Zulfiqar Ali

# Networking Essentials Notes - Section 1

## Network Orientation

**Peer-to-Peer Networks**

- No dedicated server or hierarchy also called a workgroup.
- Usually 10 or fewer workstations.
- Users act as their own administrator and security.
- Computers are in same general area.
- Limited growth.

**Server Based Networks**

- 10 or more users.
- Employs specialized servers.
    1. File and Print
    2. Application
    3. Mail
    4. Fax
    5. Communications (gateways)
- Central administration.
- Greater security.
- Centralized backup.
- Data Redundancy.
- Supports many users

**Combination Networks**

- Combines the features of both Peer to Peer and Server based networks
- Users can share resources among themselves as well as access server-based resources.

## Network Topologies

There are 4 basic topologies with variations

**Bus Topology**

- Bus consists of a single linear cable called a trunk.
- Data is sent to **all computers on the trunk**. Each computer examines EVERY packet on the wire to determine who the packet is for and accepts only messages addressed to them.
- Bus is a passive topology.
- Performance degrades as more computers are added to the bus.
- Signal bounce is eliminated by a terminator at each end of the bus.
- Barrel connectors can be used to lengthen cable.
- Repeaters can be used to regenerate signals.
- Usually uses Thinnet or Thicknet
- Both of these require 50 ohm terminator
- Good for a temporary, small (fewer than 10 people) network
- But it’s difficult to isolate malfunctions and if the backbone goes down, the entire network goes down.

**Star Topology**

- Computers are connected by cable segments to a centralized hub.
- Signal travels through the hub to all other computers.
- Requires more cable.
- If hub goes down, entire network goes down.
- **If a computer goes down, the network functions normally.**
- **Most scalable and reconfigurable** of all topologies

**Ring Topology**

- Computers are connected on a single circle of cable.

- Usually seen in a Token Ring or FDDI (fiber optic) network
- Each computer acts as a repeater and keeps the signal strong => no need for repeaters on a ring topology
- No termination required => because its a ring
- Token passing is used in Token Ring networks. The token is passed from one computer to the next, only the computer with the token can transmit. The receiving computer strips the data from the token and sends the token back to the sending computer with an acknowledgment. After verification, the token is regenerated.
- Relatively easy to install, requiring; minimal hardware

**Mesh**

- The mesh topology connects each computer on the network to the others
- Meshes use a significantly larger amount of network cabling than do the other network topologies, which makes it more expensive.
- The mesh topology is highly fault tolerant.
- Every computer has multiple possible connection paths to the other com-puters on the network, so a single cable break will not stop network communications between any two computers.

**Star Bus Topology**

- Several star topologies linked with a linear bus.
- No single computer can take the whole network down. If a single hub fails, only the computers and hubs connected to that hub are affected.

**Star Ring Topology**

- Also known as star wired ring because **the hub itself is wired as a ring**. This means it's a physical star, but a logical ring.
- This topology is popular for Token Ring networks because it is easier to implement than a physical ring, but it still provides the token passing capabilities of a physical ring inside the hub.
- Just like in the ring topology, computers are given equal access to the network media through
- The passing of the token.
- A single computer failure cannot stop the entire network, but if the hub fails, the ring that the hub controls also fails.

**Hybrid Mesh**

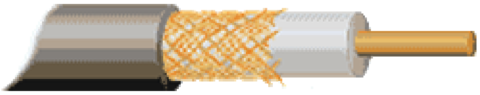
- Most important aspect is that a mesh is fault tolerant
- A true mesh is expensive because of all the wire needed
- Another option is to mesh only the servers that contain information that everyone has to get to. This way the servers (not all the workstations) have fault tolerance at the cabling level.

# Connecting Network Components

## Primary Cable Types

- **Coaxial Cable**
- **Twisted-pair**
  - UTP - Unshielded Twisted Pair
  - STP - Shielded Twisted Pair
- **Fiber-optic**

## Coaxial Cable



- Consists of a solid or stranded copper core surrounded by insulation, a braided shield and an insulating jacket.
- Braided shield prevents noise and crosstalk.
- More resistant to interference and attenuation than twisted pair cabling.
- Both thin and thick cables can use (see pp. 80-81 for pics)

  - BNC cable connectors,
  - BNC barrel connectors
  - BNC T connectors
  - BNC terminators.
- Plenum (fire resistant) graded cable can be used in false ceilings of office space or under the floor.
- Can transmit data, voice and video.
- Offers moderate security ----> better than UTP/STP

# Thinnet - RG-58 cable

- called
- 0.25" thick.
- Uses
  - BNC twist connector,
  - BNC barrel connectors
  - BNC T connectors
  - 50 ohm terminators
- Can carry signals **185 meters or 607 feet**.
- Types: (pics on page 78)

## Coaxial Cable Types

| | |
|---|---|
| RG-8 and RG-11 | **Thicknet** (50 ohms) |
| RG-58 Family | |
| RG-58 /U | Solid copper (50 ohms) |
| RG-58 A/U | **Thinnet**, Stranded copper (50 ohms) |
| RG-58 C/U | Thinnet, Military grade (50 ohms) |
| RG-59 | Broadband/Cable TV (75 ohm) video cable |
| RG-62 A/U | **ARCnet** cable (93 ohm)<br>RG-62 A/U is the standard ARCnet cable, but ARCnet **can** use fiber optic or twisted pair. |

- Each cable must have a terminator whose impedance matches the cable type
- Impedance = current resistance measured in ohms
- Terminators are resistors that prevent signal bounce or echo.

**Here are some limitations of 10Base2 Ethernet:**

- Length of trunk segment may be up to 607 feet.
- A maximum of 30 workstations is allowed per trunk.
- There may be no more than 1024 workstations per network.
- Entire network trunk length can't exceed 3035 feet (925 meters)
- The minimum cable length between workstations is 20 inches.
- The Ethernet 5-4-3 Rule for connecting segments is 5 trunk segments can be connected, with 4 repeaters or concentrators, with no more than 3 populated segments (on coaxial cable).

## Thicknet - RG-8 and RG-11 coaxial cable

- 0.5" thick
- Used for 10Base5 networks, linear bus topology
- Transmits at 10 Mbps
- Uses DIX or AUI (Attachment Unit Interface) connector - also known as DB-15 connector to connect to external transceivers.
- Vampire taps are used to attach a transceiver to the thicknet trunk.
- Can carry signals **500 meters or 1640 feet**.

- Much less flexible and far more bulky and harder to install than thinnet
- Better security than thinnet
- Better resistance to electrical interference than thinnet.
- MORE expensive than thinnet.

## Twisted-Pair Cable

- Consists of two insulated copper wires twisted around each other.
- Twisting cancels out electrical noise from adjacent pairs (crosstalk) and external sources.
- Uses RJ-45 telephone-type connectors (larger than telephone and consists of eight wires vs. Telephone's 4 wires).
- Generally inexpensive.
- Easy to install.

### Unshielded Twisted Pair (UTP)

- Maximum cable length is **100 meters or 328 feet (10BaseT)**.
- Types:
    1. Cat 1 Voice grade telephone cable.
    2. Cat 2 Data grade up to 4 Mbps, four twisted pairs.

  Category 3 and above is needed for Ethernet networks. Cat 3, 4, and 5 use RJ-45 connectors

    1. Cat 3 Data grade up to 10 Mbps, four pairs w/3 twists/ft.
    2. Cat 4 Data grade up to 16 Mbps, four twisted pairs.
    3. Cat 5 Data grade up to 100 Mbps, four twisted pairs.

  This is the cheapest cable to put in. **Exam questions ALWAYS take this as a given.**

**Here are some limitations of 10BaseT Ethernet:**

- Workstations may be no more than 328 feet from the concentrator port.
- 1,023 stations are allowed on a segment without bridging.
- The minimum cable length between workstations is 8 feet.

**Other Drawbacks**

- **UTP is particularly susceptible to crosstalk**, which is when signals from one line get mixed up with signals from another.
- Easily tapped (because there is no shielding)
- 100 meters is shortest distance => attenuation is the biggest problem here.

### Shielded Twisted Pair (STP)

- Uses a woven copper braid jacket and a higher quality protective jacket. Also uses foil wrap between and around the wire pairs.
- Much less susceptible to interference and supports higher transmission rates than UTP.
- Shielding makes it somewhat harder to install.
- Same 100-meter limit as UTP.
- Harder to tap
- **Used in AppleTalk and Token Ring networks**

## Fiber Optic Cable

- Consists of a small core of glass or plastic surrounded by a cladding layer and jacket.
- Fibers are unidirectional (light only travels in one direction) so two fibers are used, one for sending and one for receiving. Kelvar fibres are placed between the two fibres for strength.
- Good for very high speed, long distance data transmission.
- NOT subject to electrical interference.
- Cable can't be tapped and data stolen => high security

- **Most expensive** and difficult to work with.
- Immune to tapping.
- Can transmit at **100 Mbps** and way up to 2 Gbps
- Up to 2000 meters without a repeater.
- Supports data, voice and video.
- Needs specialized knowledge to install => expensive all round.

| Cable Type Comparisons | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Type** | **Speed** | **Distance** | **Installation** | **Interference** | **Cost** | **# of nodes per segment** | **# of nodes per network** |
| 10BaseT | 10 Mbps | 100 meters | Easy | Highly susceptible | **Least expensive** | 1 computer | |
| 100BaseT | 100 Mbps | 100 meters | Easy | Highly susceptible | More expensive than 10BaseT | | |
| STP | 16 to 155 Mbps | 100 meters | Moderately Easy | Somewhat resistant | More expensive than Thinnet or UTP | | |
| 10Base2 | 10 Mbps | 185 meters | Medium Difficulty | Somewhat resistant | Inexpensive | 30 | 1024 |
| 10Base5 | 10 Mbps | 500 meters | More difficult than Thinnet | More resistant than most cable | More expensive than most cable | 100 | 300 |
| Fiber Optic | 100 Mbps to 2 Gbps | 2000 meters | Most difficult | Not susceptible to electronic interference | **Most expensive type of cable** | | |

## Signal Transmission

### Baseband Transmission -- Digital

- Baseband transmission uses digital signaling over a single frequency.
- Entire communication channel is used to transmit a single signal.
- **Flow is bi-directional**. Some can transmit and receive at the same time.
- Baseband systems use **repeaters** to strengthen attenuated signals.

### Broadband Transmission -- Analog

- Broadband uses analog signaling over a range of frequencies.
- Signals are continuous and non-discrete.
- **Flow is uni-directional** and so two frequency channels or two separate cables must be used.
  - If enough bandwidth is available, multiple analog transmission systems such as cable TV AND network transmissions can be on the same cable at the same time.
  - If this is the case, ALL devices must be tuned to use only certain frequencies
- Uses **amplifiers** for signal regeneration.

### Helpful mnemonic to remember the difference:

**Baseband is "BEDR"**
**B**idirectional
**E**ntire channel taken up
**D**igital
**R**epeaters used to strengthen signal

### IBM Cabling

- Uses AWG standard wire size.
- Connected with proprietary IBM unisex connectors.
- Defines cables as types

| | | | | |
|---|---|---|---|---|
| **Type 1** | STP<br>(Shielded twisted-pair) | • Used for computers and MAU's.<br>• 101 m | These three cable types can be used in Token Ring Networks | • 16 Mbps<br>• 260 computer limit |
| **Type 2** | STP, Voice and data | • 100 m | | |
| **Type 3** | UTP; Voice grade | • **45 m**<br>• **Most common Token Ring Cable** | | • 4 Mbps<br>• 72 computer limit |
| **Type 5** | Fiber-optic | • Industry standard | | |
| **Type 6** | STP; Data patch | • Used to connect MSAU's together<br>• Used to extend Type 3 cables from one computer to the MSAU | | |
| **Type 8** | STP Flat; Carpet grade | • Limited to 1/2 the distance of Type 1 cable | | |
| **Type 9** | STP; Plenum grade | • Used under floors or in ceiling space | | |

## Important Cabling Considerations

**Installation Logistics**

- How easy is the cable to work with?

**Shielding**

- Is the area "noisy"?
- Do you need plenum grade cable => more expensive

**Crosstalk**

- Where data security is important this is a problem
- Power lines, motors relays and radio transmitters cause crosstalk

**Transmission Speed** (part of the bandwidth)

- Transmission rates are measured in Mbps
- 10 Mbps is common
- 100 Mbps is becoming common
- Fiber can go well over 100 Mbps but costs and requires experts to install.

**Cost**

- Distance costs you money

**Attenuation**

- Different cables can only transmit so far without causing too many errors

## Wireless Local Area Networks

- Used where cable isn't possible - remote sites; also when mobility is important.
- Use transceivers or access points to send and receive signals between the wired and wireless network.

**There are 4 techniques for transmitting data**

- **Infrared** transmission consists of four types;
  1. Line of sight
  2. Scatter: good within 100 ft.
  3. Reflective
  4. Broadband optical telepoint: used for multimedia requirements; as good as cable.
- **Laser** requires direct line-of-sight.
- **Narrow-band (single frequency) radio**
  - Cannot go through steel or load-bearing walls.
  - Requires a service handler.
  - Limited to 4.8 Mbps
- **Spread-Spectrum Radio**
  - Signals over a range of frequencies.
  - Uses hop timing for a predetermined length of time.
  - Coded for data protection.
  - Quite slow; Limited to 250 Kbps.

**Point to Point Transmission**

- Transfers data directly from PC to PC (NOT through cable or other peripherals)
- Uses a point-to-point link for **fast error-free transmission**.
- Penetrates objects.
- Supports data rates from 1.2 to 38.4 Kbps up to
  - 200 feet indoors or
  - 1/3 of a mile with line of site transmission.
- Also communicates with printers, bar code readers, etc.

