Ethernet

- Public Key Encryption Re-visited
- Traditional Ethernet
- LAN Components
- Switched Ethernet
- Test and Exam Hints

Public Key Encryption Re-visited

- The private key can only be used to decrypt information that has been encrypted with the user's matching public key
- Public keys can be used to verify that a message is from the actual sender, because the sender is the only one who has the private key
  - can be used for authentication and signatures
- To encrypt the message
  - Sender obtains Receiver's public key (and public exponent)
  - Sender uses Receiver's public key to encrypt message and transmit
  - Receiver uses their corresponding private key to decrypt

RSA Encryption Re-visited

- Michelle wants to send a message to Bob
- Bob generates the following
  - $n = pq$, where p and q are large primes
  - k = relative prime of (p-1)(q-1)
  - $k' = k \times k' - 1 = 0 \bmod (p-1)x\ (q-1)$
- n is the public key, k is the public exponent
- k' is Bob's private key
- p and q are destroyed
- Bob sends (n,k) to Michelle

RSA Encryption Re-visited

- Michelle encrypts the message using (n,k)
- Michelle transmits the encrypted message to Bob
- Bob decrypts the message using k'

Public Key Authentication

- Initialization
  - User creates a set of public/private keys
  - User copies their newly generated public key over to the remote host and adds it to a special file already containing any of the user's public keys generated from other local machines
- Log in
  - Host sends a random string encoded with user's public key
  - The only way to decrypt the message is using the corresponding private key (which only exists on the user's local machine, and is **never** transmitted)
  - User decrypts the message using their private key and sends it back to the host
  - Host determines if the message was correct and can determine the authenticity of user

Original Ethernet

- Described communication over a single cable shared by all devices on the network
- Is Multi-Access, when 1 node transmits all other nodes on the medium hear the transmission
- Any device attached to the cable could communicate with any other device
- Advantage of this approach, is that the network can expand easily

Ethernet Terminology

- Medium – the common communication path
  - Traditionally has been coaxial copper
  - Today is usually twisted pair or fiber optic
- Segment – A single shared Ethernet medium
- Nodes/Stations – Devices that attach to the segment
- Frame – The single message

Ethernet Frame Format

7	1	2 or 6	2 or 6	2	46-1500		4
Preamble	SOFD	Destination address	Source Address	Data Field Length	Data	Pad	Frame Check Sequence

- Preamble – 7-byte pattern consisting of alternating 0s and 1s, used for synchronization
- Start of Frame Delimiter – The special pattern 10101011 indicates the start of a frame
- Destination Address
  - If the first bit is 0, this field is a specific destination
  - If the first bit is 1 the destination address is a group address (i.e. broadcast/multicast)
  - If all bits are 1, it is a broadcast address (broadcast to all stations)

Ethernet Frame Format

- Source address – specifies where the frame comes from
- Data length field – specifies the number of bytes in the data (and pad)
- Pad – Data field must be at least 46 octets, if there is not enough data, it is padded
  - Upper length is to prevent one station monopolizing transmission
  - Lower limit is to ensure collision detections works successfully
  - 802.3 defines minimum frame length as 512 bits (64 octets)
- Frame Check Sequence – Error checking using 32-bit CRC

Start and End of Frame

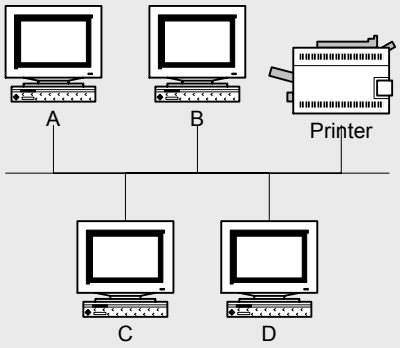
- Start of frame is signaled by the bits …10101011*xxx…*
- End of frame is signaled by the end of data transition (There may be a single final –2V -> 0v change to restore the rest state)

Slot time	512 bit times
interFrameGap	9.6ms
Attempt Limit	16
Back off limit	10
Jam size	32 bits
Max frame size	1518 octets
Min frame size	512 bits (64 octets)

