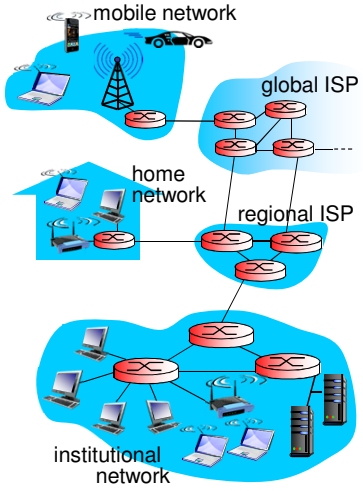
Review of the Physical and Data Link Layers

CSC 573 Internet Protocols

Spring 2019

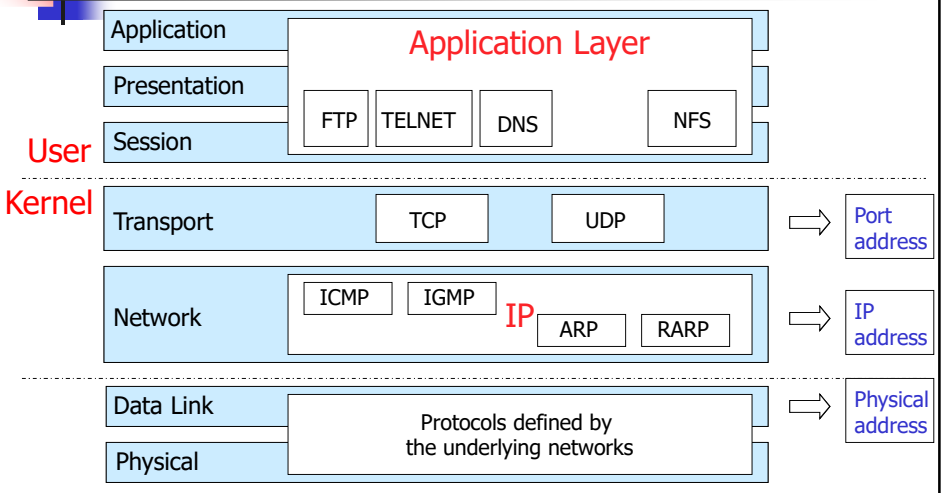
The Internet: "nuts and bolts"

- millions of connected computing devices:



khaled harfoush 2019

TCP/IP protocol stack

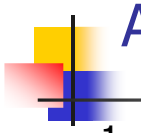


khaled harfoush 2019

Computer Networks

- Communication between *directly* connected devices. How?
  - Covered in 570 – Layers 1 and 2
- Communication between *indirectly* connected devices. How?
  - The general case
  - Will be covered in this class – Layers 3, 4 and 5

khaled harfoush 2019



Agenda

1. Physical Layer
2. Data Link Layer
3. Ethernet
4. Data Link Layer Switching

The Physical Layer

- Concerned with communication between devices *directly* connected through some *medium*

- *Media types*:

1. guided media:
   - signals propagate in solid media: copper, fiber
2. unguided media:
   - signals propagate freely, e.g., radio

Guided Media Examples

1. Twisted Pair (TP)

2. Coaxial cable

3. Fiber optic cable

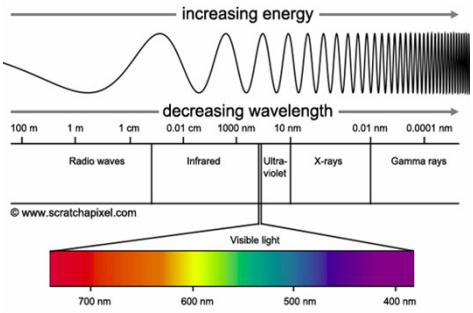
- Differ in the amount of signal interference, attenuation, supported bit rates (bandwidth), cable lengths, number of supported users, etc

