and source IP addresses.

IPSec Transport Mode



In transport mode, the security header is added after both the new and original IP header. In this case, the original addresses are not encrypted. Only the data is encrypted. The hosts exchanging the data perform the encryption and decryption. The packet is received by the router or switch, which removes the headers and forwards the packet to its destination. The receiving host decrypts the data.

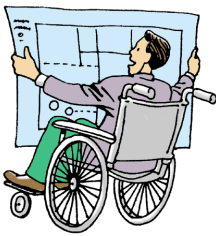
Check Your Understanding

- ◆ Describe how a packet is transmitted using tunneling protocols.
- ◆ Which tunneling protocol(s) would a company use if they were using either AppleTalk or NetWare as their operating system?
- ◆ Create a diagram of L2TP using the lesson diagrams as a model and the information presented in this lesson.

Try It Out: WAN and VPN Considerations

Materials Needed:

- Windows 95 PC
- Any Word Processor (e.g., MS Word) or Spreadsheet (e.g., MS Excel)
- Pen/Pencil and Paper
- Student Network Design Proposal Working Draft



Charting the pros and cons of various options is an important tool for the network designer. With a concise easy to read chart, it becomes easier to quickly determine what network requirements are best satisfied by what options are available.

In this activity, you are to create a chart that maps all the features and options available to a client when deciding between traditional WAN and VPN solutions.

Your chart should include information that answers questions such as:

- Will the configuration allow mobile users to easily access the company's intranet?
- Will the VPN tunneling protocol allow non-IP packets to be transmitted across the network?
- Which is the best solution with the greatest security?

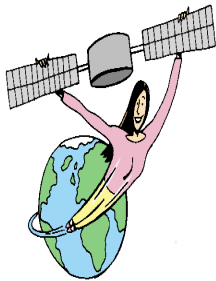
Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Accurate chart suitable for inclusion in a network design proposal	100	
TOTAL	100	

Stretch Yourself: Non-Internet Virtual Private Networks

Materials Needed:

- Windows 95 PC
- Internet Connection (optional)
- Any Word Processor (e.g., MS Word)
- Pen/Pencil and Paper
- Student Network Design Proposal Working Draft



This lesson covers information about Internet-based VPNs. It is possible to create a virtual private network over public frame relay and ATM.

1. Research VPNs using public frame relay and ATM and compare this solution over Internet-based VPNs. Document your resources.
2. Diagram how frame relay and ATM VPNs function. Include a brief caption or explanation of the diagram
3. Write a one-page recommendation describing when a client might choose frame relay, ATM, or the Internet as the foundation of a VPN.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Thorough research of non-Internet VPN solutions	40	
Diagram illustrating how frame relay and ATM VPNs operate that could be used in a network design proposal	30	
Concise and clear recommendation	20	
Documented resources	10	
TOTAL	100	

Network Wizards:

Materials Needed:

- Windows 95 PC
- Internet Connection (optional)
- Any Word Processor (e.g., MS Word)
- Pen/Pencil and Paper
- Student Portfolio
- Student Network Design Proposal Working Draft



Part One: Firewalls

A firewall is a system or group of systems that lie between an intranet and a public network (e.g., the Internet). It prohibits unwanted and unauthorized traffic from accessing the intranet, while allowing access to authorized users. The firewall essentially acts as a security gate at the network perimeter, regulating what traffic is allowed in and out. Firewalls are an important component of virtual private networks.

