CS540 - Chapter 02 - Summary

1. LAN Switching

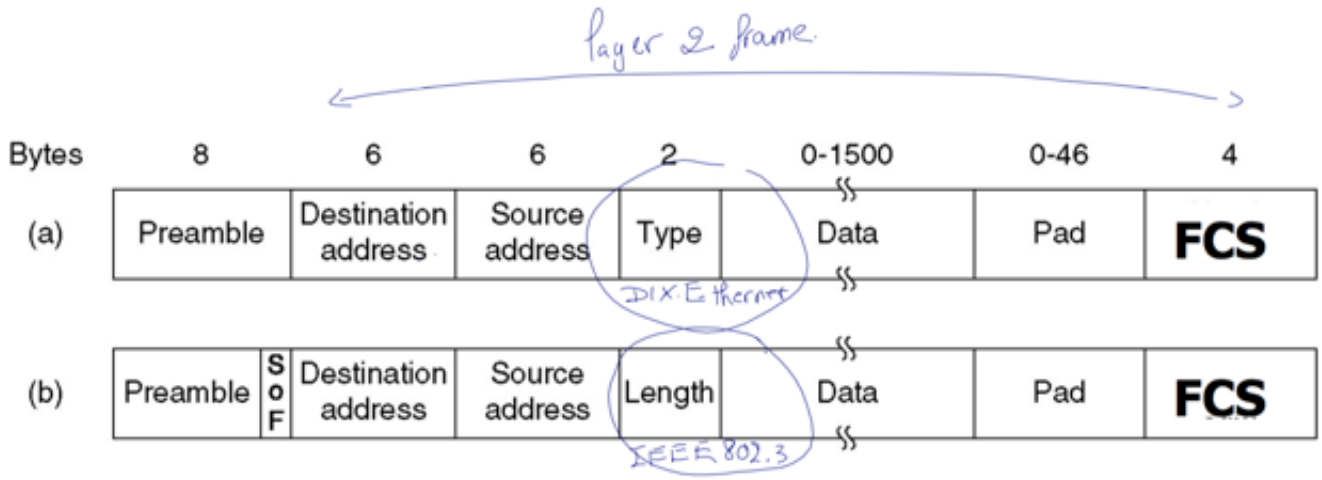
1.1. Ethernet [L2]

1.1.1. Definitions

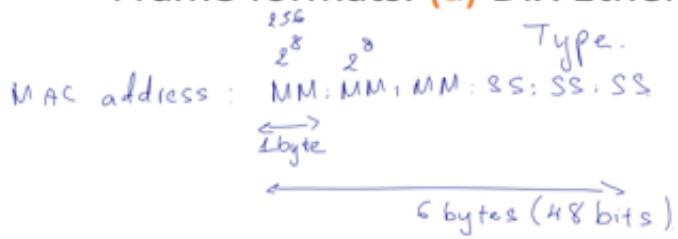
- Ethernet (802.3) includes bottom 2 layers: Physical, Data Link Layer (something just the MAC) in OSI Model.
  - Standard Ethernet: 10 Mbps
  - Fast Ethernet: 100 Mbps

    - Gigabit Ethernet: 1Gbps
    - Ten-Gigabit Ethernet: 10Gbps
- Ethernet provides **connectionless service**
    - no handshake
    - no sequence or order
    - frame has no relation to others
- and thus **unreliable service** to network layer, no ACK/NAK.

1.1.2. Ethernet Frame (802.3 MAC frame) Format

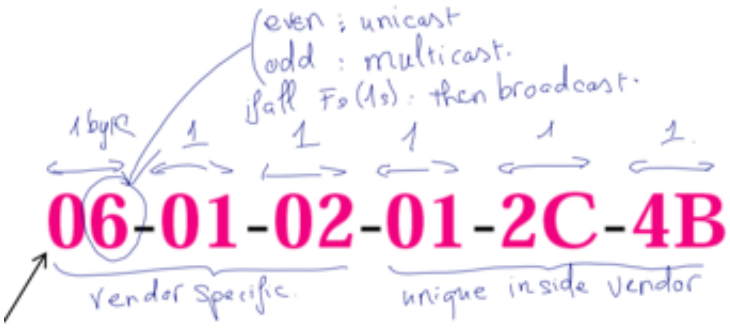


Frame formats. (a) DIX Ethernet, (b) IEEE 802.3.



