Thomas Kehoe - tjk2fa

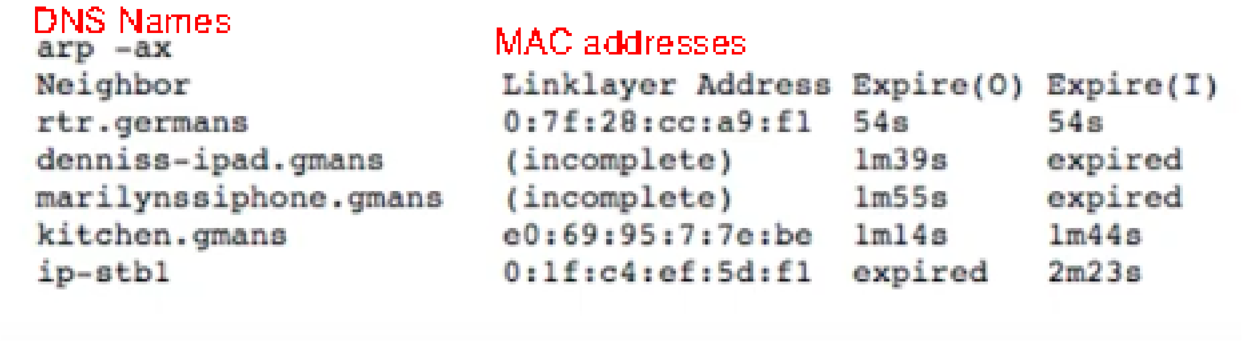
Jan 28 Lecture - Link Layer Part III

ARP Aside for Homework

- For the homework you need to construct the ARP table for each of the machines on the network

- An ARP table contains a mapping of MAC addresses to IP addresses (or DNS names, which can be translated into IP addresses by the DNS server)

- To view your machine's ARP table on OS X you can run "arp -ax"



```
arp -ax
Neighbor                    Linklayer Address Expire(O) Expire(I)
rtr.germans                 0:7f:28:cc:a9:f1  54s       54s
denniss-ipad.gmans          (incomplete)      1m39s     expired
marilynssiphone.gmans       (incomplete)      1m55s     expired
kitchen.gmans               e0:69:95:7:7e:be  1m14s     1m44s
ip-stbl                     0:1f:c4:ef:5d:f1  expired   2m23s
```