Guided Media Systems

1. Ethernet
2. Digital Subscriber Line (DSL)
3. Cable networks
4. Home networks
5. Enterprise access networks

Unguided Media Examples

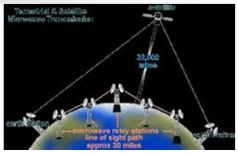
- Medium is air (or sea) -- no physical "wire"
- Signal carried in *electromagnetic spectrum*



khaled harfoush 2019

Unguided Media Systems

1. Terrestrial microwave
2. WiFi (WLANs)
3. Cellular
4. Satellite



khaled harfoush 2019

Physical Layer Responsibilities

1. Modulation
2. Multiplexing

1. Modulation

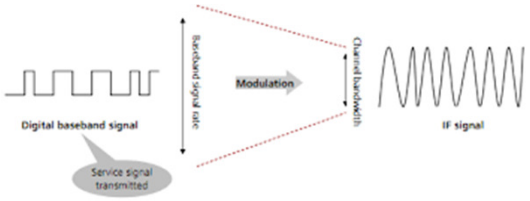
- Modulation is the process of converting symbols (*bits* of data) to *signals* (*voltage* levels) -- Before this step, the information is in the form of a bit stream

- Two types:

1. *Baseband* Modulation
2. *Passband* Modulation

Baseband Modulation

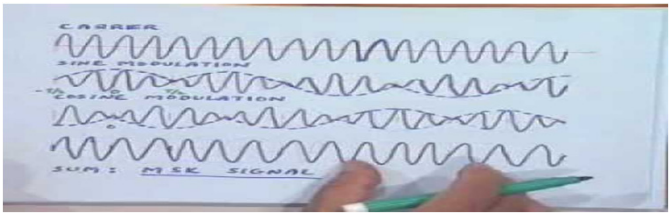
- directly converts bits (or encoded symbols) into a signal.
  - the signal occupies frequency from 0 up to a maximum that *depends on* the signaling rate
  - Used for *wired* communication, and not for *wireless*. Why??



khaled harfoush 2019

Passband Modulation

- Regulates the amplitude, phase or frequency of a *carrier signal* to convey bits.
  - The signal occupies a band around the frequency of the carrier signal.
  - Used for *wireless* communication. Why??



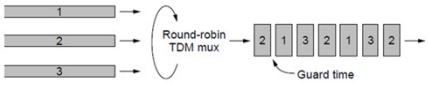
khaled harfoush 2019

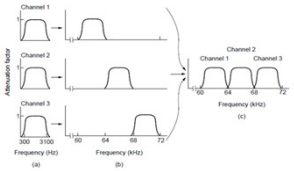
2. Multiplexing

- Multiplexing is about *sharing* communication lines among many signals *without* allowing for *contention*
- In a way, it is similar to people having many conversations in the same room.

Multiplexing Schemes

1. Time Division Multiplexing (TDM)
2. Frequency Division Multiplexing (FDM)
3. Code Division Multiplexing (CDM)





Agenda

1. Physical Layer
2. Data Link Layer
3. Ethernet
4. Data Link Layer Switching

Layer 2 Responsibilities (1/2)

1. Allows the PHY layer to know the beginning and end of a packet (*framing*) – important for correct modulation
   - Techniques: Byte count, bit stuffing, byte stuffing
2. Provides next hop information (MAC address) in *frames*. Note that *packets* are destined to *final destination* (IP address) – necessary for shared channels such as Ethernet

Layer 2 Responsibilities (2/2)

3. Media Access Control (MAC) – allowing multiple flows to compete over the same communication channel.
   - *Compare MAC to multiplexing!*

- MAC Examples:

1. ALOHA
2. CSMA/CD – in Ethernet
3. CSMA/CA – in WiFi

Layer 2 Extra Responsibilities

1. Offers different *service levels* to Layer 3
   1. Unacknowledged vs Acknowledged
   2. Connectionless vs connection-oriented
2. *Flow control* – regulate the traffic rate to avoid overwhelming the next hop
3. *Error detection/correction*

