
Lesson 2: VPN Solutions

At a Glance



There are many considerations that must be taken into account before choosing to implement a virtual private network. Companies must identify what specific problems will be solved using a VPN and what VPN solutions will best address these problems.

This lesson discusses the questions and answers needed to choose an appropriate virtual private network solution.

What You Will Learn

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

- Describe three primary reasons to implement a VPN
- Diagram the three VPN service models
- Identify major considerations when implementing a VPN
- Compare the differences between Symmetric Key encryption and Public Key encryption

Student Notes:

Tech Talk



- **Challenge Handshake Authentication Protocol (CHAP)**—An authentication protocol that improved upon Password Authentication Protocol by using an encryption key to encrypt the username and the password.
- **Diffie-Hellman Key Agreement**—An algorithm used to generate encryption keys.
- **Encryption Key**—Specific code needed to scramble or lock (encrypt) and to unlock or unscramble (decrypt) data.
- **Mobile User**—Someone who needs remote access to a corporate network in order to connect to a central site from a variety of locations.
- **Password Authentication Protocol (PAP)**—A protocol that uses a username and a password to authenticate users. In this system, the password is not encrypted.
- **Prime Number**—A number that can only be divided by it and one (e.g., 2, 5, and 7).
- **Public Key Encryption**—An encryption system in which the data is encrypted with one key and decrypted by another key.
- **Remote Access Server (RAS)**—A LAN host equipped with modems that allow remote users to connect to a network using telephone lines.
- **Symmetric Key Encryption**—An encryption system in which the data is encrypted and decrypted by the same shared secret key.
- **Telecommuter**—Someone who connects to a central site from a single location as his or her primary work environment. Often a telecommuter works from home.

Why Implement a VPN?

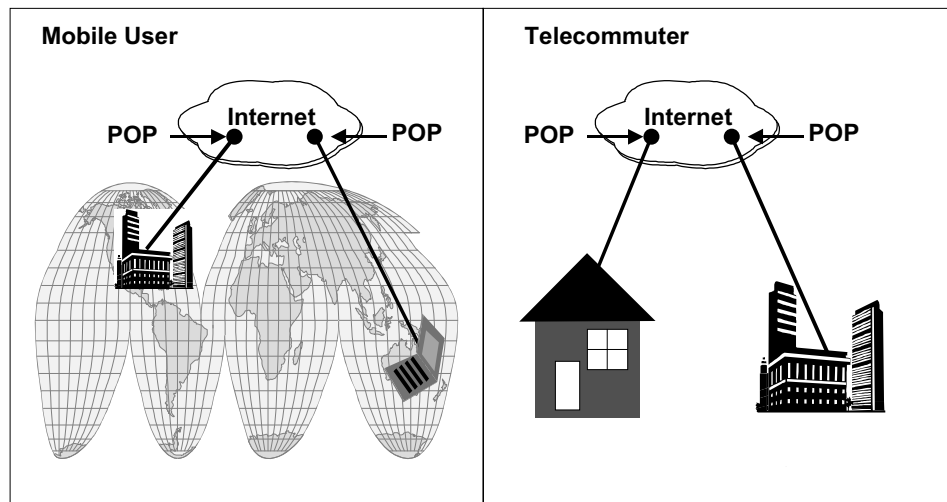
Virtual private networks are generally implemented to create remote access, extend the company's intranet, or to create an extranet between the company and its business partners.

Remote Access

To understand the needs of remote access users, it is important to understand that there is more than one type of remote user. The mobile user is someone who connects to a central site from a variety of locations. An example of this would be a sales representative who needs to connect to a corporate site while on the road, in order to send or retrieve e-mail and download essential files from the corporate server. VPNs are considered a good solution for the mobile user, since connections into the corporate site are possible through an Internet Service Provider's (ISPs) POP accounts across the world. However, when considering a VPN solution, it is important to investigate whether the ISP chosen to host the VPN has enough POP locations to serve the company's mobile users. Laws pertaining to encryption vary from country to country. How data will be secured while travelling over a VPN must also be addressed.

Another type of remote access user is the telecommuter. The telecommuter is someone who connects to a central site from a single location as his or her primary work environment. Often a telecommuter works from home and needs to connect to the corporate site to send or receive e-mails, share documents with fellow employees, and upload or download files from the corporate server. The needs of some telecommuters may be easily resolved using leased lines, i.e., ISDN, but in some cases telecommuters are located in distant locations where the cost of leased lines may be prohibitive to the company. A VPN solution lowers the cost of connection for such telecommuters. Again, choosing the right ISP and encryption procedure is important when implementing a VPN.

Remote Access Users



POP= Point of Presence

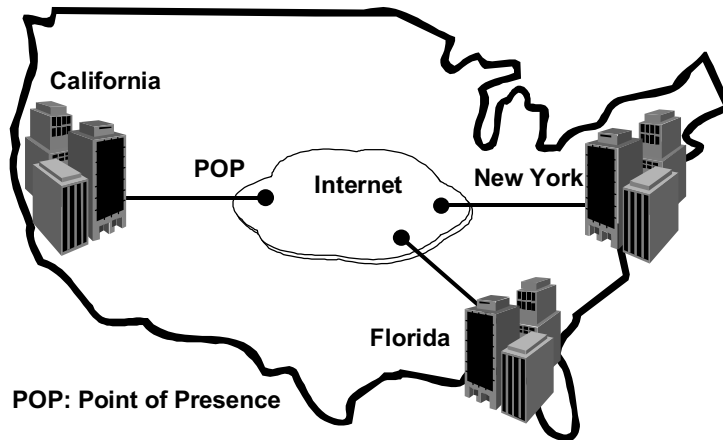
Extended Intranets

In the traditional networking model, companies purchased dedicated leased lines to link their various corporate locations into a single wide area network. This model evolved out of necessity, since it was the only available means of linking multiple locations to the central office.

