Lesson 2-3: Ethernet Basics

At a Glance

Ethernet LAN topology is currently the most common network architecture. Ethernet topologies are generally bus and/or bus-star topologies. Ethernet networks are passive, which means Ethernet hubs do not reprocess or alter the signal sent by the attached devices. Ethernet technology uses broadcast topology with baseband signaling and a control method called Carrier Sense Multiple Access/Collision Detection (CSMA/CD) to transmit data. The IEEE 802.3 standard defines Ethernet protocols for (Open Systems Interconnect) OSI's Media Access Control (MAC) sublayer and physical layer network characteristics. The IEEE 802.2 standard defines protocols for the Logical Link Control (LLC) sublayer. A solid understanding of Ethernet basics is necessary for all network personnel.

What You Will Learn

After completing this lesson, you will be able to:

- Describe Ethernet topology.

- Explain how CSMA/CD is used within an Ethernet LAN.

- Compare and contrast two Ethernet frame types.

- Describe the relationship between IEEE Ethernet standards and the OSI model.

- Troubleshoot an Ethernet problem.

Tech Talk

- **Back Off Mode**—A waiting mode in Ethernet topology where computer devices wait a specific amount of time before attempting to retransmit data after they have detected a collision.

- **Bandwidth**—The amount of data a transmission medium can carry.

- **Baseband**—A data transmission method in which the entire bandwidth of the cable is used to transmit a single signal. Only one signal can be transmitted at a time.

- **Broadband**—A data transmission method in which cable capacity is divided into multiple independent bandwidth channels. This allows several data transmissions to occur simultaneously over the cable.

- **Bus**—A bus is a common pathway (usually copper wire or fiber-optic cable) between multiple devices such as computers. A bus is often used as a backbone between devices.

- **Carrier Sense**—The ability to detect or sense the presence of other data transmissions on a network. In Ethernet technology, this ability helps avoid or prevent collisions.

- **Collision Detection**—The ability to detect whether any other devices are trying to access the network simultaneously.

- **Collision Domain**—All devices on the same Carrier Sense Multiple Access/Collision Detection wire segment are considered one collision domain. A collision in one domain does not affect any other domain on the network.

- **Contention Based**—In Ethernet topology, a computer device must wait for a turn to use the network. Computer devices must contend with other devices for network access. This means that all devices have an equal opportunity to send signals. No device has priority.

- **Ethernet**—A LAN topology based on Carrier Sense Multiple Access/Collision Detection (CSMA/CD).

- **Network Operating System (NOS)**—Software that allows computer devices to interconnect in order to transmit data across media.

- **Passive Hub**—A central connecting device in a network that joins wires from several stations, but does not provide signal processing or regeneration.

Ethernet Origins

Ethernet topology, which is based on bus and bus-star physical configurations, is currently the most frequently configured LAN network architecture. A bus is a common pathway (usually copper wire or fiber cable) between multiple devices such as computers. A bus is often used as a backbone between devices. It is a technology that has been evolving for more than 25 years and is still evolving to meet the ever increasing and changing needs of the internetworking community.

Digital Equipment Corporation and Xerox (DIX) worked together to develop the first Ethernet standards. These standards are the DIX Ethernet standards and are still in use today. As Ethernet topology became more popular, industry-wide standards became necessary. In 1985, the IEEE adopted the current Ethernet standards. These standards are called the IEEE 802.2 and 802.3 standards. They differ slightly from the DIX standards, but both define the protocols for the physical and data link layers of the OSI Model. These standards include cabling specifications, frame format, and network access conventions.

Ethernet is a passive, contention-based broadcast technology that uses baseband signaling. Baseband signaling uses the entire bandwidth of a cable for a single transmission. Only one signal can be transmitted at a time and every device on the shared network hears broadcast transmissions. Passive technology means that there is no one device controlling the network. Contention-based means that every device must compete with every o ther device for access to the shared network. In other words, devices take turns. They can transmit only when no other device is transmitting.

Ethernet popularity is a result of several factors. Ethernet technology is:

- Inexpensive

- Easy to install, maintain, troubleshoot and expand

- A widely accepted industry standard, which means compatibility and equipment access are less of an issue

- Structured to allow compatibility with network operating systems (NOS)

- Very reliable

NØRTEL
NETWORKS

Check Your Understanding

♦ Explain what is meant by passive, contention based, broadcast technology that uses baseband signaling.