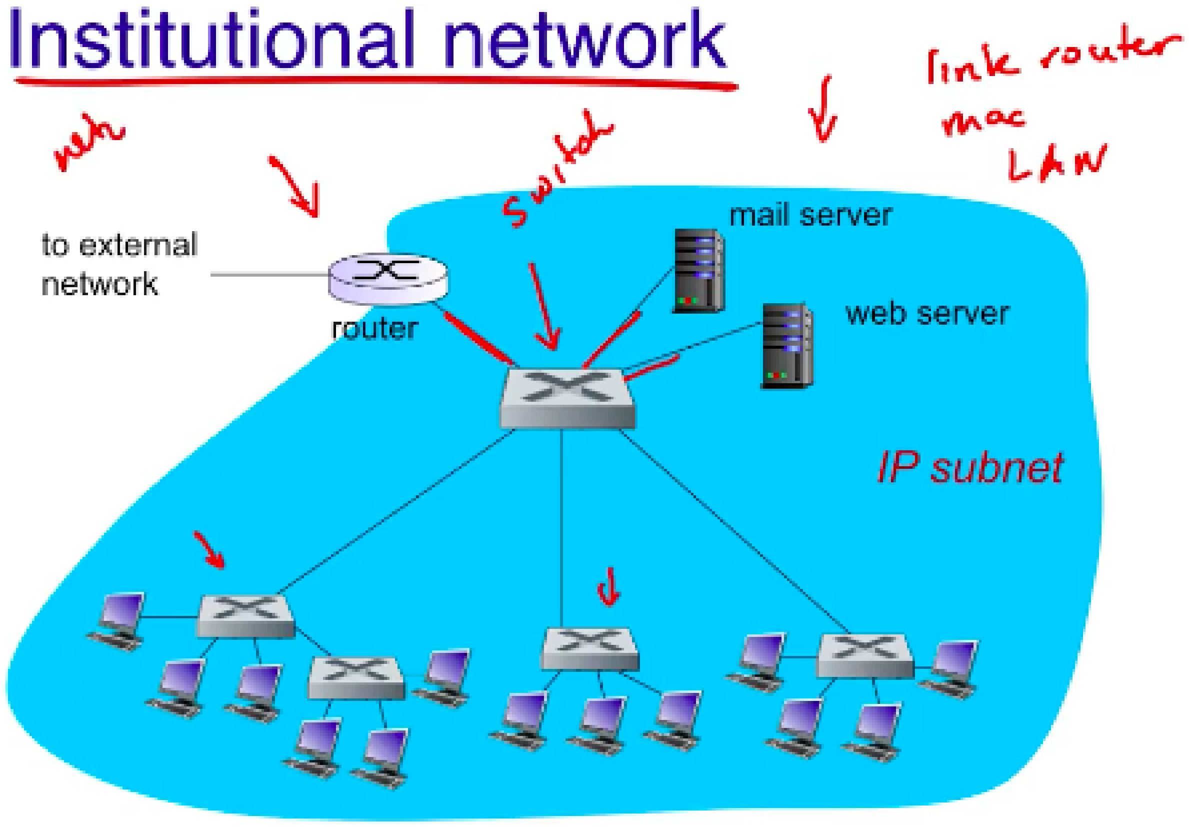
LANs

- A local area network (aka an "Institutional" network) is a group of machines connected on the link layer

- Machines on the link layer are typically connected to one another via switches, devices that are connected to multiple machines and forward traffic from one machine to another. Multiple switches can be connected to one another to form a "hierarchy of switches"

- The router acts as the gateway from the machines on the link layer to the outside network later. Once traffic passes from the link layer through the router, it becomes network layer traffic.

- A router will have a set of IP addresses which it is assigned. These IP addresses are then doled out on the LAN by a DHCP server.



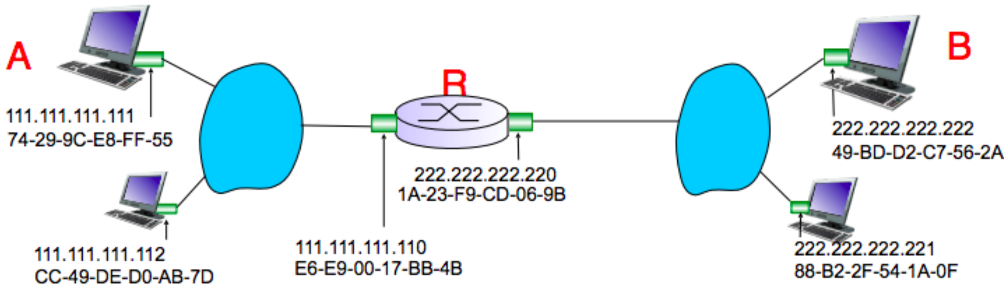
Institutional network

ARP Protocol on the link layer

- What if machine A wants to send a datagram to machine B but B's MAC address is not in A's ARP table?
- **1.** machine A broadcasts an "ARP query packet" containing B's IP address
- **2.** machine B recieves A's ARP packet and replies to A with B's MAC address
- **3.** A saves B's IP-MAC pair in its ARP table until the pair times out
- This all happens without intervention from network administrators

Addressing (routing from one LAN to another)