Extending the company's intranet permits business applications such as remote order entry, inventory, and warehousing to be built around a central company network. The flow of information from office to office becomes transparent within the company.

Although costs associated with extending the company's intranet are often reduced by the implementation of a VPN, issues created by the physical location of the various offices, security, and flexibility must be considered.

Extended Intranets

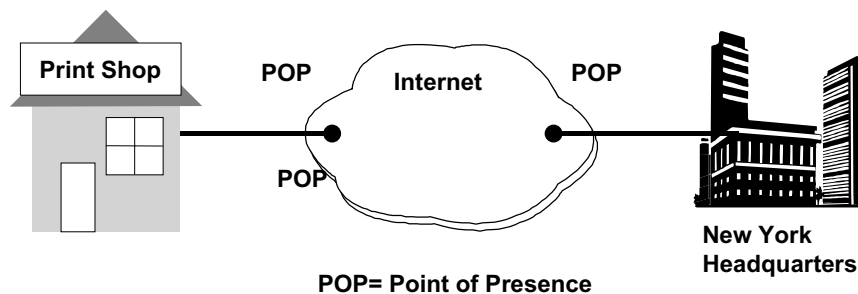


Extranets

Traditionally, information was shared between a company and its business partner using the manual services of the post office, often referred to as "snail mail" since delivery time is much slower than electronic mail. Implementing an extranet using a VPN provides easy solutions for both the company and its business partners. For example, a company may wish to order advertisement flyers from a print shop. Creating an extranet allows the print shop to acquire the information on the request electronically, which shortens the turn-around time for production. The ability to shorten the production cycle can translate into a competitive advantage for both the company and the print shop.

Connecting business partners to the company extranet raises serious issues in security, flexibility, reliability, and associated costs of operation and management of the VPN.

Extranets



VPN Service Models

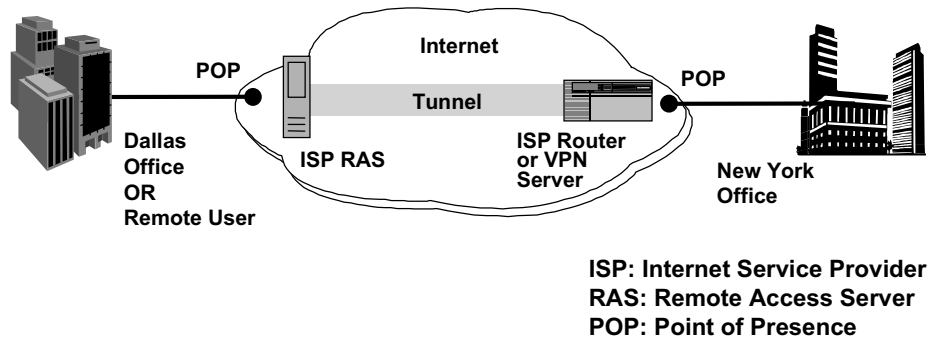
Once a company determines how a VPN will improve its business, the company must identify the service model it will use to implement the VPN. There are three service models from which to choose:

Service Provider-Service Provider (SP-SP)

In the SP-SP model, the VPN tunnel begins and ends with the ISP. The ISP provides all the equipment and expertise required to implement the VPN. The company is not required to purchase additional equipment and deal with the day to day management issues of the VPN.

In this model, the remote user dials in to the ISP's remote access server (RAS) and requests a tunnel to the company network. A RAS is a LAN host equipped with modems that allow remote users to connect to a network using telephone lines. The RAS sets up a tunnel to the ISP's router that connects to the company network. Once the tunnel is set up, the remote user has access to the company's network.

SP-SP Model

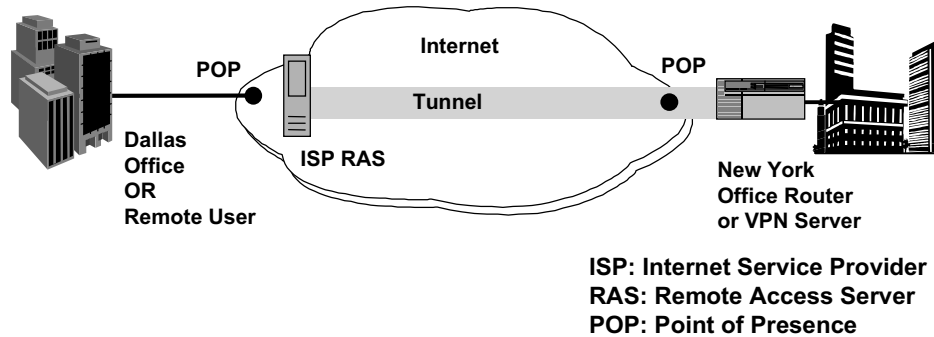


Service Provider-Enterprise (SP-E)

In the SP-E model, the VPN begins at the ISP's remote access server and ends at the router or VPN server of the company. The tunnel is created by the ISP when the remote user dials into the RAS.

