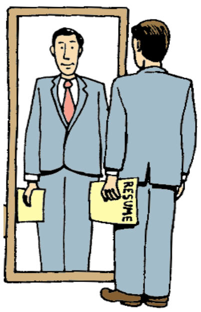
Lesson 2: Network Transmission

At a Glance



Data, voice, and video are transmitted across networks using various transmission media. It is the job of networking devices to encode, decode, and transmit signals that can be interpreted by every device connected to the network whether it is a UNIX, AppleTalk, or Windows NT networking environment. This lesson discusses the concepts that are important to understand when designing and/or maintaining switched networks.

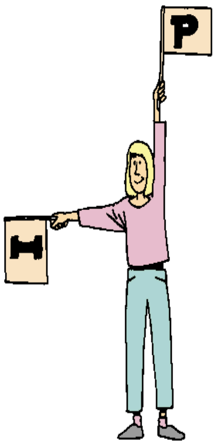
What You Will Learn

After completing this lesson, you will be able to:

- Explain how data is modulated, synchronized, and transmitted across networks
- Describe how differences in bandwidth affect the speed of transmissions
- Describe several WAN connections
- Compare and contrast physical and logical network addressing

Student Notes:

Tech Tak



- **Analog Signal**—Wave signal that changes continuously as opposed to digital signals, which are discretely valued. For example, sound is an analog signal; it is continuous and varies in strength.
- **Asynchronous Transfer Mode (ATM)**—A very fast packet switching, connection-oriented service for broadband signals that uses small packets called cells.
- **Bandwidth**—Bandwidth represents how much information can be sent at one time over a specific cable type. It measures the information capacity of a transmission cable. Bandwidth is the difference between the highest and lowest frequencies of the transmission, measured in hertz and expressed as bits per second (bps).
- **Broadband**—Transmission systems supporting bandwidth greater than 45 million bits per second (45 Mbps).
- **Cell**—A small packet of data used in certain high-speed packet switching services, such as Asynchronous Transfer Mode (ATM) and Switched Multimegabit Data Service (SMDS).
- **Circuit Switching**—Network connections in which a circuit is created to connect two LANs for a certain amount of time. In circuit switching, the connection remains until terminated. A telephone conversation is an example of circuit switching technology.
- **Connectionless Communication**—A form of communication over networks where the transmitting device can send a message without establishing a connection with the receiving device (e.g., radio). Signals are sent, but there is no mechanism for acknowledging receipt.
- **Connection-Oriented Communication**—A form of network communication in which the transmitting device must establish a connection with the receiving device before data can be transmitted, (e.g., telephone). In connection-oriented communication, the receiving device acknowledges receipt of the data.
- **Datagram**—Packets of data at the network layer.
- **Digital Signal**—A type of signal where the data is transmitted in discrete states, for example, on and off. These discrete states can be represented by binary numbers, which are interpreted by computer devices.
- **Frame**—Basic unit of data transfer at OSI Layer 2.
- **Frame Relay**—A WAN protocol, packet switching, connectionless service.

- **Full-Duplex**—Two-way, simultaneous data transmission. Each device has a separate communication channel.
- **Integrated Services Digital Network (ISDN)**—Digital telephone lines that can be used for circuit switched or packet switched data transmission.
- **Internet**—The world's largest network spanning the globe. Its origins date back to the 1960's.
- **Isochronous Service**—An isochronous network guarantees a specific amount of bandwidth and a fixed amount of time between transmission opportunities.
- **Half duplex**—Two-way data transmission that is not simultaneous. Only one device can communicate at a time.
- **Leased Line (also called Dedicated Line or Private Line)**—A non-switched connection for a WAN. Only the company that leases it uses the line, and the connection is always available.
- **Modem**—Modem is a shorthand version of the terms modulator and demodulator. A modem converts analog signals to digital signals and vice versa. This allows communication among digital computer devices via analog telephone lines.
- **Multiplexing**—A transmission that simultaneously combines two or more separate signals over a single communications channel.
- **Packet**—A packet is a basic unit of data transfer at OSI Layer 3.
- **Packet Switching**—Packet switching is a switched connection for WANs in which data from many different LANs may share a single circuit. Data is encapsulated in packets (sometimes called frames or cells) for transmission.
- **Switched Multimegabit Data Services (SMDS)**—A fast packet switching service that is connectionless.
- **Transmission Control Protocol/Internet Protocol (TCP/IP)**—The entire suite of protocols used internationally to access the Internet.
- **User Datagram Protocol (UDP)**—UDP is a connectionless transport method used to transmit messages between the Network Management System (NMS) and the agent. UDP is a standard member of the TCP/IP protocol suite.
- **X.25**—A packet switching service. X.25 is an older WAN protocol largely superceded in the United States by Frame Relay and other protocols.

Switches and Data Transmission

Layer 2 switches function much like transparent bridges by providing network connections to LANs using data link and physical layer protocols. Digital Equipment Corporation (DEC) introduced the first switch (bridge) for the purpose of transporting frames in an Ethernet network. In 1990, Layer 3 switches were developed. Layer 3 switches function much like routers providing links between different networks. They have all of the capabilities of Layer 2 switches and add the ability to implement routing protocols.

The physical layer protocols define the physical apparatus, wiring, and signaling of data. Layer 2 data link protocols control access, frame format, and address resolution at the MAC level. Layer 2 switches build and maintain tables with the MAC address of each device on the network. They learn the network logical topology, forward frames, offer full-duplex simultaneous transmissions, and conduct filtering operations. Examples of protocols employed by Layer 2 switches include Ethernet, FDDI, Token Ring, Fast Ethernet, and Gigabit Ethernet. Layer 2 switching protocols differ from Layer 3 protocols in that Layer 2 provides point-to-point rather than end-to-end management of data.

Switching technologies make it possible for a network to establish a direct path from one particular station to another. By using switching technologies, network designers can build high-speed, flexible networks. Two types of switching technologies are frame switching and cell switching. How switches function will be discussed in subsequent lessons. For now, it is important to review the concepts of how data is modulated, synchronized, and transmitted.

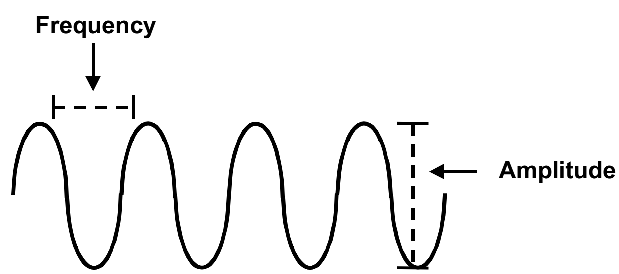
Data Transmission

Transmission of data across networks requires many considerations. Digital signals have to be modulated, synchronized, and must arrive at their destination error free and in a timely manner. This section discusses how this is accomplished.

Analog vs. Digital Signaling

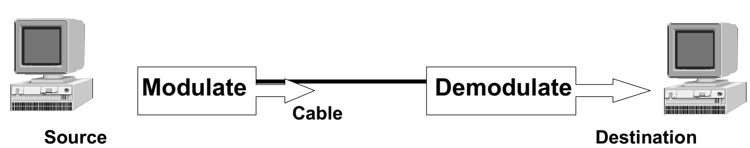
The difference between analog devices and digital devices has to do with the exactness of the signal. Digital signals are discrete, precise signals. Either there is a signal or there is no signal. Analog signals continuously change; they are therefore not as exact. For example, a traditional clock with hands that turn around the clock face is an analog device, and you can say that the time is 12:31, but the hands are at about 12:31. With a digital clock, the clock read-out says it is exactly 12:31.

Analog Wave



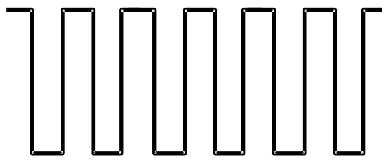
An analog signal transfers as a wave, characterized by specific amplitudes and frequencies. Analog waves are continuous. Sound travels as a wave. Telephone companies convert sound waves to electrical waves and transmit those waves through telephone lines. Computers deal with data in digital form, so data must be modulated (turned into waves) in order to travel across traditional analog telephone lines. Variations in the amplitude and frequency of the wave are used for this purpose. The converted signals are expressed as waves and transmitted across the telephone lines, where, upon receipt, they must be demodulated. The term modem is derived from these two words since a modem is a computer device that modulates and demodulates the waves.