**Multipoint Wireless Bridge**

- Provides a data path **between two buildings**.
- Uses spread-spectrum radio to create a wireless backbone up to **three miles.**

**Long-Range Wireless Bridge**

- Uses spread-spectrum technology to provide Ethernet and Token-Ring bridging for up to 25 miles.
- This costs less than T1, but T1 will transmit at 1.544 Mbps

**Mobile Computing**

- Uses wireless public carriers to transmit and receive using;
  - Packet-radio communication.

    Uplinked to satellite, broadcast only to device, which has correct address.
  - Cellular networks.

    **CDPD** same as phone, subsecond delays only, real time transmission, can tie into cabled network.
  - Satellite stations.

    Microwave, most common in USA, 2 X directional antennas, building to building, building to satellite
- Slow transmission rate: 8 Kbps - 19.2 Kbps

## Network Adapter Cards

The role of the network Adapter card is to:

- **Prepare data** from the computer for the network cable
- **Send the data** to another computer
- **Control the flow of data** between the computer and the cabling system

**NIC's** contain hardware and firmware (software routines in ROM) programming that implements the

- Logical Link Control and
- Media Access Control
- Functions of the Data Link layer of the OSI

**Preparing Data**

- Data moves along paths in the computer called a BUS - can be 8, 16, 32 bits wide.
- On network cable, data must travel in a single bit stream in what's called a serial transmission (b/c on bit follows the next).
- The **transceiver** is the component responsible for translating parallel (8, 16, 32-bit wide) into a 1 bit wide serial path.
- A unique network address or **MAC address** is coded into chips in the card
- Card uses **DMA** (Direct Memory Access) where the computer assigns memory space to the NIC
    - If the card can't move data fast enough, the card's buffer RAM holds it temporarily during transmission or reception of data

**Sending and Controlling Data**

The NICs of the two computers exchanging data agree on the following:

1. Maximum size of the groups of data being sent
2. The amount of data to be sent before confirmation
3. The time intervals between send data chunks
4. The amount of time to wait before confirmation is sent
5. How much data each card can hold before it overflows
6. The speed of the data transmission

**Network Card Configuration**

- **IRQ**: a unique setting that requests service from the processor.

| **IRQ #** | **Common Use** | **I/O Address** |
|---|---|---|
| IRQ 1 | Keyboard | |
| IRQ 2(9) | Video Card | |
| IRQ 3 | Com2, Com4 | 2F0 to 2FF |
| IRQ 4 | Com1, Com3 | 3F0 to 3FF |
| IRQ 5 | **Available** (Normally LPT2 or sound card) | |
| IRQ 6 | Floppy Disk Controller | |
| IRQ 7 | Parallel Port (LPT1) | |
| IRQ 8 | Real-time clock | |
| IRQ 9 | Redirected IRQ2 | 370 – 37F |
| IRQ 10 | **Available** (maybe primary SCSI controller) | |
| IRQ 11 | **Available** (maybe secondary SCSI controller) | |
| IRQ 12 | PS/2 Mouse | |
| IRQ 13 | Math Co-Processor | |
| IRQ 14 | Primary Hard Disk Controller | |
| IRQ 15 | **Available** (maybe secondary hard disk controller) | |

- **Base I/O port: Channel between CPU and hardware**
    - Specifies a channel through which information flows between the computer's adapter card and the CPU. Ex. 300 to 30F.

    - Each hardware device must have a different base I/O port
- **Base Memory address: Memory in RAM used for buffer area**
    - Identifies a location in the computer's RAM to act as a buffer area to store incoming and outgoing data frames. Ex. D8000 is the base memory address for the NIC.
    - Each device needs its own unique address.
    - Some cards allow you to specify the size of the buffer (16 or 32 k, for example)
- **Transceiver:**
    - Sometimes selected as on-board or external. External usually will use the AUI/DIX connector: Thicknet, for example
    - Use jumpers on the card to select which to use

## Data Bus Architecture

**The NIC must**

- Match the computer's internal bus architecture and
- Have the right cable connector for the cable being used
    - **ISA (Industry Standard Architecture)**: original 8-bit and later 16-bit bus of the IBM-PC.
    - **EISA (Extended Industry Standard Architecture):** Introduced by consortium of manufacturers and offers a 32-bit data path.
    - **Micro-Channel Architecture (MCA):** Introduced by IBM in its PS/2 line. Functions as either 16 or 32 bit.
    - **PCI (Peripheral Component Interconnect):** 32-bit bus used by Pentium and Apple Power-PC's. Employs plug and play.

## Improving Network Card Performance

- **Direct Memory Access (DMA):**
    - Data is moved directly from the network adapter card's buffer to computer memory.
- **Shared Adapter Memory:**
    - Network adapter card contains memory, which is shared with the computer.
    - The computer identifies RAM on the card as if it were actually installed on the computer
- **Shared System Memory:**
    - The network adapter selects a portion of the computer's memory for its use.
    - MOST common
- **Bus Mastering:**
    - The adapter card takes temporary control of the computer's bus, freeing the CPU for other tasks.
    - Moves data directly to the computer's system memory
    - Available on EISA and MCA
    - Can improve network performance by 20% to 70%
- **RAM Buffering:**
    - Ram on the adapter card acts as a buffer that holds data until the CPU can process it.
    - This keeps the card from being a bottleneck
- **On-board microprocessor:**
    - Enables the adapter card to process its own data without the need of the CPU

## Wireless Adapter Cards

- Used to create an all-wireless LAN
- Add wireless stations to a cabled LAN
- Uses a wireless concentrator, which acts as a transceiver to send and receive signals

**Remote-Boot PROMS (Programmable Read Only Memory)**

- Enables **diskless workstations** to boot and connect to a network.
- Used where security is important.

---------------------------------------------------------------------------------------------------------------------------

# Networking Essentials Notes - Section 2

## How a Network Functions

### The OSI Model

- International Standards Organization (ISO) specifications for network architecture.
- Called the Open Systems Interconnect or OSI model.
- Seven-layered model, higher layers have more complex tasks.
- Each layer provides services for the next higher layer.
- Each layer communicates logically with its associated layer on the other computer.
- Packets are sent from one layer to another in the order of the layers, from top to bottom on the sending computer and then in reverse order on the receiving computer.

### OSI Layers (Check out the OSI Model Summary Page) (All People Seem To Need Data Processing)

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

### Application Layer

- Serves as a window for applications to access network services.
- Handles general network access, flow control and error recovery.

### Presentation Layer

- Determines the format used to exchange data among the networked computers.
- Translates data from a format from the Application layer into an intermediate format.
- Responsible for protocol conversion, data translation, data encryption, data compression, character conversion, and graphics expansion.
- Redirector operates at this level.

### Session Layer

- Allows two applications running on different computers to establish use and end a connection called a Session.
- Performs name recognition and security.
- Provides synchronization by placing checkpoints in the data stream.
- Implements dialog control between communicating processes.

### Transport Layer

- Responsible for packet creation.
- Provides an additional connection level beneath the Session layer.
- Ensures that packets are delivered error free, in sequence with no losses or duplications.
- Unpacks, reassembles and sends receipt of messages at the receiving end.
- Provides flow control, error handling, and solves transmission problems.

### Network Layer

- Responsible for addressing messages and translating logical addresses and names into physical addresses.
- Determines the route from the source to the destination computer.
- Manages traffic such as packet switching, routing and controlling the congestion of data.

### Data Link Layer

- Sends data frames from the Network layer to the Physical layer.
- Packages raw bits into frames for the Network layer at the receiving end.
- Responsible for providing error free transmission of frames through the Physical layer.

### Physical Layer

- Transmits the unstructured raw bit stream over a physical medium.
- Relates the electrical, optical mechanical and functional interfaces to the cable.
- Defines how the cable is attached to the network adapter card.
- Defines data encoding and bit synchronization.

**The 802 Project Model**

- Defines Standards for the Data Link and Physical Layers.
- Network Adapter Cards
- WAN components
- Components used to create twisted-pair and coaxial cable networks.
- A crazy mnemonic for this table, but it works :-)
  **I L**ike **C**hanging **B**oxers **R**arely. **M**y **B**utt **F**eels **V**ery **S**exy **W**ith **D**enim

| | |
|---|---|
| 802.1 | Internet working |
| **802.2** | Division of Data Link Layer into sublayers<br>• LLC (Logical Link Control)<br>• Media Access Control (MAC) |
| **802.3** | CSMA/CD - **Ethernet** |
| 802.4 | Token Bus LAN (ARCnet) |
| **802.5** | **Token Ring** LAN |
| 802.6 | MAN (Metropolitan Area Network) |
| 802.7 | Broadband Technical Advisory Group |
| 802.8 | Fiber-Optic Technical Advisory Group |
| 802.9 | Integrated Voice/Data Networks |
| **802.10** | Network Security |
| 802.11 | Wireless Networks |
| **802.12** | **Demand Priority** Access Lan, 100 Base VG - AnyLAN |

**OSI Model Enhancements**

The bottom two layers - Data Link and Physical - define how multiple computers can simultaneously use the network without interfering with each other.

- Divides the Data-link layer in to the Logical Link Control and Media Access Control sublayers.
- **Logical Link Control**
  - Manages **error and flow control** and
  - Defines logical interface points called Service Access Points (SAP's). These SAP's are used to transfer information to upper layers
- **Media Access Control**
  - Communicates directly with the network adapter card and
  - Is responsible for delivering error-free data between two computers.
  - Categories
    - 802.3
    - 802.4
    - 802.5 and
    - 802.12 define standards for both this sublayer and the Physical layer

## Drivers

- A device driver is software that tells the computer how to drive or work with the device so that the device performs the job it's supposed to.
- Drivers are called
  Network Drivers, MAC drivers, NIC drivers.
- Provide communication between a network adapter card and the redirector in the computer.
- Resides in the Media Access Control sublayer of the Data Link layer. Therefore, the NIC driver ensures direct communication between the computer and the NIC
- The Media Access Control driver is another name for the network card device driver
- When installing a driver, you need to know these things
  - IRQ
  - I/O Port Address
  - Memory Mapped (Base Memory Address)
  - Transceiver Type

## Packets

- Data is broken down into smaller more manageable pieces called packets.
- Special control information is added in order to:
  - Disassemble packets
  - Reassemble packets
  - Check for errors

Types of data sent includes

- Can contain information such as messages or files.
- Computer control data and commands and requests.
- Session control codes such as error correction and retransmission requests.
- Original block of data is converted to a packet at the **Transport layer.**

**Packet Components**

- **Header**
  1. Alert signal to indicate packet is being transmitted
  2. Source address.
  3. Destination address.
  4. Clock synchronization information.
- **Data**
  1. Contains actual data being sent.
  2. Varies from 512 to 4096 bytes (4K), depending on the network
- **Trailer**
  1. Content varies by protocol.
  2. Usually contains a CRC.

**Packet Creation**

- Look at the example on pp. 201 - 204
- Begins at the Application layer where data is generated.
- Each layer subsequently adds information to the packet; the corresponding layer on the receiving machine reads the information.
- Transport layer breaks the data into packets and adds sequencing information needed to reassemble data at the other end => the structure of the packets is defined by the common protocol being used between the two computers.
- Data is passed through the Physical layer to the cable.

**Packet Addressing**

- Every NIC sees all packets sent on its cable segment but only interrupts the computer if the packet address matches the computer's address

- A broadcast type address gets attention of all computers on the network

## Protocols

- Protocols are rules and procedures for communication.

## How Protocols Work

**The Sending Computer**

- Breaks data into packets.
- Adds addressing information to the packet
- Prepares the data for transmission.

**The Receiving Computer (same steps in reverse)**

- Takes the packet off the cable.
- Strips the data from the packet.
- Copies the data to a buffer for reassembly.
- Passes the reassembled data to the application.

**Protocol Stacks (or Suites)**

- A combination of protocols, each layer performing a function of the communication process.
- Ensure that data is prepared, transferred, received and acted upon.

**The Binding Process**

- Allows more than one protocol to function on a single network adapter card. (e.g. both TCP/IP and IPX/SPX can be bound to the came card
- Binding order dictates which protocol the operating systems uses first.
- Binding also happens with the Operating System architecture: for example, TCP/IP may be bound to the NetBIOS session layer **above** and network card driver **below** it. The NIC device driver is in turn bound to the NIC.

**Standard Stacks**

- ISO/OSI
- IBM SNA (Systems Network Architecture)
- Digital DECnet
- Novell NetWare
- Apple AppleTalk
- TCP/IP

**Protocol types map roughly to the OSI Model into three layers:**

| | |
|---|---|
| **Application** Level Service Users | |
| | Application Layer |
| | Presentation Layer |
| | Session Layer |
| **Transport** Services | |
| | Transport Layer |
| **Network** Services | |
| | Network Layer |
| | Data Link Layer |
| | Physical Layer |

**Application Protocols**

Work at the upper layer of the OSI model and provide application to application interaction and data exchange.

**Examples:**

- APPC-IBM's peer to peer SNA protocol used on AS400's
- FTAM: an OSI file access protocol.

- X.400: international e-mail transmissions.
- X.500: file and directory services across systems.
- SMTP: Internet e-mail.
- FTP: Internet file transfer
- SNMP: Internet network management protocol.
- Telnet: Internet protocol for logging on to remote hosts.
- Microsoft SMB: client shells and redirectors.
- NCP: Novell client shells or redirectors.
- AppleTalk and AppleShare: Apple's protocol suite.
- AFP: Apple's protocol for remote file access.
- DAP (data access protocol): DECnet file access protocol.