♦ Why is Ethernet topology currently the most frequently configured LAN network architecture?
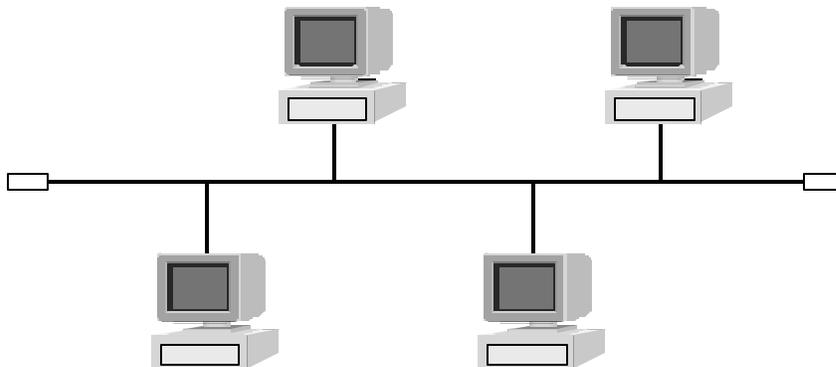
Ethernet Configuration and Communication

Ethernet Configuration

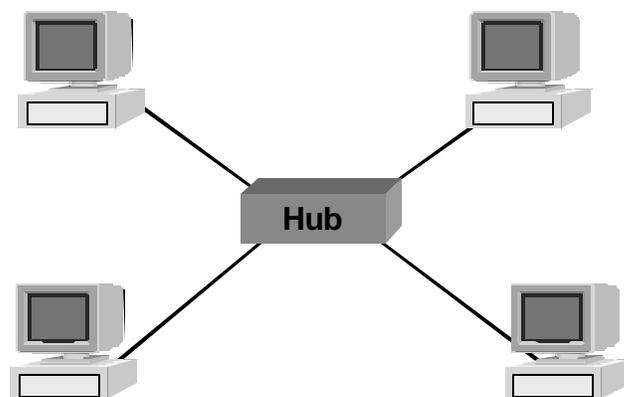Ethernet is a broadcast topology that may be structured as a physical bus or physical star with a logical bus.

Ethernet Physical Bus Topology

The physical star with a logical bus is created with the use of a hub or concentrator.

**Ethernet Physical Star/Logical Bus Topology**

Ethernet Communication

Communication protocols for Ethernet networks encompass both the data-link and physical layers of the OSI model. This lesson deals mainly with the data-link layer, which is subdivided into a Media Access Control layer and a Logical Link Control layer. Lesson 2-4 covers physical layer issues.

Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) when transmitting data. Carrier Sense allows a computer device to "sense" whether or not another transmission is being "carried" over the network. So, before a device sends data, it listens for a carrier (jam) signal. If a carrier signal is detected, it waits until that transmission is completed. Early DIX Ethernet did not have a carrier signal. Therefore, a collision was not detected until the destination device received the framed packet. The addition of a jam signal is one example of how Ethernet technology has evolved.

Multiple Access means that all devices have equal access to the network. Since Ethernet is contention-based, equal access to the network for all is ensured. No device has priority over others, nor can it lock out any other device connected to the network. Information can be transmitted at any time by any device. All devices on the network receive the transmission and check the framed packet's destination address. If the destination address matches the device's address, the device accepts the data; if the address does not match, the device simply ignores the transmission.

Ethernet Collision
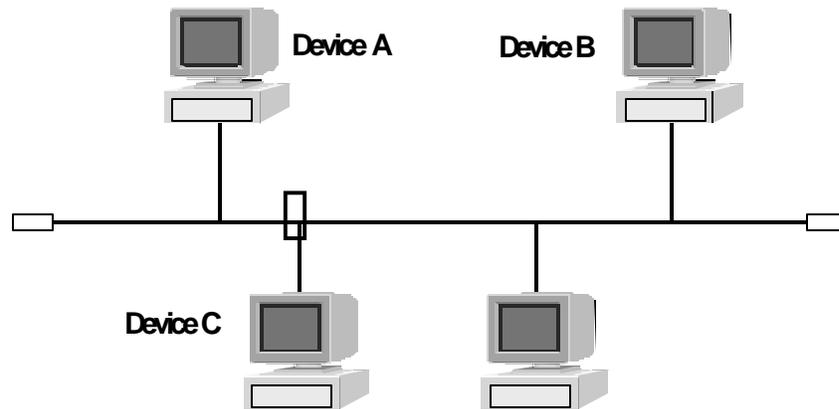
Collision Detection means that a sending device can "detect" simultaneous transmission attempts. When two or more devices try to send data at the same time, the signals collide. The illustration above shows devices A, B, and C sending signals simultaneously, and a collision occurs. When this happens, each device then transmits a jam signal, called a carrier, to alert all other devices that a collision has occurred.