Using this model, the company benefits from using the ISP's remote access equipment. This model is used when a company wants the ISP to provide the remote access, but it still wants to maintain control over the tunnel endpoint.

SP-E Model



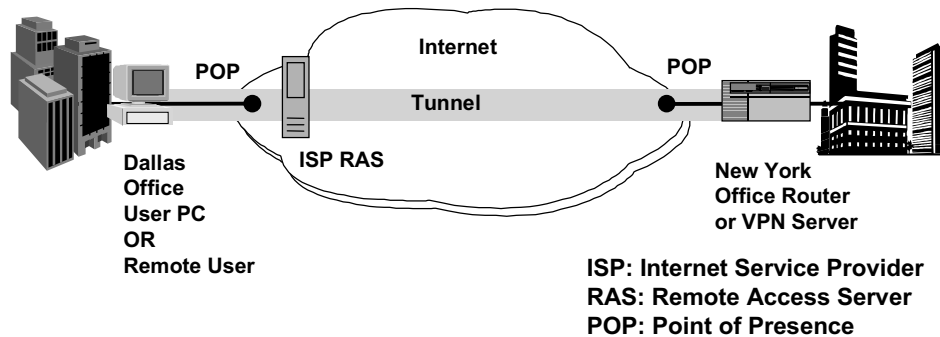
Enterprise-Enterprise (E-E)

In the E-E model, the Internet is used only as a replacement for long distance leased lines. The tunnel begins at the remote user's PC, using VPN client software, and ends at the company's router or VPN server. This model is sometimes called the LAN to LAN model.

The ISP provides only local access to the Internet through one of its POPs. The company controls and maintains both ends of the tunnel. This allows the company to use any ISP for remote access whether or not the ISP supports virtual private networks. Extranets are usually set up using the E-E model.

The disadvantage to the E-E model is the extra performance burden it places on the user's computer. The client software often requires a lot of memory and processor speed. Performance speeds may also be slower.

E-E Model



VPN Overall Considerations

Although VPNs are often considered a viable solution for many companies, there are very specific issues to be considered.

- **Availability**—Before entering into a contract with an ISP, the company should determine if the ISP has enough POPs to adequately serve remote users. There is not an ISP that can guarantee that there will be a POP available in every city, in every country. Mobile users need to have access to the company network from nearly anywhere. If a local POP does not exist in a specific location, the mobile user will pay long distance toll charges to access the company network. These charges add extra costs to using a VPN, reducing any savings originally expected from the implementation of a VPN. The company may implement a toll-free 800 number for access by remote users; however, there are fees associated with solution as well.
- **Performance**—The Internet has a high rate of redundancy. There are many different paths a packet can take on its way to its destination. This is one of the better features of using the Internet for implementing a VPN. However, it is also not uncommon that the amount of general traffic on the Internet can contribute to severe packet delays due to slow transmission rates. If a company is heavily dependent on high performance speeds, then a VPN may not be a good solution. Companies that use videoconferencing and other applications, which require faster transmission speeds, are likely to be unhappy with the results using a VPN.
- **Management**—A VPN can be a wonderful solution for those companies that leave the management to the ISP. However, if the company desires to retain control of the VPN, then the company has to deal with the day to day management. Management of a VPN entails security issues, performing audit trails to track security violations, employee training, technical support for users, and equipment decisions and configurations. If the ISP will manage the VPN, then the contract should outline specific quality of service expectations.
- **Security**—Security is the most important issue to consider when implementing a VPN. Of the tunneling protocols currently in use or under development, some provide a high level of security, others provide no security. Choosing appropriate encryption and user authentication ensures the company that their virtual private network will indeed be private.

Check Your Understanding

- ◆ List three purposes of a virtual private network.
- ◆ List the four main considerations that must be dealt with when implementing a VPN.
- ◆ What are the negative issues associated with a VPN?
 - ◆ Speculate why a network designer might suggest the use of the LAN to LAN service model for a company's VPN.

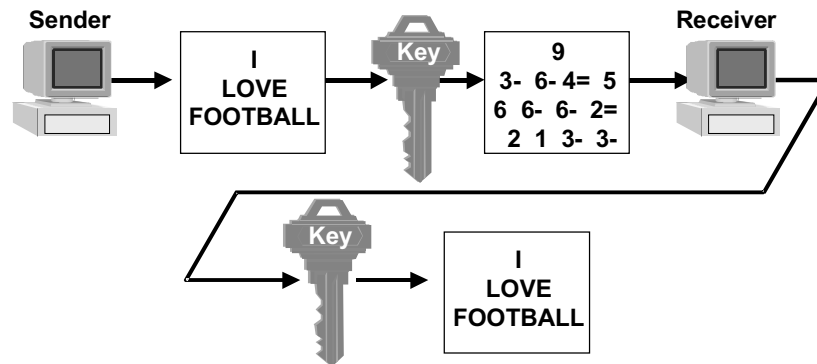
Encryption

Encryption is the process of encoding data to prevent access by unauthorized individuals during transmission. Without encryption, a company's data transmissions are vulnerable to anyone using the Internet who has access to sniffer software (e.g., Sniffer Basic). Sniffer software allows individuals to monitor network traffic and discover the source and destination address of a transmitted packet. Once this information is available, an unauthorized individual can penetrate the company firewall and gain access to the entire company network. Other analyzers allow individuals to actually read network traffic. If the data transmitted can be read, then it can be changed.