**Transport Protocols**

These protocols provide communication sessions between computers and ensure data is moved reliably between computers.

**Examples:**

- TCP (transmission control protocol): Internet protocol for guaranteed delivery of sequenced data.
- SPX (sequenced packet exchange): Novell protocol suite.
- NWLink: Microsoft implementation of IPX/SPX.
- NetBEUI: establishes communications sessions between computers and provides the underlying data transport services.
- ATP, NBP: Apple's communication session and transport protocols.

**Network Protocols**

These provide link services

They also

- Handle
  - Addressing and routing,
  - Error checking and
  - Retransmission requests.
- Define rules for Ethernet or Token Ring.

**Examples:**

- IP (Internet Protocol): packet forwarding and routing.
- IPX: (Internetwork Packet Exchange): Novell's protocol for packet forwarding and routing.
- NWLink: Microsoft implementation of IPX/SPX.
- NetBEUI: Transport for NetBIOS sessions and applications.
- DDP (datagram delivery protocol): An AppleTalk data transport protocol.

## The IEEE protocols at the Physical Layer

**802.3 (CSMA /CD - Ethernet)**

- Logical bus network
- Can transmit at 10 Mbps
- Data is transmitted on the wire to every computer but only those meant to receive respond
- CSMA /CD protocol listens and allows transmission when the wire is clear

**802.4 (Token Passing)**

- Bus layout that used token passing
- Every computer receives all of the data but only the addressed computers respond
- Token determines which computer can send

**802.5 (Token Ring)**

- Logical ring network; physical set up as star network
- Transmits at 4 Mbps or 16 Mbps

- Token determines which computer can send

## Important Protocols

**TCP/IP**

- Provides communications in a heterogeneous environment.
- Routable, defacto standard for internetworking.
- SMTP, FTP, SNMP are protocols written for TCP/IP
- Disadvantages are size and speed.

**NetBEUI**

- NetBIOS extended user interface.
- Originally, NetBIOS and NetBEUI were tightly tied together but, NetBIOS has been separated out to be used with other routable protocols. NetBIOS acts as a tool to allow applications to interface with the network; by establishing a session with another program over the network
- NetBIOS operates at the **Session layer**.
- Small, fast and efficient.
- Compatible with most Microsoft networks.
- **Not routable** and compatible only with Microsoft networks.

**X.25**

- Protocols incorporated in a packet switching network of switching services.
- Originally established to connect remote terminals to mainframe hosts.

**XNS**

- Xerox Network System.
- Developed for Ethernet LANs but has been replaced by TCP/IP.
- Large, slow and produces a lot of broadcasts.

**IPX/SPX and NWLink**

- Used for Novell networks.
- Small and fast.
- Routable.

**APPC**

- Advanced Program to Program Communication
- Developed by IBM to support SNA.
- Designed to enable application programs running on different computers to communicate and exchange data directly.

**AppleTalk**

- Apple's proprietary protocol stack for Macintosh networks.

**OSI Protocol Suite**

- Each protocol maps directly to a single layer of the OSI model

**DECnet**

- Digital Equipment's proprietary protocol stack
- Defines communications over Ethernet, FDDI MAN's and WAN's.
- DECnet can also use TCP/IP and OSI protocols as well as its own protocols
- Routable.

## Putting data on the Cable

### <u>Access Methods</u>

### The 4 major methods

- **Carrier Sense Multiple Access Methods**
    1. **With collision detection (CSMA/CD)**
    2. **With collision avoidance (CSMA/CA)**
- **Token passing that allows only a singe opportunity to send data**

- **A Demand Priority method**
- **Carrier Sense Multiple Access with Collision Detection. (CSMA/CD)**
    1. Computer senses that the cable is free.
    2. Data is sent.
    3. If data is on the cable, no other computer can transmit until the cable is free again.
    4. If a collision occurs, the computers wait a random period of time and retransmit.
    - Known as a contention method because computers compete for the opportunity to send data. (Database apps cause more traffic than other apps)
    - This can be a slow method
    - More computers cause the network traffic to increase and performance to degrade.
    - The ability to "listen" extends to a 2,500 meter cable length => segments can't sense signals beyond that distance.
- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
    - In CSMA/CA, the computer actually broadcasts a warning packet before it begins transmitting on the wire. This packet eliminates almost all collisions on the network because each computer on the network does not attempt to broadcast when another computer sends the warning packet.
    - All other computers wait until the data is sent.
    - The major drawback of trying to avoid network collisions is that the network traffic is high due to the broadcasting of the intent to send a message.
- **Token Passing**
    - Special packet is passed from computer to computer.
    - A computer that wants to transmit must wait for a free token.
    - Computer takes control of the token and transmits data. Only this computer is allowed to transmit; others must wait for control of the token.
    - Receiving computer strips the data from the token and sends an acknowledgment.
    - Original sending computer receives the acknowledgment and sends the token on.
    - The token comes from the Nearest Active Upstream Neighbor and when the computer is finished, it goes to the Nearest Active Downstream Neighbor
    - Uses "beaconing" to detect faults => this method is fault tolerant
    - **NO contention => equal access to all computers on the network**
    - NO collisions
- **Demand Priority**
    0. 100 Mbps standard called 100VG-AnyLAN. "Hub- based".
    1. Repeaters manage network access by performing cyclical searches for requests to send from all nodes on the network. The repeater or HUB is responsible for noting all addresses, links and end nodes and verifying if they are all functioning. An "end node" can be a computer, bridge, router or switch.
    2. Certain types of data are given priority if data reaches the repeater simultaneously. If two have the same priority, BOTH are serviced by alternating between the two.

       Advantages over CSMA/CD
        1. Computers Uses four pairs of wires, which can send and receive simultaneously.
        2. Transmissions are through the HUB and are not broadcast to all other computers on the network.
        3. There is only communication between the sending computer, the hub and the destination computer.

**Other methods**

**Appletalk**

- The cabling system for an AppleTalk network is called **LocalTalk**.
- LocalTalk uses CSMA/CA
- AppleTalk has a dynamic network-addressing scheme.

  - During bootup, the AppleTalk card broadcasts a random number on the network as its card address. If no other computer has claimed that address, the broadcasting computer configures the address as its own. If there is a conflict with another computer, the computer will try to use different IP combinations until it finds a working configuration.

**ARCNet**

- ARCNet uses a token passing method in a logical ring similar to Token Ring networks.
- However, the computers in an ARCNet network do not have to be connected in any particular fashion.
  - ARCNet can utilize a star, bus, or star bus topology.
- Data transmissions are broadcast throughout the entire network, which is similar to Ethernet.
- However, a token is used to allow computers to speak in turn.
  - The token is not passed in a logical ring order because ARCNet does not use the ring topology; instead the token is passed to the next highest numerical station
  - Use DIP switches to set the number (the Station Identifier) of the workstations, which you want to be beside each other so the token is passed to the next computer efficiently.
- ARCNet isn't popular anymore => ARCNet speeds are a mere 2.5 Mbps.

**Most important ARCNet facts for you to know:**

- ARCNet uses RG-62 (93 ohms) cabling;
- it can be wired as a star, bus, or star bus; and
- it uses a logical-ring media access method.

## Summary Chart

| **Feature or Function** | **CSMA/CD** | **CSMA/CA** | **Token Passing** | **Demand Priority** |
|---|---|---|---|---|
| **Type of Communication** | Broadcast-based | Broadcast-based | Token-based | Hub-based |
| **Type of Access Method** | Contention | Contention | Non-contention | Contention |
| **Type of Network** | Ethernet | LocalTalk | Token Ring<br>ARCnet | 100VG-AnyLAN |

----------------------------------------------------------------------------------------------------------------------------

## *Networking Essentials Notes - Section 3*

# Network Architectures

**Ethernet**

- Baseband signaling.
- Linear or star-bus topology.
- Usually transmits at 10 Mbps with 100 Mbps possible.
- Uses CSMA/CD for traffic regulation.
- IEEE specification 802.3.
- Uses thicknet, thinnet or UTP cabling
- Media is passive => it draws power from the computer

**Ethernet Frames**

Ethernet breaks data into frames. A frame can be from 64 to 1,518 bytes long in total. The ethernet frame itself takes up 18 bytes, so the actual data can be from 46 to 1,500 bytes.

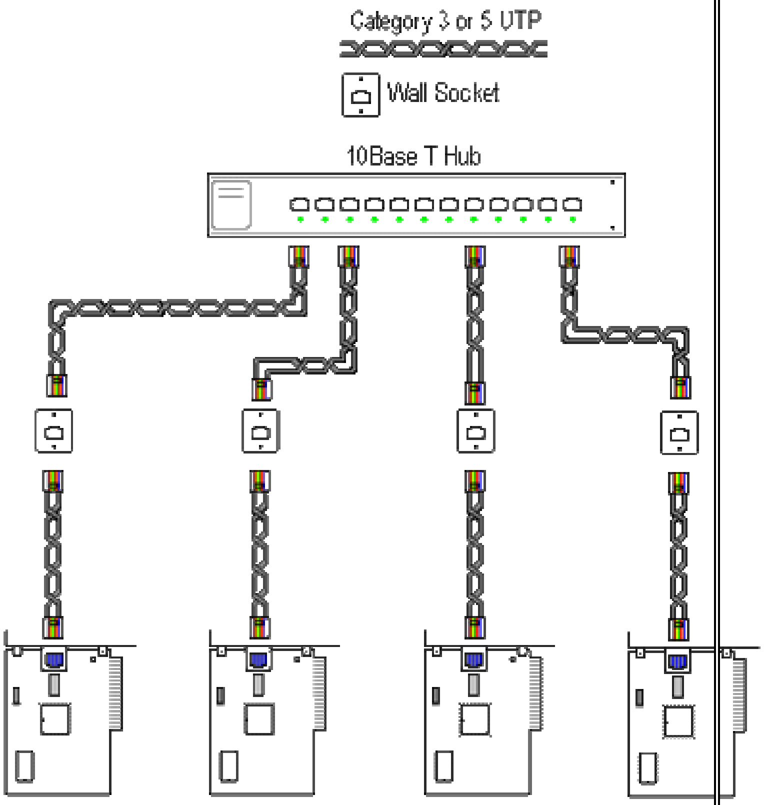
- **Preamble:** marks the start of a frame.
- **Destination and Source:** addressing information.
- **Type:** Identifies network layer protocol.
- **CRC:** error-checking data.

# Ethernet Topologies

## 10 Mbps Topologies

**10Base-T**

- **(10 = 10 Mbps; Base= Baseband; T = Twisted Pair)**
- 10 Mbps, baseband over **UTP**.
- Usually wired in a **physical star** with a hub or multiport repeater. Internally it uses a bus signaling system like other Ethernet configurations
- Maximum segment length **100 meters** (328 feet).
- Minimum between computers 2.5 meters (8 feet).
- 1024 nodes maximum on the LAN
- Category 3, 4 or 5 UTP.
- RJ-45 connectors, 4 twisted pair.
- Coaxial or Fiber backbone for larger LAN's



**10BaseT UTP NETWORK LAYOUT**

Limitations

- Maximum segment length of 100 Meters
- Hub to Hub or repeater to repeater links limited to 100 Meters

Rules

- Star topology
- 4 repeater/5 segment rule of 10Base5 is retained
- Only two nodes per segment are allowed

Cabling

- RJ-45 Connectors
- Category 3 UTP minimum, preferably Category 5

**10Base-2**

- **(10 = 10 Mbps; Base= Baseband; 2 = 2x 100 meters)**
- 10 Mbps, baseband over **thinnet**.
- **Uses bus topology**.
- Maximum segment length 185 meters (607 feet).
- Minimum between computers 0.5 meters (20 inches).
- Maximum of 30 computers per segment.
- Obeys 5-4-3 rules: Five segments, joined by four repeaters, 3 populated giving a total length of 925 meters (3035 feet).

