FIT9137 Workshop Week 6

Topics

- Application Layer
  - Virtual LANs (VLANs)

Covered Learning Outcomes:

- Analyse and formulate the functions of communication architectures of local area networks, wide area networks and the Internet.
- Examine networks using the underlying fundamental theories, models, and protocols for data transmission.

Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (peers) to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

• ACTIVITY A: Virtual Local Area Networks Tags

A VLAN is a LAN defined by software rather than physical wiring and allows to divide a LAN into multiple logical segments [1]. Each VLAN is identified by a VLAN ID and similar to a LAN, devices that are connected to the same VLAN will be assigned an IP address from the same subnet. A VLAN is not limited by physical location and can span multiple switches. The Ethernet frames that are transferred between the VLAN switches have the VIDs inserted inside the 802.1Q headers and removed before being delivered to the destination specified by the MAC address. Because of this, we cannot see the VLAN headers in the Wireshark frames when capturing from a host.

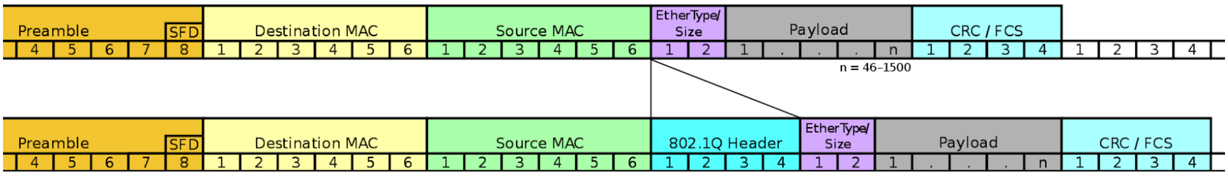


Figure 1: 802.1Q Protocol Header in Ethernet Frame

Ref: https://en.wikipedia.org/wiki/IEEE_802.1Q

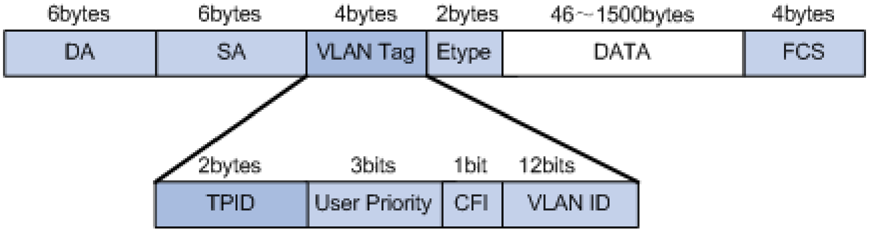
[1] Section 15.3 Virtual LANs, Data Communications & Networks, Forouzan, Behrouz A., 5th Edition, McGraw-Hill, 2013

The Monash backbone network is built from the intelligent, programmable switches that support Virtual Local Area Networks.

1. Referring to Figure-1, explain the IEEE802.1Q header of 4 Bytes called VLAN tags?

   IEEE organization define the standard as IEEE 802.1Q, often referred to as Dot1Q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. This is performed by processing at datalink layer-2, when a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership. Each frame must be distinguishable as being part of a VLAN.

   The VLAN tag contains VLAN ID + priority code, The VLAN ID is 12 bits value that can identify 4096 VLANs. Switch configuration is done by network admin, and they define which VLANs span which switches, and how switches are connected (trunks).



- **TPID** - Tag Protocol Identifier (16 bits): set to a value of 0x8100 to identify the frame as an IEEE 802.1Q tagged frame.
- **User Priority (3 bits):** indicates the priority level (0 through 7) used for QoS.
- **CFI - Canonical Format Indicator (1 bit):** specifies if the MAC address is in noncanonical (1) or canonical (0) format.
- **VID - VLAN Identifier (12 bits):** uniquely identifies the VLAN which the frame belongs to.

802.1Q Tagging The 802.1Q standard adds this information to the Ethernet header, as shown in the figure below. The priority level values range from zero (best effort) to seven (highest). These values can be used to prioritize different classes of traffic. The VLAN ID tag specifies the VLAN to which the frame belongs.

• ACTIVITY B: Inter-VLAN Communication

A network configuration is as shown in **Figure-2** below.

