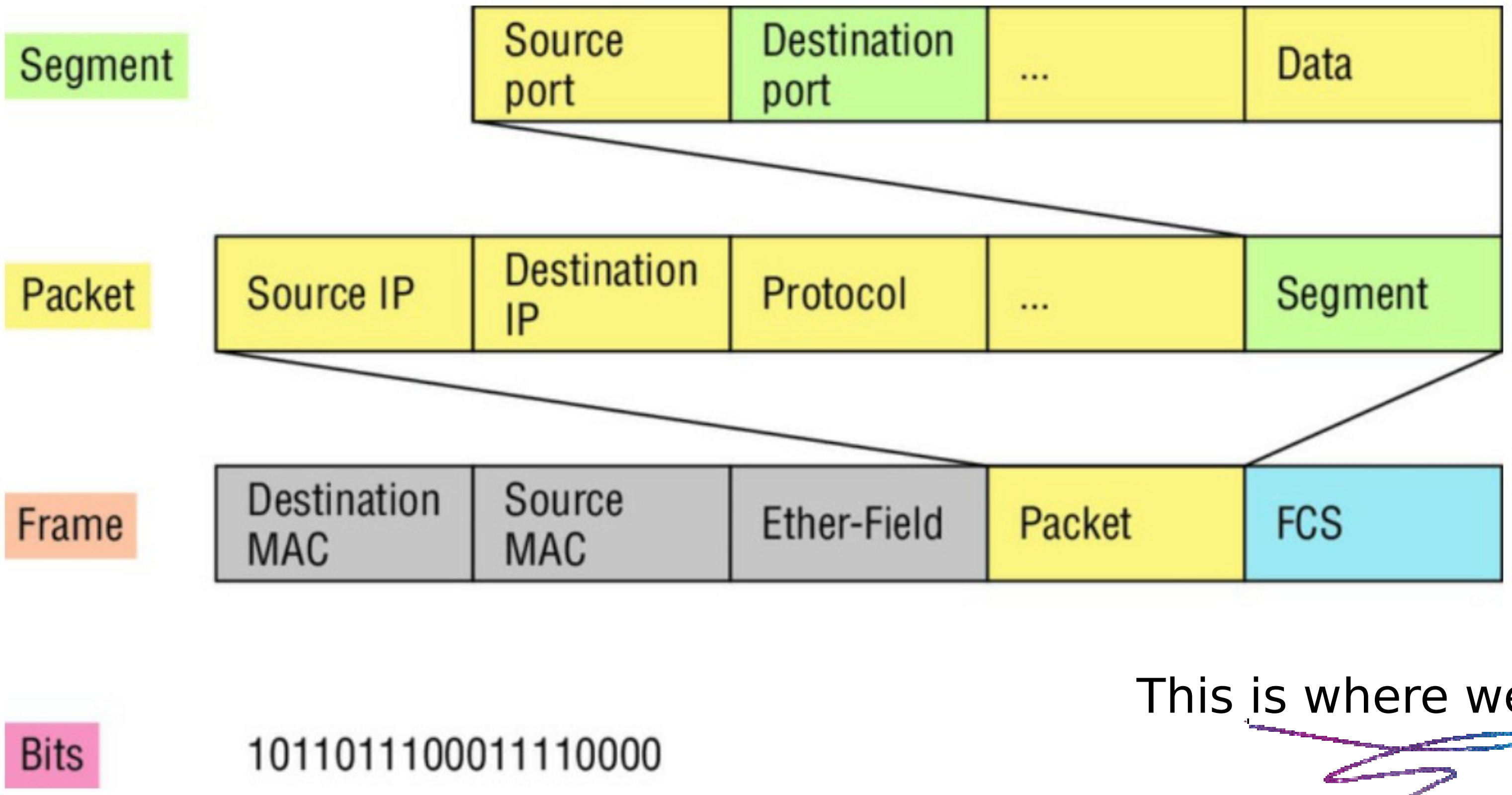
Layer 2: (Data) Link Layer

- Organises data into *frames*
- May detect transmission errors (corrupt frames)
- May support shared media
  - Addressing (unicast, multicast) – who should receive this frame
  - Access control, collision detection
- Usually identifies the L3 protocol carried

Ethernet Frames

The Data Link layer is responsible for combining bits into bytes and bytes into frames.

Frames are used at the Data Link layer to encapsulate packets handed down from the Network layer for transmission on a type of media access



Segment		Source port	Destination port	...	Data
Packet	Source IP	Destination IP	Protocol	...	Segment
Frame	Destination MAC	Source MAC	Ether-Field	Packet	FCS
Bits	1011011100011110000				

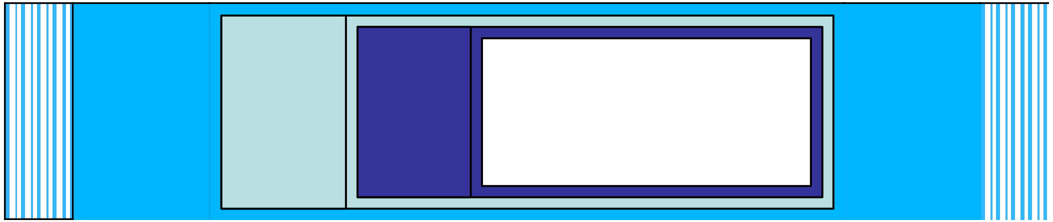
This is where we are.