Encoding/Decoding Signals Over Telephone Lines



Digital signals come in discrete states. They are not continuous, either there is a signal or there is no signal. Computers interpret these states as “ones” or “zeros.” Signals transmitted by computers are digital signals.

Digital Signal



The most important factor in all of this is that the sending and receiving devices have to be using the same method of signal interpretation. Just any signal is not enough; if the receiving device doesn’t know how to interpret the data, it is ignored or an error message is generated.

Connectionless/Connection-Oriented

Connectionless and connection-oriented data transmissions are very different. In connectionless transmission, a packet of data is sent to a destination device without establishing a connection prior to the transmission. Acknowledgment of receipt of the data is not sent to the transmitting device. Radio is an example of connectionless transmission. Radio stations broadcast their signals without establishing a prior connection with the destination. The radio station DJ hopes that there is someone out there receiving his or her signal, but the listeners do not contact the station to say that they received the message.

Connection-oriented transmission has, as its first responsibility, the task of making sure that communication between two points is possible and dependable. A connection-oriented transmission will establish a connection, then transmit data. The connection is maintained until all signals are sent. Usually there is a signal indicating the end-of-transmission with a packet-received-okay signal. A telephone conversation is an example of a connection-oriented exchange. When you answer the telephone, the transmitter (person calling) knows that a connection has been established when s/he hears you say hello.

Synchronous/Asynchronous/Isochronous

When two devices are communicating on a network, it is important that they know when to expect data and how to interpret the data they receive. The protocols for timing and coordination of data signals are either synchronous or asynchronous.

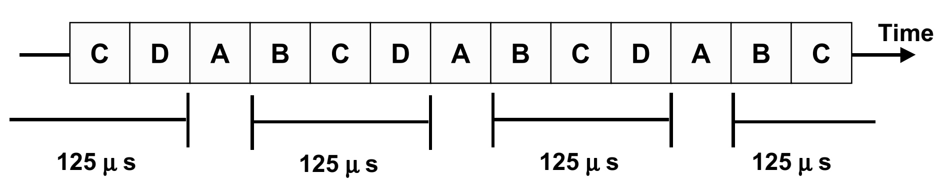
Synchronous [from prefix “sys” means with and the root “chrono” means time] transmissions occur on a regular schedule; in other words, the source and destination device in an internetwork use the same clocking signal. Either the source and destination devices are synchronized with a clocking signal that is generated by the devices (internal clocking), or they rely on an external device for timing the data stream. Synchronous connections can use either analog or digital lines. Synchronous transmissions are usually used for internal computer communications.

Asynchronous [the prefix “a” makes the word negative] transmissions do not use a synchronous clocking signal. They use start and stop bits in the packets to let the receiving device know where the data begins and ends. Since the receiving device does not expect a transmission at a particular point in time, there must be a mechanism in place to indicate the beginning and end of packets.

In an asynchronous packet-switched network, devices on a network share a pool of dynamically assigned bandwidth. Bandwidth and minimum response times are not guaranteed. Rather, they occur randomly without a common synchronous timing signal. This method of transmission is best for variable bit-rate data that are not time-sensitive, such as traditional data, rather than voice or video.

Isochronous [prefix “iso” means same] networks guarantee a specific amount of bandwidth in addition to a fixed amount of time between transmission opportunities. For example, the graphic below shows how device A is guaranteed a fixed amount of bandwidth every 125 micro seconds even though it shares the network with devices B, C., and D.

Isochronous Bandwidth



Narrow/Wide/Broadband

There are three categories of bandwidth: narrowband, wideband, and broadband.

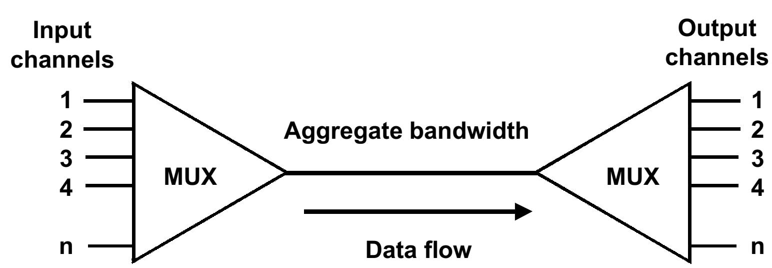
Narrowband are transmissions on single channels at speeds of ≤64 Kbps. Narrowband transmissions can also consist of multiple channels transmitting at ≤64 Kbps, as long as the total capacity of the transmissions over the media is less than wideband (1.544 Mbps).

Wideband is described in United States standards as transmission along multiple channels in the range of 1.544 Mbps to 45 Mbps.

Broadband, according to U. S. standards describes a multi-channel transmission capability of ≥45 Mbps. In Europe the threshold is ≥34 Mbps.

Multiplexing addresses bandwidth issues with a technology that allows two or more individual signals to be transmitted simultaneously over a single communications channel. Signals can either be changed (modulated) to digital or analog for transmission purposes. Multiplexing bandwidth enables a high-speed channel to transmit voice, video, and data successfully.

Multiplexing (MUX)



Check Your Understanding

- Explain the difference between a connectionless connection and a connection-oriented connection. What is a benefit of each?
- Why are timing and coordination of data signals important?
- Describe the three categories of bandwidth.
- If you were setting up a network for a company that did video conference calls on a regular basis, which bandwidth would you recommend? Why?

Wide Area Network (WAN) Protocols

When data is transmitted across wide area networks (WANs), there are several ways to transmit this traffic across communication channels. One way is circuit switching, which connects one point to one other point and holds that connection exclusively until it is broken by being terminated at either end. A second way is leased lines, or dedicated lines, which are always connected. Continuous connection ensures that one device or LAN can always connect with another; unfortunately, as you might imagine, this can be expensive. A third method is packet switching, which increases the capacity of telephone lines by allowing them to be shared by many transmitters at once. Telephone companies send packets as they come along, just as routers and Layer 3 switches do across networks. Customers are only charged for the time that data is being transmitted. Following are some examples of ways in which data is transmitted over WANs. The WAN protocols, described below, include ISDN, X.25, Frame Relay, SMDS, and ATM.

ISDN

Integrated Services Digital Network (ISDN) provides a way to digitally transmit both voice and data simultaneously across networks. Its protocols define how data is transmitted across telephone wires, how connections are made, and how errors are detected.

X.25

X.25 is a packet-switching transmission method that establishes a virtual circuit for the transmission and receipt of data. It defines the protocols used to establish communication between data terminal equipment (DTE) and data communications equipment (DCE). Even though other methods are becoming more popular, it is a connection-oriented service and is therefore the preferred choice when transmitting to areas of the world where the telephone lines may be unreliable.

Frame Relay

Frame relay is also connection-oriented, but it is much faster than X.25 and works exactly like packets in LANs. Frame and packet are often used synonymously. Unlike X.25, frame relay presumes that the network is reliable.

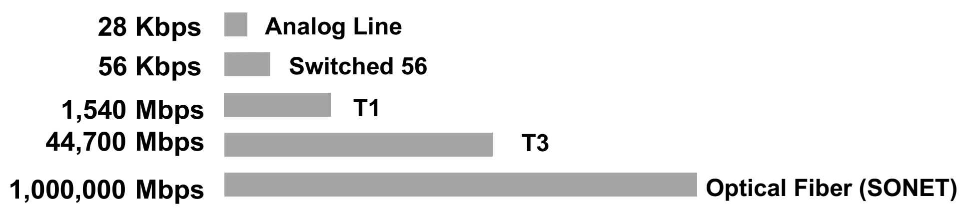
Switched Multimegabit Data Service (SMDS)

Switched Multimegabit Data Service (SMDS) converts packets into smaller cells that can be transmitted very quickly. Unlike X.25 and frame relay, SMDS is connectionless; its advantage is the speed provided by not having to wait for transmissions to be acknowledged. Its disadvantage is errors that produce large amounts of data that need to be re-transmitted.

Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is a high-speed, scalable, connection-oriented technology that converts packets into fixed length data units, called cells, that travel at speeds between 45 Mbps and 622 Mbps. These cells travel on their own schedule and data fills empty cells as they go by. Optical fiber is usually the media of choice for high-speed ATM transmissions.