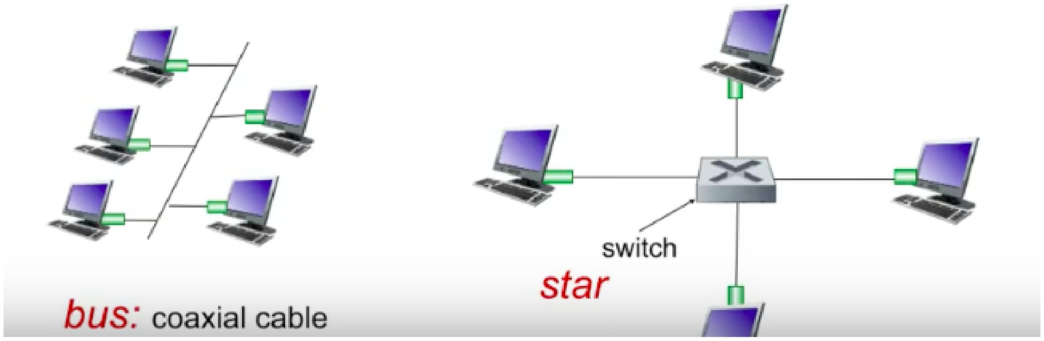
- What if machine A wants to send a datagram to machine B, which is on another LAN connected to A's LAN by router R? Assuming A knows B's IP address, and R's MAC and IP address...
- **1.** A creates an IP datagram with IP source A, dest B
- **2.** A creates link layer frame with the router's mac address as the destination, frame contains A to B IP datagram
- **3.** Frame is sent across the link layer from A to r
- **4.** When the frame gets to the router, the router strips off the MAC addresses. Then it looks at the IP addresses and figures out which interface to forward the frame on by using forwarding tables.
- **5.**The router then forwards the datagram and creates a link layer frame with B's mac address as the destination. This frame contains the A to B IP datagram.



Ethernet

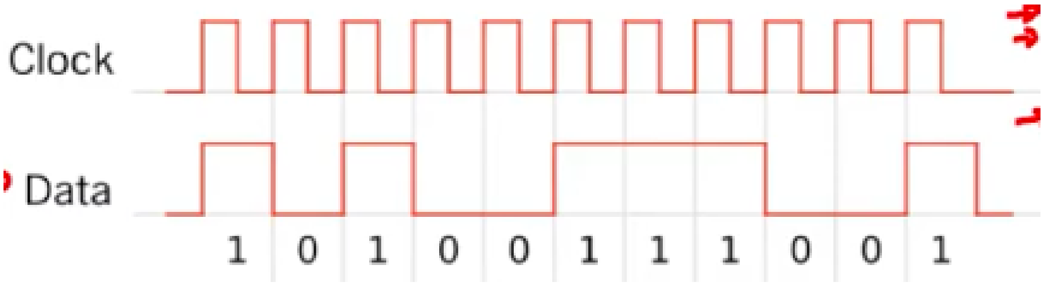
- Dominant wired LAN technology, NICs were cheap without lacking in speed
- Machines can be connected via ethernet in two ways
- **1.** Bus: All machines share one ethernet wire as a common bus. This means that all the machines can collide with one another.

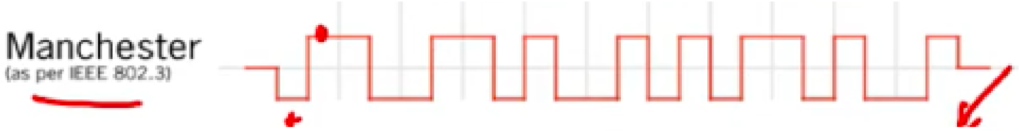
- **1.** Star: Each machine has its own wire and each machine is connected to a central switch. This way no machine can collide with any other machine.

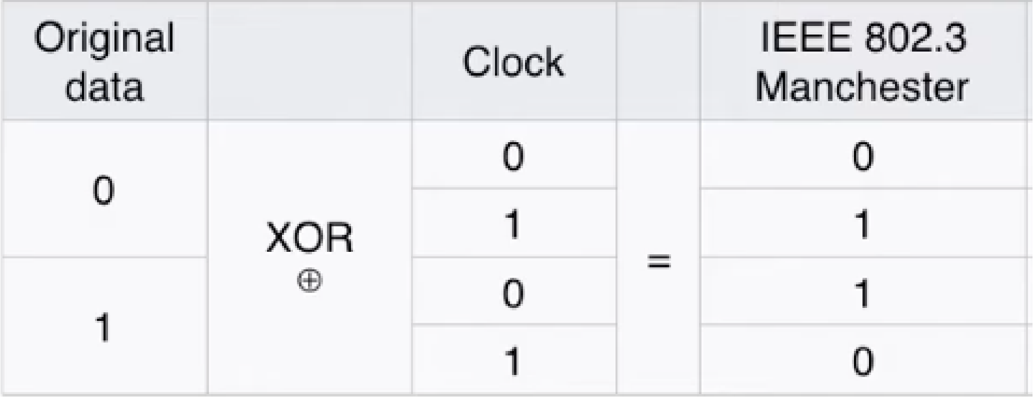


Physical Ethernet Encoding

- Ethernet uses two wires (one + one -) for transmitting and two (one + one -) for receiving.
- Encoding strategy is called Manchester encoding
- So you have a clock and then the data that you want to encode
- To encode the data you just compute its logical XOR with the clock
- To decode the signal, you just read its value right after the falling edge of the clock.
- **Note: Possible midterm question: Given some manchester encoded signal, has the packet been corrupted?**