The Ethernet Protocol

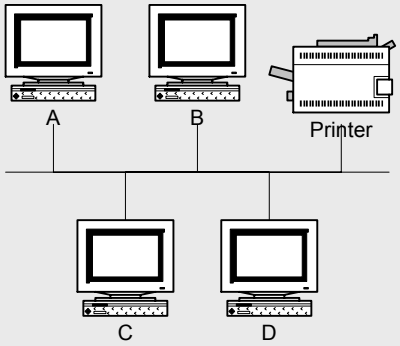
- Wait until the medium has been idle for InterFrameGap (9.6μs)
- Send preamble, start delimiter and frame, including FCS
- If a collision is detected, send jam size random bits, then stop sending and wait for a random number of slots before retrying
- Apply binary exponentional back off

Ethernet Medium



- When C transmits to the printer, A, B and D will also receive and examine the frame
- A,B,D check the destination address of the frame, and determines if the frame was determined for them, and otherwise discard the frame

Ethernet Medium

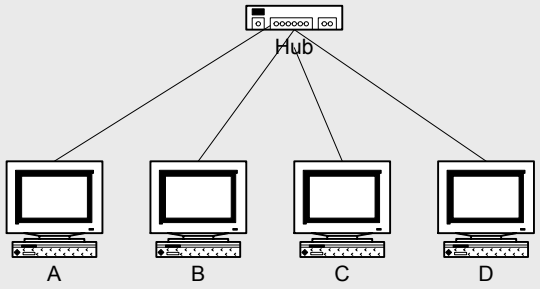


- A broadcast address, is a frame with a special destination address intended for every node on the network
  - Each node on the network will receive and process a frame with a broadcast address

Repeaters

- Each 802.3 variation has a maximum segment length
  - Signals degrade as they propagate along a segment
- Repeaters regenerate a signal and retransmit it
  - 802.3 standard allows two computers to be separated by no more than 4 repeaters

Hub



- Connects multiple Ethernet segments together, making it act as a single segment
- Every attached device shares the same collision domain
  - Only one node can transmit at a time
- When a hub receives a frame, it transmits to all of its ports, i.e. to all of its nodes

Collision Detection In Ethernet

- Ethernet nodes listen to medium during transmission
- A node detects a collision if its own transmission is returned in a garbled form (as when another node transmits at the same time)
- A single Ethernet segment is sometimes referred to as a collision domain as no two stations on the segment can transmit at the same time without causing a collision

Collision Domains

- Ethernet networks become congested if they increase in size
- If a large number of stations are connected to the same segment, many stations may attempt to transmit whenever there is an opportunity
- Collisions become more frequent and choke out successful transmissions

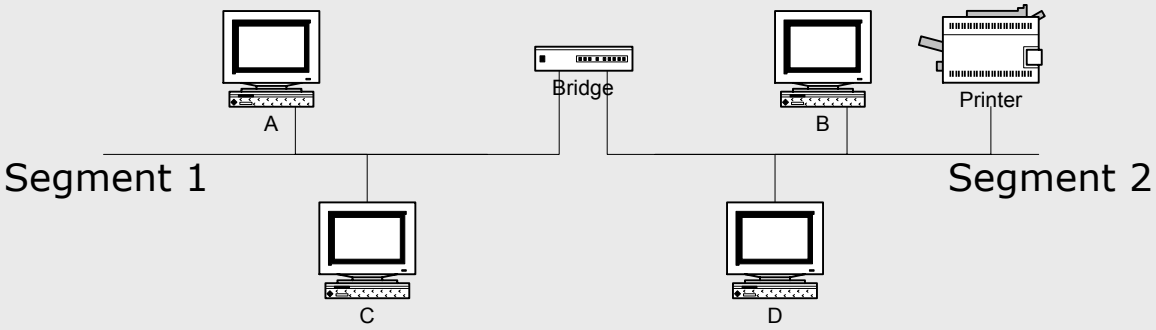
Multiple Collision Domains

- Congestion can be reduced by splitting a segment into multiple segments, thereby creating multiple collisions domains
- However, separate segments cannot share information, and a bridge between the two segments is required