**Physical Bus Cable Limits**

**10Base2 THIN ETHERNET NETWORK LAYOUT**

Limitations

- Maximum number of trunk segments = 5
- Maximum trunk segment length = 607 feet (185 meters)
- Maximum network trunk cable = 3035 feet (925 meters)
- Maximum number of stations on a trunk segment = 30

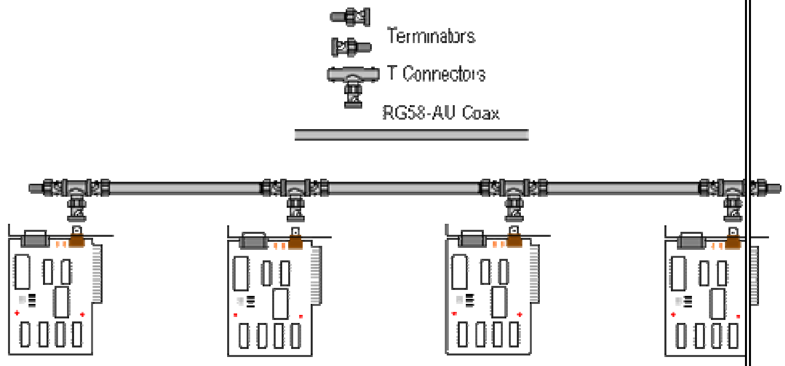
- Minimum distance between T connectors = 1.5 feet (0.5 meters)

Rules

- Each end of the trunk segment is terminated in 50-ohms
- One of the terminators is grounded
- Connector splices are kept to a minimum

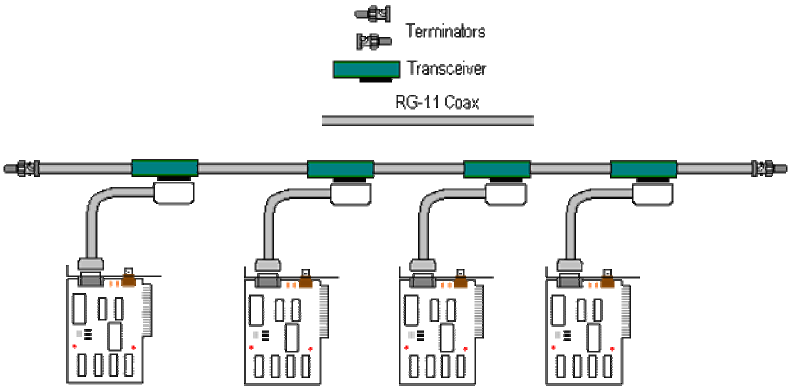
Cabling

- BNC-T type connectors
- RG58-AU 50-ohm cable, 0.2"
- **Note that you can't mix RG58 /AU and RG58 /U cable on the same network.**



**10Base-5**

- **(10 = 10 Mbps; Base= Baseband; 5 = 5 x 100 meters)**
- 10 Mbps, baseband over **thicknet**.
- Also called Standard Ethernet
- Designed to support a backbone for a large department or building. Transceivers attach to the thicknet cable and the cable AUI connector plugs into a repeater. The branching segments of thinnet plug into the repeater and connect to the computers on the network.
- **Uses bus topology**.
- Maximum segment length 500 meters.
- Minimum between transceivers 2.5 meters (8 feet)
- 100 computers per segment, 300 per network.
- Obeys **5-4-3 rule**: maximum distance can be extended to 2500 meters (8200 ft) using 4 repeaters and 3 populated segments.
- Transceiver is attached to main segment with a vampire tap.
- DIX or AUI connector is used to attach the transceiver to the network card. Maximum computer to transceiver distance is 50 meters. This distance is not included in the 5-4-3 calculation.



## 10Base-5 Summary

| | |
|---|---|
| Maximum segment length | • 500m (1640 ft)<br>• Typically used as backbone to connect Thinnet-based network. |
| Speed | 10 Mbps |
| Maximum taps | 100 |
| Maximum segments | • 5 |
| Maximum repeaters | • 4 |
| Maximum segment | • 3 |

| | |
|---|---|
| with nodes | • Due to attenuation, only 3 of 5 segments can actually contain network connection. Other 2 segments can be used to connect the network over long distance. |
| Maximum nodes per segment | 100 |
| Maximum nodes for network | 300 |
| Minimum distance between nodes | 2.5m (8 ft) |
| Maximum overall length with repeaters | 2.5 km |
| Maximum AUI drop cable length | 50m |

1. **10Base-F?**
    - **(10 = 10 Mbps; Base= Baseband; FL =fibre optic)**
    - Allows long cable runs between repeaters, like between buildings
    - Maximum segment length 2000 meters.
    - **10BaseFL** - Used for linking computers in a LAN environment.
    - **10BaseFP** - Used for linking computers with passive hubs from maximum cable distance up to 500m
    - **10BaseFB** - Used as a backbone between hubs.
    - Baseband signal over a fiber-optic cable.
    - Need concentrator (fiber-optic hub) ® Star wired (star topology) . Either active or passive
    - Long distance.
    - Very expensive. Difficult to install.
      Maximum segment length - 2000m
      Maximum segments- 1024
      Maximum segment with nodes- 1024
      Maximum nodes per segment- 1
      Maximum nodes per network- 1024
      Maximum hubs in a chain- 4

## 100 Mbps Topologies

- **100VG-AnyLAN (IEEE 802.12)**
    - 100 Mbps data rate.
    - Star topology over Category 3, 4 and 5 UTP.
    - Uses demand priority access.
    - Combines element of traditional Ethernet and Token Ring and supports Ethernet and token ring packets.
    - Faster than Ethernet
    - Demand priority access method => two priority levels, low and high
    - Intelligent hubs can filter individually addressed frames for enhanced privacy.
    - Expensive
    - Uses RJ-45.
    - Cable - require 4 pairs wire
        - Categories 3, 4 UTP- 100m
        - Category 5 UTP - 150m

        - Fiber-optic- 2000m
    - Uses star topology and defines how child hub can be connected to a parent hub to extend the network.
      Minimum length between nodes - 2.5m
      Maximum segments- 1024
      Maximum nodes per segment- 1
      Maximum nodes for network- 1024
- **100BaseT? (Fast Ethernet)**
    - Uses CSMA/CD on a star-wired bus.
    - There are 3 specifications:
        - 100BaseT4: Uses pair category 3, 4 or 5 UTP.
        - 100BaseTX: Uses 2-pair category 5 UTP or STP.
        - 100BaseFX: Uses 2-strand fiber-optic.

## Ethernet Frame types

**Ethernet 802.2** - NetWare 3.12 and 4.x - IEEE 802.3 standard compliance.
Includes field in Ethernet 802.3 and LLC (Logical Link Control)
**Ethernet 802.3** - NetWare 3.11 and before
Includes CRC
**Ethernet SNAP** (SubNetwork Address Protocol) - AppleTalk
**Ethernet II** - TCP/IP
**Segmentation**

- Can be performed with bridges or routers.
- Reduces traffic on network segments to increase performance.

## Token Ring

- IEEE 802.5 specification.
- Star wired ring topology (logical ring)
- Uses token passing access method.
- Can have higher transmission speeds than Ethernet
- It has larger frames than Ethernet => more can get transferred over the wire in any given time.
- Uses IBM STP Types 1, 2 and 3 cabling. (Can be UTP)
- Transmits at 4 and 16 Mbps. (16 Mbps cards will slow down to 4 Mbps if put on that kind of network, but the 4 Mbps cards can't speed up.
- Baseband transmission
- Data travels in one direction only
- Each computer acts as a unidirectional repeater
- Deterministic method of cable access. Computers cannot use the cable unless they have the token. Therefore, computers can't force their way onto the network like CSMA/CD (Ethernet)
- First computer online is assigned to monitor network activity.

**Token Ring Components**

- Multistation Access Units (MAU's)
- Multistation Access Units (MSAU's)
- Smart Multistation Access Units (SMAU's)
- Computers attach directly to the MSAU in a physical star to form a logical ring.
- Each MSAU has 10 connection ports ==> can support 8 clients with 2 ports for ring in and ring out.
- Each ring can have as many as 33 MSAU's
    - 70 computers with UTP
    - 260 computers with STP.
- Up to 12 MSAU's can connect to each other

- The MSAU can sense if a computer is down and then disconnect it from the ring => built-in fault tolerance
- Cabling
    - Most token ring systems use IBM type 3 cabling.
    - STP or UTP to a hub, IBM type 1,2,3 cable
        - Type 1: 101m from MSAU to PC
        - STP: 100m from MSAU to PC
        - UTP: 45m from MSAU to PC
        - Type 3: 150 feet from MSAU to PC
    - Token ring networks are well suited to fiber optic cable: data travels in only one direction in it.

**Here are some limitations of Token Ring:**

- The maximum number of workstations is 260 on Type 1 or fiber optic cable at 16 Mbps.
- The maximum number of workstations is 72 on Type 3 cable at 4 Mbps.
- The distance between MSAUs (Multistation Access Units) is 100 meters (Type 1 cabling) to 45 meters (Type 2 cabling).
- Each ring can have up to 33 MSAUs.
- Maximum distance of the ring is 4 kilometers with fiber optic cable.

**Token Ring and Ethernet Comparison**

Token Ring

- Can have higher transmission speeds than Ethernet
- Supports more computers on a single segment (up to 260)
- More expensive than Ethernet
- Harder to install than Ethernet
- Is more fault tolerant because of the beaconing process

## AppleTalk

- Local talk
    - CSMA/CA access method
    - 3 things happen when devices attached
        1. Device assigns itself an address randomly
        2. Device broadcasts the address to see if it's used
        3. If not, the device will use it the next time it's online again
    - Bus or tree
    - STP
    - Max. 32 devices
- Apple share
    - File server on an AppleTalk network
    - Divided into zones
- EtherTalk
    - 802.3
    - Allows protocols to run on Ethernet coaxial cable
- TokenTalk
    - 802.5
    - Allows Macintosh to connect to token ring network

## ARCnet

- IEEE 802.4 specification - almost
- Cable
    - Uses RG-62 (93 ohm) (most common) or
    - RG-59 (75ohm) coaxial cable.

    - Can also use UTP.
- Uses token passing on a star-bus topology.
- Token moves from computer to computer in numerical order.
- Transmits at 2.5 Mbps.
- ArcNet plus - 20 Mbps
- Connected by cable to hub
    - 93 ohm RG-62 A/U - 610m max., star
    - 93 ohm RG-62 A/U - 305m max., bus <= notice less distance on hub
    - RJ-11, RJ-45 UTP - max. 244m on star or bus
- Hubs can be
    - Passive => merely relay signal
    - Active => regenerate and relay signal
    - Smart => add diagnostic features, such as reconfiguration detection

**Here are some limitations of ARCNet:**

- Bus segment length for coaxial cable is a maximum of 1000 feet, with a limit of 8 workstations per coaxial segment.
- Bus segment length for twisted pair is a maximum of 400 feet, with a limit of 10 workstations per twisted-pair segment.
- There is a maximum of 255 workstations per network.
- Workstations can be located up to 600 feet from the active hub.
- The maximum distance from passive hubs to active hubs is 100 feet; the maximum distance between two active hubs is 2000 feet.
- The maximum distance allowed between workstations is 20,000 feet.
- There can be no more than four workstations on a passive hub, no more than 100 feet from a hub.
- Passive hubs cannot be connected to other passive hubs.

----------------------------------------------------------------------------------------------------------------------------

## Networking Essentials Notes - Section 4

# Network Operations

**Network O/S setup**

- 2 Major Types of Multitasking
    1. **Preemptive** - O/S can take control of the processor without the task's cooperation
        - Advantage of preemptive multitasking: CPU activity can be switched from local tasks to a network task
    2. **Non-preemptive (Cooperative)**
        - The task itself decides when to give up the processor
        - No other program can run until the non-preemptive program gives up the control of the processor
- **A Network O/S**
    - Ties together all the PCs and peripherals in the network
    - Coordinates the functions of all PCs and peripherals in a network
    - Provide security for and access to database and peripherals in a network
- **Client Software**
    - **Redirector**
        - Process of forwarding requests is done by a redirector
        - Intercepts requests in the PC
        - Determines if they should be left alone to continue in the local PC's bus or redirected out to the network to another server
    - **Designator**

        - A piece of software that manages the assignment of drive letters to both local and remote network resources or shared drives
            - e.g. share drive in other PC, alphabet as a designator, such as G:
        - When an association is made between a network resource and a local drive letter (mapping a drive), the designator takes care of remembering the path to the network resource.
        - When users or applications access the drive, the designator substitutes the resource's network address for the drive letter **before** the request is sent to the redirector.
    - **Peripherals**
        - Redirectors can send requests to either computers or peripherals (e.g. LPT1: or Com1 can refer to local OR network printers. Just give these ports a path to the network device.
- **Server Software**
    - Makes it possible to SHARE resources (data, printers, modems, etc.) with workstations
    - Provides network security as well
    - Makes sure two users don't use the same resources at the same time.
    - Managing users - create, privileges, remove users
    - Network management tools to track network behaviour
    - The server also
        - Provides logon authentication for users
        - Manages users and groups
        - Stores management, control, and auditing tools for network administration
        - Provides fault tolerance for protection of network integrity
- **Windows NT Server**
    - When installing you must
        - Name the domain or workgroup
        - Name the server
    - The 1st server installed in a domain must be installed as the primary domain controller (PDC), every domain is required to have one and only one PDC
    - A backup domain controller
        - Keeps a copy of the domain's directory database
        - Authenticates logons
        - Can be an application server
    - Configuring the network adapter card - default protocol for NT server is TCP/IP
    - TCP/IP installation
        - **IP address**
            - Logical 32-bit address to identity a TCP/IP host
            - Has two parts: network ID and host ID
        - **Subnet mask** - is used to mask a portion of the IP address so that TCP/IP can distinguish the network ID from the host ID - 255.255.0.0
        - **Default gateway** - (gateway = ROUTER) - For communication with a host on another network, an IP host must be configured with a route to the destination network otherwise only communication on the local segment
        - **Manual install** - assign IP address, subnet mask and the default gateway
        - **Automatic install** - DHCP (Dynamic Host Configuration Protocol) service,
            - When a DHCP server is configured on the network, clients that support DHCP (NT W/S & NT Server) can request TCP/IP configuration info (IP address, subnet mask, default gateway and so forth) from the DHCP server

## Networking Printing

- Here's the remote printing process:

1. The PC's redirector put the print job onto the network cable
2. Print server's network software takes the print job from the cable and send it into a queue with other items waiting from access to the shared printer

- UNC syntax: \\print_server_name\printer_share_name
- Network uses a **spool** (simultaneous peripheral operation on line)
- a spooler is a memory buffer in the print server's ram that holds print jobs If there are too many print jobs to fit into RAM, the overflow wait to print on the print server's hard drive.
- To share a printer you must:
  - Load printer drivers so the printer will print correctly
  - Create a share name for the printer
  - Identify a port so the redirector will know where to send the print job
  - Set the information and output parameters so the network operating system will know how to handle and format the print job.
- **PDL** - (Printer Description Language)
  - The printer uses the PDL to construct text and graphics to create the page image
  - PDLs are like blueprints
- You can manage the printer remotely

# E-mail

## E-mail system components

**X.400 Components**

- X.400 defines a whole range of protocols for transferring mail between e-mail servers.
- The Three main components are:
  - UA=> user agents
  - MTA => Message Transfer Agent
  - MTS => Message Transfer System
- E-mail Client (UA, User Agent) responsible for all user interaction such as
  - Reading and composing messages. It runs on the
- MTA (Message Transfer Agent) responsible for transferring messages from
  - One user's mailbox to another or to other MTAs for delivery.
- MTS
  - Responsible for transferring messages of all types for the UA that creates the message to the destination UA
- Directory services Personal Address Book, Global Address List.