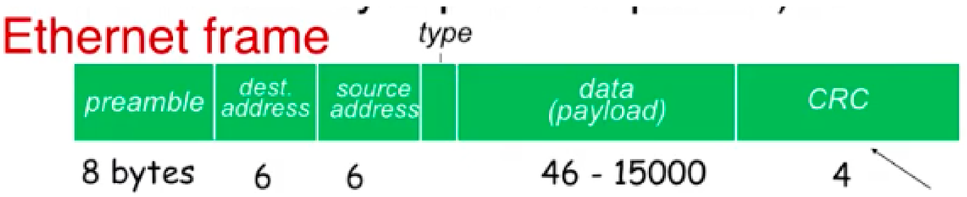






Original data		Clock		IEEE 802.3 Manchester
0	XOR ⊕	0	=	0
		1		1
1		0		1
		1		0

Ethernet Frame structure



- The **Preamble** is a repeating pattern of ones and zeroes followed by a terminal pattern of two ones. This is used to determine the period of the clock that was used for the manchester encoding.
- seven of these −− > 10101010 followed by this − > 10101011
- The **Addresses** are 6 byte destination and source MAC addresses. The receiving NIC will examine the dest. address and only pass it on to the software if it matches the NIC's own MAC address or it is a broadcast (FF-FF-FF-FF-FF-FF).
- The **type** indicates what protocol is being used at the higher layer (usually IP, possibly Novell IPX, AppleTalk, etc)
- The **CRC** is used for error checking (see previous lectures). If an error is detected, the frame is dropped.

More about Ethernet

- Ethernet is...
- **Connectionless:** There is no handshaking between sending and receiving NICs
- **Unreliable:** NIC will just drop frames if the CRC is invalid
- Ethernet's MAC protocol for when multiple machines are on the same bus is unslotted CSMA/CD with binary backoff

How Switches Work

- A switch is a link layer device that takes an active role. It examines and stores incoming frames from link layer devices and selectively forwards them to other devices.
- Switches are **transparent**. This means that other hosts do not know that a switch is there.
- Switches are **self learning**. This means that switches do not need to be configured. Instead, they will learn which NIC card is on which port on their own.
- To do this, the switch will listen for broadcasts from each device. When it receives a broadcast on any port, it notes the MAC address of the broadcasting machine and associates it with that port in a table.
- Switches also allow for multiple simultaneous transmissions to occur by buffering packets coming to and from each machine. For example, if the switch receives an A to B packet and a C to A packet at the same time, it will simply buffer them and then send them out one at a time.

Switch forwarding table

- How does the switch know which machine is on which interface? Each switch has a switch table, and each entry in that table has the MAC address of a host, the interface to reach that host, and a time to live field.

- When a frame is received from a sender machine, the switch notes the MAC address of the sender and what interface it came on, and puts an entry in the table.

- If the frame's destination is the same as the interface it came on, the switch drops the frame

- Otherwise, the switch will look in its table for an entry matching the destination MAC address of the frame. If it does not contain an entry, the switch will **flood** and send the packet on all of its interfaces

- Multiple switches can be connected together and work in the same way as if you just have one switch

Switches vs routers

- **Both are "store and forward"**

- Routers: Network layer devices (examine network layer headers)

- Switches: Link layer devices (examine link layer headers)

