Lesson 3-2: WAN Considerations

At a Glance

In the previous lesson, WAN Configurations, you learned about the physical media, the kinds of switching, and some of the protocols and services used for transmitting information across long distances. Setting up a wide-area network requires careful planning. Each situation is different and each situation will change over time. Network designers choose a specific combination of media, protocols, services, and service providers after considering many factors. These factors include the nature of traffic that will travel across the WAN, cost, reliability, and security. This lesson will introduce the questions that should be answered before a WAN is established.

What You Will Learn

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

• Define quality of service (QoS) and explain how it can determine how various types of information are transmitted over a WAN.

• Define Committed Information Rate and explain how it affects the transmission of data over a WAN.

• Define error rate and packet loss and explain why these are important considerations on a WAN.

• Explain how a WAN can maintain security.
Tech Talk

- **Authentication**—A way of verifying that data actually comes from where it says it does and hasn’t been changed on the way (data authentication), or that a user logging on to a network is really who he or she claims to be (user authentication).

- **Committed Information Rate (CIR)**—The minimum rate at which a link commits to transfer data across the link.

- **Congestion**—Heavy traffic on a connection that decreases the bandwidth available for any particular user.

- **Encryption**—Changing data into a code that can only be read by deciphering with a key.

- **Error correction**—A part of the data transmission process that ensures that data arrives at its destination correctly.

- **Firewall**—A device (or software in a router) that protects the security of a LAN by filtering out certain types of traffic.

- **Proxy server**—A server that functions between a LAN and a WAN and hides the individual addresses of workstations on the LAN by replacing them with a proxy address.

- **Public key encryption**—A method of protecting the security of information. Each user has two encryption keys, one public and one private.

- **Quality of Service (QoS)**—The required bandwidth (and speed of delivery) for a particular packet of data.

- **Redundancy**—Back-up systems or circuits that are ready to be used when a part of the network fails.

- **Tunneling**—Putting frames from one protocol inside of frames of another protocol. This might be done to convert frames from a LAN into frames that can be routed across a WAN.
Traffic on a WAN

In the previous lesson, you learned about three types of connections for wide area networks:

- **Leased lines**, in which a circuit is open all the time and is used only by one computer or LAN to connect to one other computer or LAN.

- **Circuit switched lines**, in which a circuit between one computer or LAN and one other computer or LAN is created each time there is data to transmit. The circuit stays open until the call is ended.

- **Packet switched lines**, in which data transmissions from many local area networks are divided into packets (or frames or cells) that travel across the wide area network on shared circuits and are then reassembled at their destination.

Each of these options has advantages and disadvantages depending on the nature of traffic. Traffic is the general term for anything that travels over the lines. This might be a voice call, a fax, a computer data file, a videoconference or many other kinds of information.

There are three important questions about traffic that you must answer in order to determine what kind of switching, as well as what kind of media and protocols to use for a wide area network.

- **How often is traffic transmitted?**
- **What kind of traffic is transmitted?**
- **How much traffic is transmitted?**

In the previous lesson you learned how the first question (How often is traffic transmitted?) relates to the kind of switching.

Some traffic comes in short bursts with long spaces in between. Email is a good example of this kind of traffic. A WAN connection that is used primarily for email might work fine on a circuit switched connection. The network user would only pay each time a connection is made.

A constant or near-constant flow of information across the network would become too slow on a circuit switched connection, held up by the wait to connect each time data had to be transmitted. A stock exchange transmitting trading information would be an example of this kind of traffic. A leased line might work best for this kind of WAN use.

Leased lines, however, are expensive. Many networks have times when traffic is intermittent like the email example, and also times when traffic is steady. For these networks, a packet switching service may work best. The remainder of this lesson will focus on packet (or frame or cell) switched wide area networks.
Quality of Service

The world is heading toward unified networks. Soon you will be able to transmit voice telephone calls, faxes, digital images, video, and even television on the same network. The beginning of this technology is called broadband, in which a medium such as coaxial cable or optical fiber, carries multiple channels.