**X.500**

- Is a set of directory services developed to help users in distributed networks locate users on other networks to whom they want to send messages
- Post Office (Information store, Message store) location of all user messages.

## E-mail protocols

### Transport/Delivery protocols

- **POP3** (Post Office Protocol) and **IMAP4** (Internet Mail Access Protocol)
  - Describes how e-mail client interact with email server.
- **SMTP** (Simple Mail Transport Protocol)
  - Describes how e-mail servers transfer email message to their intended recipients.
  - SMTP works with other e-mail programs to provide both a client and a server the function to send and receive e-mail messages.
  - Used on the Internet, UNIX and in the TCP/IP stack
- **MIME** (Multipurpose Internet Mail Extension)
  - Defines the method in which files are attached to SMTP messages.

- **MHS** (Message Handling Service) within NetWare
  - Similar to X.400 => one computer on the network is the MHS sever and it translates messages between computers that may be using different e-mail systems

**Directory Services**

- **LDAP** (Lightweight Directory Access Protocol)
- X.500 (see above)

**Messaging APIs**

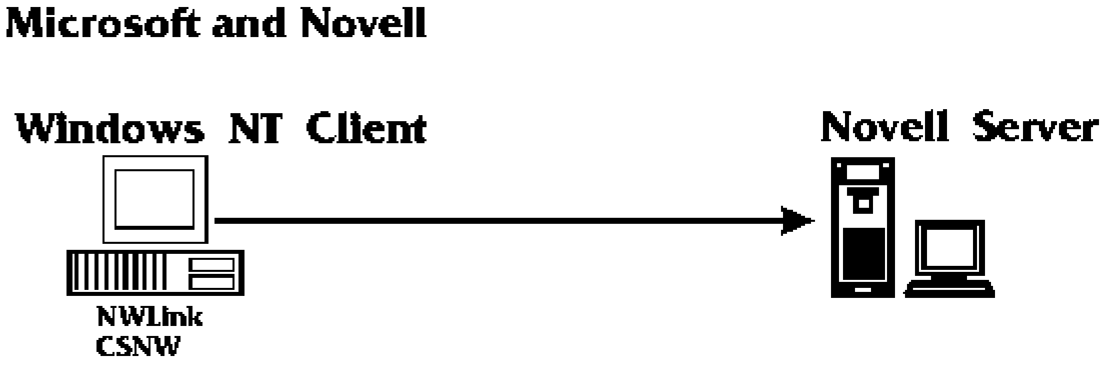
- **MAPI** (Message Application Programming Interface)
  - MS standard and incorporated throughout all of its office products.
- **VIM** (Vendor-Independent Messaging) from Lotus
- Scheduling

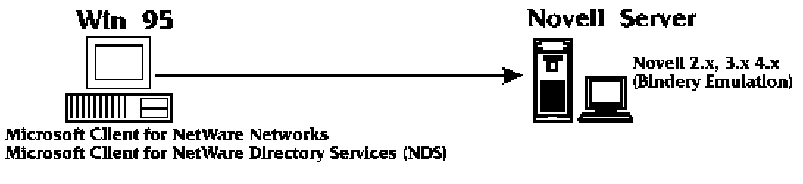
## Groupware

- eg. BBS, Internet news, Interactive conferences, MS Exchange, Lotus Notes.
  - Group discussions
  - Workflow automation.
  - Help Desk
  - Collective document creation.
  - Internal publishing

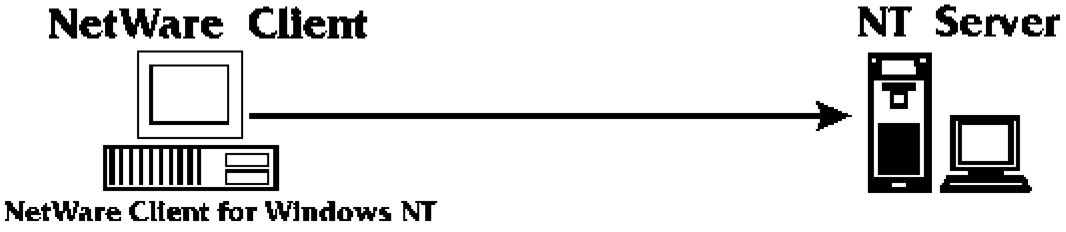
## Networks in a Multivendor Environments

- Server's O/S, the client's O/S & the redirector have to be compatible
- Different clients have to be able to understand each other to communicate. How can you get this done?
  - **The client solution**
    - Implement the appropriate redirector on the client, the redirector forwards your request to the appropriate destination
    - Use multiple redirectors to communicate with different clients

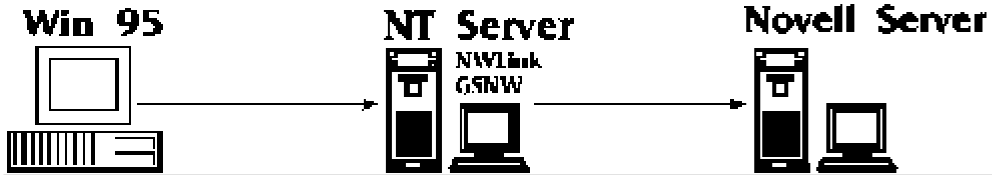



Win 95
Novell Server
Novell 2.x, 3.x 4.x
(Bindery Emulation)
Microsoft Client for NetWare Networks
Microsoft Client for NetWare Directory Services (NDS)

**Novell provides redirectors for MS-DOS, OS/2 and NetWare Client for Windows NT**



- o **The server solution**
    - ▪ Install a service on the service
    - ▪ E.g. to let MAC clients share network resources, add Service for Macintosh; Add FPNW for NetWare clients



## Client/Server Computing

- **Centralized Computing**
    - o Here the application operates on the server and all clients interact with the central application through client side interface terminals - dumb terminals
    - o When a client requests data from a database, the system moves all the data across the network to the client
    - o This causes the network to slow down for other clients
- **Client/Server Computing**
    - o The client computer makes a request and a computer acting as the server fulfills the request
    - o The client software uses the structured query language (SQL) to translate what the user sees into a request that the database can understand. **Therefore portions of the application reside on the client and some on the server.**
    - o Here's an example using SQL:
        - ▪ The client requests the data
        - ▪ The request is translated into SQL
        - ▪ The SQL request is sent over the network to the server
        - ▪ The database server carries out a search on the computer where the data exists
        - ▪ The requested records are returned to the client
        - ▪ The data is presented to the user
    - o The application (MS Access for example) is the client, or FRONT END
    - o The database server (SQL Server) is the server or BACK END
- **The Client**
    - o The front end client runs an application that
        - ▪ Presents an interface to the user (this doesn't reside on the server at all)
        - ▪ Formats requests for data
        - ▪ Displays data it receives from the server
    - o The user uses an on-screen form, called a search key to specify search requests
    - o The data can be presented to the user in various ways - different users access the same database to present information in a way that suits them

- Front End Tools
  - Query tools
  - User applications
    - e.g. Excel provides front end access to back end databases
  - Program development tools
    - Visual Basic is used to develop front-end tools to access backend data.

- **The Server**
  - Usually dedicated to STORING and MANAGING data
  - Most of the database activity happens on the server
    - Sorting
    - Data updates, additions, deletions, and protection
  - Stored procedures
    - Short, pre-written data-processing routines used by client applications
    - Stored on the server and can be used by any client
    - One stored process can be called by any number of client applications instead of having to incorporate the same routine into the code of each program
    - This means
      - Processing is done on the server instead of the client
      - Network traffic is reduced because one request begins a series of stored procedures on the server instead of many different requests
      - Security controls can prevent unauthorized use of some procedures
- **Client / Server Architecture**
  - Single server
  - Multiple servers with special tasks
    - Distributed server arrangements
      - Servers across a WAN link synchronized to endure they all have the same data in common
      - Data Warehouse. One server stores large amounts of data and forwards the most sought after data to intermediate servers that format the data. This off loads some of the processing from the intermediate servers that care contacted by clients (pic. p.409).

**Advantages of the Client / Server Environment**

3. Less network traffic => only results of query are sent over the network
4. The server is more powerful that the client and does most of the processing
5. More RAM and storage space on server means you don't have to spend as much MONEY on each client
6. Back end data is more easily secured and BACKED UP

---------------------------------------------------------------------------------------------------------------------

# Networking Essentials Notes - Section 5

## Network Support and Administration

- **Five management areas**
  1. User administration
  2. Resource management
  3. Configuration management
  4. Performance management
  5. Maintenance

# Managing Network Accounts

## User Administration

**Profiles**

- Used to structure a network environment for certain users
- This may be for security
- Can also control the user's logon environment
- Profiles include network connections and program items that appear when the user logs on. These can include:
  - Printer connections
  - Window sizes and positions
  - Icons
  - Mouse settings
  - The screen arrangement of colors
  - Screen savers

Rights apply to the system as a whole; permissions apply to a certain object.

**Types of Groups**

- **Local** Groups => things
- **Global** Groups => People
- **Special** Groups => internal system access -- Interactive, Network
- **Built-In** Groups => Administrator, Users, Operators Groups, Guests

---

**Administrator Responsibilities**

- Creating and Managing Accounts
- Security
- Training and supporting users
- Updating and implementing new software
- Archiving and data backup
- Preventing data loss
- Monitoring and regulating server storage space.
- Tuning the network
- Virus protection
- Troubleshooting
- Upgrading and replacing hardware
- Adding new computers

**Security Models**

Two different security models have evolved:

- Password-protected shares (**share-level**): each resource has a password
  - There are 2 levels of passwords: Read access and Full Control Access
- Access permissions (**user level**): Rights are assign on a user by user basis. More secure than the share level method.

**Other Methods of Network Security**

- **Auditing**
  - Audit records show the users that have accessed or attempted to access specific resources in security log
- **Diskless computers**
- **Data Encryption**
  - Data can't be stolen from the cable. When the data gets to the proper PC, a key, the code for deciphering encrypted data, decode the bits into understandable info.

- DES data encryption standard
- CCEP commercial COMSEC endorsement program

- **Virus protection**
    - The 4 standard measures to take when protecting against viruses:
        - Passwords to reduce the chance of unauthorized access
        - Well planned access and privilege assignments for all users
        - Profiles to structure the network environment
        - A policy determining what software can be loaded

## Managing Network Performance

- **Bottlenecks**
    - One device uses noticeably more CPU time than the others
    - These devices tend to become bottlenecks:
        - CPU,
        - Memory,
        - Network card,
        - Disk controllers,
        - Network media
- **Windows NT Performance Monitor**
    - View operations in both real time and recorded time for: processors, HDD, memory, network utilization, network as a whole
    - Can record the performance data
    - Send an alert to the network manager
    - Run utility that can adjust the system back into acceptable ranges
    - Establish a baseline of system management
- **Simple Network Management Protocol (SNMP)** - in a SNMP environment, programs called agents are loaded onto each managed device. The agents monitor network traffic and behaviour in these key network components in order to gather statistical data. This data is stored in a management information base (MIB)
- SNMP components include: hubs, servers, interface cards, routers and bridges
- The MIB collects data and the management program
    - Presents the information in the form of graphs or charts AND/OR
    - Sends the information to database program for analysis

**Total System Management**

- **Microsoft System Management Server (SMS)**
    - Centralized administration of computers in a WAN
    - **Inventory Management** - collects and maintains an inventory of hardware and software for each computer and stored in a SQL server database, info. like RAM, CPU, HDD size...
    - **Shared Application Management** - shared application can also distributed to a server for client's access
    - **Software Distribution**
        - SMS can install and configure new software or upgrade previously installed software
        - Also, it can run commands on the client such as virus scans
    - **Remote Control and Network Monitor** - provide help desk and diagnostics utilities to control remote client directly and access to remote client

## Avoiding Data Loss

**Tape Backup**

| Method | Description |
|---|---|
| Full Backup | Backs up and marks selected files, whether or not they have changed since the last backup |
| Copy | Backs up selected files without marking them as backed up |
| Incremental Backup | Backs up and marks selected files only if they have changed since the last backup |
| Differential Backup | Backs up selected files only if they have changed since the last backup w/o marking them as backed up |

**The difference between Incremental and Differential**

IF => **Incremental** Fast to backup; Slow to Restore => Marks files as backed up
=> **Differential** Slow to backup; Fast to Restore

**UPS**

- Power source to run the server for s short time
- Safe shutdown management service
- Prevent any more users from accessing the server
- Send an alert message to the network admin.
- Power is restored while UPS is active, the UPS will notify users that the power has returned

**Fault Tolerant Systems** - Windows NT supports Raid 0,1 and 5. For the exam, worry only about them.

- RAID 0 - **disk striping**
  - Disk striping divides data into 64k block and spreads it equally in a fixed rate and order among all disks in an array
  - NOT FAULT TOLERANT
- RAID 1 -
  - **Disk mirroring** - actually duplicates a partition and moves the duplication onto another physical disk
  - **Disk duplexing** - is a mirrored pair of disks with an addition disk controller on the second drive
  - The only RAID solution that can house the system files in the Boot partition
- RAID 4 - **disk guarding**
  - One drive is a dedicated parity drive, data is striped to multiple drives and then its parity sum is calculated, which is written to the dedicated parity drive
  - Works best for large block operations
- RAID 5 - **striping with parity**
  - Data is striped across multiple drives and then its parity sum is calculated, which is also striped across multiple drives (not a dedicated parity drive)
- **Sector sparing - hot fixing**
  - Automatically adds sector - recovery capabilities to the file system while the computer is running
  - If bad sectors are found during disk I/O, the fault tolerance driver will attempt to move the data to good sector and map out the bad sector - **only for SCSI, not ESDI or IDE**

---

## Networking Essentials Notes - Section 6

## Larger Networks

Some components can be installed which will increase the size of the network within the confines of the limitations set by the topology. These components can:

- Segment existing LANs so that each segment becomes its own LAN.
- Join two separate LANs.
- Connect to other LANs and computing environments to join them into a larger comprehensive network.