All devices then go into back off mode and wait a random amount of time before attempting to retransmit data. The random time provision prevents simultaneous retransmissions. All devices on the same Carrier Sense Multiple Access/Collision Detection wire segment are part of the same collision domain. A collision domain is defined as those devices that share CSMA/CD of the same wire. Two or more collision domains are connected together with an internetworking device such as a router, bridge, or switch. With the use of internetworking devices, large networks are created which include multiple collision domains.

When a collision occurs it affects all the devices on the same collision domain. It does not affect devices on any other collision domains within the same network. You can think of two collision domains as two roads that are on different sides of a bridge. You can travel up to the bridge on either side, but must get permission to cross the bridge. On an Ethernet collision domain, frames of data travel within their own domain unless they need to talk to a device on the other side of the bridge. If it is necessary to talk to a device on the other side of a bridge, the bridge must give permission for the frame to cross the bridge to reach the other collision domain. Bridges are capable of this because they are store and forward devices: they store the frame from the source domain until permission is granted to forward it. The requirement is to keep traffic and collisions to a single collision

domain whenever possible. Collision domains are also called segments in Ethernet.

Ethenet Collision Domain

Single collision domain #1
(Segment 1)

Bridge

(Internetwork Device)

Single collision domain #2
(Segment 2)
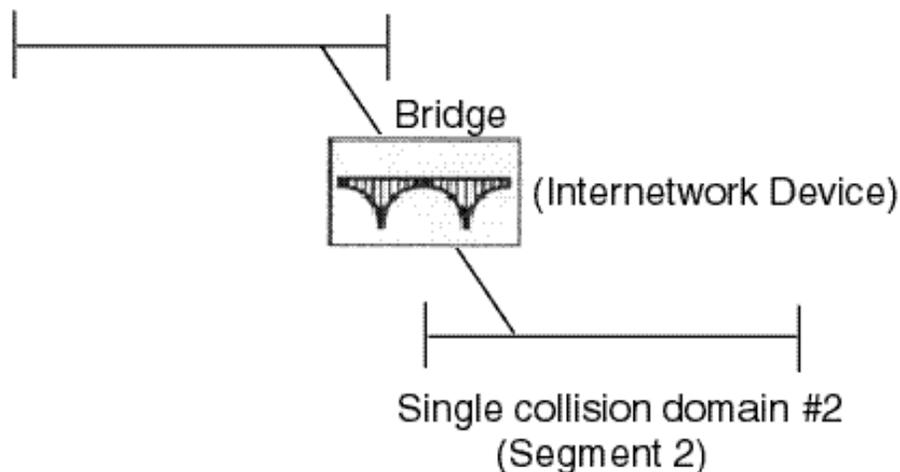
Data transmitted from one device to another on the same collision domain will not affect any other collision domains. This allows each collision domain to continue to transmit with no effect on each other except when a device needs to talk to a device on another collision domain. When this is required, the frame must be sent across one or more internetworking devices to reach its destination. Each internetworking device must allow the frame to pass. As the frame reaches each collision domain the port of the internetworking device must contend for the right to transmit according to the rules of CSMA/CD.

To better understand CSMA/CD, think about trying to make a telephone call. Many of us have more than one telephone in our homes (a telephone network). When you pick up the telephone to make a call, you "sense" a dial tone or someone else on the line. If there is a dial tone, you proceed with your call. If the telephone line is currently in use, you can not make a call at this time and you try again later. This is similar to Ethernet Carrier Sense protocols.

All telephones in the house can be used at any time to make calls. All phones in the house have equal access to the telephone network. This is comparable to Multiple Access.

> Should two individuals in the house attempt to make a phone call simultaneously, both hear dial tone; neither party senses a carrier, (someone else on the line). However, like Ethernet technology, only one individual can use the line at any one time. Both parties must

hang-up and wait a random amount of time before making a second attempt. This is how Ethernet's Collision Detection protocols work.