Description

- Frame Structure
    - **Preamble**: 8 bytes (DIX) or 7 bytes (802.3 frame)
        - SOF/SFD: 1 byte (802.3 frame) of start frame delimiter, 10101011
    - **Destination Address / Source Address**: 6 bytes (= 48 bits) of MAC address MM:MM:MM:SS:SS:SS



    - First 3 bytes specify the vendor, last 3 bytes is unique inside the company.
    - **Categories**:
        - **Unicast** (1 recipient): 2nd digit is **even**. Eg: 4**A**:30:10:21:10:1A
        - **Multicast** (group of recipients): 2nd digit is **odd**. Eg: 47:20:1B:2E:08:EE
        - **Broadcast** (all stations): all 1s or Fs.
  - **Type** or **Length** (2 bytes)
    - Type: in **DIX Ethernet**, when its **value ≥ 0x600**
    - Length: in **802.3 MAC frame**, when its **value < 0x600**. Indicates number of butes in data field.
  - **Data**: packet content
  - **Pad**: Zeros are added if data length is **less than 46 bytes**
  - **FCS**: or CRC, check at receiver, if error, discard frame.
- **Frame length** should be between **64 bytes** to **1518 bytes**. Otherwise, it will be dropped.
  - Minus off 18 bytes of header and trailer, the **data size** should be **46 bytes to 1500 bytes**.