1. Explain why having a **layer 2 loop** in a network will be **problematic**. Explain why layer 2 loops are used and how the problem is **resolved**.
   (Hint: To answer this question research and understand the Spanning Tree Protocol)

   Broadcast messages will loop around forever as there is no mechanism to remove them in layer 2. For redundancy so there are multiple paths available in case there are link failure and depending on the design distribution or core switch failure. The switches run *Spanning Tree* protocol and block links that create loops. The switches continuously exchange messages and will bring blocked ports back up when there are link failures.

In the diagram the link between sw2 and sw3 is blocked by spanning tree protocol (sw1 is the root switch).

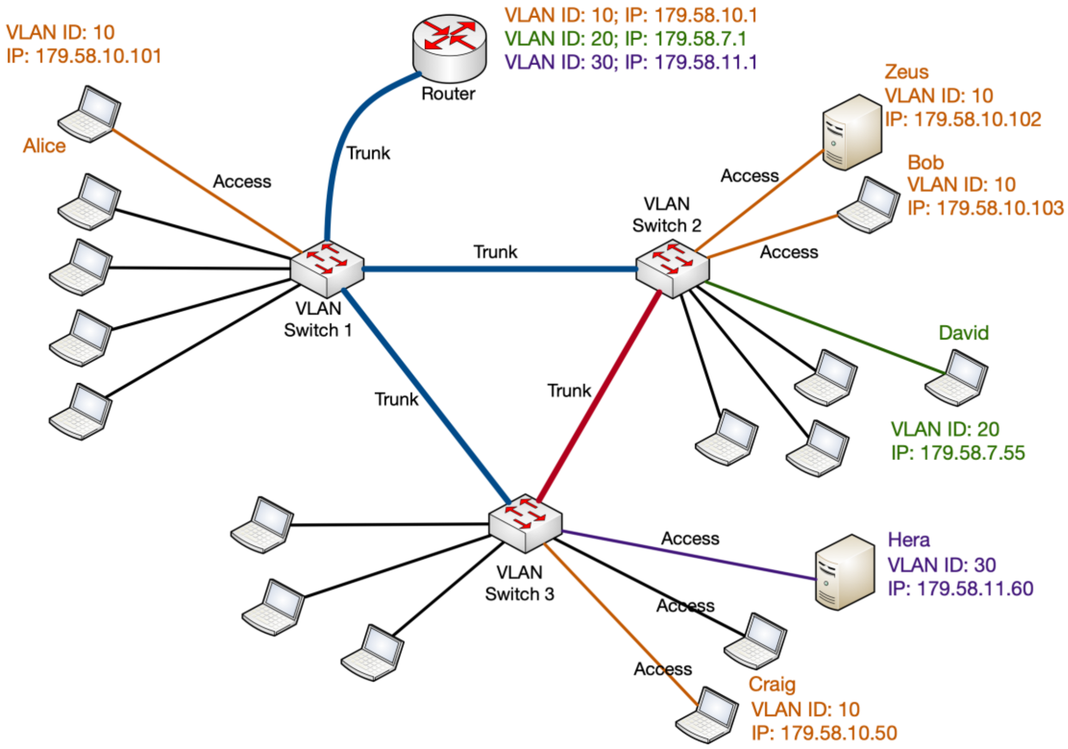


Figure 2: Network Configuration of Talos Corp.

2. Explain the process when **`Alice`** accesses a service on **`Zeus`** server.

   Alice to sw1 through access port, Zeus is via link to sw2 which is a trunk port, frame will be tagged with VLAN ID 10 and will be sent to sw2. sw2 finds Zeus locally connected and the port is an access port so removes the tag and sends out that port.

3. Explain the process when **`Alice`** accesses a service on **`Hera`** server.

   Hera is not in the same VLAN hence the communication must go through the default gateway which is the router's interface in VLAN 10. Alice sends its message with Hera's destination IP but MAC address of the Router in VLAN 10. sw1 receives the message from an access port in VLAN 10 finding the Routers MAC address and outgoing port being trunk tags the frame with VLAN 10 and sends to to Router. Router opens up the frame routes it to VLAN 30 and the port being trunk tags it with VLAN 30 and sends out the frame. sw1 finds the MAC address of Hera in its MAC address table (or flood it if not found) and sends it out the trunk port to sw3 (assuming the link between sw2 and sw3 in blocked by spanning tree). sw3 finds the MAC address of Hera in its MAC address table and the port being an access port removes the tag and send out the frame.