Comparison of Transmission Speeds



File Type	File Size	At 64 Kb/s	At 1.54 Mb/s	At 10 Mb/s	At 16 Mb/s	At 100 Mb/s
CAD File	2 MB (compressed)	31.0 sec	1.30 sec	0.2 sec	0.125 sec	0.02 sec
CAD File	8 MB (not compressed)	2 min	5.20 sec	0.8 sec	0.5 sec	0.08 sec
Chest X-ray (14" by 17")	59 MB (not compressed)	15 min	38.0 sec	5.9 sec	3.6 sec	0.59 sec
High resolution facsimile	70 MB (compressed)	18 min	45.0 sec	7.0 sec	4.4 sec	0.7 sec
CT Scan Set (40 images)	167 MB (not compressed)	43 min	1.8 min	16.7 sec	10.4 sec	1.67 sec
High resolution facsimile	560 MB (not compressed)	2.4 hours	6 min	56.0 sec	35.2 sec	5.6 sec

Check Your Understanding

- Describe X.25, Frame Relay, Switched multimegabit Data Service, and Asynchronous Transfer Mode.
- What advantage does connectionless packet switching have over connection oriented switching?
- What disadvantage does connectionless cell switching have over connection oriented switching?

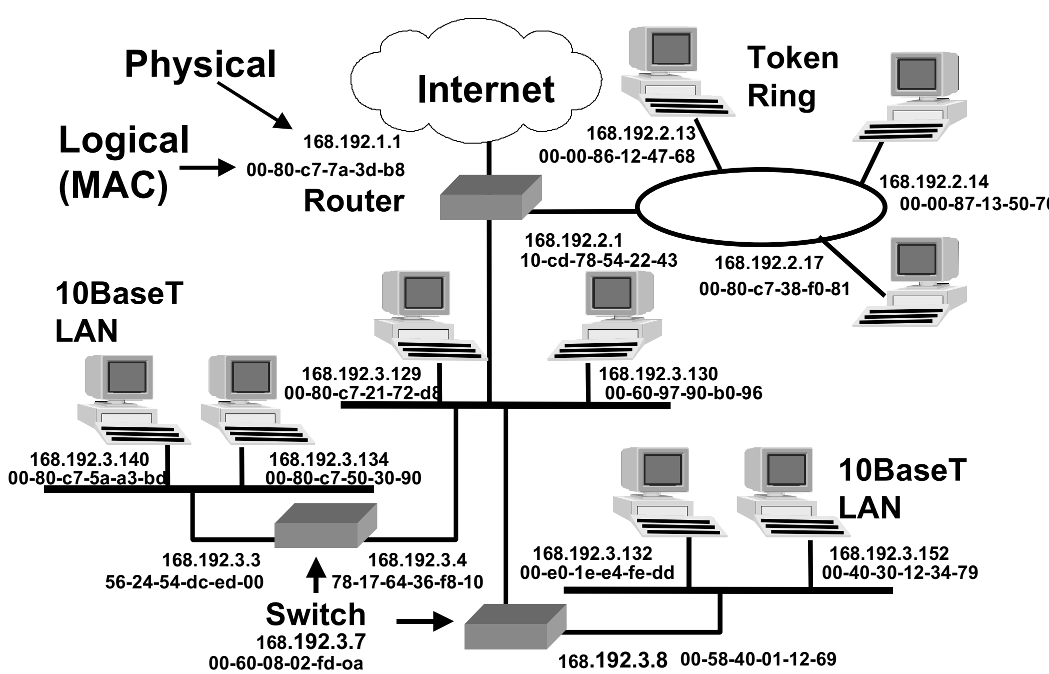
Internetworking Addressing

One important point to remember about addressing is that each device on a network has two addresses: a Layer 2 MAC "physical" hardware address and a Layer 3 IP "logical" address. Physical addresses do not change and are used to identify a piece of equipment. A physical address is more like a "name" or identification for a particular device. Logical addresses, on the other hand, may change depending on the location of a device and/or how it is configured. An individual may sit at a particular workstation. That workstation's MAC address will remain the same whether the network administrator assigns that workstation "logically" an IP address for the sales department segment of the network or the manufacturing segment.

Physical (MAC) Internetworking Addressing

Layer 2 protocols are responsible for identifying the source and destination MAC addresses of devices on a LAN. LAN switches, Layer 2 devices, use MAC addresses when transmitting from a source to destination device on the same physical network.

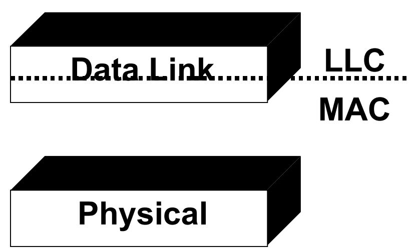
Physical and Logical Addresses



A MAC address is the physical address of a device on a LAN and is expressed in hexadecimals: 00-80-C7-7A-3D-B8 is an example of a MAC address. A unique MAC hardware address is assigned when the device is first manufactured and remains with the device unless the NIC is replaced. The MAC address does not change and is considered the "physical" address of the network device. Typically, physical addresses are used when data is transported within LANs.

MAC addresses are Layer 2, data link layer addresses. Switches learn the physical addresses of devices connected to a network and build MAC address tables. They then forward packets of data according to internal reference tables of MAC addresses. The LLC sublayer is responsible for identifying and passing data to the network layer.

OSI Data Link Sublayers



Logical (IP) Internetworking Addressing

WAN switches use upper level protocols to switch, or route, data from one network to another network. WAN switches are Layer 3 devices and are typically referred to as switching routers. Switching routers use the logical IP addresses of a device. IP addresses are configured either statically (manually by a network administrator) or dynamically based on the network topology. The logical address uniquely identifies a network device and its network segment.

The IP address identifies a device as a component of a specific network. If the computer device is moved to another network, it will retain its MAC (physical) address but be assigned a different IP (logical) address that indicates it is a device on the new network.

Check Your Understanding

- Explain the difference between physical and logical network addresses.
- Why is it sometimes necessary to use IP addresses?

Try It Out

Materials Needed:

- Windows 95 PC
- HyperTerminal software
- Site Manager software
- Classroom Network

Configuring Workstation(s)/Setting up LAN Networking Lab Equipment

Before networking resources can be used, they must be physically connected with the correct interfaces and the devices must be configured. These directions will assist you with configuring your workstation, physically setting up the LAN, and configuring the BayStack ARN Router.

Part 1: Directions for Configuring Workstation(s)

Before physically setting up the network, first configure the workstation(s) you will use to test for connectivity. If the workstation(s) is/are already configured proceed to Part 2.

Create File and Print Share Permissions

In order to communicate with networking equipment, devices must be configured. Although this step is not necessary to configure the Router; however, it is useful and is needed if you plan to share resources.

Power up your workstation(s) and proceed with the following directions.

1. Click Start.
2. Click Settings.
3. Click Control Panel.
4. In the Control Panel, double-click the Network icon.
5. On the Configurations tab page in the Network dialog box, click File and Print Sharing.
6. Select both the printer and file sharing boxes.
7. Click OK. This will return you to the Configuration tab page of the Network dialog box.
8. Click OK to close the Network dialog box.

9. Double-click the My Computer icon on the desktop.
10. Double-click the C Drive icon.
11. Right-click the file or program you plan to share.
12. Click Properties.
13. Click the Sharing tab.
14. Click the Shared As button and the Full button. When you click Full, the folder can be accessed, read, and modified by anyone on the network.
15. Click Apply.
16. Click OK. A hand should appear on the folder. You can use this folder for any data you wish to share with other devices on your network.
17. Why might a network administrator limit access to shared folders to some individuals?
18. Give an example of a situation where this might happen.

Identifying Your Computer for a LAN

1. On the Windows 95/98 window, click the Start button.
2. Click Settings.
3. Click Control Panel.
4. In the Control Panel, double-click the Network icon.
5. In the Network dialog box, click the Identification tab.
6. Enter the computer name and workgroup name you plan to use.
7. Click OK.

   You will be prompted to restart your computer at this point so that the new configuration settings take place. However, do not restart your at this time. Continue until you complete the rest of the configurations.
8. Click the Start button, click Settings, and click Control Panel.
9. In the Control Panel, double-click the Network icon.
10. In the Network dialog box, click Add.

11. In the Select Network Component Type dialog box, highlight **Client.**

12. Click Add.

13. In the Select Network Component window, highlight **Microsoft and Client for Microsoft Networks**.

14. Click OK.

15. Close the window by clicking the X.

16. In the Network dialog box, select the Configuration tab. Highlight **Client for Microsoft Networks**.

17. Click Properties. Make sure the logon and restore network connections option button is checked.

18. Click OK.

Configuring Adapters

In order to complete this step, you must know which type of NIC you have on your workstation.