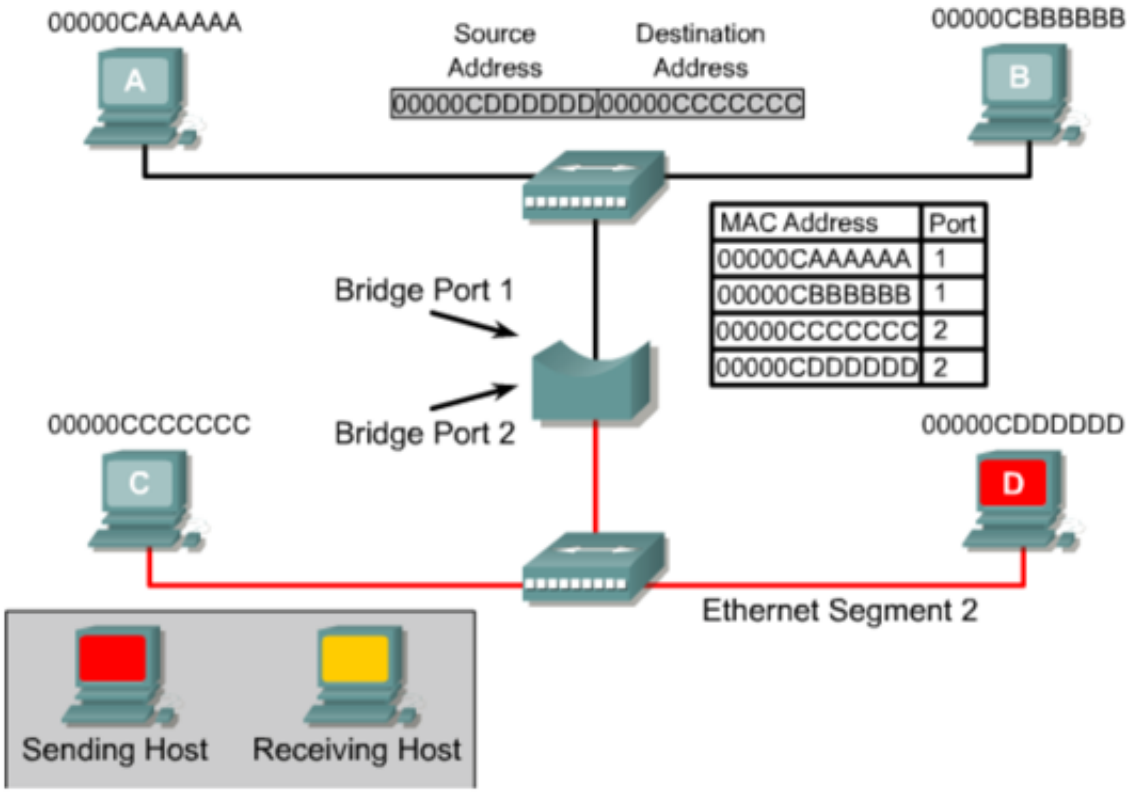
1.2. Hub, Bridge, Switch

1.2.1. Hub

- L1 device as it just receives packet and floods it out to all ports except the incoming.
  - Notes: **L2** device checks **MAC address**. **L3** device checks **IP address**.
- Same functionality as a multiport repeater.
- Fast, but no brain and thus causing data collision and wasting bandwidth.

1.2.2. Bridge

- L2 device
- Is a hub with an **additional check which side the flooding should go out**. Thus it does records the originator's port (source MAC+port).



- Use broadcast/flood if it does not know where to forward to (usually when it first starts)

1.2.3. Switch

- L2 device.
- A **multi-ports bridge**, it also records the originator's ports (source MAC+port) into the forwarding table for future broadcasting/forwarding.
- Use broadcast/flood if it does not know where to forward to (usually when it first starts)

1.3. Frame Forwarding Algorithm

When a frame arrives:

1. Record the source MAC address + port into forwarding table.
    - Set the expiry timer.
2. Search its forwarding table for the dest MAC address
3. If dest MAC address is found, forward to the corresponding port (if port not blocked).
4. If NOT, broadcat to all ports (except incoming).

1.4. Misc

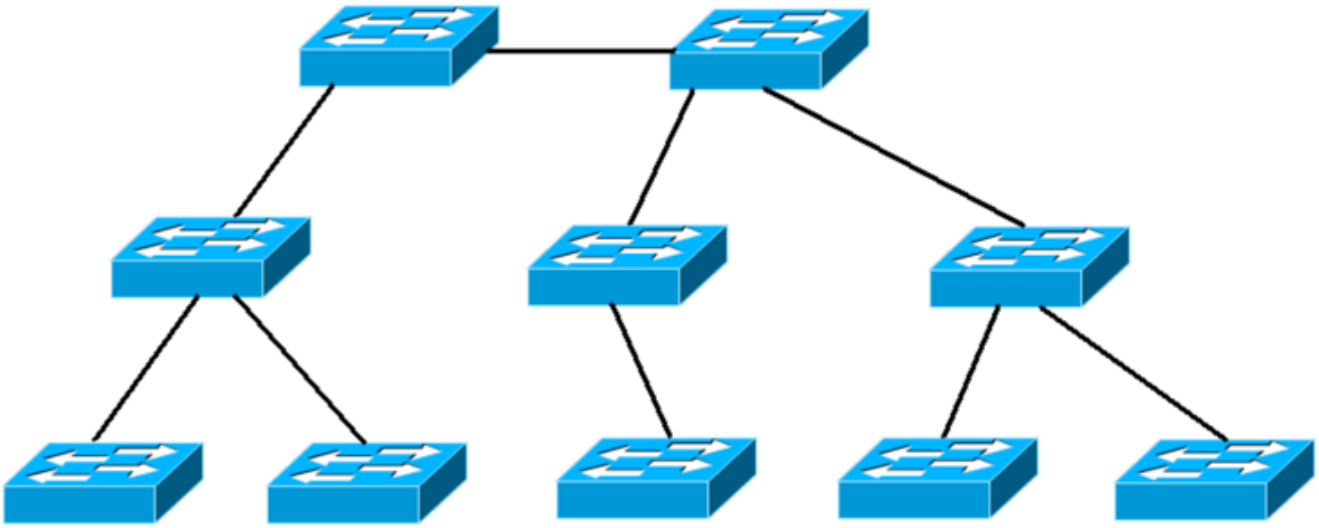
- Wireless is 802.11
- Switch modes

- Store and forward: entire frame is received before sent out.
- Cut through: as soon as the dest MAC addr is received, the frame is sent without waiting for entire frame. –> no CRC check (as CRC is in the MAC trailer)