Encryption/Decryption Keys

Encryption basically scrambles the message using a key, or special code, in such a way that a key is also needed to unscramble the message once it arrives to its destination. Think of the key as the special information used to alter the message so that only those who have knowledge of the special information can read the message. School children often send encrypted messages to each other using some "secret key" that helps them code and decode the message amongst them.

Secret Keys



KEY: A B C D E F G H I J K L M N O P Q R
 1 2 3 4 5 6 7 8 9 1- 2- 3- 4- 5- 6- 7- 8- 9-
 S T U V W X Y Z
 1= 2= 3= 4= 5= 6= 7= 8=

Frequently, prime numbers are used as encryption keys. A prime number is a number that can only be divided by itself and one (e.g., 2, 7, and 13). Multiplying two prime numbers results in a product that can only be divided by the original prime numbers, and the product itself and one ($2 \times 2 = 4$). A mathematician uses factoring to find the original prime numbers used to create the product. Factoring the number 21 results in the prime factors of 3 and 7. If the encryption key were 21, then breaking the code would be very easy. But encryption systems use much larger numbers.

The actual length of a key is measured in bits. The longer a key, the greater the difficulty in cracking the code used to encrypt the data. In the past, 40-bit and 56-bit key lengths have been used. However, with the speed and power of computing increasing, these key lengths are no longer considered highly secure. 128-bit keys are now the standard where possible.

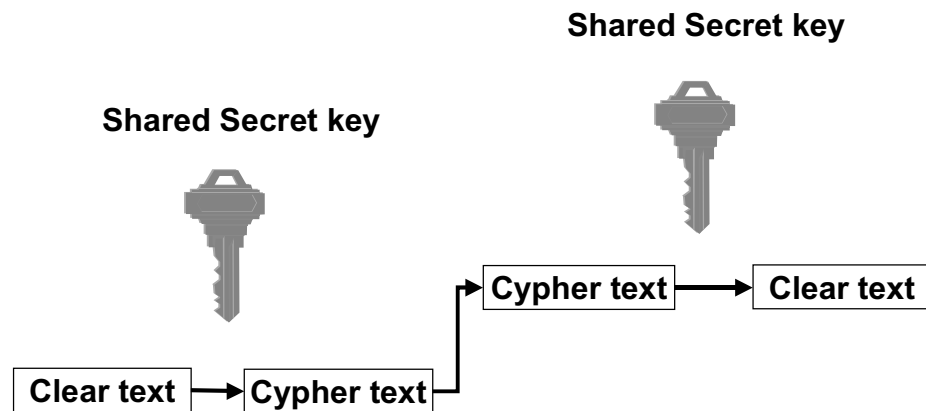
Different countries have laws that govern the use of encryption. Some countries simply do not allow encryption and others limit the size of the encryption key. When considering implementing a VPN between countries, a network designer should investigate the laws of all the countries involved to identify problems associated with encryption.

There are two types of key encryption systems: secret and public.

Symmetric Encryption

Symmetric encryption algorithms require that both the sender and the receiver have the same shared secret key. The sender encrypts the data with the shared secret key and the receiver decrypts the data with the same key. To ensure privacy within the company, the key must be kept secret from unauthorized users. This can pose a major problem for a company. The secrecy of a key is not guaranteed. Anyone who acquires the key can read the messages transmitted across the VPN. Consequently, companies must change the secret key often. Symmetric encryption is sometimes referred to as secret key encryption.

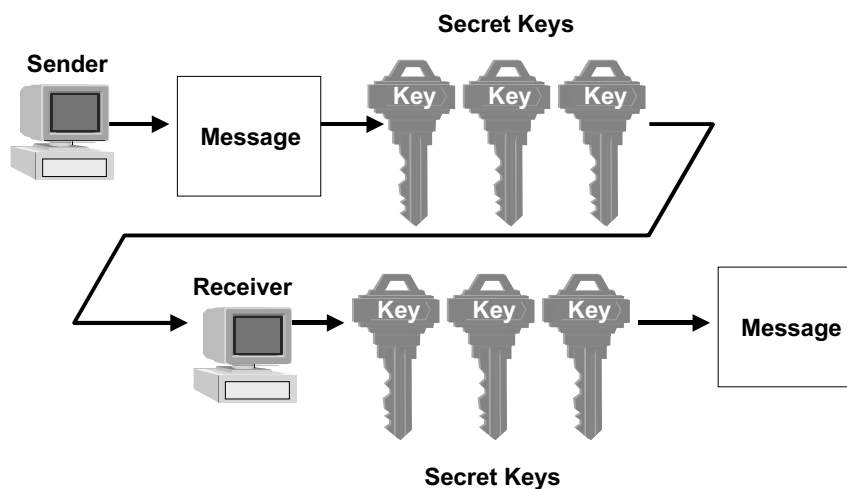
Symmetric Key Encryption



Triple-DES is a symmetric encryption algorithm based on the Data Encryption Standard (DES) endorsed by the United States federal government in 1977. DES used a single key with a 56-bit key length. Triple-DES employs a 112-bit key length, and also uses two or more keys to encrypt a message. This process ensures added security since all the keys must be used and used in the correct order.

The symmetric key encryption systems are very simple and fast.