In summary, a computer device checks to see if the transmission media is busy, recognizes that multiple devices access the network, and detects when a collision has taken place and goes into back off mode.

Check Your Understanding

♦ Explain CSMA/CD in your own words.

♦ When your teacher asks a question in class, what might the result be if everyone answered the question simultaneously?

♦ What rules do use in your class use to prevent simultaneous responses?

♦ How is a polite conversation similar to CSMA/CD protocols?

Ethernet Frames

In Ethernet, both the data link and the physical layers are involved in the creation and transmission of frames. The physical layer is related to the type of LAN cabling and how the bits are transmitted and received on the cable. The data link layer is divided into sublayers, the Logical Link Control (LLC) and the Media Access Control layers (MAC). The frames created by these layers contain several fields that are processed by Network Interface Cards (NICs) in the sending and receiving devices.

Ethernet and the OSI Layers
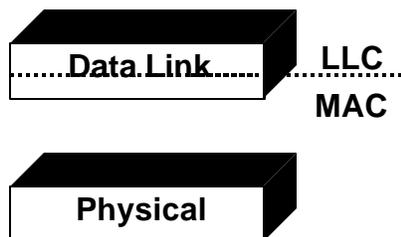
The MAC sublayer address is the physical hardware address of the source and destination computer. It is called the MAC layer address and should not be confused with the network address. All devices on a LAN must be identified by a unique MAC address. This sublayer controls which computer devices send and receive the data and allows NICs to communicate with the physical layer. IEEE 802.3 protocols control the format of the MAC sublayer frame fields.
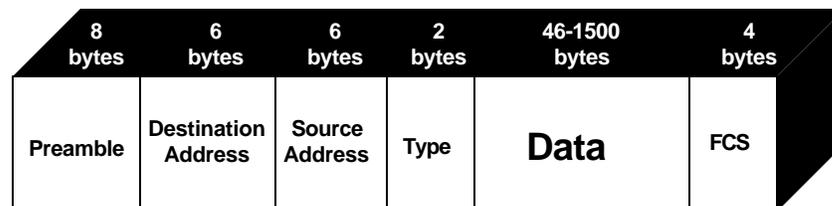
The next level of processing is the LLC sublayer. It is responsible for identifying and passing data to the network layer protocol. Two LLC protocols are IP and Novell's IPX.

Frame Format

The two frame formats discussed in this lesson are DIX frames, which are what the Internet uses, and IEEE 802.3 frames. It should be noted that if one device uses an 802.3 NIC and the other device uses a DIX Ethernet NIC, they would not be able to communicate with one another. Devices must create the same Ethernet frame format in order to be compatible. Although only the 802.3 IEEE frames format is outlined in the standard, both formats are in use today. One way to tell them apart is that the DIX frame has a "type" field, which defines the protocol used for the frame, and IEEE 802.3 has a "length" field in its place. IEEE 802.3 also has additional fields not used with the DIX format.

The DIX, also called Ethernet II, frame includes the following fields:

DIX Frame (Ethernet II)

8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Preamble	Destination Address	Source Address	Type	Data	FCS

The Preamble of the frame (the first 7 bytes) indicates the start of a new frame and establishes synchronization conditions between devices. The last byte, or start frame delimiter, always has a 10101011-bit pattern. This byte indicates the start of a frame.

The Destination Address is the hardware (MAC) address of the receiving device, and the source address specifies the hardware (MAC) address of the sending device.
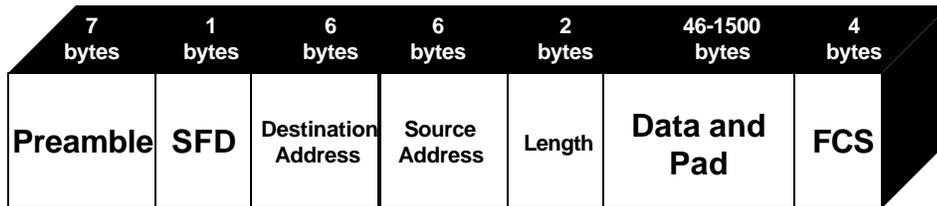
The Type field specifies the network layer protocol used to send the frame, for example TCP/IP.

The Data field is for the actual data being transmitted from device to device. It also contains information used by the network layer and indicates the type of connection.

The Cyclic Redundancy Check (CRC) checks that the frame is received free from corruption.