1. In the Network dialog box, click Add.

2. In the Select Network Component Type window, highlight **Adapter**.

3. Click Add.

4. Choose your manufacturer and adapter from the list. If the manufacturer of your adapter does not appear in this window, you will have to download the driver from the Internet or use the software that comes with the adapter.

5. Click OK.

Configuring Protocol Components

1. Before enabling NetBEUI to communicate over a network, its driver must be installed on your computer.

2. In the Select Network Component Type window, highlight **Protocol**.

3. Click Add.

4. In the Select Network Protocol Window, highlight **Microsoft and NetBEUI**.

5. Click OK. You will see the Network dialog box Configuration tab next. Notice that the NetBEUI protocol has been added.

6. What is the purpose of installing NetBEUI?

Configuring the Service Components

1. In the select Network dialog box, click Add.

2. In the Select Network Component Type window, highlight **Service**.

3. Click Add.

4. In the Select Network Service window, on the left, highlight **Microsoft**. On the right side highlight, **File and printer sharing for Microsoft Networks**. At this point, you may have to install the network service.

5. Close the Select Network Component Type window by clicking the X.

6. In the Network dialog box Configuration tab, highlight **NetBEUI (adapter manufacturer name**), and click Properties.

7. Check to see if Client for Microsoft Networks and File and Printer Sharing for Microsoft Network boxes are checked.

8. Click OK

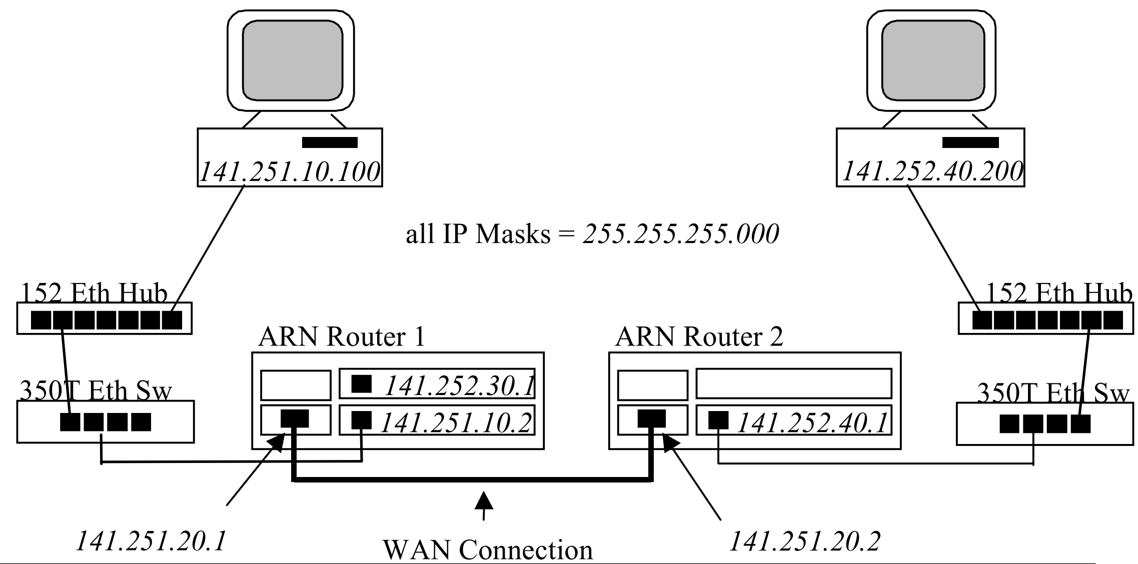
9. Click OK to close the Network window. At this point, you are ready to share the folder you created at the beginning of this lab.

   Restart the computer at this time so the new configurations will take place.

Part 2: Physical LAN Setup and Configuring ARN Router

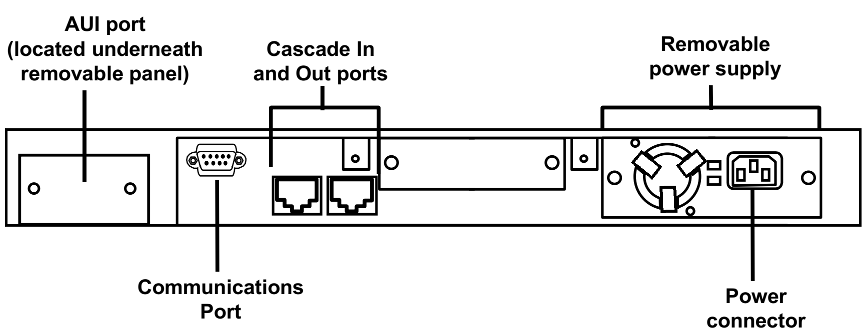
The illustration below shows a simple network setup with IP addresses. Your instructor will supply you with IP addresses for your network.

Physical Setup With Suggested IP Addresses



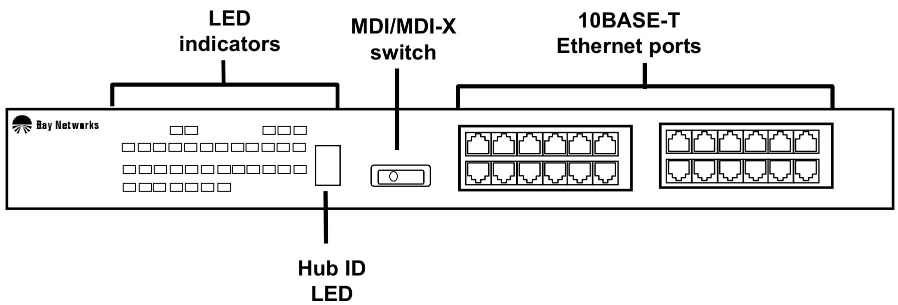
Connecting 150 Series BayStack Hubs to Workstations and Cascading Hubs

1. Plug in the power cord to rear panel of the hub.



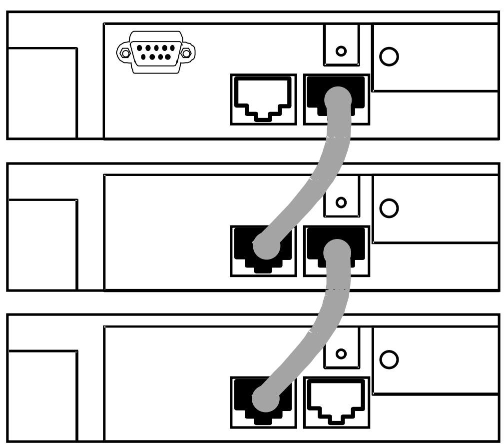
2. Plug the other end of the AC power cord into the grounded AC power outlet. The hub should power up immediately since there are no on/off toggle switches on the box.

3. Observe the LEDs to verify connectivity.

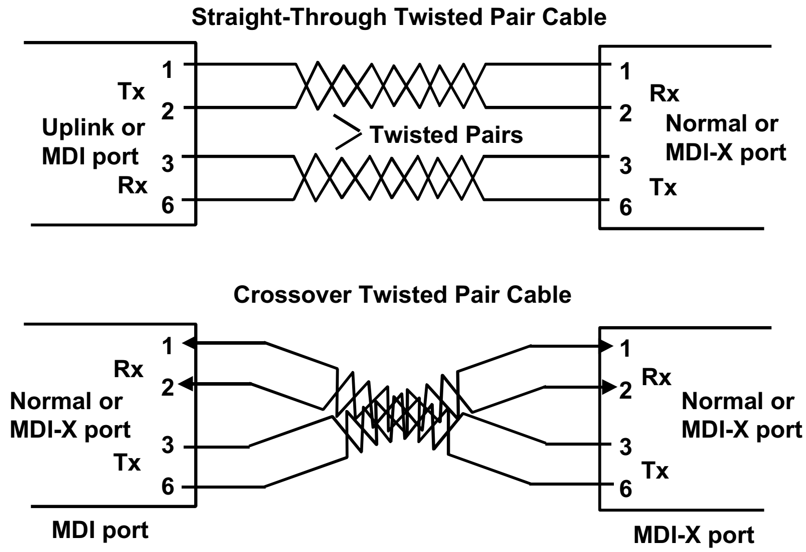


4. To connect the workstation to the hub, use a STP/UTP straight through cable with RJ-45 connectors at each end. Insert one of the connectors into the NIC RJ-45 interface and the other connector into any one of the ports on the front of the hub.