Instead of one connection for telephone service, another connection for videoconferencing, and another for carrying data, a single WAN connection can carry all of the information. Of course, this means that the connection must have a high bandwidth and must be able to handle the different needs of different kinds of traffic.

Different types of traffic require different bandwidths. If you are trying to watch a video or a teleconference being transmitted across a WAN, you need the packets of video data to arrive one after the other very quickly. If this happens, you will see a smooth picture. If there is a delay between packets, then you will see a “jerky” picture. Videoconferencing requires a high quality of service.

In contrast, email can be sent with a low quality of service. Most people do not read email as it arrives, so delays in the arrival of packets do not cause problems. Remember that a delay means less than a second (much less). Even if you read your email once every minute, you would not notice delays in the arrival of email.
With older X.25 packet switching networks there are many factors along the route that can delay the arrival of data. Packets are forwarded from switch to switch through the network. Each switch must read the destination of the packet before it can send it on in the correct direction. Each time the address must be read, it delays the packet just slightly. Another delaying factor happens because each packet may take a different physical path through the network. This means that different packets might take longer to get to their destination. A packet sent later may travel a faster route and arrive earlier. At the destination, the packets are sorted into the correct order. This sorting process also delays the arrival of transmissions.
In newer cell switching services, such as ATM, the packet (called a cell) includes information in its header that tells the network what quality of service the data needs. Compare this to the post office offering different delivery options: regular first class, second day, and priority overnight. When the post office sees a priority mail envelope come through, it gives it special service to make sure it gets where it’s going on time. ATM networks can give different cells different service depending on the quality-of-service information in the cell header.

Check Your Understanding

♦ What is an important difference between a leased line and a packet switched connection?

♦ What factors can delay a transmission?
Reliability

As you learned in the WAN Configurations lesson, many companies pay to use WAN connections through a phone company or an Internet Service Provider instead of building their own WAN connections. A primary reason for this is cost. It can be very expensive to set up a WAN. Once the network is set up, a network administrator must monitor and repair the network when anything goes wrong. For many companies, it’s much less expensive to pay a provider to maintain the circuits.

Redundancy

Another reason to use a service provider for a WAN connection is redundancy. If a company owns a dedicated line between its two offices and something happens to that line, the company has no WAN until that line is fixed. Phone companies and other WAN providers have huge networks with many lines going between major cities. If something goes wrong with one line, there are other paths that data can take to get to its destination. The company using the network may not ever notice there was a problem. These back-up paths are called redundant circuits.

Redundant Circuits

One place there may not be redundant circuits is in the connection between the LAN and the WAN. A very high bandwidth connection such as optical fiber with ATM can potentially carry all of the traffic from a company. If something happens to that connection, there is no WAN.
Committed Information Rate

The rate at which data is transmitted across a WAN connection isn’t always what the advertising promises. Phone lines do not always transmit data at the highest bandwidth possible. A good example is the analog phone lines you might use to access the Internet from a home computer. These lines are capable of transmitting data at 56 Kbps, but they only use that bandwidth some of the time. If you buy a “56K” modem (don’t confuse this with a Switched 56 telephone line) and read the fine print, you will learn that the maximum bandwidth for downloading data from the Internet is actually 53 Kbps. You will also learn that the maximum bandwidth for uploading data is limited by the analog telephone line to 33.6 Kbps. (Uploading includes all the mouse clicks and keystrokes you enter to display Web pages.)

Committed Information Rate

When you use a packet switching service such as X.25 or Frame Relay, you are sharing the telephone lines inside the phone company network with many other users. Compare this to a highway for automobiles and trucks. When there is heavy traffic on a highway, the speed of travel decreases. Heavy traffic, called congestion, can also slow the transmission speed on telephone company circuits. If you use the Internet much, you know that late afternoon on a Friday is a slow time to browse the Web.

When it provides packet switching service, a phone company may use any of a variety of services to move the data and it may send the data through
its network along any path it chooses, as long as the data arrives on time and uncorrupted at the other end. The phone company does not promise that your data will always receive the maximum bandwidth. For example, if you contract with a phone company for a 1.544 Mbps connection, your data will not always receive 1.544 Mbps of bandwidth. Sometimes there just is not enough bandwidth for everyone.