IEEE 802.3 Frame Format

The IEEE standard was adopted in 1985. The 802.3 frame format is below:

7 bytes	1 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Preamble	**SFD**	**Destination Address**	**Source Address**	**Length**	**Data and Pad**	**FCS**

Fields one and two perform the same function as the DIX preamble; however, the fields are separate. The Start Frame Delimiter (SFD) has the same 10101011-bit sequence found at the end of the DIX preamble. Both formats use the same number of bytes to perform the synchronization of the signals.

The Destination and Source Addresses can be either 2 or 6 bytes. Whether 2 or 6 bytes are used, all devices within the same network must use the same format. IEEE protocols specify that a 10Mbs network must use 6 bytes. The 2 byte length is obsolete.

The Length field indicates the number of bytes in the data field. If the data field is less than the required 46 bytes, a pad field is added to the data frame. The bytes added for padding purposes are usually zeros.

The data field contains the data to be transmitted from device to device.

The Frame Check Sequence (FCS) field is used as an error detection function. The error detection function is a calculation completed by both the source and destination devices. If the calculations do not match, an error is then generated.

IEEE 802.2 LLC Frame

In between the length field and the data/pad field, is the 802.2 LLC field.

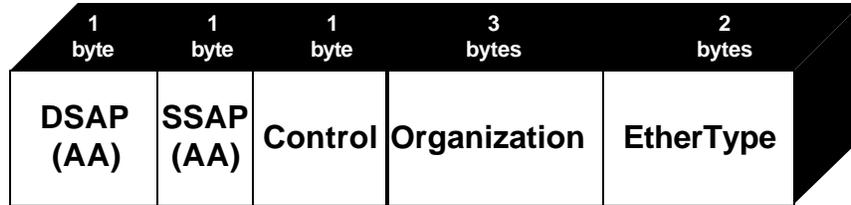| 7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Preamble	SFD	Destination Address	Source Address	Length	Data and Pad	FCS

1 byte	1 byte	1 byte
DSAP	SSAP	Control
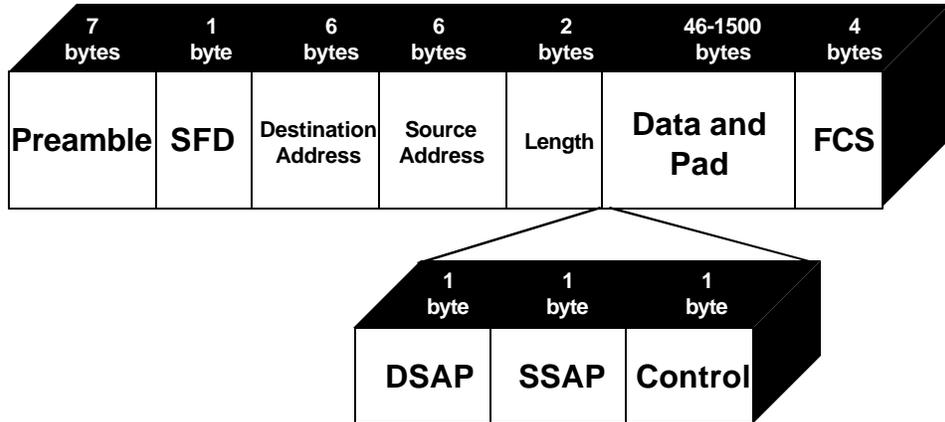
- DSAP, destination service access protocol, is the protocol processing layer the data is to be sent to.

- SSAP, source service access protocol, is the protocol used to encapsulate the data at the source.

- Control is the field that defines the type of LLC frame this is.

NORTEL
NETWORKS

SNAP Format of 802.2

1 byte	1 byte	1 byte	3 bytes	2 bytes
DSAP (AA)	SSAP (AA)	Control	Organization	EtherType

SNAP (Sub-Network Access Protocol) was created by the IEEE to identify the Network layer protocol used. The original Ethernet version 2.0 Type field had been reused as a Length field by the IEEE when creating the IEEE 802.3 standard. SNAP was defined to enable this Length field to remain while also allowing the vendor and protocol to be defined in the first 40 bits of the Data field. Together, these two fields (Organization and EtherType) are called the Protocol ID.

- AA in the DSAP or SSAP fields indicates that the LLC field is using SNAP format.

- Control is the field that defines the type of LLC frame this is.