5. To cascade more than one hub together, stack the hubs and connect them together with STP or UTP crossover cable with RJ-45 connectors at each end. Insert one of the RJ-45 connectors in the Out port on the back panel of the hub and the other connector in the In port of the next hub in a daisy chain fashion.



Port 1 will accept either a crossover or straight through cable. If you use port 1 with a straight through cable be sure the MDI/ MDI-X toggle switch is switched to MDI-X. If you use a crossover cable, be sure the MDI/ MDI-X toggle switch is switched to MDI.



6. The LED for the port should turn green to show connectivity.

7. Explain why you have to adjust the toggle switch to MDI-X when you use port 1 with a straight through cable.

Connecting BayStack 350 Series Switch to the LAN

1. Plug in the power supply to the rear of the switch. Observe LEDs for connectivity.

2. Using a crossover cable insert one of the RJ-45 connectors into any port on the front of hub and the other RJ-45 connector into any port on the front of the switch. The switch and hub are now interconnected and should be able to communicate.

Adding a Router to the LAN

1. Connect the BayStack ARN Router to the 350T Switch via the RJ-45 ports on the front panel of the boxes. Be sure to use a straight-through cable.

2. Insert the Flash Memory Card into the router, label side up with arrow pointed at the router. Push card until you get a snug fit. Check the write-protect switch on the Flash Memory Card, it should be set to the left, which is the unprotected position.

3. Power up the equipment and wait for the router to go through its diagnostic procedure. LEDs should light up to show connectivity.

4. To connect the workstation to the ARN router console port, you need:
   a. A serial console/modem cable with a 9-pin receptacle at one end and a 25-pin plug at the other. Cable model number 110307 - Nortel Networks.
   b. A null modem crossover adapter with two 25-pin receptacle connectors. Cable model number 110308 – Nortel Networks. (The serial console/modem cable and the null modem crossover adapter may be packaged together as order number 110310 - Nortel Networks.)
   c. A standard AT serial cable with a 25-pin plug connector.

5. Insert the 9-pin receptacle end of the console cable (110307 - Nortel Networks) into the console port found on the back of the switch.

6. Connect the null modem crossover adapter (110308 - Nortel Networks) to the 25-pin plug.

7. Connect the other end of the null modem crossover adapter to the 25-pin plug of the serial cable.

8. Connect the cable's 9-pin recptacle into the workstation 9-pin plug Com port.

Configuring BayStack ARN Router

Before you can operate the ARN, you must install both an *image* and a *configuration* file. The local file is the *image* file, called *arn.exe* and is used to boot the router. You also need a *configuration* file, called *config*. (By convention this file is often called "little" *config*.) This is done using the HyperTerminal software that comes with Windows 95/98.

You will use the Quick Start procedure, a Technician Interface (TI) batch file called *inst_arn.bat,* to configure the router's initial IP interface, an Ethernet port. You will then use TI to verify that the circuit is operational.

When you conduct "Quick Start", which is the TI command *""inst_arn.bat"* you are configuring your first IP interface, which Site Manager will then use to manage the router. All settings made from one screen to the next are stored into active memory (DRAM). From DRAM, the configuration changes are immediately active with no need of a boot. You do have to store the config changes into off-line memory, Flash. This is done toward the end of "Quick Start" install, when you save the changes to the file called *startup.cfg*.

The procedure for this lab is largely taken from the user manual *Installing and Operating BayStack ARN Routers*. Refer to the manual for additional information.

1. Access HyperTerminal via Windows > Start >Programs, >Accessories > **HyperTerminal**. If it is not installed on your computer, you must do so now.

   To install HyperTerminal, go to Windows > Start > Settings > Control Panel > **Add/Remove Programs**. Highlight the Windows setup tab. Highlight Accessories, click Details, highlight communications and double-click, check HyperTerminal, and click OK. (You may need the Windows 95/98 operating system software CD-ROM/disks.)

2. Double-click the hypertrm.exe icon.

3. Give your HyperTerminal a name and press Enter.

4. Use the Connect using: pull down menu in the Phone Number window, and highlight Direct to Com 1. (This is the 9-pin port at the rear of the workstation that will cable you to the console/TI interface of the ARN router.

5. In the COM1 Properties window, be sure that you have the following settings:

   Bits per second: **9600**

   Data bits: **None**

   Stop Bits: **1**

   Flow control: **None**

6. Click OK. You are now ready to use HyperTerminal to interface with the ARN router.

7. Use the File pull down menu and highlight Save, which will save the HyperTerminal setup as a file.

8. Create a desktop shortcut for quick access. Return to the HyperTerminal folder and right-click the icon you just created. From the pull-down menu, highlight Create Shortcut. Drag the icon to the desktop and highlight Move Here. You can now use this icon to access HyperTerminal's Technician Interface, TI.

9. Log-in to the command line by typing the word **Manager** (case sensitive) and pressing Enter.

   The HyperTerminal window you see at this point is referred to as the Technician Interface TI, (sometimes called the command line interface). It is through this interface window that you are able to configure remote devices.

10. Check for the "little" *config* file on the routers' flash. "Little" *config*, is a configuration file stored on the router's flash, which when booted onto the router, only activates the TI console port. All other router parameters are left at default.

    The "little" *config* file should be 132 bytes in size for the ARN Router (see TI command, **dir**). If it is larger, it is not the original "little" *config* file, and you need to delete this *config* file.

11. To delete an incorrect "little" *config* file, type the following at the prompt:

    del config

12. To re-create a new “little” *config* file using TI, type the following:

    copy ti_arn.cfg config

    ti_arn.cfg is the backup file for “little” *config*. Both files should be 132 bytes in size for the ARN.

13. To boot the router with “little” *config* ,type the following TI command:

    boot (or **boot arn.exe config**)

    The *arn.exe* file is the ARN’s router image software.

    The *config* file is the “little” *config*, which enables only the TI console port.

14. Examine the router after the boot. Type the following:

    show hardware configuration (**sho har con**).

    This should show that *config* is the active configuration file.

15. Type:

    show ip circuits (**sho ip cir**)

    Should show “no circuits found” meaning that no IP address is configured on any of the router’s ports.

    show console configuration (**sho con con**)

    Should show that the two 9-pin console ports (console & modem) on the rear of the ARN are “Up” and configured for 9600, 8, N, 1. If not, make the changes before you continue.

16. Type:

    getcfg

    Should show that the ARN will load its image software & configuration file from the router’s local flash.

    Boot image = **local**

    Boot configuration = **local**

    If the *image* and *config* are not shown as local, do the following:

17. Type:

    bconfig config local

    bconfig image local

18. Type:

    getcfg to check to see if the settings are now local

Configure the Ethernet Port with an IP Address

Site Manager will need an IP address configured in the router in order to manage and configure the router. To do so, you run a file called, *inst_arn.bat*.

1. From TI, type:

   inst_arn.bat

2. Choose Ethernet on Base Module as the port for the IP address.

   Keep the port name: **E11.**

   Set the IP address:

   141.251.10.1 (router 1) or other IP

   141.252.10.1 (router 2) or other IP

   Set the IP mask: **255.255.255.0**

   If you make a mistake anywhere during the install, (quick start) you must reboot because you have created a phantom port. If this is the case quit the program and begin again.

3. Use default settings for the rest of the steps.

4. Router automatically pings the new IP address you assigned to the router – ping should be successful.

5. Enter **your PC's IP address** and press Enter; the router now pings your Site Manager.

6. Type **N** (no) for configuring another port.

7. When finished, you should see the TI prompt, [**1:1**], on the TI screen.

8. To test for an active IP circuit, type:

   show ip circuit (**sho ip cir**)

   Should show only one IP circuit with the IP address & mask that you just configured.

Configuring the Routers via Site Manager (Windows 95 only)

Open Site Manager, the proprietary management software supplied with the BayStack ARN Router CD-ROM, and via the Connection button, enter the **IP address of your router** (s). (If Site Manager is not yet installed on the workstation, you must do so at this point.) Site Manager cannot be installed on Windows 98.

1. Make the following settings:

   IP Address: IP address you assigned to the router's Ethernet port

   Identity: **public**

   Time: **1**

   Retries: **1**

2. Click OK. You should see the router's IP address listed as being "Up" and in the lower left corner in red letters "Connected to SNMP Agent."

3. Enter Configuration Manager and configure the rest of the router with Site Manager.

   Tools > Configuration > Manager > **Dynamic**

   A new window appears showing the routers ports.