Phone companies usually sell more bandwidth than they actually have. They assume that not all customers will need all their bandwidth at the same time. When there is congestion, there may not be enough bandwidth for all customers. Some data won't get through.

Compare this to airlines that overbook flights. The airlines know that some people are going to cancel their tickets at the last minute or just not show up for the flight, so they sell more tickets than they have seats. But sometimes, for example on flights from Florida on Sundays in winter, too many customers show up to use their seats. Then the airline has a problem, and they have to manage people off the flight. First the airline asks for volunteers and if you volunteer to miss the flight, you might get a bonus like cash or a free ticket. If not enough people volunteer, the airline chooses people. The first people who lose their seats are the people flying standby. The next people chosen to give up their seats are the ones who paid the least. A similar process happens over a Wide Area Network. On a WAN, the equivalent of the price you pay for a ticket is the price you pay for a Committed Information Rate (CIR). The CIR is the amount of bandwidth that the phone company guarantees to allocate to your data transmissions. The CIR might be half or less of the maximum bandwidth possible.

In a wide area network, the switch at the border between you and the WAN constantly watches the amount of data you send. If, in any given one second interval, you transmit more than your CIR for that second, the switch marks all the frames over the CIR as “discard eligible.” This is like an airline marking a passenger as standby. If there is no congestion in the network, this mark has no effect whatsoever. If, on the other hand, some switch, somewhere in the network is congested, it will discard all “discard eligible” frames before it discards any unmarked frame. If your frames are being discarded, your applications will begin to act jerky and generally unresponsive.

The higher the CIR, the more the connection will cost. The customers who pay for a higher CIR are like the airline passengers who pay for a more expensive ticket—they are less likely to get bumped off. To save money, some companies contract for a CIR of zero. This means that their data is always “flying standby.” When there is very heavy traffic, their data might get no bandwidth at all, and not get through.
Lesson 3-2: WAN Considerations

Error Correction

When you talk on the phone, there are times when you might hear noises other than the voice of the intended person at the other end of the line. On a regular telephone, you might hear static or clicking. On a cordless phone you might hear a hum or buzz when you get near a television or computer. On a cellular phone you might hear other people’s conversations when the frequency of your phone is very close to the frequency of another cellular phone in use nearby.

For a phone conversation, noise on the line might be just a minor inconvenience, but when digital data is being transmitted, noise on the line can cause bits of data to change. A change in a single bit can mean a program won’t work, or a file won’t open. It’s very important that data be transmitted without errors.

Error rates

The best way to avoid errors is to choose a WAN connection that has a low error rate. Different media and protocols have different error rates. These are measured as the number of wrong bits divided by the number of bits transmitted. If there were one wrong bit in every 100 bits transmitted, the error rate would be 1/100 or 0.01. A more convenient notation for this is $10^{-2}$. A negative exponent of 10 represents the number of places to the right of the decimal point (for example, $10^{-4} = .0001$).

A twisted pair analog network will yield an error rate of $10^{-5}$ (One wrong bit for every 100,000 bits transmitted. A digital network running on the same twisted pair copper wires will yield an error rate of $10^{-7}$. Digital fiber optic systems have an error rate of $10^{-11}$ to $10^{-14}$, which is almost perfect.

Another way that error rates are expressed is by the number of dropped packets. When the network discovers that bits have been corrupted in a packet, the packet is discarded or dropped and, depending on the network, a new packet is requested or the packet is just ignored.

Finding errors

Network protocols include error correction. This means they have algorithms to check the data they receive to make sure it is the same as the data that was sent. There are a number of different methods for finding errors. One way is by using a checksum. Before it sends a data packet across the WAN connection, the sending node adds the binary values of all the bits in the packet and comes up with a number called a checksum. It includes the checksum in the packet. The receiving computer then does the same calculation when the packet encounters the protocol in the matching OSI layer. If the packet transmitted okay, the result of the calculation at the receiving end will be the same as the checksum included by the sending computer. If the result of the calculation at the receiving end is
different from the checksum then the receiver can assume that the message has been corrupted.