2. SPT (Spanning Tree Protocol)

2.1. Definitions

- Redundancy design in LAN is good for failover, however it creates **loops**.
  - Loops cause **broadcast storm**, **multiple frame transmission** and **inconsistent switch tables**.
- So people invtented **STP (Spanning Tree Protocol)** (IEEE 802.1d), to eliminate loops but still keep redundancy.
- SPT: a tree topology with
  - NO loops
  - NO device left out

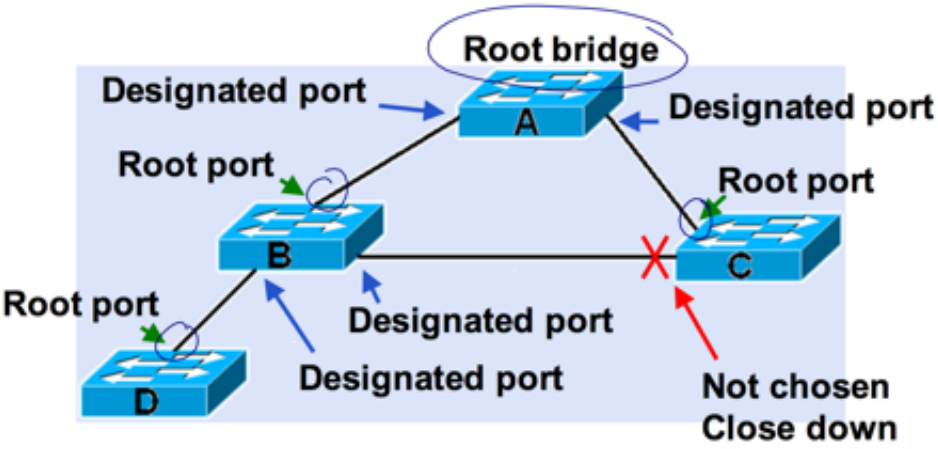


- All switches run STP by default.

2.2. Spanning Tree Algorithm

1. Select & nominate "Root Bridge/Switch". Priority given to lower bridge ID by exchanging BPDUs (Bridge Protocol Data Unit) or by manual configuration.
   - Bridge ID contains priority, VLAN ID, and MAC address
     - Priority ranges [1-65536], default to 32768, change in multiple of 4096.
   - Process
     - BPDU frames (switch BID and root ID) are sent out every 2 seconds when a switch starts. A switch identifies itself as root at first.

    - By **comparing the BID and Root ID**, all bridges come to agreement of the root BID.
    - Default MAC address for BPDU is 01:80:C2:00:00:00 (or 01:80:C2::)
2. On each bridge/switch (except the root one), select 1 "root port", which has the lowest cost path to the root bridge.
    - Cost is inversely proportional to link speed, i.e. **lower cost for faster link speed**.
    - If same cost, use port (higher) **priority** and (lower) **port number**.
3. On each segment (link), select 1 "designated port", which has the **lowest cost path** to the root bridge.
    - If same cost, use the one with (lower) bridge ID.
4. Close down other ports.