- These functions may be implemented at higher layers of the TCP/IP stack

Agenda

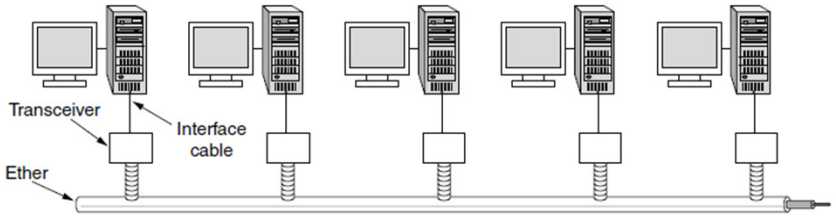
1. Physical Layer
2. Data Link Layer
3. Ethernet
4. Data Link Layer Switching

Ethernet

- *Wired* Network
- IEEE standard 802.3
- Two Ethernet types:
  1. *Classic* Ethernet
  2. *Switched* Ethernet
     A. Fast Ethernet
     B. Gigabit Ethernet
     C. 10 Gigabit Ethernet

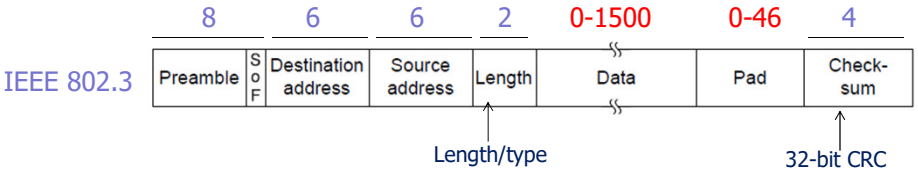
1. Classic Ethernet

- One shared coaxial cable to which all hosts attached
  - Cable up-to 185 meters per coax segment handling at most 30 machines (why? Has to do with MAC protocol - next)
  - Up to 10 Mbps



Frame Format

- Data size is at least 46 bytes and at most 1500 bytes – Maximum Transfer Unit (MTU) is 1500 bytes (why? Has to do with MAC protocol - next)
- *Destination* address could be a *unicast*, *broadcast*, or *multicast* address. *Source* address should be ---



MAC Protocol

- is *CSMA/CD*
- Time is divided into discrete slots whose length is equal to 2τ (51.2μsec)
- Random delay (backoff) after collision is computed with BEB (Binary Exponential Backoff)
- After a collision,
  - After 1st collision, a STA waits for 0 or 1 slot times before trying again
  - After 2nd collision, a STA waits for 0, 1, 2, or 3 slot times before trying again
  - After 10th collision, a STA waits for x slots, where x is chosen at random between 0 and 2^{10}-1
  - Further collisions leads to freezing the randomization

CSMA/CD

- When a station has data to send:

1. *Sense* to the channel to see if anyone else is transmitting.
2. If channel is *idle* then
   transmit frame
   detect collision for a 2τ period (contention slot)
   If *collision* detected then
   1) Abort transmission
   2) Wait for a random period (*follow BEB*)
   2) Start all over

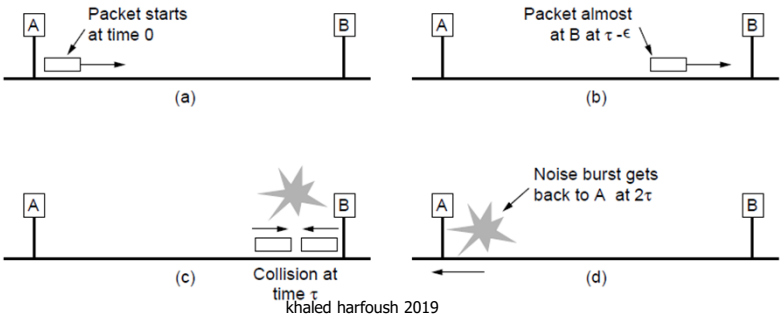
   Else
   1) Wait for a random period (*follow BEB*)
   2) Start all over

How are Collisions Detected?