- Organization is the field that indicates which organization created the protocol identified in the EtherType field, though generally this is coded as all zeros by most organizations.

- EtherType is a two-byte identifier for the protocol being used to encapsulate the data. For example, IP is indicated by the code 0x08-00, ARP by 0x08-06 and NetWare IPX/SPX by 0x81-37.

Depending on how the vendor decided to manufacture the Ethernet hardware, the hardware will create frames that are either DIX, 802.3, or 802.2 with SNAP.

Frame Types

There are three types of frames; each has a different purpose. The three types are:

- Unicast

- Multicast

- Broadcast

If the first bit of the frame is 0, it is Unicast; if it is 1, it is multicast. Broadcast frames always have 1 as the second bit.

A Unicast frame is addressed to a single network device. This means that the frame is to be read only by the device that matches the destination address. All other devices in the collision domain will receive a copy of the

frame but will discard it because it does not match their destination address. The address used is the MAC address or hardware address of the network device.

A multicast frame is addressed to several but not all devices. All devices that are a part of the specified group may read the frame. A multicast address is a deviation from the normal hardware address. For example, a group of devices are assigned access to a particular server on the network. They are the only devices that receive frames announcing the availability of that server. Any device that does not belong to this group will ignore or discard these frames.

A broadcast frame is addressed for all network devices to read and process. A broadcast address is a unique address used only for broadcast frames. It is not a hardware address. Broadcast frames are transmitted across bridges and switches; however, routers will stop broadcast frames.

Check Your Understanding

♦ Describe what the LLC layer does.

♦ What do the MAC sublayer protocols specify?

♦ Create a table that compares a DIX frame and an IEEE 802.3 frame.

♦ Compare and contrast unicast, multicast, and broadcast frames.

NORTEL
NETWORKS

Try It Out

Ethernet LAN

As you complete this lab, keep a record of the problems you encounter, how you solve them, notes indicating how you would prevent these problems from occurring the next time you encounter this situation, and any other thoughts you feel should be incorporated into your portfolio. This information is critical to discovering some very simple troubleshooting techniques.

Recall from the cabling lesson that there are tip and ring wires on cables. You crimped a straight-through, category 5 cable, with a RJ-45 connector. Your computer transmits straight through. In order to receive transmissions, the cable or the device you're connecting to must be crossover. That is because the Tx pin/wire on one device must eventually enter the Rx pin/wire on the end device. Hubs are crossover devices, that is, the crossover takes place internally. As a result, you use straight through cables to connect your computer to the hub.

Media dependent interface (MDI) is the IEEE standard for the interface to unshielded twisted pair (UTP) cable.

In order for two devices to communicate, the transmitter of one device must connect to the receiver of the other device. The connection is established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

Ports that implement the crossover function internally are known as MDI-X ports, where X refers to the crossover function.

Ethernet single collision domains may be configured in several ways. In this lab you will configure a single collision domain using a single hub. Work in groups of three or four. All the members of your team will connect their computers to the hub and your team will become an Ethernet segment.

Materials Needed

- Manual for BayStack 153 10BaseT Hub

- Power cords for Hub network connectivity

- Straight through cable you crimped in Unit 1

Part 1: Identify Hardware

1. Obtain the BayStack 153 10BASE-T Hub documentation from your teacher.

2. Read Chapter 1: Introduction, Features, and Description, pages 1-1 to 1-4.

3. Obtain the diagram of the BayStack 153 10BASE-T Hub that you placed in your portfolio during the Connectivity and Internetworking Devices lesson.

4. Refer to pages 1-5 and 1-6 of the Hub documentation. Label all of the parts. Keep diagram in your portfolio.

5. Attach the power cord to the back of the hub and power on the hub.

   ♦ How many host (RJ-45) ports on the hub? What are the configuration settings available for port 1? How is the configuration set for port 1? What is the configuration for the other ports? MDI or MDI-X? What type of port is on the NIC on the back of your computer? What is the configuration of the NIC card port? MDI or MDI-X?

Part 2: Connecting to the Hub

1. Use the straight through cable you crimped or obtain another straight through cable from your teacher. Connect from your NIC to a host port on the hub.

   ♦ Why do you need to use a straight through cable? Did the Link LED turn to green for your connection?   Yes or No

2. If the link did not turn to green, contact your teacher.

3. After all team members are connected to the hub, verify that all LEDs on the LED display on the hub where workstations are connected are green.