### Error Checking

One problem with a checksum is that there can be offsetting errors. If one bit in the packet changes from 0 to 1 and another bit changes from 1 to 0, the sum of all the bits will still be the same and the error will not be caught. A better way of finding error is called a cyclical redundancy check (CRC). Instead of just adding the bits to find a checksum, CRC divides the data into parts and then divides those parts by a certain number. The remainder is used like the checksum. At the receiving computer the protocol repeats the calculation. If the remainder is the same, the data is okay. CRC catches many more kinds of errors than a simple checksum.

### Correcting errors

Different WAN protocols handle error correction in different ways. For example, switches in an X.25 network make a copy of each packet before sending it on to the next switch. Each switch also checks for errors in the packets it receives. X.25 uses Cyclical Redundancy Check (CRC). If it finds an error, the X.25 node requests retransmission of the corrupt packet from the sending switch. The sending switch uses the copy of the packet it made and transmits it again.

Frame relay and other broadband technologies eliminate error recovery functions from the network. Instead, the routers and the PCs on the LANs at either end, not the network itself, handle error correction. Error correction is left to higher layers in the protocol stack.
Check Your Understanding

♦ Why can a packet switching customer save money on a WAN connection by having a CIR of 0?

♦ What kind of WAN connection has the lowest error rates?

♦ Name two different types of error detection on a WAN. Which is more effective?

♦ Which devices on the network perform error correction in an X.25 network? Which devices perform error correction in a frame relay network?

Security

Using WAN connections across public data networks, especially the Internet, means you share your circuits with other users. This has advantages and disadvantages. An advantage is that you don't have to spend a lot of money to build and maintain your own circuits. A disadvantage in using a public network is that there are many opportunities for other people to see, and even intercept, what you are sending. That could be a big problem if you are sending such information as your credit card number or the design for your latest invention. Another disadvantage to using a public network is that the same telephone line that allows you to connect out to distant networks can allow someone else to connect in and see what’s on your LAN. That could be a big problem if that person has harmful intentions.
Encryption

Encryption keeps people from reading your data unless you want them to. When you encrypt something, you translate it into a secret code, called cipher text. In order to decipher it, the person you are sending it to needs a key. Only someone with the key can read your data.

Basic Encryption

<table>
<thead>
<tr>
<th>Plain Text</th>
<th>Encryption Key</th>
<th>Cipher Text</th>
<th>Encryption Key</th>
<th>Plain Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>=18+5=23=</td>
<td>W</td>
<td>=23-5=18=</td>
<td>R</td>
</tr>
<tr>
<td>E</td>
<td>=5+5=10=</td>
<td>J</td>
<td>=10-5=5=</td>
<td>E</td>
</tr>
<tr>
<td>A</td>
<td>=1+5=6=</td>
<td>F</td>
<td>=6-5=1=</td>
<td>A</td>
</tr>
<tr>
<td>D</td>
<td>=4+5=9=</td>
<td>I</td>
<td>=9-5=4=</td>
<td>D</td>
</tr>
<tr>
<td>T</td>
<td>=20+5=25=</td>
<td>Y</td>
<td>=25-5=20=</td>
<td>T</td>
</tr>
<tr>
<td>H</td>
<td>=8+5=13=</td>
<td>M</td>
<td>=13-5=8=</td>
<td>H</td>
</tr>
<tr>
<td>I</td>
<td>=9+5=14=</td>
<td>N</td>
<td>=14-5=9=</td>
<td>I</td>
</tr>
<tr>
<td>S</td>
<td>=19+5=24=</td>
<td>X</td>
<td>=24-5=19=</td>
<td>S</td>
</tr>
</tbody>
</table>

You might have used secret codes when you were younger (or maybe you still do) that worked like this: You translate a message into code using a key. The key might include several steps such as:

1. Change the letters to numbers, 1 to 26.
2. Add five to each number, for numbers larger than 26 start back at 1.
3. Convert the number back to a letter.