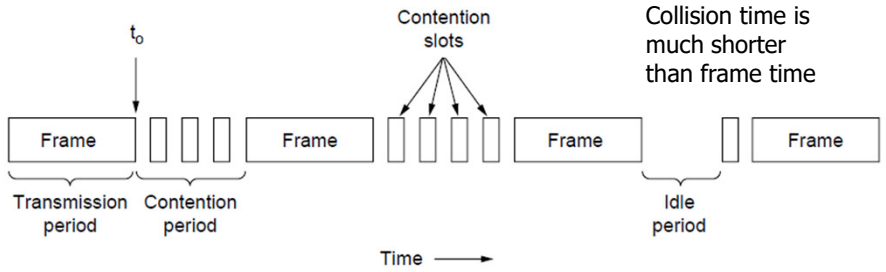
- While transmitting frame, the station hardware listens to the channel.
- If the signal it reads back is different than the one transmitted, then a collision exists
- Will not detect a collision when transmitted 0's are colliding with other 0's.

Time to Detect a Collision

- Collisions can occur and take as long as 2τ to detect
  - τ is the time it takes to propagate over the Ethernet
  - *Leads to minimum packet size for reliable detection (why?)*



CSMA/CD Life Stages

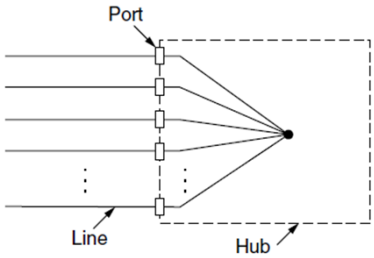


Reasons for max/min frame size

- Max size (MTU) mostly to ensure that no one station will claim the channel for a long period of time.
- Min size is to ensure that each frame takes at least 2τ *amount of time* to transmit on the cable. Recall that collisions are detected *while* transmitting a frame, and it takes at least 2τ amount of time to detect collisions

Ethernet using Hubs

- *Hubs* are *PHY layer* devices. They only relay bits. Nothing more.
- Wires all lines into a single collision domain

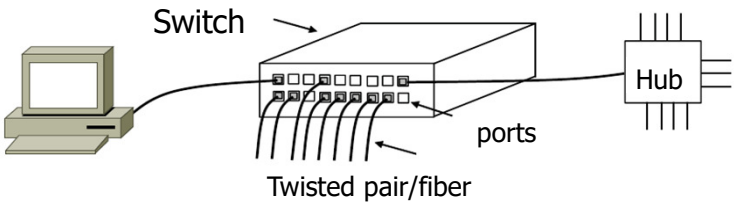


- Ethernet STAs can be connected through hub instead of using a long cable – *same performance*

khaled harfoush 2019

2. Switched Ethernet

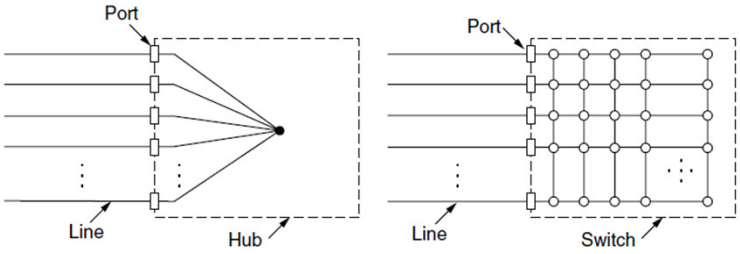
- Uses a *switch* to connect user cables (instead of long cable or hub)
- Makes it easier to manage cables/identify problems
- Switches and hubs look similar but are very different



khaled harfoush 2019

Hubs vs Switches

- *Hubs* (layer 1 devices) wire all lines into a *single collision domain* (*CSMA/CD still needed*)
- *Switches* (layer 2 devices) isolate each port to a *separate collision domain* (*CSMA/CD not needed with full-duplex lines*)



khaled harfoush 2019

Switch Details

- Receiving a frame over one port, the switch transmits the frame using the port corresponding to the frame's destination MAC address. So, need to be able to