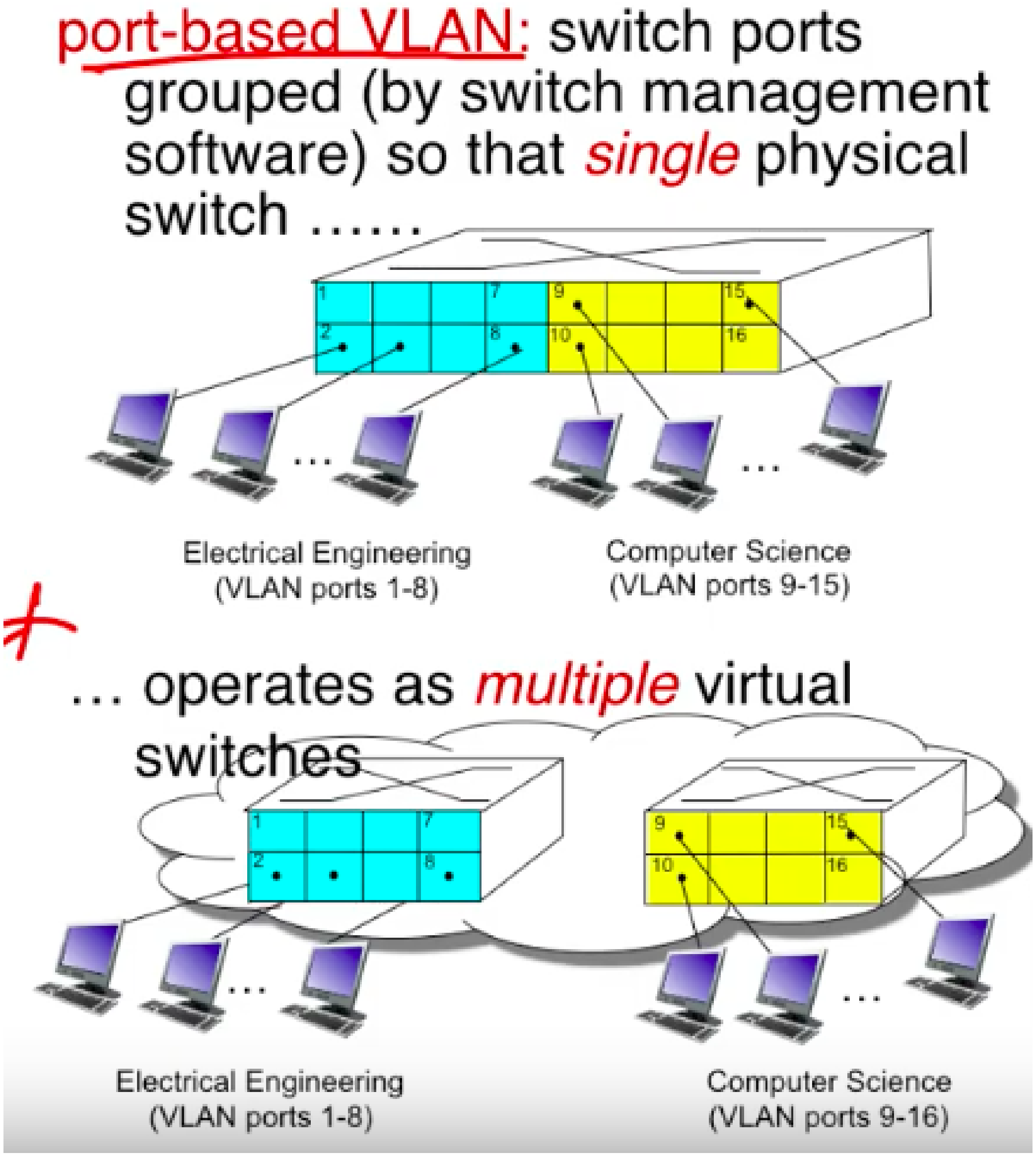
- **Both have forwarding tables**

- Routers: compute tables using routing algorithms and IP addresses

- Switches: build forwarding tables using flooding, learning

VLANs

- Some switches can be configured so that their ports can be grouped into multiple "virtual LANs". See the pic below



port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……

… operates as *multiple* virtual switches

1
2
7
8
9
10
15
16
…
Electrical Engineering (VLAN ports 1-8)
Computer Science (VLAN ports 9-15)
1
2
7
8
9
10
15
16
…
Electrical Engineering (VLAN ports 1-8)
Computer Science (VLAN ports 9-16)

- This grouping means that traffic on ports 1-8 cannot reach ports 9-16 on the LAN. Instead, it must go through the network layer. This can help reduce excessive flooding caused by having a massive LAN.