Triple-DES Encryption



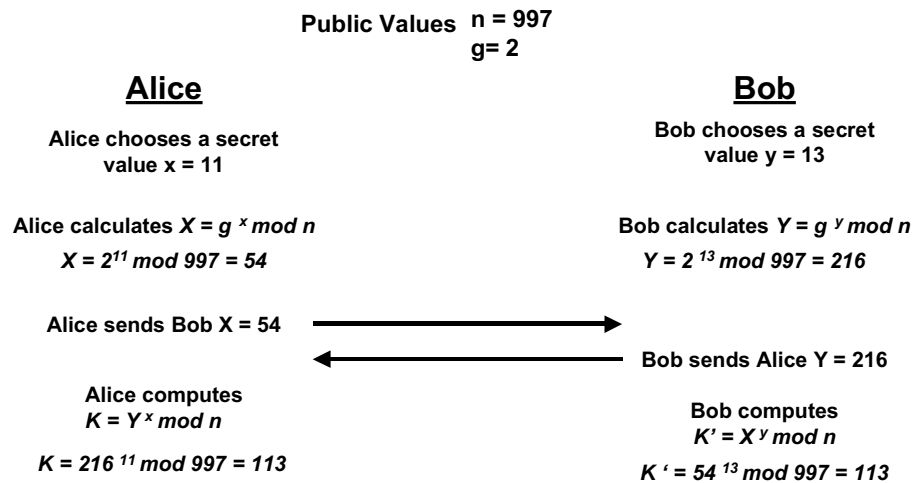
Other secret or symmetric encryption algorithms include:

- **IDEA**—The International Data Encryption Algorithm uses a 128-bit key. This is a European algorithm.
- **Blowfish**—This is a new algorithm that uses a variable key length up to 448 bits.
- **CAST**—This algorithm uses either a 128-bit or a 256-bit key length.

Diffie-Hellman Key Agreement

The Diffie-Hellman key agreement algorithm allows multiple users to independently calculate a shared secret using only public values. This algorithm is only used to generate keys; it is not used to encrypt data. The Diffie-Hellman key agreement is a common component of many encryption systems.

Simplified Diffie-Hellman Key Agreement



The example above is a simplified version of the Diffie-Hellman key agreement. Bob and Alice need to arrive at a shared secret value. Follow the steps.

1. The first two public values, n and g , are agreed upon. (This lesson will not discuss how the public values are selected.)
2. Alice and Bob then select their secret values (x for Alice and y for Bob). In this example, the values selected are only two-digit numbers, but real encryption systems often use 300-digit secret values.

3. Alice computes $X=g^x \text{ mod } n$ as follows: $X=2^{11} \text{ mod } 997$. Mod represents the mathematical term modulo, which essentially means that 2^{11} is divided by 997 and the remainder is X. So, 2,048 divided by 997 equals 2 with a remainder of 54. Therefore, X is 54.
4. Bob computes $Y=g^y \text{ mod } n$ as follows: $X^{13} \text{ mod } 997$. After calculation, Y is found to be 216.
5. Alice and Bob exchange the X and Y values (54 and 216).
6. Alice uses the Y value (216) to calculate the shared secret key (K) using the formula, $K= Y^X \text{ mod } n$. After calculation, $K=113$.
7. Bob uses the X value (54) to perform the same calculation for arrive at the secret key (K). After calculation, $K=113$.
8. Bob and Alice can use the shared secret key, 113, to encrypt information exchanged between them.

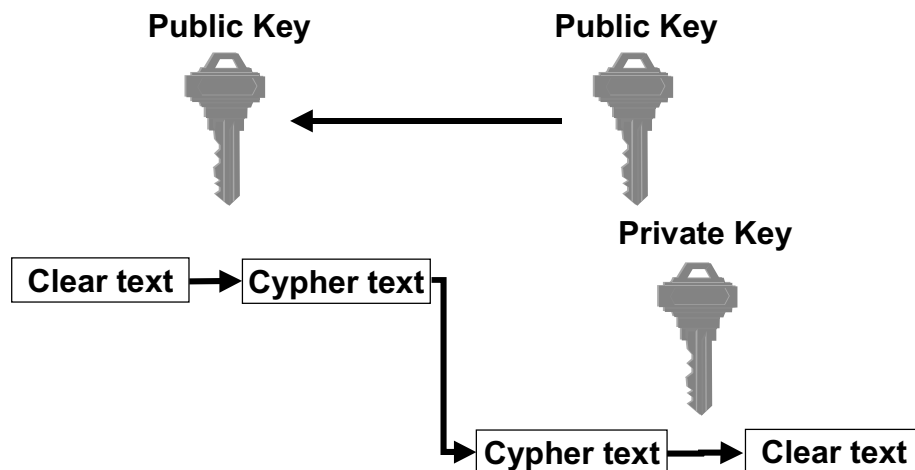
As can be seen, this is a very complicated procedure even when presented in a simplified example. Remember all that is accomplished using this algorithm is the creation of a secret key.

Public Keys System

In a public or asymmetric key system, data is encrypted with one key and decrypted by another key. These keys are referred to as the public key and the private key. Public keys can be placed on a public key server or exchanged by e-mail. Then, when someone wants to send a secure message they simply look up the receiver's public key, encrypt the data, and send it. When the data is received, the recipient decrypts the data using the secret key. In order for this to remain secure, the secret key must never be exposed. This is a much slower approach to encryption than symmetric encryption systems.

The Rivest Shamir Adleman (RSA) encryption is a public key algorithm that is used by Netscape Navigator and Microsoft's Internet Explorer.

Public Key Encryption RSA



User Authentication

Before encryption keys are exchanged, it is necessary to determine if the sender and the receiver are authorized users. It is important to know that the key is coming from the correct authorized sender and that the key is going to the correct authorized receiver. Without authentication, an encryption key could end up in the wrong hands and create a major security problem within the VPN.