1. Need to queue incoming frames
2. Check an incoming frame destination MAC address in Layer 2 header
3. Associate STAs MAC addresses with ports
4. Transmit frame over corresponding port

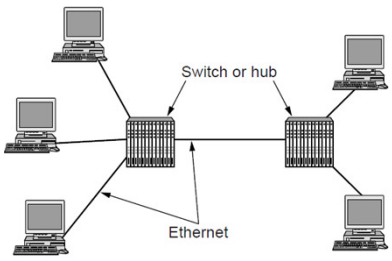
khaled harfoush 2019

Advantages of Switches

1. *No collisions* so capacity is used more efficiently
2. Multiple frames can be sent *simultaneously* by multiple STAs – Switch needs buffering though
3. Frames between two STAs are *not observed* by other STAs – Security benefit

Switched Ethernet Variants

A. *Fast* Ethernet (100 Mbps)
B. *Gigabit* Ethernet (1 Gbps)
C. *10-Gigabit* Ethernet (10 Gbps)



Switched Ethernet Details

- Improvements in performance made possible with
  1. Cable from twisted pair CAT 3 to CAT 5 to fiber
  2. Using higher clocking speeds and higher bandwidth
  3. More signal levels (symbols)
- Backward compatibility still maintained through a negotiation step
- CSAM/CD still used when there hubs in the network so *cable lengths and frame size relation* still needs to be maintained in order to detect collisions in this case

Agenda

1. Physical Layer
2. Data Link Layer
3. Ethernet
4. Data Link Layer Switching

Motivation

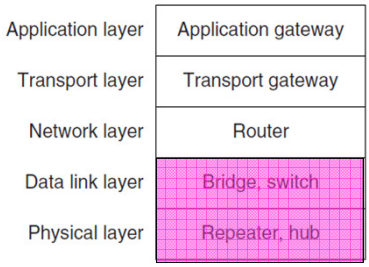
- There are cases in why multiple LANs may need to be joined.
  - Examples?
  - Solution: *Bridges/switches*, hubs, etc
- There are cases in which one LAN may need to be treated as multiple logical LANs.
  - Examples?
  - Solution: *VLANs*

Agenda

1. *Joining LANs*
2. Splitting LANs

Joining LANs

- Examples of Networking devices used to join networks:
  1. Repeaters
  2. Hubs
  3. Bridges/Switches



Belong to different layers of the TCP/IP stack.
What does that mean?

khaled harfoush 2019

1. Repeaters

- Physical layer devices– do not understand frames, packets or headers
- A signal appearing on one cable is amplified and put on another cable

khaled harfoush 2019

2. Hubs

- Physical layer devices– do not understand frames, packets or headers
- A hub has a number of input lines that it joins – Frames arriving on any line are forwarded to all other lines
  - No signal amplification though
- Creates a *single collision domain*

khaled harfoush 2019

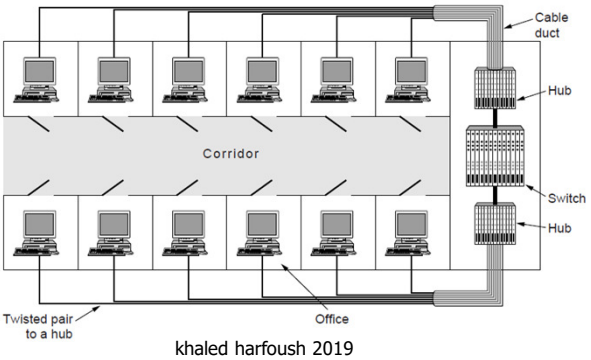
3. Bridges/Switches

- Data link layer devices–understand layer 2 frames and check them
- A switch has a number of input lines/ports that it joins – Frames arriving on any line are forwarded to line connected to the frame destination – *How?*
- Unlike a hub, each port is isolated to be its *own collision domain*