4. PING will be used to verify each connection.

5. Select the Start menu, select Programs, and select MS DOS Prompt. A window similar to the following is presented on the screen

NORTEL
NETWORKS

```
MS-DOS Prompt

10 x 20 ▼   □ 🖹 🖺 ✛ 🖼 🖳 A


Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1998.

C:\WINDOWS>ping 141.252.10.99

Pinging 141.252.10.99 with 32 bytes of data:

Reply from 141.252.10.99: bytes=32 time<10ms TTL=128
Reply from 141.252.10.99: bytes=32 time<10ms TTL=128
Reply from 141.252.10.99: bytes=32 time<10ms TTL=128
Reply from 141.252.10.99: bytes=32 time<10ms TTL=128

Ping statistics for 141.252.10.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\WINDOWS>
```
6.

7. Press Enter. Four ping frames will be sent to verify connectivity to the IP address you requested.

   ♦ Were you successful? Yes or No

8. If you were not successful, check all connections and the status LEDs of each host port.

   ♦ Are there any amber LEDs? Yes or No

   If the answer is yes, verify the connection to the computer, the cable quality, the accuracy of the IP address assigned to the computer you are tying to reach and the accuracy of your PING request.

   ♦ Did you find the problem? Yes or No

   If you cannot resolve your problem, ask the teacher for help.

   ♦ Can you PING all members of your team? Yes or No

   ♦ Have you configured one or two collision domains?

9. Record the IP addresses on the diagram you created for the structured cabling lesson.

When you have successfully proven connectivity to all team members and your instructor, you have completed this lab.

Rubric: Suggested Evaluation Criteria and Weightings

Criteria	%	Your Score
Participation and teamwork	20	
Accurately followed directions	25	
Thorough and accurate answers to questions	30	
Portfolio. Clarity of notes, relevance of potential solutions for future similar problems	25	
TOTAL	**100**	

NORTEL
NETWORKS

Stretch Yourself

Troubleshooting Ethernet LANs

Materials Needed

- BayStack 152 Hub and documentation

- LAN

Directions: Refer to the documentation that came with the BayStack 152 Hub. Record the answers to the questions in your portfolios for future troubleshooting recommendations.

Each of the ports has an LED to indicate port status. The LEDs indicate link, activity, and partitioning status. The port status indicators always come on when the hub is powered on. In normal operation, after the POST (power-on self-test) is completed, the LEDs turn off.

Answer the following questions regarding the description of Hub Status LEDs.

♦ When the Master is green, what does that indicate?When the Con is green, what does that indicate?

♦ When the AUI is green and blinking, what does that indicate?

♦ When the Runt is amber, what does that indicate?

♦ When the F/A is amber, what does that indicate?

♦ When the L/C is amber, what does that indicate?

♦ When the Other is amber, what does that indicate?

♦ When the Isolate is amber, what does that indicate?

♦ What does the Hub ID tell you?

Rubric: Suggested Evaluation Criteria and Weightings

Criteria	%	Your Score
On time delivery of assignment	15	
Questions and answers added to portfolio for future reference.	25	
Completeness and accuracy of answers questions	60	
TOTAL	**100**	

Network Wizards

Troubleshooting an Ethernet LAN Case Study

A small company has hired you to solve their networking problem. The wait time for access to email and other services at the company is very slow, resulting in lowered productivity. The network is an Ethernet LAN, bus topology (physical and logical), with 55 devices all connected to the same collision domain. There are three user groups: sales (30 devices), accounting (5 devices), and marketing (18 devices), each with its own server.

The company executives know a little bit about LANs and connectivity devices; however, they do not know whether to purchase a repeater, a bridge, a hub, or a combination of these devices.

Materials Needed

- None

Your assignment is to prepare a document with a proposed solution to their problem. The document must contain the following:

- Explain the shortcomings of bus topology in this case. Suggest an alternative topology and defend your choice.

- Provide a computer-generated sketch of the proposed topology.

- Prepare documentation that explains the purpose of a hub, repeater, router, bridge, and switch, and relate these devices to their corresponding OSI layer. Explain which devices will help solve their problem and tell them why.

- Prepare a one-page summary of your proposed solution.