You whisper the key to your friend so no one else can hear, or you pass it to him/her in a note that s/he swallows after memorizing. Then you send the message. This is called secret key or symmetric encryption. Both the sender and the receiver know the key but no one else does. Secret key encryption works pretty well when you can whisper the key to the receiver, but it doesn’t work so well when you want to give the key to someone far away across a WAN. If you could send them the key without worrying about it being intercepted then you probably don’t need encryption to begin with!
A safer method of encryption is called public key encryption. With public key encryption, each user has two keys, one public key that everyone knows and one private key that only the sender knows. Each key is a very large number that is used in a function to change the characters in the message. When someone sends you a message enciphered with your public key, only you can decipher it using your private key.

**Public Key Encryption**

![Public Key Encryption Diagram]

**Authentication**

Authentication is a way of making sure that information sent from a person actually comes from that person. A malicious person may want to put information onto a LAN that doesn’t belong there, for example, a virus. To gain access to the LAN, the person might pretend to be an authorized user by using the authorized user’s address. To an unprotected LAN, that information will look like it came from the authorized user. To prevent this kind of intrusion from happening, a LAN might use data authentication or user authentication.
Public key encryption, described above, also works in reverse for data authentication. The firewall using public key encryption can be set to accept only encrypted information from certain addresses. The encrypted messages are deciphered using public keys. In order for a message to be decipherable using a public key, it must have been encrypted using the matching private key, which means it is authentic.

Another form of authentication prevents unauthorized users from logging onto a network. The most common type of user authentication is a user password that must be typed in before gaining access.
Firewalls

A firewall protects the security of a network by restricting the information that is allowed to pass between the LAN and the WAN. The simplest firewall is a router that sits between the WAN and the LAN. All data from the WAN must pass through the router. The router may perform encryption and authentication. It may also be set to only allow transmissions that:

- Are coming in or going out.
- Are of a certain type (email, telnet, ftp, and so on).
- Contain certain data or do not contain certain data.
- Come from a particular address or do not come from a particular address.
- Arrive before or after a certain time of day.

A DMZ

Some companies may want stronger protection. They might hire a company that specializes in security to set up a small network, called a “DMZ”, or Demilitarized Zone. Any information coming in from the WAN must pass through the DMZ before it gets onto the LAN. The DMZ contains a firewall server that does authentication and encryption using special software, as well as a proxy server.
Proxy Servers

Each computer on a network connected to the Internet must have an address. If a hacker learns the address of a particular computer inside your LAN, that person can use that information to get inside the LAN. When you send email, your messages contain the address of your computer. When you browse the web, every click of your mouse is actually a message sent across the Internet to the server that contains that web page. The mouse click also includes your computer’s address. Companies that send junk email, called spam, collect the IP addresses of computers that have accessed certain websites. Then they send email directly to those addresses.

A proxy server hides the address of the sending computer before passing data out to the Internet. It does this by using its own address to replace the address of any computer on the LAN. The replacement address is called a proxy address. When a spammer tries to use the address, the mail goes to the proxy server instead of directly to a workstation on the LAN. The proxy server can then be set to reject messages from addresses that are known to be sources of spam.
Virtual Private Networks

In the WAN Configurations lesson, you learned that some WANs called Virtual Private Networks (VPNs) use the Internet. Even though the data travels across the Internet, to a user at either end, a VPN seems like a leased line: the connection is always open and the data always goes to the same place. Sending data across the Internet in a VPN is known as “tunneling.” By using a tunnel, packets from specific sources, for example, a credit card approval from a bank, can be automatically separated from all the other data travelling on the network. The tunneled data can also be given higher quality of service.

Internet Service Providers (ISPs) offer VPNs. Since a LAN connected to the Internet can communicate with any other LAN connected to the Internet, a VPN is actually a way of making that connection more secure. To make the VPN private, the data is encrypted and authenticated.