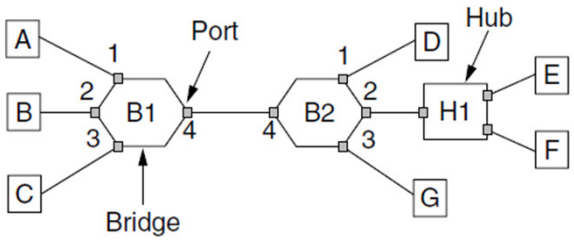
khaled harfoush 2019

Uses of Bridges/Switches

- Common setup is a building with centralized wiring
  - *Bridges* (*switches*) are placed in or near wiring closets

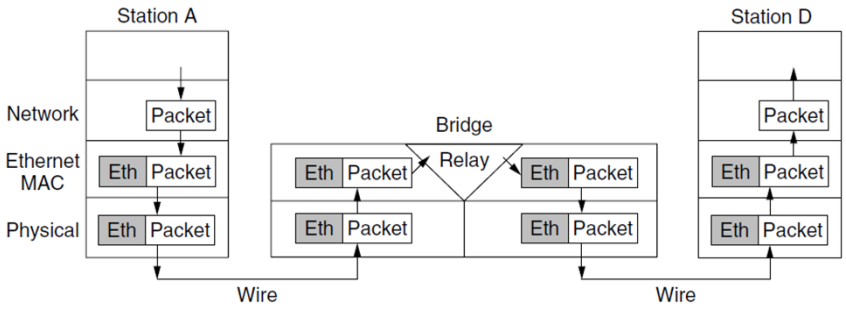


Example



Bridges as Layer 2 Devices

- Use but don't remove Ethernet header/addresses
- Do not inspect Network (Layer 3) header



khaled harfoush 2019

Bridge Use Requirements

1. plug-and-play (no manual setup steps)
2. No hardware changes other than hooking LAN cables to bridge ports
3. No Software changes
4. Transparency (no STA should be aware that there is a bridge in the middle)

khaled harfoush 2019

Q

- How can the bridge know the port corresponding to each STA?

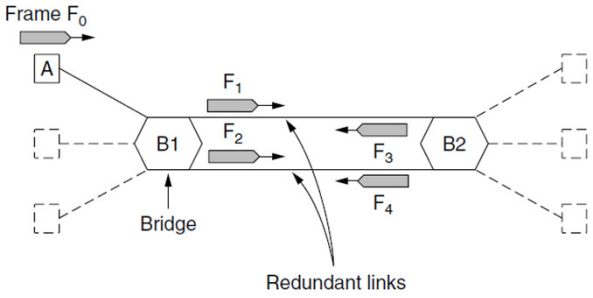
1. Learning Bridges
2. Spanning Tree Bridges

1. Learning Bridges

- Learning algorithm associates MAC address with bridge ports.
- Upon receiving a frame
  1. Associates *source address* on frame with *input port*
  2. Output Frame through port associated with frame's destination address
  3. *Unlearned destinations* are sent to *all* other ports
- Needs no configuration

Problem

- Redundant links improve reliability
- Bridge topologies with loops will cause frames to circulate for ever. Solution? *Spanning Tree*



khaled harfoush 2019

Q

- How can the bridge know the port corresponding to each STA?

1. Learning Bridges
2. Spanning Tree Bridges

khaled harfoush 2019

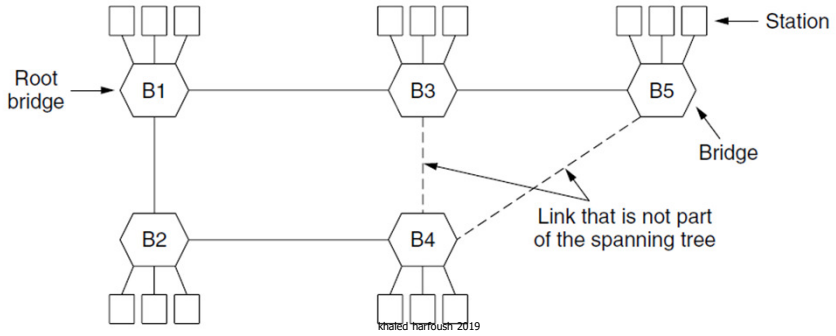
Spanning Tree Bridges

- Bridges run a distributed algorithm to arrange themselves as nodes in a Minimum Spanning Tree (*MST*) – Tree then no loops
- Bridges need to elect a *root* for the MST
  - The one with the *least* MAC address is used as root.

