Networking Essentials (DEVICES)

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:
    1. V.32 signaling
    2. V.42 error control
    3. 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.

Network Bridge

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

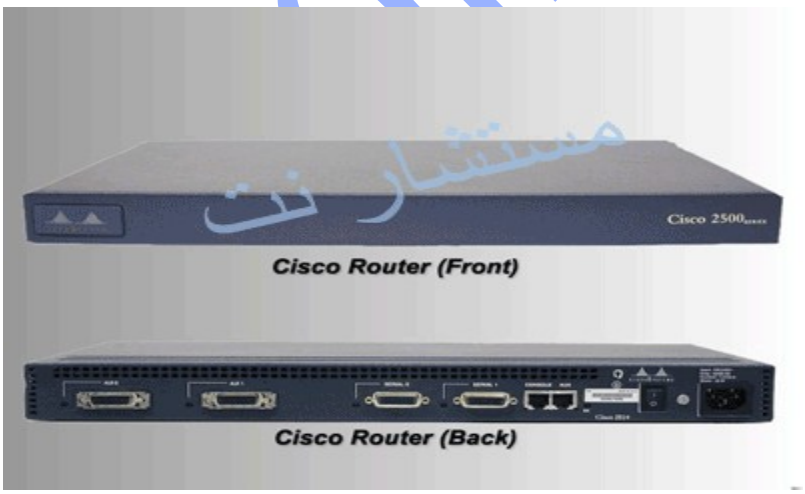
- increase the number of attached workstations and network segments
- since bridges buffer frames, it is possible to interconnect different segments which use different MAC protocols
- since bridges work at the MAC layer, they are transparent to higher level protocols

- 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

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 • forwards all addresses it knows, but only out the appropriate port	• routers filter addresses. • It forwards particular protocols to particular addresses (other routers) • if the router doesn't recognize a destination address, the packet is usually discarded
• works with all protocols	• only works with routable protocols • 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

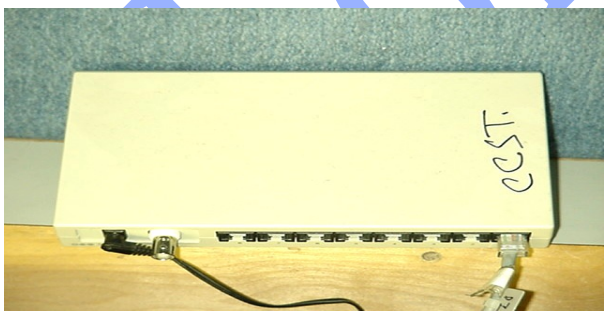
- Combine the best qualities of both bridges and routers
- First, a brouter checks to see if the protocol is routable or non-routable
- Route selected routable protocols.
- They can bridge non-routable protocols. Like a Bridge, they use the MAC address to forward to destination. They act like a router 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

: HUB



Switches: Switch is a layer 2 and multi-port device. Switch provides similar functions as a hub or a bridge but has more advanced features that can temporarily connect any two ports together. It contains a switch matrix or switch fabric that can rapidly connect and disconnect ports. Unlike Hub, a switch only forward frame from one port to the other port where the destination node is connected without broadcast to all other ports.

Figure4: D-Link 24-Port 10/100

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.