Preparing data to be sent through a VPN is typically the job of the router that runs a tunneling protocol. A tunneling protocol puts data packets from a LAN into packets that transmit over the Internet. A router isn’t necessary, even laptops can run the software necessary to use a VPN. Windows 95, 98, and NT include this software.
Check Your Understanding

- Why is public key encryption safer than basic encryption?

- What is the purpose of authentication?

- What is the purpose of a firewall?
Try It Out

Building a WAN

In this exercise you will:

- Connect the two LANs in your lab together to create a WAN
- Verify the setup of the WAN by printing and viewing the router’s configuration file
- Make a drawing of the WAN, by combining the drawings of the individual LANs
- Use ping to verify that the WAN is functioning.
- Disconnect the WAN and try pinging and/or transmitting a file to see and document what happens

Materials Needed

- BayStack ARN Router documentation
- Two functioning switched LANs
- Cables and connectors necessary to form a WAN

Part 1: Connect the LANs

1. Connect a router to each switch
   
   You will be referring to Chapter 1: Installing the BayStack Advanced Remote Node Router in the BayStack ARN Routers book.
   
   a. Find the section in the book entitled “Understanding the ARN Module Locations.” Inspect your router.

   ♦ What is the base module configuration of your router?
   
   ♦ Are there any expansion modules installed?
   
   ♦ Are there any adapter modules installed?
b. Find the section in the book that describes cables.

- To connect your router to an Ethernet 10BASE-T network, what kind of cable will you need?
- What type of connectors should it have?

2. Request the appropriate cables from your instructor. Install the cable between the router and the switch. You can plug the cable into any port on the switch.

Students should request a straight through cable with RJ-45 connectors.

When you connect the cable to the switch,
- one LED on the switch will light constantly
- another LED on the switch will flash intermittently
- an LED on the router will flash intermittently.

- Explain what each of these LEDs means.

3. Connect the routers to one another by their serial interfaces (also called a WAN interface.)

Refer to the router manual.

- What kind of cable is needed?
- What transmission rates is the cable capable of carrying?
Lesson 3-2: WAN Considerations

♦ How does this compare to the LAN connections?

♦ What kind of connectors does it have?

Other router manufacturers may use different connectors for their WAN interfaces.

The cable students will use, the V.35 cable, is a crossover cable. Normally the cable from the router would be a straight-through cable between the router and a CSU/DSU. The CSU/DSU would connect to the telephone company line. Because you will not be connecting this network to the telephone network, you will simulate a WAN by using a crossover cable, which simulates the phone company connection and eliminates the need for a CSU/DSU.

Refer to the router diagram and connect the WAN cable to the serial interfaces on each router.

♦ What happens when you connect the routers together?

Part 2: Verify the setup of the WAN using Technician Interface (TI)

In this part of the lab, you will inspect the Layer 1 and 2 status of the WAN interfaces. If they are operational, their status will be “up.”

1. Start MS-DOS on your PC

2. Telnet to the local router (check your diagram and use the IP address of the Ethernet port for your LAN). Example: `telnet 141.251.10.1`
3. At the login screen, type **Manager**.

![Login screen](image)

You are now communicating with the router using Technician Interface, a language somewhat similar to MS-DOS. You will next check to see which ports on the router are operational. To do this you’ll use a program that is kept in the memory on the router.

4. To make sure you can find the program you need in the router’s memory, type **cd 1a**:

![Program list](image)

5. To get a list of programs found on the router type **Menu**.
6. To check which ports are operational, type 6. You will see this screen:

![Telnet - 141.251.101](image)

Running show circuits base

<table>
<thead>
<tr>
<th>Slot</th>
<th>Conn</th>
<th>Circuit</th>
<th>State</th>
<th>MAC Address</th>
<th>DFI</th>
<th>MTU</th>
<th>HW Filter</th>
<th>Line Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>E11</td>
<td>Up</td>
<td>00-00-A2-62-44-08</td>
<td>5</td>
<td>1518</td>
<td>Disabled</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>E12</td>
<td>Down</td>
<td>00-00-A2-05-F1-24</td>
<td>5</td>
<td>1518</td>
<td>Disabled</td>
<td>10 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot</th>
<th>Conn</th>
<th>Circuit</th>
<th>State</th>
<th>MAC Address</th>
<th>Number</th>
<th>MTU</th>
<th>Protocol</th>
<th>Addr</th>
<th>Addr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>S12.B2</td>
<td>Up</td>
<td>00-00-A2-62-94-05</td>
<td>00201302</td>
<td>1600</td>
<td>PPP</td>
<td>STD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Press Enter to continue.