The Password Authentication Protocol (PAP) is a protocol that uses a username and a password to authenticate users. Essentially, the password and the username are compared to a stored database to make sure they are correctly matched. In this system, the password is not encrypted, which makes it very vulnerable to the outsiders snooping around.

Another protocol, the Challenge Handshake Authentication Protocol (CHAP) improved upon PAP by using an encryption key to encrypt the username and the password.

RADIUS

The Remote Authentication Dial-In User Service (RADIUS) is an authentication system used by many ISPs for authenticating remote users. RADIUS consists of a client remote access server (RAS), and a separate RADIUS server.

When the user dials into the client remote access server, his or her username and encrypted password are forwarded to the RADIUS server as a request for authentication. In addition to the username and password, the request also includes the client identification number and the port number accessed by the user.

The server validates the request, decrypts the password, and forwards the information to be authenticated by PAP or CHAPS. If the information is correct, then the server sends a message back to the client accepting the user. If the information is incorrect, a rejection message is returned to the user.

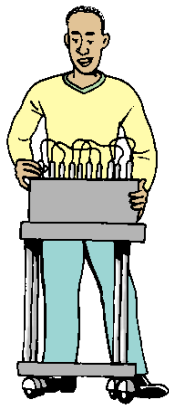
Check Your Understanding

- ◆ Define the term "encryption key."
- ◆ Describe the basic differences between symmetric key and public key encryption.

Try It Out: Network Threat Analysis-Tiger Teams

Materials Needed:

- Windows 95 PC
- Internet Connection
- Any Word Processor (e.g., MS Word) or Spreadsheet (e.g., MS Excel)
- Pen/Pencil and Paper
- Poster Board
- Student Portfolio



In this activity, you will learn about Tiger Teams. You will form a Tiger Team and using an example network that employs a LAN, Remote Access Services, Intranet, Internet, and Extranet, your team will complete a threat analysis for security vulnerabilities and plan security measures to counter them. You will learn about firewalls, viruses, and other threats to network security.

Part 1: What is a Tiger Team?

The term "tiger team" originates from military jargon. The term describes a team of individuals who are highly trained in tactics for sneaking into security systems. They are used to test the security systems of civil defense installations by the military. If the team is successful in infiltrating a "secured" building, they leave notes around to indicate they were there. A new brand of tiger teams have been created called "crackers". Crackers test the security of a network.

1. Research more about the roles of tiger teams and crackers. Use the Internet or any source you find appropriate.
2. Within a group of five, share what you discovered about tiger teams, crackers, and the techniques they employ to crack into a network.
3. Choose one subject, either information about a tiger team or a special technique used by crackers, and create a poster that presents an informative display for the classroom.

Part 2: Identify Threats to Networks

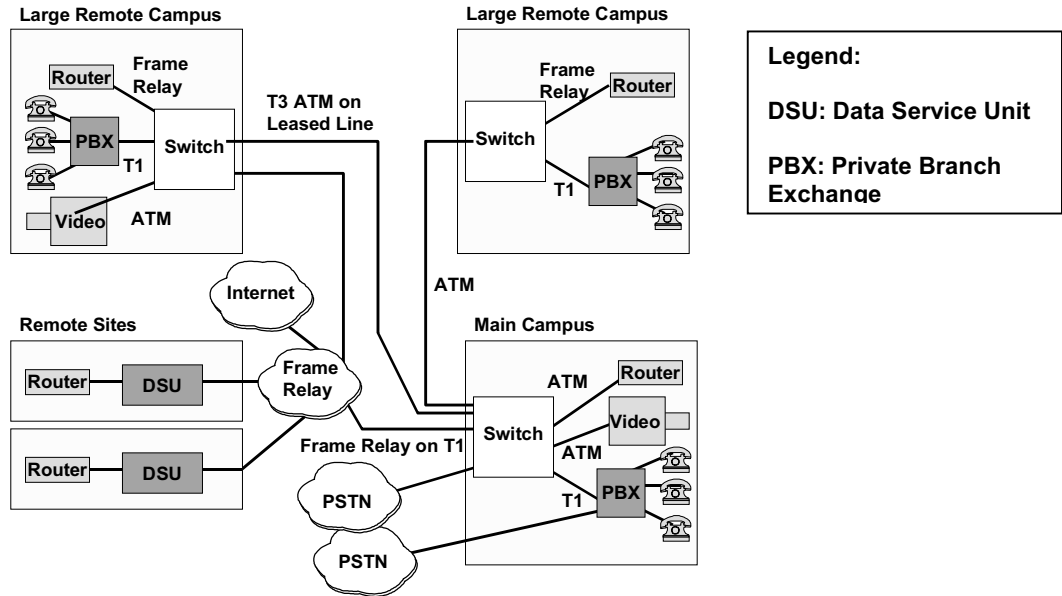
Any time a network sends data across public networks, or moves data into areas that are not physically secured, the network is vulnerable to security threats. Examples of typical threats might include: violation of privacy, theft of data, corruption of data, computer viruses, e-mail spamming, and flooding of protocols to interrupt network services.

Network Designers have devised ways to minimize the threats of attack they face. Some of the most important techniques are access control (passwords) and firewalls.