   White box = **configured ports**

   Blue box = **unconfigured ports**

Configure the Router's Name

1. Click Platform > Edit System Information > System Name:

   router 1 or router2

Configure the WAN/Serial Port (COM2) for PPP, IP, & RIP

1. Click COM2 >Add Circuit >OK

   WAN Protocols > PPP > **OK**

2. Select Protocols > IP & RIP > **OK**

   IP Configuration: **IP Address** = (router's IP address)

   Subnetmask = 255.255.255.0

Configure the WAN/Serial Port's Internal Clock Speed

1. Click the COM2 box
2. Click Edit Line.
3. Clock Source: **Internal**
4. Internal Clock Speed: **1.25 MB**

Configure the Second Ethernet Port (Router 1)

1. Click XCVR2 > Add Circuit > **OK**
2. Select Protocol > IP & RIP > **OK**

   IP Configuration: **IP Address**

   Subnet Mask: **255.255.255.0**

Testing the Router's Configuration

1. Type:

   show circuit base (**sho cir bas**)

   This shows Layer 1 & 2 status of your ports. The Ethernet & WAN ports should be:

   State = **Up**

2. Type:

   show ip circuits (**sho ip cir**)

   This is the status of Layer 3 (IP). The Ethernet & WAN ports should be

   State = **Up** with correct **IP addresses & masks**

3. Type:

   ping (IP address of the remote PC)

   Your LAN is now configured. Do the same for LAN 2 and connect to form a WAN.

4. Why is it important for each device to have a unique IP address?

5. Use MS-DOS and ping for connectivity. Was your ping successful? If not, go back and troubleshoot the problem until your ping is successful. Save your successful ping window and have instructor sign below to indicate that your group successfully completed this exercise.

Instructor Signature.____

Disassemble the LAN/WAN setup.

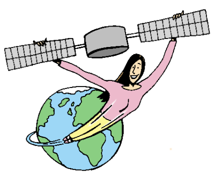
Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	**%**	**Your Score**
Accurate answers to lab questions that indicate a thorough understanding of concepts covered in this lab	20	
Portfolio entries complete	20	
Group participation and cooperation	20	
Able to complete setup and configuration with minimal assistance from instructor	20	
Successful ping	20	
TOTAL	**100**	

Stretch Yourself

Materials Needed:

- Windows 95 PC
- BayStack 350T Switch and owner's manual
- DB-9 console/service port connector



Configure BayStack 350T Switch IP Address

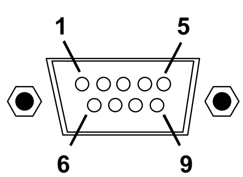
In addition to customizing network devices, network operators need to know how to restore equipment to its default settings. This activity will show you the original factory default settings.

Keep a record of your activities in your portfolio for later reference. Also record all of the default settings for future reference.

The DB-9 console/service port connector is configured as a data communications equipment (DCE) connector. The DSR and CTS signal outputs are always asserted; the CD, DTR, RTS, and RI signal inputs are not used.

♦ Why is it important to know the pin assignments?

DB-9 (RS-232-D) Console/Service Port Connector



DB-9 console/service port connector

DB-9 Console/Service Port Connector Pin Assignments

Pin	Signal	Description
1	CD	Carrier detect (not used)
2	TXD	Transmit data (output)
3	RXD	Receive data (input)
4	DTR	Data terminal ready (not used)
5	GND	Signal ground
6	DSR	Data set ready (output always asserted)
7	RTS	Request to send (not used)
8	CTS	Clear to send (output always asserted)
9	RI	Ring indicator (not used)
Shell		Chassis ground

1. Connect your workstation to the console port of the switch.
2. Configure the Console/Service Port Configuration terminal for 9600 baud, 8 data bit, no parity, and 1 stop bit.
3. Power up the switch and watch the startup sequence and the self-tests of the switch. You can verify proper operation of the switch by observing the front-panel power and diagnostics LEDs, which will turn green after running the self-test diagnostics.
   - ♦ How much time did it take for the switch to boot and get the CI main menu on your terminal application?
4. From the main menu, select Reset to Default Settings.
   - ♦ What happens?
5. Choose Yes and press Enter.
   - ♦ What happens?
6. Select IP Configuration. Press Enter.
   - ♦ What is the BootP Request Mode? What are the other choices?

   There should be no IP address at this point.

7. Return to the main menu. Click SNMP Configuration.
   - Record default data below.
8. Return to the main menu. Click Switch Configuration. Choose the Port Configuration option.
   - Which links (ports) are up? Why? What does the autonegotiation feature do? Why might this be important?
9. Proceed through the main menu choices and record any information you that will assist you in further labs. Record the default values for any other configurable parameters on the switch.
10. Go to the System Characteristics menu and record the switch's MAC address. ______________________________________ . Look at the back panel on the switch.
    - What do you notice about the different series of numbers?
11. Select the IP Configuration window. Before setting the IP configurations, you will choose a BootP Request Mode.
    - What are the possible choices? Describe what each of these parameters allows/does not allow.
12. See your instructor for an IP address for the switch. Set the appropriate BootP request mode for your network. Configure the IP address, the subnet mask, and the default gateway. When you have completed the IP configurations, ping to check connectivity.
    - Why might you need a default gateway? When is it not always necessary to have a gateway IP address?

- Was your ping successful? _________ If not, troubleshoot possible problems. If you are unable to ping successfully, see your instructor.

Be sure to record the IP address, subnet mask, and default gateway numbers that you used.

Rubric: Suggested Evaluation Criteria and Weightings:

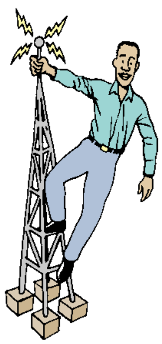
Criteria	**%**	**Your Score**
Accurate answers to lab questions that indicate a thorough understanding of concepts covered in this lab	30	
Portfolio entries complete	30	
Active participation in activity	20	
Able to complete activity with minimal assistance from instructor	10	
Successful ping	10	
Other		
TOTAL	**100**	

Network Wizards

Materials Needed:

- Classroom Network
- Optivity Software

Discovering the Network



This lab activity is designed to give you experience using network management software to “discover” the hardware components in your network. The classroom network you will use for this lab was set up in Lesson 1-1, and is ready for you to use.

In this lab, you will practice running the Autodiscovery process in HP OpenView Optivity to find, identify, and map hardware components in the network. You will also use Optivity Analysis to learn more about the topology and connectivity of the network. During the course of the lab, you will configure HP OpenView, Campus Command Center (CCC), and Optivity Analysis and generate, update, and use Optivity views and OpenView network maps.

Part 1: Generating and Using HP OpenView Maps

In the first part of this lab, you will identify your network, run the discovery software, and create maps of network components. The software you will be using to discover and map your network is HP OpenView Autodiscovery and some of the Optivity applications.

Once you have mapped your network, you will learn how to launch some of the main Optivity applications from HP OpenView maps.

The Optivity software also has its own discovery process, which you will run in the second part of this lab. It allows Optivity applications to run independently, without depending on the HP OpenView discovery process.

Keep a log of your experiences during this activity and prepare a summary of your experiences and an insightful analysis of how a network manager might use this software to help improve network performance.

Submit this summary to your instructor and place it in your portfolio.

1. Identify which networks you want to discover.

   HP OpenView lets you control the extent of network discovery. You can decide just how much, or how little, of the network you want to look at. In very large and complex networks, you can use several network management stations to manage different portions of the network.

In this step, you will tell the Open View software exactly which subnetworks, in your classroom network, you would like to include in your initial discovery process. In the discovery process, you may choose to discover only some of your subnets, or all of them.

a. Before you begin, you should verify that the computer on which you will run the OpenView software is properly connected. To do that, ping your classroom network default router and your team's NMM. You can refer to the diagram your teacher gave you for these numbers.

Note

If any ping test fails, determine the cause of the problem and correct it with help from your instructor, BEFORE you begin this activity.

---

b. Double–click the Optivity 7.0 icon to open Optivity and HP OpenView. Sign on as **manager** with no password.

c. On the Autodiscovery menu, choose Configure, then drag right and choose Discovery Networks.

   The Configure Discovery Networks window opens.

d. In the IP Subnet Mask box, type the subnet mask provided by your instructor.

e. Type the IP address of the classroom network's default router in the IP Default Gateway box.

f. Enter the read community string, if necessary.

g. In the Networks field, type the number of an IP subnetwork and the Subnet Mask you want to discover in your classroom network and click Add.