Encapsulation

- Each layer provides services to the layer
- above Each layer makes use of the layer
- below

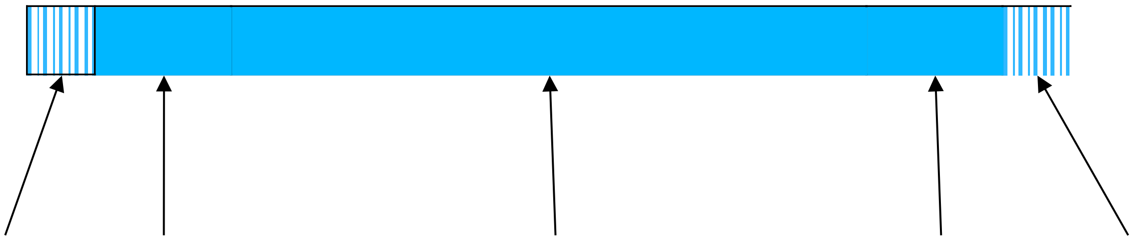
Data from one layer is *encapsulated* in frames of the layer below

Encapsulation in action



- L4 segment contains part of stream of application
- protocol L3 datagram contains L4 segment
- L2 frame has L3 datagram in data portion

Example Layer 2: PPP

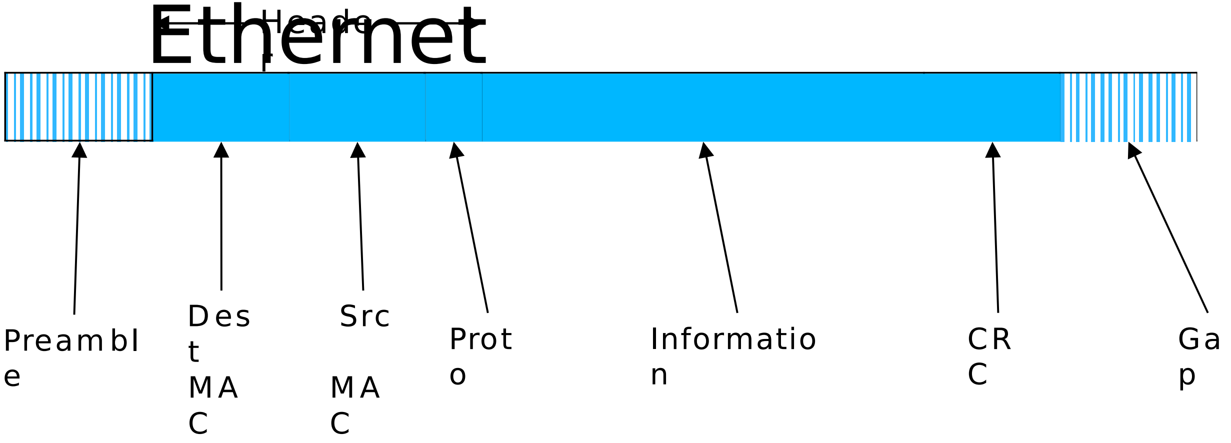


Flag Protocol Information

CRC Flag

- Also includes link setup and negotiation
  - Agree link parameters (LCP)
  - Authentication (PAP/CHAP)
  - Layer 3 settings (IPCP)

Example Layer 2: Ethernet



Header

Preamble

Dest MAC

Src MAC

Proto

Information

CRC

Gap

- MAC
- addresses Protocol: 2
- bytes
  - e.g. 0800 = IPv4, 0806 =

Types of equipment (contd)

- Layer 2: **Switch, Bridge**
- Receives whole layer 2 frames and selectively retransmits them
- Learns which MAC address is on which port
- If it knows the destination MAC address, will send it out only on that port
    - Otherwise, it sends it out on all ports
- **Broadcast** frames must be sent out of all ports, just like a hub
- Doesn’t look any further than L2 header

Switches

A Layer 2 switch is a network device that creates one collision domain per port and forwards data frames only on the outbound port that reaches the destination of the frame.