1. Using resources of your choice, research the types of firewalls that exist and how they work.
2. Diagram how each firewall functions as a network security measure. Include in your diagram where each firewall solution is placed in the network's infrastructure. Quality and neatness is important.
3. Write a short "white paper" about firewalls to accompany your diagrams. A white paper is a merely a technical report about a specific subject. White papers are often posted on the WWW for anyone to download.
4. Document your resources.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Thorough research and documented resources	25	
Quality diagrams clearly demonstrating firewall functions	50	
Concise white paper	25	
TOTAL	100	

Part Two: Network Design Portfolio Case Study

Using the results from your pre-site questionnaire, you must create a simplified Statement of Work for your case study client. There are really no hard and fast rules for creating a Statement of Work. The statement is much like a contract you might create between yourself and a customer requesting that you mow their lawn. In such a contract you might include specifications for the following:

1. How often you will mow the lawn.
2. What day and time you will mow the lawn.
3. How much you will charge for the service.
4. An agreement whether you will use your lawnmower or the customer's lawnmower.
5. If you use your equipment, are there any specifications as to the quality of your equipment? Do you need to use a specific brand to satisfy the customer?
6. What quality is expected? You may need to agree on how short the lawn is mowed and whether you are responsible for mowing the hard to get areas (e.g., the grass around a light pole).
7. What are the responsibilities of the customer? For example, will the customer remove obstacles in the lawn?
8. What happens if you are sick and unable to mow the lawn? Must you find a substitute?

A lawn-mowing contract is fairly simple. A statement of work for network design is far more complicated. Generally, a statement of work includes:

1. A written interpretation of the customer's objectives. What does the customer want to accomplish? For example, the customer may desire remote access for mobile users.
2. When will the work be completed? In your case, you will only have one "deliverable," the completed network design proposal.
3. What will be included in the project? Some network designers not only provide the design, but also arrange for installation and configuration or other services. In your case, you will only include the design.
4. How much you will charge for your services. Your services are free!
5. What level of detail is needed in the design document? Generally, the design will include:
 - a. Network requirements. (You will outline your customer's requirements. For example, how many users are connected to the network? Are there remote users? Are there other office locations that need to be connected to the intranet?)
 - b. Basic rules governing the network design. (You will determine, as best as you can, what rules apply to your network design. For example, an ISDN-BRI line provides only 2 B channels for data transmission or voice for a total available bandwidth of 128 Kbps using Multilink PPP. If your client expressed a need for greater bandwidth, then ISDN-BRI can not be used.)
 - c. Network diagrams. (You must create diagrams to support your recommendations.)
 - d. Routing architecture. (You will not complete this aspect of the network design proposal unless you have already taken the Routing course within the NetKnowledge course sequence. If you have completed the Routing course, you have the option to include recommendations on routing protocols, but this is not required.)
 - e. Addressing plan. (You will include only a very basic addressing scheme with subnetting information. You are not expected to be an expert on IP addressing.)
 - f. Network design. (You will complete a network design proposal outlining recommendations for changes and implementation.)

Part Three: Case Study Statement of Work

1. For your Statement of Work, create a professional form that can be used repeatedly to outline what services you would perform as a network designer. Think of the statement as a detailed invoice that itemizes each service you will complete for the client.
2. When you have completed your Statement of Work, present it to your teacher for review and comments.
3. Incorporate any comments your teacher shares with you and then present the statement to your case study client.
4. Request that the client review the statement and offer any suggestions for improvement or clarification.
5. Incorporate the client's comments into the statement and place the statement in your portfolio.

Summary

What is a VPN?

In this lesson, you learned the following:

- The key features of a traditional WAN
- The key features of a virtual private network
- The advantages and disadvantages of traditional WAN and VPN solutions
- The key features of PPTP, L2F, L2TP tunneling protocols, and IPsec
- The development of a Statement of Work for a network design proposal

Review Questions

What is a VPN?