## Modems

- Modems share these characteristics
  - A serial (RS-232) interface
  - an RJ-11C telephone line connector
- Telephones use analog signal; computers use digital signal. A modem translates between the two
- **BAUD** refers to the speed of the oscillation of the sound wave on which a bit of data is carried over the telephone wire
- The BPS can be greater than the baud rate due to compression and encode data so that each modulation of sound can carry more than one bit of data is carried over the telephone line. For example, a modem that modulates at 28,000 baud can actually send at 115,200 bps => bps is the most important parameter when looking at throughput.
- There are 2 types of modems

**Asynchronous Communications (Async)**

- Use common phone lines
- Data is transmitted in a serial stream
- Not synchronized, no clocking device => no timing
- Both sending and receiving devices must agree on a start and stop bit sequence
- **Error control**
  - A parity bit is used in an error checking and correction scheme called parity checking
  - It checks to see if the # of bits sent = # of bits received
  - The receiving computer checks to make sure that the received data matches what was sent.
  - 25 % of the data traffic in async communications consists of data control and coordination
  - MNP (Microcom Network Protocol) has become the standard for error control
  - Later LAPM (Link Access Procedure for Modems) is used in V.42 modems (57,600 baud).
    - It uses MNP Class 4.
    - LAPM is used between two modems that are V.42 compliant
    - If one or the other modems is MNP 4 - compliant, the correct protocol would be MNP Class 4
- Communication performance depends on
  1. **Signaling or channel speed** - how fast the bits are encoded onto the communications channel
  2. **Throughput** - amount of useful information going across the channel
     - You can double the throughput by using compression. One current data compression standard is the MNP Class 5 compression protocol
     - V.42 bis is even faster because of compression.
       - bis => second modification
       - terbo => third, the bis standard was modified
- This is a good combination:
  0. V.32 signaling
  1. V.42 error control
  2. V.42bis compression

| Standard | BPS |
|---|---|
| V.22 bis | 2400 |
| V.32 | 9600 |
| V.32bis | 14,400 |

| | |
|---|---|
| V.32terbo | 19,200 |
| V.FastClass (V.FC) | 28,800 |
| V.34 | 28,800 |
| V.42 | 57,600 |

**Synchronous Communication**

- Relies on a timing scheme coordinated between two devices to separate groups of bits and transmit them in blocks known as frames
- NO start and stop bits =. a continuous stream of data because both know when the data starts and stops.
- If there's error, the data is retransmitted
- Some synchronous protocol perform the following that asynchronous protocols don't:
  1. Format data into blocks
  2. Add control info
  3. Check the info to provide error control
- The primary protocols in synchronous communication are:
  1. Synchronous data link control (SDLC)
  2. High-level data link control (HDLC)
  3. Binary synchronous communication protocol (bisync)
- Synchronous communications are used in almost all **digital** and network communications
- 2 types of telephone lines:
  1. **Public dial network lines** (dial-up lines) - manually dial up to make a connection
  2. **Leased (dedicated) lines** - full time connection that do not go through a series of switches, 56 Kbps to 45 Mbps

## Repeaters

- Repeaters
  - EXTEND the network segment by REGENERATING the signal from one segment to the next
  - **Repeaters regenerate BASEBAND, digital signals**
  - Don’t translate or filter anything
  - Is the least expensive alternative
  - **Work at the Physical layer of OSI**
- Both segments being connected **must use the same access method** e.g. an 802.3 CSMA/CD (Ethernet) LAN segment can't be joined to a 802.5 (Token Ring) LAN segment. Another way of saying this is the Logical Link Protocols must be the same in order to send a signal.
- BUT repeaters **CAN move packets from one physical medium to another**: for example can take an Ethernet packet from a thinnet coax and pass it on to a fiber-optic segment. Same access method is being used on both segments, just a different medium to deliver the signal
- They send every bit of data on => NO FILTERING, so they **can pass a broadcast storm** along from on segment to the next and back. So you want to use a repeater when there isn't much traffic on either segment you are connecting.
- There are limits on the number of repeaters, which can be used. The repeater counts as a single node in the maximum node count associated with the Ethernet standard [30 for thin coax].
- Repeaters also allow isolation of segments in the event of failures or fault conditions. Disconnecting one side of a repeater effectively isolates the associated segments from the network.
- Using repeaters simply allows you to extend your network distance limitations. It does not give you any more bandwidth or allow you to transmit data faster.
- Why only so many repeaters are allowed on a single network: "propagation delay". In cases where there are multiple repeaters on the same network, the brief time each repeater takes to clean up and amplify the signal, multiplied by the number of repeaters can cause a noticeable delay in network transmissions.

- It should be noted that in the above diagram, **the network number assigned to the main network segment and the network number assigned to the other side of the repeater are the same.**
- In addition, the traffic generated on one segment is propagated onto the other segment. This causes a rise in the total amount of traffic, so if the network segments are already heavily loaded, it's not a good idea to use a repeater.
- A repeater works at the Physical Layer by simply repeating all data from one segment to another.

**Summary of Repeater features**

- Increase traffic on segments
- Limitations on the number that can be used
- Propagate errors in the network
- Cannot be administered or controlled via remote access
- No traffic isolation or filtering

## Summary:

**A repeater**

- Connects two segments of similar or dissimilar media
- Regenerates the signal to increase the distance transmitted
- Functions in the Physical Layer of the OSI model
- Passes ALL TRAFFIC in both directions

- Use a repeater to improve performance by dividing the network segments, thus reducing the number of computers per segment (This is what it says in the book, but it doesn't make sense to me)
- Do NOT use a repeater when:
  - There is heavy network traffic
  - Segments are using different access methods
  - You need any kind of data filtering.

**Amplifiers** are just like repeaters, but generate a BROADBAND, analog signal. That analog signal can have different frequencies and carry both voice and data.

# Bridges

- Have all the abilities of a repeater
- **Bridges can**
  - Take an overloaded network and split it into two networks, therefore they can divide the network to isolate traffic or problems and reduce the traffic on both segments
  - Expand the distance of a segment
  - Link UNLIKE PHYSICAL MEDIA such as twisted-pair (10Base T) and coaxial Ethernet (10Base2)
  - **VERY IMPORTANT**: they can link UNLIKE ACCESS CONTROL METHODS, on different segments such as Ethernet and Token Ring and forward packets between them. Exam Cram says this is a Translation Bridge that can do this - not all bridges - but my observation is questions don't necessarily mention the distinction.
- Bridges work at the Data Link Layer of the OSI model => they don't distinguish one protocol from the next and simply pass protocols along the network. (use a bridge to pass NetBEUI, a non-routable protocol, along the network)
- Bridges actually work at the MEDIA ACCESS CONTROL (MAC) sublayer. In fact they are sometimes called Media Access Control layer bridges. Here's how they deal with traffic:
  - They listen to all traffic. Each time the bridge is presented with a frame, the source address is stored. The bridge builds up a table, which identifies the segment to which the device is located on. This internal table is then used to determine which segment incoming frames should be forwarded to. The size of this table is important, especially if the network has a large number of workstations/servers.

  - They check the source and destination address of each PACKET
  - They build a routing table based on the SOURCE ADDRESSES. Soon they know which computers are on which segment
  - Bridges are intelligent enough to do some routing:
    - if the destination address is on the routing table and is on the SAME SEGMENT, the packet isn't forwarded. Therefore, the bridge can SEGMENT network traffic
    - If the destination address is the routing table, and on a remote segment, the bridge forwards the packet to the correct segment
    - if the destination address ISN'T on the routing table, the bridge forwards the packet to ALL segments.
    - **BRIDGES SIMPLY PASS ON BROADCAST MESSAGES, SO they too contribute to broadcast storms and don't help to reduce broadcast traffic**
- **Remote Bridges**
  - Two segments are joined by a bridge on each side, each connected to a synchronous modem and a telephone line
  - There is a possibility that data might get into a continuous loop between LANs
  - The SPANNING TREE ALGORITHM (STA)
    - Senses the existence of more than one route
    - Determines which is the most efficient and
    - Configures the bridge to use that route
    - This route can be altered if it becomes unusable.
    - **Transparent bridges** (also known as spanning tree, IEEE 802.1 D) make all routing decisions. The bridge is said to be transparent (invisible) to the workstations. The bridge will automatically initialize itself and configure its own routing information after it has been enabled.
- **Comparison of Bridges and Repeaters**
  - **Bridges**
    - Regenerate data at the packet level
    - Accommodate more nodes than repeaters
    - Provide better network performance than repeaters because they segment the network
- **Implementing a Bridge**
  - It can be an external, stand-alone piece of equipment
  - Or be installed on a server
- **Summary from MOC:**
  - Bridges have all the features of a repeater
  - They connect two segments and regenerate the signal at the packet level
  - They function at the Data Link layer of the OSI model
  - Bridges are not suited to WANs slower than 56k
  - They cannot take advantage of multiple paths simultaneously
  - They pass all broadcasts, possibly creating broadcast storms
  - Bridges read the source and destination of each packet
  - They PASS packets with unknown destinations
  - Use Bridges to:
    - Connect two segments to expand the length or number of nodes on the network
    - Reduce traffic by segmenting the network
    - Connect
      - Unlike MEDIA (e.g. 10BaseT and 10Base2)
      - Unlike ACCESS CONTROL METHODS (Ethernet and Token Ring)

**The advantages of bridges are**

  - Increase the number of attached workstations and network segments

- Since bridges buffer frames, it is possible to interconnect different segments which use different MAC protocols
- Since bridges work at the MAC layer, they are transparent to higher level protocols
- By subdividing the LAN into smaller segments, overall reliability is increased and the network becomes easier to maintain
- **Used for non routable protocols like NetBEUI which must be bridged**
- Help localize network traffic by only forwarding data onto other segments as required (unlike repeaters)

**The disadvantages of bridges are**

- **The buffering of frames introduces network delays**
- Bridges may overload during periods of high traffic
- Bridges which combine different MAC protocols require the frames to be modified before transmission onto the new segment. This causes delays
- In complex networks, data is not sent over redundant paths, and the shortest path is not always taken
- Bridges pass on broadcasts, giving rise to broadcast storms on the network

**Sample Question:**
You want to connect an Ethernet network in one part of an office building to a Token-ring network down the hall. Both networks use NWLink IPX but must eliminate the IPX addressing and use only NetBEUI on both segments when they are joined. Which connectivity device do you choose which will allow the two networks to communicate, but at the same time reduce network levels.
Device should you use?

1. Repeater
2. Bridge
3. Router
4. Gateway

B - they are testing here to see if you know what a translation bridge can do.
**Some bridges can't connect different segments that use different media schemes, but a translation bridge can.** A translation bridge will also reduce network traffic because it can analyze packets based on MAC address and if it finds them to be from the same segment as the originating they are simply discarded instead of being passed on to a non-local segment. The bridge can do this using address information stored in its bridging table.