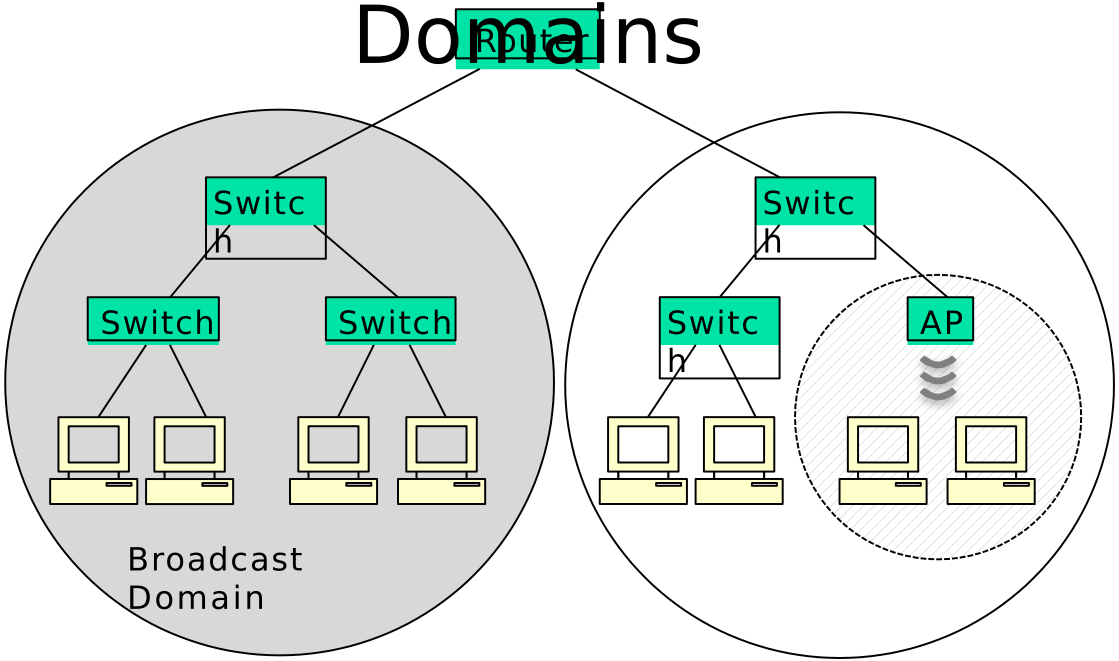
A Layer 2 switch must accomplish three tasks:

✦ Learn about the MAC addresses of devices connected to the switch (Address Learning)

✦ Decide whether to forward frames it receives from host devices or other switches(Flooding, forwarding and filtering frames)

✦ Avoid creating any Layer 2 loops.

Traffic Domains



Collision Domain: where several devices share one communication medium (e.g. wireless networks)

Broadcast Domain: all devices on the same sub-network

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

broadcast domain refers to a group of devices on a specific network segment that hear all the broadcasts sent out on that specific network segment.

collision domain refers to a network scenario wherein one device sends a frame out on a physical network segment forcing every other device on the same segment to pay attention to it.

Address learning: The process by which a Layer 2 switch learns which MAC address is connected to each switch port. The process involves the switch saving the port number where each frame enters along with the source MAC address of that frame. The incoming port number and the MAC address are saved in a MAC address table.

Flooding: The process by which a Layer 2 switch forwards a frame out on all outbound ports except on the port through which that frame came in. A switch floods a frame whenever it does not find the frame's destination MAC address in the MAC address table. It also floods broadcast frames.

Forwarding: The process by which a Layer 2 switch forwards a frame on the outbound port saved in the MAC address table for that destination MAC address.

Avoiding loops: The process by which Layer 2 switches eliminate trans- mission loops created by redundant interswitch links. The Spanning Tree Protocol (STP) handles this process.

Address Learning

- MAC addresses learned by each switch

S1

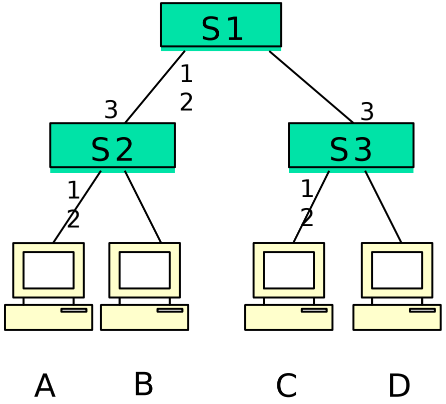
MAC	Port
A.	1
B.	1
C.	2
D.	2

S2

MAC	Port
E.	1
F.	2
G.	3
H.	3

S3

MAC	Port
C	1
D	2
A.	3
B.	3



How Address Learning Works

- After receiving a frame with the source MAC address X on port Y, it “learns” that X is connected to port Y
- Learned MAC address and the corresponding port are added to the MAC Address Table ("bridge forwarding table")
- Later, when it receives a frame with destination MAC address = X, it can send it out only on port Y, and not on other ports
- If the destination MAC address of a received frame is not in the MAC Address Table, it must be sent out on all ports (like a hub)

Address Learning (contd)

- If a switch port is connected to a single computer, then only its Ethernet address will be associated with that port
- If a switch port is connected to another switch (or hub or AP), then a number of Ethernet addresses may be associated with that port
- Entries in the forwarding table may expire, or be forced out if it runs out of space
- A managed switch will let you inspect its forwarding table

Address Resolution Protocol(ARP)

Address Resolution Protocol (ARP) is used to resolve (find) the physical (MAC) address of a host or network device when only its logical (IP) address is known.

The client sends a request to a remote host asking for resolution of a certain address, and the remote host identifies the required address and returns the query to the client. This is useful for identifying and communicating with Ethernet hosts on a local-area network (LAN).