   Repeat this step for each IP subnetwork your instructor asks you to discover in the classroom network.

   These entries will determine which subnetworks will be discovered.

h. Click OK.

2. Run OpenView Autodiscovery.

Now that you have configured OpenView for discovery, and identified the subnetworks to be discovered, you will start the discovery process. In this step, you run the OpenView discovery process, which creates a map file containing information about all of the manageable devices it finds on your network.

a. Pull down the Autodiscovery menu and choose Discover, then choose Discover Routers.

b. Click Yes when the system prompts you to start router discovery.

   The system takes a short time to query the default router and to obtain the ARP cache for each router in the classroom network. No notification is generated when that process is complete.

c. To view the progress of the discovery process, pull down the Autodiscovery menu and choose Discover, then choose Discovery Manager, then click start discovery.

d. After discovery is complete, close the Discovery Manager window.

   The Discovery Manager window will show you all of the devices it has discovered, and the current status of the HP OpenView discovery process. If not all the devices on your network have been discovered, click the Start Discovery button.

e. The discovery process continues on a regular schedule to discover new devices added to the network, and to remove from its maps those devices taken off the network.

   To change the schedule of the discovery process, pull down the Autodiscovery menu and choose Configure, then choose Discovery Schedule.

f. Change the timer for IP Discovery to **5** minutes.

g. Change the timer for Extended Discovery to **10** minutes and click OK.

   These timer values are for convenience during class only. The actual values you should use depend on the frequency of configuration changes on your network. To reduce SNMP traffic, you should set the timers to as long an interval as possible, which still ensures accuracy of your network maps.

3. View and Lay out OpenView maps.

   Now that you have successfully completed discovery of your network, you will be able to display your network maps, by following the instructions in this step.

Note

To start over with an empty map file, pull down the File menu, choose New, and confirm the operation. Then redo step 2 to discover your network again and to generate a new map file.

---

a. Pull down the Autodiscovery menu and choose Layout, then choose Do Basic Layout.

b. Select Yes when the system asks whether or not to proceed.

OpenView takes a short time to generate maps from the map file. Two types of maps will be generated. The ALLNETS map provides the Internetwork View for the entire discovered network. A separate network map is created for each subnetwork you have identified. These network maps are linked to each subnetwork icon on the Internetwork View.

If the system does not find an Advanced NMM for each subnetwork selected for discovery, the Select Flat Network to Describe window opens.

c. To identify manually a representative NMM, click the Describe button on the Select Flat Network to Describe window. In the window that opens, enter the IP address and other information provided by your instructor for your representative NMM.

d. Once you have your ALLNETS map displayed, you can verify the manageability of each subnetwork on the map, by clicking the right mouse button on each network icon and choosing Describe.

   The Describe Device window that opens contains information about the NMM devices in that subnetwork.

e. Verify the host name, IP address, management type (SNMP or Ping), and the community strings.

f. All NMMs and router agents should use the SNMP management type. The subnetwork icon should change to a cloud and be green.

g. Click Cancel.

4. Finding and adding node information to the database.

   Once you have discovered your network and its subnetworks, you can add information on individual network nodes to the Optivity database. In this step, you will discover nodes and add them to your database.

   a. Pull down the OpenView Applications menu and choose Node Discovery.

      This adds information about nodes to the Optivity database. This step is necessary to ensure that Find Nodes will work for all segments. Opening NodalView for a segment has the same effect for a single segment.

   b. After Node Discovery has completed, select Tools and Find Node.

   c. Select IP Address and enter the IP address of your neighbor's management station.

   d. Click Find.

e. The display will show you information about the hub your neighbor is connected to, and what views you may select to see more information about the hub.

f. Click Cancel to close Find Node.

5. Open Optivity Views from HP OpenView maps.

   In this step, you will be opening some Optivity views to verify that Optivity has been installed correctly on your computer, and that the Optivity and HP OpenView databases are synchronized. More information about these views is presented in subsequent lab activities.

   a. Select a subnetwork icon the HP OpenView Internetwork View. This icon should show a cloud inside a green circle.

   b. Pull down the Applications menu and choose Flatnet View.

      The Optivity Flat Network View for the selected subnetwork is displayed.

   c. Click the right mouse button on a segment icon on the Flat Network View, select Views, and choose Segment View.

      The Segment View is displayed, showing the Nortel Networks hubs and the IP address or host name of the NMM within a segment, including all of the interconnections between hubs.

   d. Click the right mouse button on a hub icon, select Views, and choose Expanded View.

      The Expanded View is displayed, showing a real-time display of the faceplate and connections for the selected hub.

   e. Close the Expanded View and Segment View.

   f. Click the right mouse button on a segment or ring icon on the Flat Network View, select Views and choose NodalView.

      The NodalView is displayed, showing the nodes connected to the selected segment or ring. NodalView is a statistical view of a segment or ring. Explore the kinds of information that are provided in this view.

   g. Close the NodalView and Flat Network View.

   h. Select a router on the HP OpenView Internetwork View.

i. Select RouterMan from the HP OpenView Applications menu.

   The system displays the RouterMan window for the router that you selected. You can receive information on the router, interfaces on the router, or protocols running on the router. Each section provides Config, Fault, Perf, and Utilization. These give information on the router's configuration, faults or error states, performance, and utilization. Explore the very useful information you find here.

j. Close RouterMan.

Part 2: Autodiscovery for Optivity Campus Command Center

In Part 1 of the lab, you used HP OpenView to discover, map, and add node information to the map database. You also opened Optivity Views from HP OpenView maps.

Now, in Part 2 of the lab, you will learn to open Optivity CCC, run Autodiscovery, and configure the CCC options. CCC has a convenient toolbar for its important application components. You can find out what each icon means by holding the right mouse button over the icon.

1. Configure and run Optivity Autodiscovery.

   In this step, you will run the Optivity discovery process, which is separate from, and independent of, the HP OpenView discovery process that you learned about and used in the first part of this activity.

   a. Pull down the HP OpenView Applications menu and choose Campus Command Center.

      The Autodiscovery window opens.

      The first time you open CCC, the Autodiscovery window always opens. After the first time you use it, if you need to open the Autodiscovery window manually, click the Autodiscovery button in the CCC toolbar or pull down the CCC Applications menu and choose Autodiscovery.

   b. Click the IP Discovery tab in the Autodiscovery window.

   c. In the All Subnets list, select each subnetwork you want to add to the Discover Subnets list and click Add.

   d. If your team's subnetwork is not listed in the All Subnets list, enter the subnet number in the Subnet Address field and click Add.

      The subnetwork is added to the Discover Subnets list.

   e. To help discover devices in a subnetwork, CCC has a capability to ping through a range of IP addresses. You can either select a subnet to Range Ping, by double–clicking on a subnet address in the All Networks section, or you can manually add the specific range of addresses you want to ping. For example, From: 141.251.1.1 To: 141.251.1.254. Click on the subnets you want to ping.

f. Click Add to add your selected subnet or range to the list. You will need to do this for each subnet, or range, you wish to discover.

g. Select Router Discovery Using Router Tables in the lower left corner of the window.

   Click the Discover button to begin Autodiscovery.

The discovery utility automatically stops when the process is complete. The status is given in the bottom right of the CCC Autodiscovery window. Let the discovery process complete before proceeding to the next portion of the lab.

2. Schedule Autodiscovery.

   Like the HP Open View discovery process, CCC has a schedule option that enables its discovery process to continues on a regular schedule to discover new devices added to the network, and to remove from its maps those devices taken off the network.

   In this step, you will learn to schedule the Optivity discovery process to run on a regular basis.

   a. Open the Autodiscovery window by clicking the Autodiscovery button in the CCC toolbar, or by pulling down the CCC Applications menu and choosing Autodiscovery.

Note

To open this window before a discovery process is complete, you must stop the discovery process.

   b. Click the Scheduler tab.

   c. To schedule discovery at intervals of two hours, click the Start at Intervals Of button and type the number **2** in the Hrs box.

      Optivity Autodiscovery will now automatically start every two hours. You can start Autodiscovery at any time, regardless of the schedule, by clicking the Discover button on the IP Discovery tab.

   d. Click OK.