## Routers

- Determine the **best path** for sending data and filtering broadcast traffic to the local segment. They DON'T pass on broadcast traffic
- Work at the **Network layer** of OSI => they can switch and route packets across network segments
- They provide these functions of a bridge
  - Filtering and isolating traffic
  - Connecting network segments
- Routing table contains
  1. All known network addresses
  2. How to connect to other networks
  3. Possible paths between those routers
  4. Costs of sending data over those paths
  5. Not only network addresses but also media access control sublayer addresses for each node
- **Routers**
  - REQUIRE specific addresses: they only understand network numbers which allow them to talk to other routers and local adapter card addresses

  - Only pass Packets to the network segment they are destined for.
  - Routers don't talk to remote computers, only to other routers
  - They can segment large networks into smaller ones
  - They act as a safety barrier (firewall) between segments
  - They prohibit broadcast storms, because broadcasts and bad data aren't forwarded
  - Are slower than most bridges
  - Can join dissimilar access methods: a router can route a packet from a TCP/IP Ethernet network to a TCP/IP Token Ring network
- Routers don't look at the destination computer address. They only look at the NETWORK address and **they only pass on the data if the network address is known** => less traffic
- Routable protocols:
  - DECnet, IP, IPX, OSI, XNS, DDP (Apple)
  - Routable protocols have Network layer addressing embedded
- Non-routable protocols:
  - LAT, NetBEUI, DLC
  - Non-routable protocols don't have network layer addressing

### Choosing Paths

- Routers can choose the best path for the data to follow
- Routers can accommodate multiple active paths between LAN segments. To determine the best path, it takes these things into account:
  - If one path is down, the data can be forwarded over on alternative route
  - Routers can listen and determine which parts of the network are busiest.
  - It decides the path the data packet will follow by determining the number of hops between internetwork segments
- **OSPF (Open Shortest Path First)**
  - Is a link-state routing algorithm
  - Routes are calculated based on
    - # of hops
    - Line speed
    - Traffic
    - Cost
  - TCP/IP supports OSPF
- **RIP (Routing Information Protocol)**
  - RIP is the protocol used to determine the # of hops to a distant segment.
  - Uses distance-vector algorithm to determine routes
  - TCP/IP & IPX support RIP
- **NLSP (NetWare Link Services Protocol)**
  - is a link-state algorithm for use with IPX
- There are 2 types of routers
  - **Static** - manually setup and config the routing table and to specify each route
  - **Dynamic**
    - Automatic discovery of routers
    - Use information from other routers

## Distinguishing between Bridges and Routers

### Both bridges and routers

  - Forward packets between networks
  - Send data across WAN links
- **A Bridge**
  - **Recognizes the address of EACH computer on it's segment and forwards packets on the basis of the destination address**

  - Either recognizes the address or it doesn't, and forwards the packet accordingly
  - Forwards all broadcast messages to all ports, except to the port from which the broadcast message came. Every computer on every segment receives this broadcast
- **A Router**
  - Works at the NETWORK layer and thus takes more information into account when determining what to forward and where to forward it to.
  - Routers recognize the addresses of other routers and determine which packets to forward to which routers

**Multiple Paths-- important**

- **Bridges recognize ONE PATH between networks**
- **Routers can search between multiple paths and determine the best path at the moment**

**The 4 KEY pieces of information that distinguish bridges and routers:**

| Bridges | Routers |
|---|---|
| • Recognize the MAC sublayer addresses (i.e. the addresses of the network cards on its own segment) | • Routers recognize **network addresses** not individual computer addresses |
| • Forwards everything it doesn't recognize and<br>• Forwards all addresses it knows, but only out the appropriate port | • Routers filter addresses.<br>• It forwards particular protocols to particular addresses (other routers)<br>• If the router doesn't recognize a destination address, the packet is usually discarded |
| • Works with all protocols | • Only works with routable protocols<br>• Non-Routable = NetBEUI, DLC, LAT |

**Because they make path choices and filter out packets the segment doesn't need to receive they**

- Help lessen network congestion
- Conserve resources
- Boost data throughput
- Make data delivery more reliable

**Because is works at the network layer, a router can connect networks that use**

- Different architectures
- Different media access control methods -- for example, they can connect an Ethernet segment to a Token-Ring segment

Summary of Router features

- Use dynamic routing
- Operate at the protocol level
- Remote administration and configuration via SNMP
- Support complex networks
- The more filtering done, the lower the performance
- Provides security
- Segment networks logically
- Broadcast storms can be isolated
- Often provide bridge functions also
- More complex routing protocols used [such as RIP, IGRP, OSPF]

## Brouters

- Combine the best qualities of both bridges and routers

- First, a brouter checks to see if the protocol is routable or non-routable
- Route selected routable protocols.
- They can bridge non-routable protocols. Like a Bridge, they use the MAC address to forward to destination. They act like a router for one protocol and a bridge for all the others
- More cost effective than individual bridges and routers.
- SO, use a brouter when you have routable and non-routable protocols.

## Hubs

There are many types of hubs:

- **Passive hubs** are don't require power and are simple splitters or combiners that group workstations into a single segment
- **Active hubs** require power and include a repeater function and are thus capable of supporting many more connections.
- Intelligent hubs provide
    - Packet switching
    - Traffic routing

## Gateways

- The TRANSLATOR -- allows communications between dissimilar systems or environments
- A gateway is usually a computer running gateway software connecting two different segments. For example an Intel-based PC on one segment can both communicate and share resources with a Macintosh computer or an SNA mainframe. Use gateways when different environments need to communicate. One common use for gateways is to translate between personal computers and mainframes
- GSNW is a gateway to allow Microsoft clients using SMB to connect to a NetWare server using NCP.
- Gateways work at the Application --> Transport layer
- They make communication possible between different architectures and environments
- They perform protocol AND data conversion / translation.
- They takes the data from one environment, strip it, and re-package it in the protocol stack from the destination system
- They repackage and convert data going from one environment to another so that each environment can understand the other environment's data
- Gateway links two systems don't use the same
    1. Protocols
    2. Data formatting structure
    3. Languages
    4. Architecture
- **They are task specific** in that they are dedicated to a specific type of conversion: e.g. "Windows NT Server -> SNA Server Gateway"
- Usually one computer is designated as the gateway computer. This adds a lot of traffic to that segment
- **Disadvantages**
    - They slow things down because of the work they do
    - They are expensive
    - Difficult to configure
- Remember, gateways can translate
    - Protocols e.g. IPX/SPX --> TCP/IP
    - And data (PC --> Mac)
    - E-mail standards --> an e-mail gateway that translates on e-mail format into another (such as SMTP) to route across the Internet.

--------------------------------------------------------------------------------------------------------------------------------------

## Networking Essentials Notes - Section 7

# WAN Transmission

Communication between LANs over a WAN link will involve one of these technologies

- Analog
  - These use conventional telephone lines, with voice signaling (modem) technologies
- Digital
  - These use digital grade telephone lines, with digital technologies all the way
- Packet Switching
  - These use multiple sets of links between sender and receiver to move data

## Analog

- Dial-up line
  - Via public switched telephone network (PSTN)
  - Requires modems which are slow
  - Inconsistent quality of service
- Dedicated line
  - Fast
  - Reliable
  - Expensive
  - Service provider can implement **line conditioning** (a service that reduces delay and noise on the line, allowing for better transmissions) can make the leased lines even more reliable,

## Digital

- Digital Data Service (DDS) provide point-to-point synchronous communications at:
  - 2.4 Kbps
  - 4.8 Kbps
  - 9.6 Kbps or
  - 56 Kbps
- Guarantees full-duplex bandwidth by setting up a permanent link from each endpoint
- 99% error free
- **Doesn't requires modem, requires bridge or router through a device called a CSU/DSU**. This device translates standard digital signals a computer generates into bipolar digital signals used by synchronous communications
- Available in several forms:

| | # of T channels | Speed |
|---|---|---|
| DDS | | |
| T1 | 1 | 1.544 Mbps |
| T3 | 28 | 45 Mbps |
| T4 | 168 | 274.7 Mbps |
| Switched 56 | | 56 Kbps |

## T1

- Point to point transmission => no switching
- Uses two-wire pairs (1 pair to send, 1 to receive)
- Full-duplex signal at **1.544 Mbps**
- Used to transmit digital, voice, data and video signals

- Multiplexing - signals from different source are collected into a component called a multiplexer and fed into one cable 8,000 times a second
- A **T1 divides into 24 64 Kbps channels**. Subscribers can lease one 64 Kbps channel known as a Fractional T-1.
    - Each channel can transmit at 64 Kbps. This is called a DS-0
    - The whole 1.544 Mbps is known as DS-1
- Connecting a T1 line to your network is similar to a connecting a DDS or frame relay line. **You will need a T1-compatible CSU/DSU, and a bridge or router**. To distribute the T1's bandwidth between voice and data traffic, **you will need a multiplexer/demultiplexer to combine voice and data signals for transmission**, and separate them upon reception.

## T3

- Equivalent to 28 T-1 lines
- T3 and Fractional T-3 leased line service provides voice and data service from 6 Mbps to **45 Mbps**
- **REALLY expensive**
- T-1 uses copper wire, while T-3 uses fiber optic cables or microwave transmission equipment.

## Switched 56

- In reality, a Switched 56 line is nothing more than a circuit-switched version of a standard 56 Kbps DDS leased line. As customers pay only for connection time, resulting costs are usually significantly lower than those of a dedicated line.
- Is a LAN to LAN digital dial-up service
- 56 Kbps
- Used on demand => not dedicated => less expensive.
- Both ends must be equipped with a Switched 56 compatible CSU/DSU to dial-up another switched 56 site.

## Packet Switching

- Switching (as in switched connections) refers to finding a path for data transmission across a number of potential links between sender and receiver. On the other hand, analog and digital connections require a fixed connection to exist, at least for the duration of each communication session. Switching methods include both circuit switching and packet switching. Essentially, when data is received on an incoming line, the switching device must find an appropriate outgoing line on which to forward it. These switching devices are usually called routers, based on the functions they perform.
- Data package is broken into packers and each package is tagged with a destination address and other info.
- Relayed through stations in a computer network
- Data paths for **individual packets** depend on the best route at any given instant. The main point is that the small, individual packets are all take their own route to the destination, and an error in any one of them is easier to correct than a huge chunk of data
- These networks are sometimes called "any to any networks"
- Can use a virtual circuit
    - Logical connection between the sending computer and the receiving computer
    - Not actual cable, but bandwidth used on demand
    - Can use a **Switched Virtual Circuit** to establish a connection over a specific route.
    - **Permanent Virtual Circuits** allow the customer to pay for only the time that the line is used.

# Advanced WAN

## X.25

- Speed peaks at **64 Kbps** - Newer versions can be up to 2 Mbps

- A set of protocols incorporated in a packet-switching network
- Uses switches circuits and routes as available to provide the best routing at any particular time. The situation is always changing.
- Uses telephone lines - slow - MUCH error checking => this is a major disadvantage
- Synchronous packet-mode host or other device and the **public data network (PDN)** over a dedicated or leased-line circuit
- DTC/DCE interface
- **A PAD is also needed - Packet Assembler / Disassembler**
- And X.25 gateway is needed between the LAN and the Public Data Network
- See pic on p. 595.

## ISDN

- **Basic Rate (BRI)** is 3 data channels
  - 2 for 64 Kbps - 64 Kbps channels are known as B (Bearer) channels, carry voice, data or image
  - 1 for 16 Kbps - the 16 Kbps channel is D channel which carries signaling and link management data
  - This makes a total of 144 Kbps of bandwidth.
  - Basic rate is called 2B+D
  - **The two B channels can be used together for 128 Kbps data stream**
- **Primary Rate (PRI)** ISDN takes **the entire bandwidth of a T1 link** by providing
  - 23 B Channels at 64 Kbps
  - 1 D Channel at 64 Kbps
- ISDN is a **dial-up service**, not dedicated, not bandwidth on demand
- Right now, ISDN is about 5 times as fast as the fastest modem
- You can transmit voice and data with ISDN

## Frame Relay

- Like X.25 Frame Relay is a packet-switching technology
- Uses **variable-length** packets
- It establishes a logical path that's **called a Permanent Virtual Circuit** (PVC) between end-points. PVCs take fixed paths, so a PVC is the equiva-lent of a dedicated line in a packet-switched network. The path is fixed, so network nodes don't have to waste time calculating routes. Frame relay connections operate at speeds **between 56 Kbps and 1.544 Mbps** because they use PVCs, and there is no built-in error checking.
- Again, the PVC transmits at Data Link Layer. Because Frame Relay uses a PVC, the entire path from end to end is known => **faster because no fragmentation or reassembly or best path routing is needed**
- Can supply **bandwidth on demand**
- Over digital leased-line
- Frame relay connections to a network **require you to use a frame relay-compatible CSU/DSU** to create the physical connection to the WAN, and a **router or bridge** to move traffic from the LAN to the WAN, and the WAN to the LAN, as needed.
- In summary, Frame relay costs less than a dedicated line or an ATM connection and **provides data transmission rates of up to 1.544 Mbps over conventional or fiber optic media.**

## ATM

- **Fixed-sized packets** over broadband and Baseband LANs or WANs
- **155 Mbps to 622 Mbps or more**
- ATM can accommodate **voice, data, fax, real-time video,** CD-quality audio, imaging, and multimegabit data transmission.

- ATM is like frame relay because **it assumes noise-free lines and leaves error checking to devices at either end of a connection.** Also, **ATM creates a PVC between two points across an ATM network** as part of setting up a communication session.
- ATM Technology
  - Broadband cell relay method that transmit data in **53-byte cells rather than in variable-length frames. This uniform cell size is a big factor for speed => uniformity is easier to switch, route and buffer.**
  - Cell consists of 48 bytes of application info and 5 bytes of ATM header data => a consistent uniform package
- In theory, up to 1.2 Gigabits per second, but can transmit normally at 155 Mbps
- Can be used in LANs and WANs
- Hardware like routers, bridges have to be ATM compatible
- Switches are multiport hubs
- Any media type is OK
  - Media recommended
    - T3 (45 Mbps)
    - FDDI (100 Mbps)
    - Fiber channel (155 Mbps)
    - OC3 SONET (155 Mbps)
- ATM can even interface with frame relay and X.25.

**About Optical Carrier Levels, T-Carrier Rates, And More**
The Optical Carrier rating level for standard ATM technologies is cus-tomarily abbreviated as OC-n, where n is a multiplier applied to the basic OC level 1 rate (OC-1) of 51.84 Mbps. OC-1 describes the basic transmission rate for SONET communications. Table 10.1 (seen later in this chapter) summarizes most of the WAN service types that we cover in this chapter, along with their common abbreviations, basic characteristics, maximum throughput rates, and associated transmission technologies. - *Exam Cram* p. 197

## Fiber Distributed Data Interface (FDDI)

- 100 Mbps token passed ring network that uses Fiber optic cable
- Used for Metropolitan Area Networks (MAN) to connect within the same city so this isn't really a WAN technology
- 100 km (62 miles) max. Length => not really a WAN technology
- FDDI **uses fiber optic cable** to serve as
  - "Backend network" that handle file transfer
  - Serve as a backbone for other low capacity LANs
  - LANs that require large bandwidth
    - Video
    - CAD
    - CAM
- **Token Passing**
  - Not the same as token passing in 802.5
  - Here a computer can transmit as many frames as it can produce within a predetermined time before letting the token go. When it is finished transmitting, it lets the token go.
  - Because the computer releases the token when it's finished, there may be several frames on the ring at once.
  - FDDI is not like a regular Token Ring network because **more than one computer at a time can transmit a token so that multiple tokens can circulate on the ring at any one time**.
  - This is why FDDI is faster than regular Token Ring 802.5 => 802.5 only allows one token at a time to transmit.