1. Using the Internet, research threats to networks and put together a comprehensive list including the ones described above.
2. For each of the threats you identified, list some of the strategies used to eliminate or reduce that threat. When you are finished, you should have a good list of threats and threat reduction strategies.
3. Share your list in a class discussion and create one comprehensive list.
4. Create a chart that clearly displays the list of threats and corresponding strategies against the threats.
5. Place this chart in your portfolio.

Part 3: Perform a Threat Analysis of a Network Topology

1. In the network topology diagram below, there are a number of points of vulnerability. Working in your team of five, apply your knowledge of threats to network security to create a list of vulnerabilities in this network. List at a minimum of five threats.



2. You are the Tiger Team! Identify everything from passwords left on user's desks, and easy to guess passwords, to Internet attacks.

3. Use this table below to document your Threat Analysis:

Location in Network	Threat
A.	
B.	
C.	
D.	
E.	

4. On the network topology diagram above, mark a letter that indicates (at least one place) where each threat exists.

Part 4: Identify Strategies to fix Network Vulnerabilities

Network designers and managers must design and implement "fixes" to security problems.

1. Now that you have identified the threats, you must design or identify fixes for each of the vulnerabilities or threats you identified.
2. Use the table below to document your strategies to correct the security threats. You may need to do additional research on security solutions.
3. Share your team's analysis and strategies in class discussion.
4. Place the results of this activity in your portfolio.

Threat	Strategy to Fix
A.	
B.	
C.	
D.	
E.	

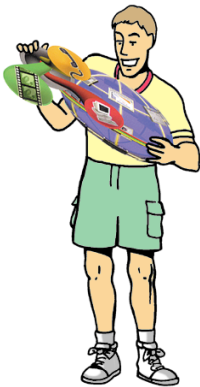
Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Poster presentation suitable for classroom display	25	
Identification of security threats documented in table and on diagram	25	
Identification of strategies for fixing security threats documented in table	25	
Participation in class discussion and inclusion of activity in portfolio	25	
TOTAL	100	

Stretch Yourself: Pretty Good Privacy (PGP) Software

Materials Needed:

- Windows 95 PC
- 3.5" IBM Formatted High Density Floppy Disks (1-3 per team)
- Internet Connection
- Any Word Processor (e.g., MS Word)
- Downloaded PCP 6.5.1 Freeware, Manuals, and Documentation



PGP 6.5.1 is encryption freeware distributed by the Massachusetts Institute of Technology (MIT) in cooperation with Philip Zimmerman, the original author of PGP, Network Associates, Inc., and with RSA Data Security, Inc.

PGP enables users to exchange encrypted messages and to secure files stored on their computers. The program also allows the user to create self-decrypting archives so those files sent to a person without PGP and can still be viewed.

The software is available via the World Wide Web and may be downloaded free of charge. There are PGP versions for Windows 95, 98, and NT, and for the MacOS 7.61 and up. The URL for a description of PGP and links for downloading the program is located at <http://web.mit.edu/network/pgp.html>. Although the web site indicates that the program can be downloaded from the MIT FTP site, this is no longer true. The program must be downloaded from the web site. In addition, users must complete a distribution authorization form indicating that the program will not be used for commercial purposes and that the user is a U.S. citizen.

Included in the download is the full PGP program, an introduction to cryptography, the PGP Command Line Guide, and the PGP User's Guide.

In this activity you are to complete the following:

1. Working in a team of three to five students, download and install the PGP 6.5.1 version compatible with your computer's operating system.
2. Read the document provided, "The Basics of Cryptography." This document provides a very good overview of cryptography and how PGP uses a hybrid cryptosystem as the basis for its encryption functions.

3. Read the user's guide and refer to it to complete the following steps.
 - a. Create a private and public key pair.
 - b. Exchange the public key with your team members.
 - c. Each team member should validate the public keys they have received.
 - d. Create a file (e.g., a word document) that you will encrypt.
 - e. Place the file in a folder on the desktop for easy access.
 - f. Encrypt the file following the directions provided in the user's guide.
 - g. Copy the encrypted file onto a floppy disk and exchange the file with your team members.
 - h. Your team members will also give you an encrypted file.
 - i. After exchanging files, decrypt the files and print out the contents of the file.
 - j. There are multiple ways to encrypt a file. If you have time try more than one method.
 - k. Success of this activity is measured on your ability to encrypt and decrypt a file using keys created by you and your team members.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Cooperative team work	25	
Successful key creation	25	
Successful file encryption	25	
Successful file decryption	25	
TOTAL	100	

Network Wizards:

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

Part One: Ethics Debate

There are many ethical issues involving computers and cyberspace. With the advent of the Internet, these issues have become heightened. The Internet provides access to networks that never before were threatened by such a large audience. Hackers (or crackers) are attempting to enter networks everyday. The Internet also provides easy access to information often not considered appropriate for children.

In this activity, you will work with two teams of five students to research one of two ethical questions and debate the issues. Your team will be graded on how well you present your supporting arguments and what resources you bring to the debate to support your position.

The Ethical Issues

1. "Hackers: Are they public servants or malicious criminals?" (Hayward, 1997) If they are criminals, how should they be punished?
 - Pro: Hackers provide a public service by demonstrating the weakness of a network's security system.
 - Con: Hackers are malicious invaders of corporate networks looking for secrets and causing problems that create downtime for the corporation.