a. The fourth column, State, tells you which circuits have connections. Complete the table:

<table>
<thead>
<tr>
<th>Circuit</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. When you are finished looking at the list of circuits:
   a. Press Enter to return to the menu.
   b. Type q to quit the menu and return to the Telnet prompt.
   c. Pull down the Connect menu and select Disconnect to exit from Telnet.
   d. Close the Telnet window.
   e. Go on to the next part of the lab.
Part 3: Verify that the WAN is functioning

In this part of the lab, you will check the Layer 3 (IP) functionality of the WAN. You will ping each step along the route from a PC connected to one LAN through the WAN link to a PC connected to the other LAN.

1. Start MS-DOS on any PC connected to either LAN.
2. Ping the port on the router connected to your LAN.
3. Ping the port on the router connected to the WAN.
4. Ping the port on the other router connected to the WAN.
5. Ping the other workstation.
6. Try disconnecting a machine from the distant LAN and ping that machine.
   ♦ What is the result?

Part 4: Diagram the Network

1. Create a network topology diagram that includes the WAN. Use the diagrams you have already created for the LANs.
Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct physical setup and cabling</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Verification of setup using software monitors</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Verify operation using networked computers</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100</strong></td>
<td></td>
</tr>
</tbody>
</table>
Stretch Yourself

Tracing the Route

In this exercise, you will use Sniffer Basic to document the route of the data from a workstation on one LAN to the workstation on the other LAN.

Materials Needed

- Basic Sniffer software
- Word processing software
- Clint/Server LAN
- Server with
  - Large share-enabled file
  - Small share-enabled file
  - Video share-enabled file
- LAN diagrams of classroom network created for previous lessons

Start the Sniffer Basic application.

1. If this is the first time you are using Sniffer Basic, you will be prompted to choose your NIC.

2. You will see this screen.
Measuring Traffic

In this exercise, you will observe the transmission of various data types and file sizes. You will then classify the data types by their requirements

- email message
- email message with attachment
- place small file on other LAN
- place large file on other LAN
- Edit word processing document that resides on server on other LAN
- Play movie that resides on server on other LAN

1. Classify the transmission
   - size of packets
   - number of packets
   - time it takes for entire transmission
   - frequency of packets
   - speed of packets

Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful use of tools</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Demonstrate understanding of measured data</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Generalization of concepts to new examples</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
Network Wizards

Committed Information Rates/Traffic Requirements Research

Materials Needed

- Internet connection

Committed Information Rate

Research committed information rates. What CIR does your school network use? What are the differences in cost for a T1 line with a CIR of 0 versus a T1 line with a CIR of 512 Kbps. Is it possible to get a T1 line with an actual bandwidth of 1.544 Mbps? How could you do this?

Traffic Requirements

Read the information sheet on the web site [http://www.abl.ca/videxp.htm](http://www.abl.ca/videxp.htm) and answer the following questions.

1. What is the product being advertised?
2. Who is the intended customer?
3. How would the product work?
4. What would be an advantage in using the product?

Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear communication with system administrator and other resources</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Prepare precise, informative documentation</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Demonstrated understanding of encryption process</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100</strong></td>
<td></td>
</tr>
</tbody>
</table>
Summary

In this lesson, you learned the following:

- Define quality of service and explain how it can determine how various types of information is transmitted over a WAN.
- Define Committed Information Rate and explain how it affects the transmission of data over a WAN.
- Define error rate and packet loss and explain why these are an important consideration on a WAN.
- Explain how a WAN can maintain security.