Rubric: Suggested Evaluation Criteria and Weightings

Criteria	%	Your Score
On time delivery of proposed solution document	20	
Thorough explanation of the shortcomings of bus topology and defense of proposed topology changes	20	
Accurate sketch of proposed topology	20	
Complete and accurate explanation of the various computer devices, their relationship to the OSI layers, and which ones will help solve the company's networking problems	20	
Plausibility of the proposed solution	20	
TOTAL	**100**	

Summary

In this lesson, you learned to do the following:

- Describe Ethernet topology.

- Explain how CSMA/CD is used within an Ethernet topology.

- Compare and contrast two Ethernet frame types.

- Describe the relationship between Ethernet standards and the OSI model.

- Set up an Ethernet LAN and ping to check for connectivity.

- Troubleshoot an Ethernet problem scenario.

Review Questions   Name_____

Lesson 2-3: Ethernet Basics

Part A

1. Which type of transmission do all devices on the shared network hear and accept?

    a. Unicast

    b. Multicast

    c. Broadcast

    d. Baseband

2. Which type of signaling uses the entire bandwidth of a cable for a single transmission and allows only one signal at a time?

    a. Unicast

    b. Multicast

    c. Broadcast

    d. Baseband

3. When all devices have equal access to the network and no one device has priority over another device, what is this called?

    a. Carrier Sense

    b. Multiple Access

    c. Collision Detection

    d. Collision Domain

4. What is the term used to describe the ability of a device to sense simultaneous transmission attempts and wait a random amount of time before retransmitting data?

    a. Carrier Sense

    b. Multiple Access

    c. Collision Detection

    d. Collision Domain

5. What is the ability to listen for a jam signal before transmitting data called?

    a. Carrier Sense

    b. Multiple Access

    c. Collision Detection

    d. Collision Domain

6. Ethernet standards include specifications for which of the following?

    a. Cabling

    b. Frame format

    c. Network access conventions

    d. All of the above

7. What are the two IEEE Ethernet standards called?

8. What is the name for the Ethernet standards developed by Xerox, Intel, and Digital Equipment Corporation?

9. What type of topology configuration(s) does Ethernet employ?

10. List five reasons for the popularity of Ethernet LAN topology.

NØRTEL
NETWORKS

Part B

Matching: Match the part of the frame with its definition.

1. ___ Preamble	A	One byte code in the LLC field used to identify the protocol that will encapsulate the data field
2. ____ Start of Frame	B	Hardware address of the destination device
3. ___ Destination Address	C	Actual information being transmitted
4. ___ Source Address	D	Specifies the protocol used for sending the frame
5. ___ Type Field	E	Specifies the length of the data within the frame
6. ___ Length Field	F	Type of frame check that detects errors that occur in the frame during transmission
7. ___ Pad	G	Added to the data field of IEEE 802.3 when the data is less than 46 bytes
8. ___ Data	H	Establishes synchronization and transceiver conditions
9. ___ DSAP	I	Field with 10101011 sequence separate
10. __ CRC	J	Hardware address of the sending device

Part C

♦ Name the two data link sublayers.

♦ Which sublayer of the OSI do the IEEE 802.2 standards control?

♦ Which sublayer of the OSI do the IEEE 802.3 standards control?

♦ What do the MAC sublayer protocols specify?

♦ Explain how the data link and physical layers are involved in the creation and transmission of frames.

Scoring

Rubric: Suggested Evaluation Criteria and Weightings

Criteria	%	Your Score
Part A: Describe Ethernet topology. Explain how CSMA/CD is used within an Ethernet topology	30	
Part B: Compare and contrast two Ethernet frame types	40	
Part C: Describe the relationship between Ethernet standards and the OSI model	30	
TOTAL	**100**	
Try It Out: Set up an Ethernet LAN and ping to check for connectivity.	**100**	
Stretch Yourself: Troubleshoot Ethernet LANs	**100**	
Network Wizards: Troubleshoot possible Ethernet problems	**100**	
FINAL TOTAL	**400**	

Resources

Aschermann, Robert (1998). <u>MCSE Networking Essentials for Dummies</u>. *IDG Books Worldwide, Inc.* Forest City, California.

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

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

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

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

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

Derfler, Jr., Frank J., & Freed, L. (1998). <u>How Networks Work</u>, Fourth Edition. *Macmillan Computer Publishing/Que Corporation.* Indianapolis, Indiana.

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

Microsoft Corporation (1998<u>). Dictionary of Computer Terms</u>, *Microsoft Press*, Redmond, Washington.

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

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

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