- **Topology**
    - Dual-ring
        - **Primary ring** is for traffic; a redundant **second ring** for backup
        - When the primary ring breaks down, the secondary ring reconfigures itself and flows in the opposite direction
        - REDUNDANCY is one of the key features of this technology.
    - **500 computers max.**
    - More than one computer can transmit at a time - **they share the bandwidth;** for example, when 10 computers transmit, each does so at 10 Mbps
    - There must be a repeater every 2 Kms or less
    - Computers connected to both rings are CLASS A stations and help to reconfigure the network if the first ring fails. CLASS B stations are only connected to the one, primary ring.
    - FDDI can have point-to-point links to a hub => it can be set up using a star ring topology
- **Beaconing**
    - All computers on an FDDI network are responsible for monitoring faults in the network
    - A computer that detects a fault sends a signal called a BEACON onto the network. If it sees it's upstream neighbour is sending a beacon it stops. This goes on until the only computer sending a beacon is the one directly downstream from the faulty computer. This process stops when a beaconing computer receives its own beacon => this means the beacon made it around the ring
- **Media**
    - FDDI uses fiber-optic. This means
        - Immune to electromagnetic interference
        - **Secure because fiber optic doesn't emit a signal that can be monitored and cannot be tapped**
        - Able to transmit long distances before needing a repeater
    - FDDI on copper wire is called CDDI => can be done, but it has FAR less distance

## Synchronous Optical Network (SONET)

- SONET is a fiber optic WAN technology used to deliver voice, data, and video at speeds in multiples of 51.84 Mbps
- The **basic OC-1 level specifies a data rate of 51.84 Mbps**, and is based on the DS1 basic rate defined for SONET. T**he most common level is OC-3 or 3 x 51.84 Mbps or 155.52 Mbps**. OC-3 is the most common SONET implementation in use today, even though the specification defines OC-48 at 2.48 Gbps.
- Uses fiber-optic
- Summary: **SONET is a fiber optic WAN technology used to deliver voice, data, and video at speeds up to 622 Mbps, and beyond.**

## Switched Multimegabit Data Service (SMDS)

- Switching service that provides data transmission in the range between 1.544 Mbps (T1 or DS1) to 45 Mbps (T3 or DS3).
- Connectionless service that, like ATM, uses fixed-length 53 bytes cells.
- Like ATM and frame relay, it provides no error checking, leaving that up to devices at the connection points.
- IEEE 802.6 (MAN) specification.
- is a dual bus topology that forms a ring that is not closed

## Other WAN Tidbits:

- E1 (European Trunk Line) is the T-1 digital equivalent
- The transmission rate is 2.048 Mbps
- See table p. 199 Exam Cram for other tidbits, most of which have been noted here.

# Network Troubleshooting

**Planning**

- Prevention and a proactive program of preventative maintenance are the best approaches to avoid problems.
- Policies and procedures should be determined during the network planning stages and should include;
    - Backing up the network.
    - Planning security.
    - Standardization of hardware and software.
    - Upgrade maintenance.
    - Documentation which may include;
        - Map of the network
        - Server information and backup schedules
        - Software information
        - Telephone numbers of vendors and tech support
        - Copies of service agreements
        - Record of problems and solutions

**Network Utilities**

- The ISO identifies five areas of network management;
    1. Accounting management
    2. Configuration management
    3. Fault management
    4. Performance management
    5. Security management
- Network Monitoring
    - Can be performed with Performance Monitor in NTServer.
    - A baseline should be established under normal conditions for future reference.

**Troubleshooting Methodology**

1. Set the problem's priority.
2. Identify the problem's symptoms.
3. Develop a list of possible causes.
4. Test to isolate the cause.
5. Study the results of the test to identify a solution.

# Tools

- **Digital Volt Meter (DVM)**
    - Another name is a Volt /Ohm Meter
    - Checks for resistance on cables, terminators and barrel connectors
        - Cables and barrel connectors should provide 0 resistance
        - Terminators in 10Base2 and 10Base5 networks should provide 50 ohms of resistance
    - Use as a continuity checker for cables.
    - A continuity check can reveal a short where:
        - Two parts of the same cable are exposed and touching
        - Part of cable is touching another conductor such as metal surface
- **Time-Domain Reflectometer (TDR)**
    - Sends sonar-like pulses down the cable to identify any kind of a break, short or imperfection that might affect performance
    - Can locate a break within a few feet of the actual separation in the cable
- **Advanced Cable Testers**
    - Work at OSI layers 2, 3, and 4 and can display more complex information.
    - Can indicate if a particular cable or NIC is causing problems

  - Can display:
    - Message and error frame counts
    - Excess collisions
    - Congestion errors
    - Beaconing
- **Oscilloscopes**
  - Measures signal voltage per unit of time
  - Can identify
    - Breaks,
    - Shorts,
    - Bends
    - Opens (breaks in the cable)
    - And attenuation data.
- **Network Monitors**
  - Software that tracks all or part of network traffic.
- **Protocol Analyzers**
  - Can perform packet capture, decoding and transmission in **real-time**.
  - Most useful network analysis tool.
  - They look inside the packet to identify problems
  - They have a TDR in them
  - They can
    - Identify the most active computers
    - Identify computers sending error-filled packets
    - Identify, view and filter certain types of packets
    - Help analyze network trends
    - Check various components, connections by generating test packets
    - Set up alerts like Performance Monitor

**Support Resources**

- Microsoft TechNet
- BBS's
- User Groups
- Periodicals
- Internet
- Microsoft Network

**Common Troubleshooting Situations**

- Cable and other physical layer problems.
- Power fluctuations.
- Upgrades
- Changes in client computer configuration.
- Server crashes.
- Poor network performance resulting from some change or user application.

---------------------------------------------------------------------------------------------------------------------------

# Networking Essentials Notes - Section 8

## OSI Model Layers

| Layer | Function | Protocols | Network Components |
|---|---|---|---|
| **Application**<br>**User Interface** | • Used for applications specifically written to run over the network<br>• Allows access to network services that support applications;<br>• Directly represents the services that directly support user applications<br>• Handles network access, flow control and error recovery<br>• Example apps are file transfer, e-mail, NetBIOS-based applications | DNS; FTP; TFTP; BOOTP; SNMP; RLOGIN; SMTP; MIME; NFS; FINGER; TELNET; NCP; APPC; AFP; SMB | Gateway |
| **Presentation**<br>**Translation** | • Translates from application to network format and vice-versa<br>• All different formats from all sources are made into a common uniform format that the rest of the OSI model can understand<br>• Responsible for protocol conversion, character conversion, data encryption / decryption, expanding graphics commands, data compression<br>• Sets standards for different systems to provide seamless communication from multiple protocol stacks<br>• Not always implemented in a network protocol | | Gateway<br>Redirector |
| **Session**<br>**"Syncs and sessions"** | • Establishes, maintains and ends sessions across the network<br>• Responsible for name recognition (identification) so only the designated parties can participate in the session<br>• Provides synchronization services by planning check points in the data stream => if session fails, only data after the most recent checkpoint need be transmitted<br>• Manages who can transmit data at a certain time and for how long<br>• Examples are interactive login and file transfer connections, the session would connect and re-connect if there was an interruption; recognize names in sessions and register names in history | NetBIOS<br>Names Pipes<br>Mail Slots<br>RPC | Gateway |
| **Transport**<br>**Packets; flow control & error-handling** | • Additional connection below the session layer<br>• Manages the flow control of data between parties across the network<br>• Divides streams of data into chunks or packets; the transport layer of the receiving computer reassembles the message from packets<br>• "Train" is a good analogy => the data is divided into | TCP, ARP, RARP; SPX<br>NWLink<br>NetBIOS / NetBEUI<br>ATP | Gateway<br>Advanced Cable Tester<br>Brouter |

| | | | |
|---|---|---|---|
| | identical units<br>• Provides error-checking to guarantee error-free data delivery, with on losses or duplications<br>• Provides acknowledgment of successful transmissions; requests retransmission if some packets don't arrive error-free<br>• Provides flow control and error-handling | | |
| **Network**<br>**Addressing; routing** | • Translates logical network address and names to their physical address (e.g. computername ==> MAC address)<br>• Responsible for<br>o Addressing<br>o Determining routes for sending<br>o Managing network problems such as packet switching, data congestion and routing<br>• If router can't send data frame as large as the source computer sends, the network layer compensates by breaking the data into smaller units. At the receiving end, the network layer reassembles the data<br>• Think of this layer stamping the addresses on each train car | **IP**; ARP; RARP, ICMP; RIP; OSFP; IGMP;<br>**IPX**<br>NWLink<br>NetBEUI<br>OSI<br>DDP<br>DECnet | Brouter<br>Router<br>Frame Relay Device<br>ATM Switch<br>Advanced Cable Tester |
| **Data Link**<br>**Data frames to bits** | • Turns packets into raw bits 100101 and at the receiving end turns bits into packets.<br>• Handles data frames between the Network and Physical layers<br>• The receiving end packages raw data from the Physical layer into data frames for delivery to the Network layer<br>• Responsible for error-free transfer of frames to other computer via the Physical Layer<br>• This layer defines the methods used to transmit and receive data on the network. It consists of the wiring, the devices use to connect the NIC to the wiring, the signaling involved to transmit / receive data and the ability to detect signaling errors on the network media | **Logical Link Control**<br>• Error correction and flow control<br>• Manages link control and defines SAPs<br>802.1 OSI Model<br>802.2 Logical Link Control<br>**Media Access Control**<br>• Communicates with the adapter card<br>• Controls the type of media being used:<br>802.3 CSMA/CD (Ethernet)<br>802.4 Token Bus (ARCnet)<br>802.5 Token Ring<br>802.12 Demand Priority | Bridge<br>Switch<br>ISDN Router<br>Intelligent Hub<br>NIC<br>Advanced Cable Tester |
| **Physical**<br>**Hardware; raw** | • Transmits raw bit stream over physical cable<br>• Defines cables, cards, and physical aspects | IEEE 802<br>IEEE 802.2 | Repeater<br>Multiplexer |

| | | | |
|---|---|---|---|
| **bit stream** | • Defines NIC attachments to hardware, how cable is attached to NIC<br>• Defines techniques to transfer bit stream to cable | ISO 2110<br>ISDN | Hubs<br>• Passive<br>• Active<br>TDR<br>Oscilloscope<br>Amplifier |

------------------------------------------------------------------------------------------------------------------------

### Networking Essentials Notes - Section 9

## Networking Essentials - Memory Sheet

## Cables and Stuff

| Type | Cable Type | Length (meters) | Connector | Nodes Per Segment | Nodes Per Network |
|---|---|---|---|---|---|
| 10BaseT | | | | | |
| 10Base2 | | | | | |
| 10Base5 | | | | | |
| 10BaseFL | | | | | |
| 100BaseT4 | | | | | |
| 100BaseTX | | | | | |
| 100Base FX | | | | | |
| 100VG-AnyLan | | | | | |

| UTP Category | Mbps | Type | | Length | Connector |
|---|---|---|---|---|---|
| Category 1 | | Voice | Telephone cable | | |
| Category 2 | | Data | 4 twisted-pairs | | |
| Category 3 | | Data | 4 twisted-pairs - 3 twist per foot | | |
| Category 4 | | Data | 4 twisted-pairs | | |
| Category 5 | | Data | 4 twisted-pairs of copper wire | | |

| **Coaxial Cable** | | Ohms |
|---|---|---|
| RG-8 and RG-11 | | |
| **RG-58 Family** | | |
| RG-58 /U | | |
| RG-58 A/U | | |
| RG-58 C/U | | |
| RG-59 | | |
| RG-62 | | |

## IRQ & Cables

| IRQ # | Common Use | I/O Address |
|---|---|---|
| IRQ 1 | | |
| IRQ 2(9) | | |
| IRQ 3 | | ______________ |
| IRQ 4 | | ______________ |
| IRQ 5 | | |
| IRQ 6 | | |
| IRQ 7 | | |
| IRQ 8 | | |
| IRQ 9 | | ______________ |
| IRQ 10 | | |
| IRQ 11 | | |
| IRQ 12 | | |
| IRQ 13 | | |
| IRQ 14 | | |
| IRQ 15 | ______________________________________________ | |

**What four things do you need to configure for an adapter card install?**

1
2
3
4

**IBM Cabling**

| | | | |
|---|---|---|---|
| Type 1 | | 2-pair 22AWG | Used for computers and MAU's. |
| Type 2 | | 2-pair 22AWG<br>+ pair 26 AWG for voice | |
| Type 3 | | 4 solid, unshielded twisted pair 22 or 24 AWG | |
| Type 5 | | 2 fibers | Industry standard |
| Type 6 | | 2-pair 26 AWG | |
| Type 8 | | 2-pair 26 AWG | Limited to 1/2 the distance of Type 1 cable |
| Type 9 | | 2 STP cables | |

**802 Project Model**

| | |
|---|---|
| 802.1 | |
| 802.2 | |
| 802.3 | |
| 802.4 | |
| 802.5 | |
| 802.6 | |
| 802.7 | |
| 802.8 | |
| 802.9 | |
| 802.10 | |
| 802.11 | |
| 802.12 | |
| | |

## Access Methods

| Feature or Function | CSMA/CD | CSMA/CD | Token Passing | Demand Priority |
|---|---|---|---|---|
| Type of Communication | | | | |
| Type of Access Method | | | | |
| Type of Network | | | | |