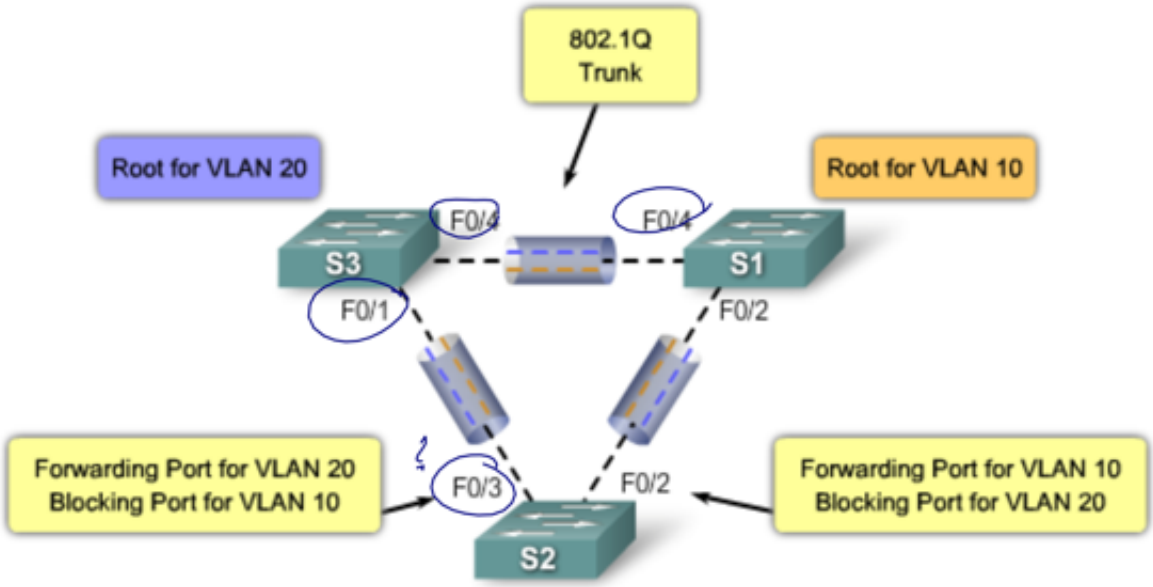


2.3. Port States & Timers

- **Port states** in STP: Blocking (closed port), Listening (listen for BPDUs), Learning (learning MAC addresses), Forwarding (in operation), Disabled.
- **Timers**: up to 50 secs for a broken link to become alive. Blocking 20 sec, Listening 15 sec, Learning 15 secs.
- Cisco use PortFast to quickly revive a port from blocking to forwarding.

2.4. Misc

- Notation F0/0, F0/1 meaning
    - F: media type. F (Fa) is Fast Ethernet, G (Gi) is Gigabit Ethernet, T (Ten) is Ten Gigabit Ethernet.
    - Slot #: the slot number
    - Port #: the port number of the specified slot.



- Initial enhancement of SPT: **PVST+**: is to separate STP for each VLAN.
- Ultimate enhancement of STP: **RSTP**: faster SPT, same BPDU structure but different port states and timers. Faster to heal (6 seconds).

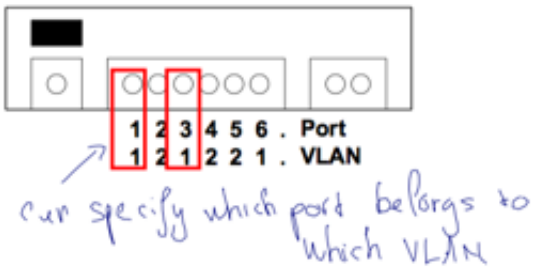
3. Virtual LAN

3.1. Definitions

- **Broadcast Domain**: is a network segment in which any device can transmit data directly to each other without going through a router.
- A router (L3 device) breaks up a broadcast domain.
- A VLAN is a group of hosts with a common set of requirements that **communicate as if they were attached to the same broadcast domain regardless of their physical location**.
- **VLAN = Subnet**

3.2. VLAN

- VLAN are assigned on the switch port (port number + VLAN number)