Rubric: Suggested Evaluation Criteria and Weighting

Criteria	**%**	**Your Score**
Successful completion of activity	15	
Accurately follows directions	15	
Complete, accurate responses to lab activity questions	15	
Complete summary of experiences and an insightful analysis of how a network manager might use this software to help improve network performance	20	
Summary included in portfolio	15	
Participation and cooperative teamwork during activity	20	
Other		
TOTAL	**100**	

Summary

Lesson 2: Network Transmission

In this unit, you learned to do the following:

- Explain how data is modulated, synchronized and transmitted across networks
- Describe how differences in bandwidth affect the speed of transmissions
- Describe several WAN connections
- Compare and contrast physical and logical network addressing

Review Questions

Lesson 2: Network Transmission

Directions: Select the best answer.

1. Packet assembly begins at which layer of the OSI model?
   a. Presentation
   b. Application
   c. Physical
   d. Session
   e. Transport
2. Which statement is false?
   a. Digital signals come in discrete states
   b. Analog signals are continuous
   c. Sending and receiving devices can use different methods of signal interpretation
   d. Computers interpret analog signals as ones and zeros
3. Which statement is true?
   a. Analog signals are more exact
   b. Digital signals are waves
   c. Analog signals are not continuous
   d. Computer data must be modulated to travel across telephone lines
   e. Modems only modulate digital signals
4. With connectionless transmission:
   a. The transmitting device does not know whether data arrives at the destination
   b. The transmitting device sets a connection before transmitting data
   c. The telephone is an example of this kind of transmission
   d. This type of transmission is very slow

5. Which of the following is false for connection-oriented transmission?
   a. The connection point does not always know when all signals are sent
   b. A connection is established before data is transmitted
   c. The connection between the two points is more dependable than connectionless transmission
   d. The telephone is an example of this kind of transmission
6. Asynchronous communication:
   a. Uses the clock to determine when transmission begins
   b. Uses the clock to determine when transmission ends
   c. Uses a start bit to tell when transmission begins and a stop bit to tell when transmission ends
   d. Does not always know when transmission ends
7. Which of the following is false?
   a. Synchronous transmission is an important device that lets the network know when to expect data
   b. Synchronous transmission is only digital
   c. Synchronous transmission relies on the clock
   d. The clock can be external or internal
8. Which of the following is true?
   a. The monitor uses half duplex
   b. The mouse uses half duplex
   c. The keyboard uses full duplex
   d. All of the above
9. Which of the following would definitely need broadband bandwidth?
   a. A Web page with a listing of all members of an organization
   b. A Web page advertising great car prices
   c. A Web page with multiple large images and video clips
   d. A Web page listing Web sites about jobs

10. Which of the following is false?
    a. Bandwidth is partially responsible for the speed at which data is transmitted on the Web
    b. Bandwidth is a not a big issue for the Web
    c. The growing number of users on the Web effects bandwidth
    d. The growing amount of multimedia on the Web effects bandwidth
11. Which is the most expensive way to connect LANs?
    a. Leased lines
    b. Circuit switching
    c. Packets over the telephone lines
    d. Frame relay
12. Which of the following WAN protocols is connectionless?
    a. Integrated Services Digital Network (ISDN)
    b. X.25
    c. Frame Relay
    d. Switched Multimegabit Data Service (SMDS)
    e. Asynchronous Transfer Mode (ATM)
13. What kind of transmission does not presume that the network is reliable?
    a. Integrated Services Digital Network (ISDN)
    b. X.25
    c. Frame Relay
    d. Switched Multimegabit Data Service (SMDS)
    e. Asynchronous Transfer Mode (ATM)
14. Which transmission method uses optical fiber as the media of choice?
    a. Integrated Services Digital Network (ISDN)
    b. X.25
    c. Frame Relay
    d. Switched Multimegabit Data Service (SMDS)
    e. Asynchronous Transfer Mode (ATM)

15. Which transmission method is very fast, if no errors occur?
    a. Integrated Services Digital Network (ISDN)
    b. X.25
    c. Frame Relay
    d. Switched Multimegabit Data Service (SMDS)
    e. Asynchronous Transfer Mode (ATM)
16. Which transmission method presumes that the network is reliable?
    a. Integrated Services Digital Network (ISDN)
    b. X.25
    c. Frame Relay
    d. Switched Multimegabit Data Service (SMDS)
    e. Asynchronous Transfer Mode (ATM)
17. Which of the following statements is true?
    a. Layer 3 switches are nothing more than routers
    b. Layer 3 switches simplify network design
    c. New connections are needed to use layer 3 switches
    d. Simultaneous transmissions are not supported by layer 3 switches
18. Which of the following statements is false?
    a. Connectionless transmissions do not require an acknowledgement
    b. Connection-oriented transmissions remain open until the source device knows that all of the data has been received, error-free, by the destination mode
    c. Half duplex transmissions are in one direction and full duplex transmissions are in both directions
    d. It is not necessary to synchronize data transmissions

19. Which of the following is a packet-switching transmission method that establishes a virtual circuit and is the preferred choice when transmitting to areas of the world where the telephone lines may be unreliable?

    a. Frame relay

    b. X.25

    c. Asynchronous Transfer Mode

    d. Switched Multimegabit data service

20. The ____________________ layer of the OSI is responsible for identifying the source and destination MAC addresses.

    a. Logical link layer

    b. MAC layer

    c. Network layer

    d. Data link layer

Scoring

Criteria	%	Your Score
Check Your Understanding		
Explain how data is modulated, synchronized and transmitted across networks	25	
Describe how differences in bandwidth affect the speed of transmissions	25	
Describe several WAN connections	25	
Compare and contrast physical and logical network addressing. Demonstrate knowledge of data transmission basics	25	
Try It Out: BayStack 350T 10/100 Autosense Switch Features	**100**	
Stretch Yourself: BayStack 350T Switch to Defaults/Configure Switch IP Address	**100**	
Network Wizards: Switches	**100**	
Lesson Review	**100**	
FINAL TOTAL	**500**	

Resources

Aschermann, Robert (1998). *MCSE Networking Essentials for Dummies*. IDG Books Worldwide, Inc. Foster City, California.

Baker, R. (1996). *Data Communications Home Page*. Available: www.georcoll.on.ca/staff/rbaker/intro.sht [1999, May 13].

Bert, Glen (1998). *MCSE Networking Essentials: Next Generation Training Second Edition*. New Riders Publishing, Indianapolis, Indiana.

Black, Darryl P. (1999). *Building Switched Networks: Multilayer Switching, QoS, IP Multicast, Network Policy, and Service Level Agreements.* Addison-Wesley, Reading, Massachusetts.

Casad, Joe. et al. (1997). *MSCE TestPrep Networking Essentials.* New Riders Publishing, Indianapolis, Indiana.

Chellis, James; Perkins, Charles; & Strebe, Matthew (1997). *MCSE Networking Essentials Study Guide.* Sybex Inc., Alameda, California.

CMP Media, Inc. (1999). FDDI fundamentals. In *Data Communications Tech Tutorials* [Online]. Available: www.data.com/Tutorials/FDDI_Fundamentals [1999, April 20].

Computer and Information Science, Ohio State University (No date). *Data Communications Cabling FAQ.* [Online].Available: www.cis.ohio-state.edu/hypertext/faq/usenet/LANs/cabling-faq/faq.html [1999, May 13].

Groth, David. Bergersen, Ben. Catura-Houser, Tim. (1999). *Network+ Study Guide.* Sybex Inc., Alameda, California.

Hayden, Matt. (1998). *Sam's Teach Yourself Networking in 24 Hours.* Sam's Publishing, Indianapolis, Indiana.

Nortel Networks (1998). *Internetworking Fundamentals: Student Guide.* Bay Networks Inc. Billerica, Massachusetts.

Nortel Networks (1999). *NetKnowledge: Internetworking Fundamentals.* Nortel Networks, Billerica, Massachusetts.

Nortel Networks (1999). *NetKnowledge: Routing.* Nortel Networks, Billerica, Massachusetts.

Palmer, Michael J. (1998) *Hands-On Networking Essentials with Projects,* Course Technology, Inc. Cambridge, Massachusetts.

Spurgeon, Charles E. (1997). *Practical Networking With Ethernet,* International Thomson Computer Press, Boston, Massachusetts.

The Siemon Company (1997). *Siemon Guidelines to Industry Standards* [Online]. Available: www.siemon.com/horiz.html [1999, March 3].

Trinity College Dublin, Computer Science Department, Networks & Telecommunications Research Group (No date). *The OSI Reference Model.* Available: ganges.cs.tcd.ie/4ba2/index.html [1999, May 13].