Bridges

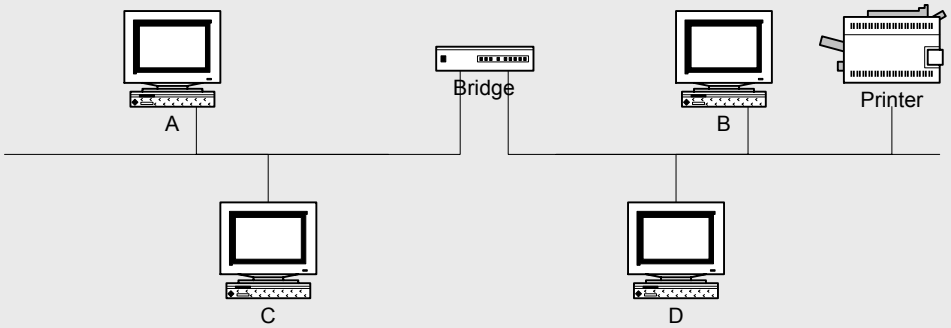
- Bridges address problems with segmentation and multiple collision domains
- Help regulate traffic
- Take advantage of Ethernet's Multiple Access, where every node is seen by every other node on the segment
- Can send and receive traffic, but do not generate any traffic of their own
- Similar to repeater, but can choose to drop certain frames

Bridges



- Bridge connects segments 1 and 2
- If A transmits to C on segment 1, the bridge drops the frame and doesn't pass it onto segment 2
- If A transmits to D, bridge forwards the frame to segment 2
- Bridges reduce unnecessary traffic

Bridges



- If A transmits to D, bridge forwards the frame to segment 2
- Bridges can also allow multiple simultaneous transmissions to occur
  - B can transmit to D
  - A can transmit to C

Modern Ethernet

- Modern Ethernet uses twisted pair or fiber optics
- Transmits at 100, or even 1,000 Mbps
- Uses switches

Switches

- Switches are the modern counterparts of bridges
- Essentially offer a *dedicated segment* for every node on the network
  - Replace the shared medium
- Every segment connects to a switch
- A switch can connect many single-station segments

Switches

- Because segments consist of only a node and a switch, the switch picks up every transmission before it reaches another node
- Upon receiving a frame, the switch then forwards it to the appropriate segment, determined by the frame's destination address
- Similar to a bridge, but because a segment contains only one node, frame is always transmitted to the one intended recipient
- Switched Ethernet allows multiple transmissions at once

Switched Ethernet

- Traditional Ethernet was half duplex
  - Information can only move in one direction at a time
- In a switched network nodes never directly transmit to each other
- Switched networks use twisted pair or fiber optic cabling
  - Both use separate conductors for sending and receiving data
- Eliminates the need for collision detection
- Nodes can transmit at the same time the switch transmits to them

Switched Ethernet

- Provides a private connection between two nodes on a network
- Speeds up the rate at which data is sent
- Eliminates collisions
- Allows full duplex transmissions
  - Stations can send and receive at the same time, doubling the maximum theoretical ‘speed limit’ of Ethernet and ‘fast Ethernet'
- Switches connections point-to-point between stations talking to each other, providing in effect a dedicated connection
- CSMA/CD is no longer required, so a frame is just forwarded

Switch Operation

- When a switch receives a frame it saves the originating MAC address and port
- Switch then selectively transmits from specific ports based on the MAC destination address of the frame
  - If the MAC address is unknown, or a broadcast, or multicast address it transmits to all stations, except the incoming
  - If the MAC address is known, it forwards the frame to only the port corresponding in the destination MAC address table

Ethernet Summary

- Ethernet has been used in the industry for nearly 30 years
- Has kept up with other technologies
- It is a well known, and popular standard
- Is well understood, and relatively easy to maintain and configure

Recommended Reading

- Understanding Data Communications and Networks
  - Section 6.2

Test and Exam Hints

- Hamming Codes
- CRC
  - Create a CRC for the following 8-bit message: 10101101, using the polynomial 1011
- Huffman Trees
- LZW
- BWT

Test and Exam Hints

- RSA Encryption
  - Theory only
- Differences between polyalphabetic ciphers, Shamir, Merkle's Puzzles and Diffie-Hellman
- Security using public key encryption
- Key differences between traditional and modern Ethernet

Test and Exam Hints

- CSMA/CD
- Switched Ethernet
- Components of a LAN
  - Bridge, Hub, Segment, Switch, Node

- Good luck with the rest of the course and exam