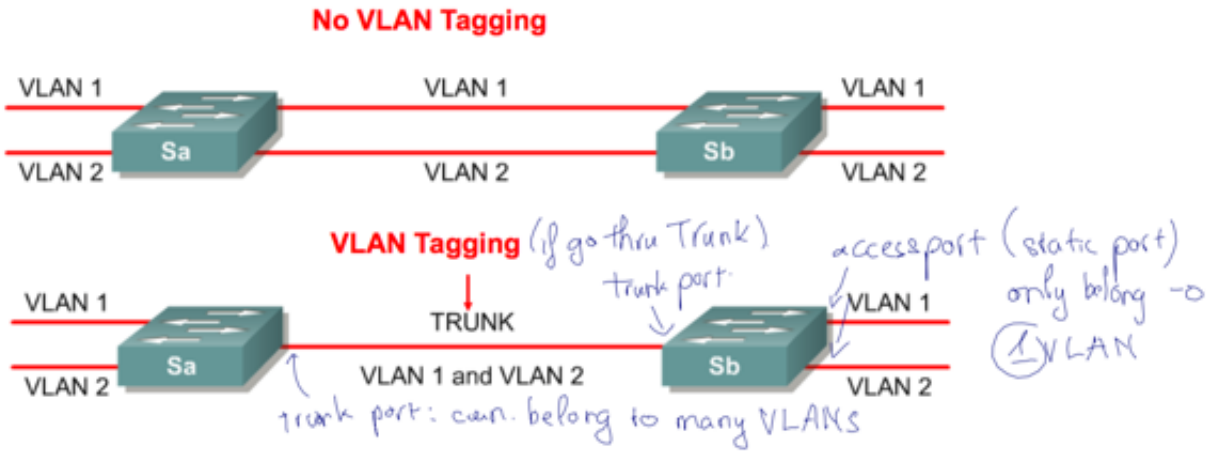


- VLAN assignment:
  - Connect the host to a **correct port** on the switch.

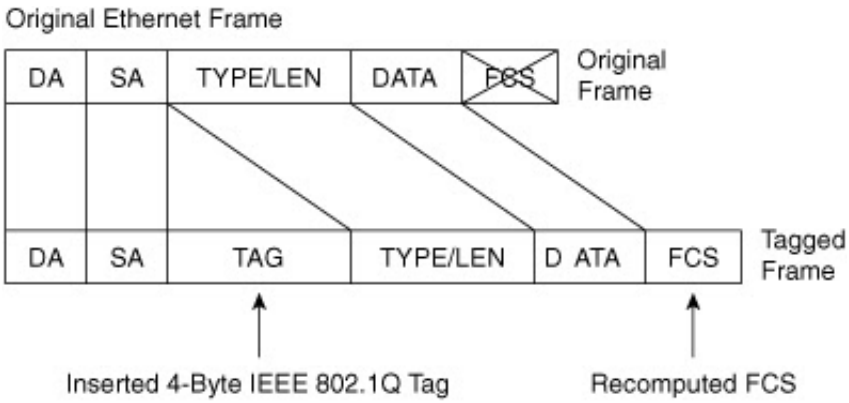
    - Assign the host the **correct IP** of the VLAN.
- Main **benefits** of VLAN: Security, Ease of Management. In detail:
    - Security
    - Cost Reduction
    - Higher Performance
    - Broadcast Storm Mitigation
    - Improved IT Staff Efficiency
    - Simpler project or application management
- VLAN number ranges 1-4094 (12 bits)

3.2.1. VLAN Tagging (Trunk) 802.1q

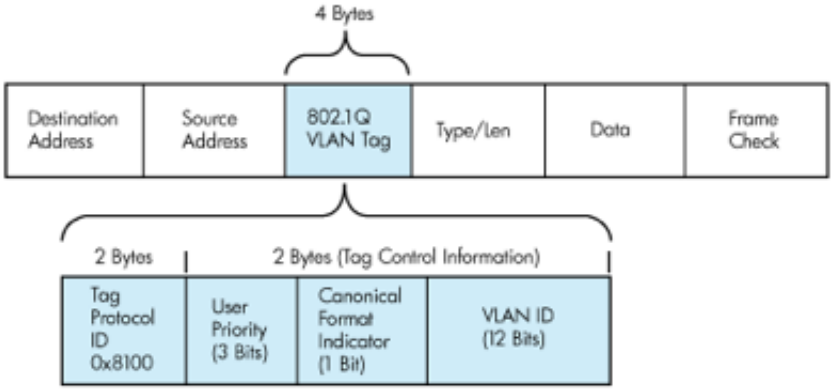
Tagging is a technique to allow a single connection between 2 switches to serve multiple VLANs.



- 802.1q header (TAG) is added for the recipient to detect this is a tagging VLAN packet. FCS is also recalculated.



- The recipient switch strips off the header and forwards the packet to the corresponding VLAN.
- The 802.1q header is 4 bytes long:



- Trunk link does not belong to a specific VLAN.
- **Native VLAN**: is the untagged VLAN on an 802.1q trunked switchport. For any switch, native VLAN is default to VLAN 1.