Part A:

1. What type of transmission lines is usually used for traditional WANs?
 - a. Analog telephone circuits, POP, and ISDN
 - b. ISDN, T1, and POP
 - c. T1, ISDN, and analog telephone circuits
 - d. The Internet
 - e. POP
2. Transmission rates of an ISDN-BRI line offers
 - a. Up to 128 Kbps using multilink PPP.
 - b. Up to 64 Kbps per channel without multilink PPP
 - c. Up to 24 Kbps
 - d. A and B only
 - e. None of the above
3. ISDN-PRI has 23 B Channels, offering up to 1.52 Mbps bandwidth.
 - a. True
 - b. False

4. The leased lines used in traditional WANs
 - a. Are considered public and provide no security.
 - b. Have very slow transmission rates compared to VPN solutions.
 - c. Are private lines and provide dedicated bandwidth.
 - d. Have a low availability rate.
 - e. Cannot be increased to provide additional bandwidth.
5. The costs of using leased lines are dependent on
 - a. The level of security desired.
 - b. The bandwidth provided
 - c. The distance required to link offices.
 - d. B and C only
 - e. None of the above

Part B:

1. Virtual private networks are created using
 - a. Private leased lines between intranets.
 - b. Shared IP networks between intranets.
 - c. Purchased private cable connections between intranets.
 - d. All of the above
 - e. None of the above
2. The word "private" in virtual private networks means
 - a. A VPN is a private network.
 - b. A VPN is capable of transmitting private communications.
 - c. A VPN is a form of encryption that ensures privacy.
 - d. A VPN guarantees the use of dedicated lines.
 - e. A VPN uses leased lines not available to other companies.
3. IP-in-IP Encapsulation
 - a. Is a VPN tunneling protocol.
 - b. Allows IPX packets to be hidden inside IP packets.
 - c. Is a process of placing IP packets inside other IP packets.
 - d. Is a process of placing AppleTalk packets inside IP packets.
 - e. Is a process of authenticating IP packets travelling across a VPN.

4. Privacy in VPNs is provided by using
 - a. Digital signatures.
 - b. Tunneling.
 - c. Passwords.
 - d. Encryption of data.
 - e. All of the above
5. VPNs offer a high degree of availability because
 - a. The ISP guarantees dedicated bandwidth for the VPN.
 - b. The Internet has an enormous web of connections or routes that a packet can take to get to its destination.
 - c. The transmitted packets are sent by a dedicated route to get to their destination.
 - d. The ISP controls the number of users of the VPN.
 - e. None of the above.

Part C:

1. Compare the advantages and disadvantages of traditional WANs and VPNs.

Part D:

1. Fill in the chart with the appropriate information about PPTP, L2F, and L2TP..

Protocol	OSI Layer	Supports AppleTalk (Yes/No)	Supports IPX (Yes/No)	Client-enabled (Yes/No)	Provider (ISP) Enabled (Yes/No)	Authentication Services Provided (Yes/No)	Encryption Service Provided (Yes/No)
PPTP							
L2F							
L2TP							

2. Which tunneling protocols support frame relay, SONET, and ATM?
3. Describe briefly how IPSec provides security for packets travelling across a tunnel.

Scoring

Criteria	%	Your Score
Part A: Identify key features of a traditional WAN.	25	
Part B: Identify key features of a virtual private network.	25	
Part C: Compare the advantages and disadvantages of traditional WAN and VPN solutions.	20	
Part D: Identify key features of PPTP, L2F, L2TP tunneling protocols, and IPSec.	30	
TOTAL	100	
Try It Out:	100	
Stretch Yourself:	100	
Network Wizards: Develop of a Statement of Work for a network design proposal.	100	
FINAL TOTAL	400	

Resources:

Fowler, D. (1999). Virtual Private Networks: Making the Right Connection. San Francisco: Morgan Kaufmann Publishers, Inc..

Nortel Networks. (1998). Understanding and Implementing Virtual Private Networking (VPN) Services: A White Paper. Available Online: <http://www.baynetworks.com/products/Papers/2746.htm>.

Nortel Networks. (1999). VPN Enterprise Solutions Training CD. Part Number AYSL24005. Santa Clara, CA: Nortel Networks, Inc..

Scott, C., Wolfe, P., & Erwin, M. (1999). Virtual Private Networks. Sebastopol, CA: O'Reilly & Associates.