Example

After the algorithm runs:

- B1 is the root, two dashed links are turned off
- B4 uses link to B2 (lower than B3 also at distance 1)
- B5 uses B3 (distance 1 versus B4 at distance 2)



Q

1. How does the size of switch table scale with the number of hosts in the network?

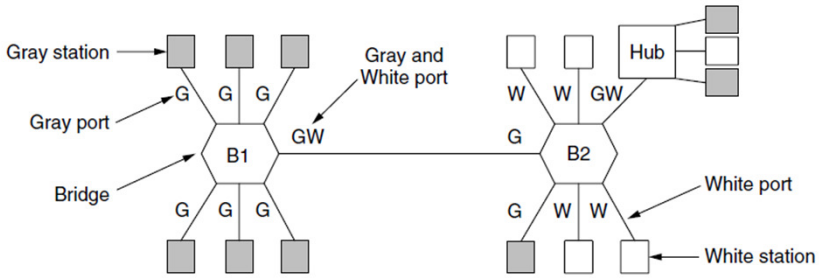
2. What is the impact of flooding protocols (e.g. ARP, DHCP) on a large network only relying on bridges and hubs?

Agenda

1. Joining LANs
2. *Splitting LANs*

Virtual LANs

VLANs (Virtual LANs) split one *physical* LAN into *multiple logical* LANs to (1) ease management tasks, (2) reduce the scope of flooded frames, and/or (3) for security reasons

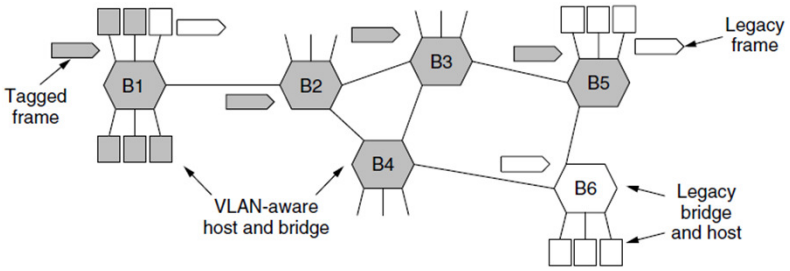


khaled harfoush 2019

IEEE 802.1Q

Bridges need to be aware of VLANs to support them

- In 802.1Q, frames are tagged with their "color"
- Legacy switches with no tags are supported

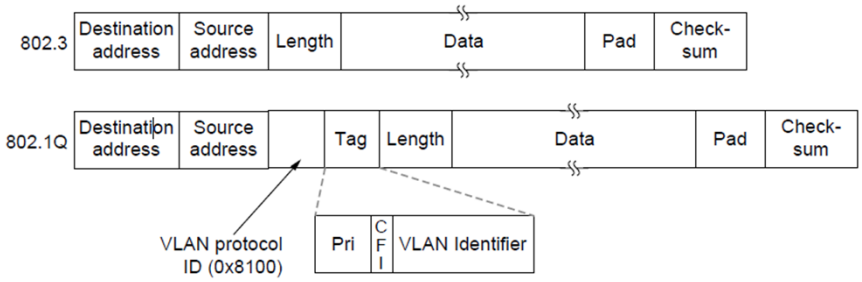


khaled harfoush 2019

IEEE 802.1Q Frame Header

802.1Q frames carry a color tag (VLAN identifier)

- Length/Type value is 0x8100 for VLAN protocol



Next Lecture

1. Addressing