2. Blocking Software: Blocking software (e.g., CyberPatrol) allows parents and schools to prevent children from viewing Internet sites they feel are inappropriate. Should schools implement blocking software? Does the implementation send a message of distrust to the students or merely provide a means for the schools to protect their students? Should students be held to a standard of responsibility?
- Pro: Blocking software is the best means of preventing students from accessing inappropriate Internet sites. Students cannot be trusted to make responsible decisions. The schools are simply protecting students.
 - Con: Blocking software is not the best way to teach students responsibility. It sends a message that the school does not trust students and prevents students from making a choice. Students should be protected from such censorship activities and given the right to make their own choices.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Thorough research and quality resources	25	
Cooperative team work to produce a united debate team	25	
Supportive arguments during debate	50	
TOTAL	100	

Part Two: Network Design Portfolio Case Study

Statement of Work

If you have not already done so, you should put the final touches on your Statement of Work.

On-Site Interview

If your organization's contact has not reviewed your Statement of Work, take the document with you for your on-site interview. You can review the statement as part of your interview. Also, take with you the pre-site questionnaire. You may want to refer to it during your interview.

The on-site interview serves as a "kick-off" meeting for you to meet all the individuals you may need to interact with as you prepare your network design proposal.

There are a few points to remember when you set up the meeting.

- Call ahead and set a day and time for the interview/meeting. Be considerate of your contact's work schedule, but do not be afraid to remind him or her that you are constrained by your school hours. Try to keep your meeting to one hour. If you cannot get a convenient time to meet, then you will have to complete your design with the information given to you on paper. If necessary, that is fine.
- Arrive to the meeting on time. Do not be late. If you have to be late for any reason, call and inform your contact that you will be late. Apologize upon your arrival for being late.
- Dress professionally. This may be your first exposure to some of the organization's network professionals. You want to give a good first impression.
- Be prepared. Have your questions ready. You may not know all the questions that you need to ask. Do not be afraid to admit that you are learning and need some help identifying key concepts.
- Take notes. If a point comes up in the conversation that you do not understand, ask for more explanation.
- When you are done, thank your hosts for their time. Offer to type your notes and send them to your contacts for review and comment. Your contacts may remember the conversation differently or may have added comments after they have thought about it later.

The on-site interview is used to detail the information you gathered from the pre-site questionnaire. Your goal is to:

- Clarify the organization's business requirements. What are the most important applications used? For example, does the organization have a database that everyone accesses for information or does the organization participate in video conferencing? Do they have many mobile users?
- Understand the state of the current network and what the organization's desires for their network in the future. For example, does the organization plan to implement Voice over IP or a VPN? What problems currently exist for the network?
- Document the current network topology and performance issues.
 - What is the campus configuration? Are there multiple locations? What applications are used locally by employees? What is the topology of the LANs.
 - What is the WAN configuration? What locations need to be connected? What are the bandwidth requirements? Is availability an issue?
 - What is the IP address scheme? (Do not worry if the organization will not share this information.)
 - Does the company have remote users? How many? Where are they located?
 - What security issues are present or expected?
- Make arrangements to interview the organization's network professionals individually (if possible). Some of the individuals you may want to interview include the Chief Information Officer (if possible), the Director of networking or Manager of Information Systems, the network operations manager, the network technicians, and the end user.
- Make arrangements to either work with the organization's network professionals to gather electronic data or acquire written information about the network's performance.

Summary

VPN Solutions

In this lesson, you learned the following:

- The three primary reasons to implement a VPN
- How to diagram three VPN service models
- The major considerations when implementing a VPN
- The differences in Symmetric Key encryption and Public Key encryption

Review Questions

VPN Solutions

Part A:

1. Describe in three short paragraphs, the three reasons a company would consider implementing a virtual private network.

Part B:

1. Diagram the Service Provider-Service Provider VPN model. Label the diagram and indicate where the tunnel begins and ends.

2. Diagram the Service Provider-Enterprise VPN model. Label the diagram and indicate where the tunnel begins and ends.

3. Diagram the Enterprise-Enterprise VPN model. Label the diagram and indicate where the tunnel begins and ends.

Part C:

Identify each statement as either true (T) or false (F).

1. The number of POPs is not important in determining if an ISP can provide adequate availability to a VPN.

2. The Internet has a high rate of redundancy, which ensures a packet will arrive to its destination across a VPN.

3. VPNs are a good solution for companies that use videoconferencing and other applications that require high transmission speeds.

4. Management of a VPN is often handled by the ISP.

5. VPN performance is lowered by excess traffic on the Internet.

6. If a company decides to let the ISP manage its VPN, then it should contract for a specific quality of service.

7. Performing audit trails to track security violations is a VPN management task.

8. Security is always guaranteed using a VPN.

9. Technical support for users of a VPN is not necessary.

10. It is important to choose appropriate encryption and user authentication methods when implementing a VPN.

Part D:

1. What is an encryption key?

2. What is a Symmetric Key encryption?

3. What is Triple-DES?

4. What is a Public Key encryption system?

Scoring

Criteria	%	Your Score
Part A: Describe three primary reasons to implement a VPN.	20	
Part B: Diagram the three VPN service models.	30	
Part C: Identify major considerations when implementing a VPN.	30	
Part D: Compare the differences in Secret Key Encryption systems and Public Key Encryption systems.	20	
TOTAL	100	
Try It Out:	100	
Stretch Yourself:	100	
Network Wizards:	100	
FINAL TOTAL	400	

Resources:

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

Gates, B. (1996), The Road Ahead. New York: Penguin Books.

Hayward, D. (1997). Hackers: Friends or Foes? Available Online:
<http://www.techweb.com/wire/news/1997/1997/09/0915hackers.html>.

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.