Review Question

Lesson 3-2: WAN Considerations

Part A

1. Which type of switching provides lowest delays?
   a. ATM
   b. Packet switching
   c. Circuit switching
   d. Open circuit leased line

2. Which type of switching introduces the greatest delays?
   a. ATM
   b. Packet switching
   c. Circuit switching
   d. Open circuit leased line

3. Which application requires the highest quality of service?
   a. Electronic mail
   b. Video conferencing
   c. Audio broadcasting
   d. Web browsing
4. Which application requires the least quality of service?
   a. Electronic mail
   b. Video conferencing
   c. Audio broadcasting
   d. Web browsing

5. Which switching method provides a flexible quality of service based on need?
   a. ATM
   b. Packet switching
   c. Circuit switching
   d. Open circuit leased line

Part B

1. If you pay for a Committed Information Rate on a WAN connection
   a. You are guaranteed a certain available data rate
   b. Attempts to send data at a greater rate will always fail
   c. Data sent at a greater rate may be discarded
   d. You have access to a private connection

2. A Committed Information Rate is used to select traffic when
   a. The WAN is not busy
   b. The WAN is congested
   c. High-priority traffic is on the WAN
   d. You send data slowly

3. Packets are marked as exceeding the Committed Information Rate by
   a. The sending device
   b. The receiving device
   c. The company router
   d. The switch which connects your network to the WAN
Part C

1. Network error rates are measured as
   a. The number of good bits divided by the number bad bits
   b. The number of good packets added to the number of bad packets
   c. The number of bad bits divided by the number of good bits
   d. The number of bad bits subtracted from the number of good bits

2. Which technique detects more kinds of errors?
   a. Checksum
   b. Cyclical redundancy check
   c. Circuit switching
   d. Authentication

3. X.25 networks detect and correct errors by
   a. Checking the CRC and requesting a new copy of a bad packet from the sending switch
   b. Using a checksum and discarding bad packets
   c. Allowing the routers and devices on the sending an receiving LANs to detect and handle errors
   d. Using the lowest level of the protocol stack

4. Frame relay networks detect and correct errors by
   a. Checking the CRC and requesting a new copy of a bad packet from the sending switch
   b. Using a checksum and discarding bad packets
   c. Allowing the routers and devices on the sending and receiving LANs to detect and handle errors
   d. Using the lowest level of the protocol stack
Part D

1. To verify that the sender of an encrypted message is who they say they are
   a. Use the sender’s public key to decrypt the message
   b. Use the sender’s private key to decrypt the message
   c. Use your public key to decrypt the message
   d. Use your private key to decrypt the message

2. To send an encrypted message that only the recipient can read
   a. Use the recipient’s public key to encrypt the message
   b. Use the recipient’s private key to encrypt the message
   c. Use your public key to encrypt the message
   d. Use your private key to encrypt the message

3. Which function is not provided by a firewall?
   a. Encryption and authentication
   b. Blocking connections to specific addresses
   c. Blocking connections from specific addresses
   d. Hiding the addresses of local computers when they connect to other networks

4. Which function does a proxy server provide?
   a. Encryption and authentication
   b. Blocking connections to specific addresses
   c. Blocking connections to specific addresses
   d. Hiding the addresses of local computers when they connect to other networks
5. A virtual private network (VPN)
   a. Requires a private leased line
   b. Uses encryption to make private network connections across the Internet
   c. Requires users to connect to a dial-up server
   d. Can only transport TCP/IP protocols

### Scoring

**Rubric: Suggested Evaluation Criteria and Weightings**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part A: Define quality of service and explain how it can determine how various types of information is transmitted over a WAN.</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Part B: Define Committed Information Rate and explain how it affects the transmission of data over a WAN.</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Part C: Define error rate and packet loss and explain why these are an important consideration on a WAN.</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Part D: Explain how a WAN can maintain security.</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Try It Out</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Stretch Yourself</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>For Network Wizards</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>FINAL TOTAL</td>
<td>400</td>
<td></td>
</tr>
</tbody>
</table>
Resources


