Lecture 3a - VLANs

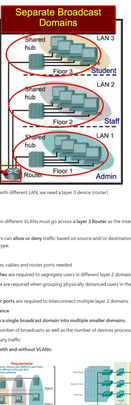
Type: Lecture
Materials: Empty
Reviewed: ☑

1. Overview of VLANs

- **VLAN Definitions:**
  - A VLAN is a **logical partition** of a **Layer 2 network**
  - Multiple partitions (VLANs) can be created
  - Each **VLAN** is a **broadcast domain**
  - VLANs are mutually **isolated** and **packets** can only pass between them via a **Layer 3 device**
  - The **hosts** grouped within a VLAN are typically **unaware** of the **VLAN's existence**

⇒ VLANs effectively allow you to divide your physical switch into a number of virtual switches.

- **Traditional switched LANs:**
  - Physical topology is closely related to logical topology
  - Workstations must be grouped by their physical proximity to a switch
  - To communicate among LANs, each segment must have a separate interface (fa0/0,fa0/1) on the backbone device (router)



⇒ To communicate with different LAN, we need a layer 3 device (router)

- **Benefits of VLANs:**
  - **Security**
    ⇒ Traffic between different VLANs must go across a **layer 3 Router** as the intermediate device.
    ⇒ Layer 3 routers can **allow or deny** traffic based on source and/or destination IP, as well as the application type.
  - **Cost reduction**
    ⇒ Fewer switches, cables and router ports needed
    - Fewer **switches** are required to segregate users in different layer 2 domains
    - Fewer **cables** are required when grouping physically distanced users in the same layer 2 domain.
    - Fewer **router ports** are required to interconnect multiple layer 2 domains
  - **Better performance**
  - **VLANs break up a single broadcast domain into multiple smaller domains.**
    ⇒ reduces the number of broadcasts as well as the number of devices processing them
    ⇒ less unnecessary traffic
- **Compare network with and without VLANs:**

⇒ Without VLAN:

- We need lots of routers, which will be expensive
- 4 Ports each
- 3 hubs / floor
- 9 Broadcast domains
- Inefficient traffic flow

2. VLAN Communications

- **Intra VLAN Communications**
  - When a host communicates with another host in the **same VLAN**
  - This type of communication only requires **layer 2 (Switch)** devices as intermediate devices.
- **Inter VLAN Communications**
  - When a host communicates with a host in a **different VLAN**
  - A **router** is required as the intermediate device for **layer 3** processing.

3. VLAN Assignment

3.1: VLAN Ranges on Catalyst Switches

- Cisco **Catalyst 2960** and **3560 Series** switches support over **4,000** VLANs
- **VLANs are split into two categories:**
  - **Normal range VLANs**
    - VLAN numbers from **1 to 1,005**
    - Configurations stored in the vlan.dat (in the flash memory)
  - **Extended Range VLANs**
    - VLAN numbers from **1,006 to 4,095**
    - Configurations stored in the running configuration (NVRAM)
- **VLANs 1002-1005, VLAN 1** are configured by default
- Some limitations to Extended VLANs – should limit use to normal VLANs

3.2: VLAN Switch Ports

- Step 1: Create the VLAN on switch
  - All core/distribution layer switches need to know all VLANs for traffic they will see
  - All access layer switches need to know all VLANs for devices connected to them
- Step 2: assign switchports to particular VLAN
  - Default switchport mode is automatic – instead force mode
  - Non-used ports should be shutdown and not assigned to used VLAN
- Step 3: for Management VLANs, create the virtual interface and assign the IP address
  - Remember gateway to allow inter-VLAN access

3.3: VLAN Access Ports

- Port can only belong to one VLAN
- Traffic is normal – untagged – Ethernet frames
- Network devices are unaware of VLAN
- Network devices see normal Ethernet network
- Traffic is restricted based on
  - Only traffic for that VLAN
  - Contents of switch CAM Table

3.4: VLAN Membership

Static VLAN

- Ports manually assigned to a VLAN
- Configured with `switchport access VLAN ID`
- Requires reconfiguration if circumstances change

Dynamic VLAN

- Membership is configured using a **VMPS** – VLAN Membership Policy Server
- Based on source Mac address of device

4. VLAN Trunking

- **VLAN Trunks**
  - **Inefficient** to connect switches using **Access Ports** – need one connection for each VLAN
  - **Trunks** allow a **single connection** to carry traffic of multiple VLANs
  - Traffic is still segmented Frames are **tagged** to allow the receiving switch to know which VLAN traffic belongs to
- **VLAN Tagging**

⇒ **VLAN Tagging** is used when a link needs to carry traffic for more than one VLAN.

Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened
802.1Q	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN ID

There are two major methods of frame tagging, Cisco proprietary **Inter-Switch Link (ISL)** and IEEE 802.1Q.

⇒ Cisco recommends using **802.1Q**.

- **Configuring IEEE 802.1q Trunk Links**

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Force the link to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify a native VLAN for untagged 802.1Q trunks	`S1(config-if)# switchport trunk native vlan vlan_id`
Specify the list of VLANs to be allowed on the trunk link.	`S1(config-if)# switchport trunk allowed vlan vlan#,vlan#`
Return to the privileged EXEC mode.	`S1(config-if)# end`

5. Dynamic Trunking Protocol

- **Overview:**
  - Cisco solution to **automatically** configure switch **port state**
  - **Dynamic Trunking Protocol (DTP)** manages trunk negotiation
  - Cisco proprietary protocol
  - Default, enabled in Cisco **Catalyst 2960** and **3560 switches**
  - The default DTP configuration for Cisco Catalyst **2960 and 3560** switches is **dynamic auto**
- **Negotiated Interface Modes**
  - Cisco Catalyst 2960 and 3560 support the following trunk modes:
    - `switchport mode dynamic auto`
    - `switchport mode dynamic desirable`
    - `switchport mode trunk`
    - `switchport nonegotiate`

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

6. VLAN Types

- **Available VLAN Types**
  - Data VLAN
  - Default VLAN
  - Native VLAN
  - Management VLAN
  - Voice VLAN
- **Data and Default VLANs**

Data VLAN

- Configured to Carry data traffic
- User VLANs for networked devices and computers

Default VLAN

- Default setting on unconfigured switch
- Cisco – VLAN 1
- Same features as other VLANs except it cannot be deleted or renamed
- Default – Carries all **Layer 2** control traffic

- **Native and Management VLANs**

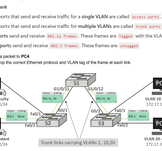
Native VLAN

- Backwards compatibility with other switches
- Non tagged frames on an
- Ethernet Trunk will be assumed to belong to this VLAN
- **Best practice** – change from VLAN 1

Management VLAN

- Default – VLAN 1
- Assigned with IP address for network layer connectivity to switch

- **Voice VLANs**



7. Quizzes

- By creating VLANs in a switched Ethernet network we can segregate users in multiple, isolated ...
  ⇒ **broadcast domain** (Link)
- VLANs help reduce the size of broadcast domains, which in turn improves network performance.
  ⇒ **TRUE**
  - **Explanation:**
    VLANs break up a single broadcast domain into multiple smaller domains.
    ⇒ reduces the number of broadcasts as well as the number of devices processing them
    ⇒ less unnecessary traffic
- **Fill in the blank**
  - Switch ports that send and receive traffic for a **single VLAN** are called `access ports`.
  - Switch ports that send and receive traffic for **multiple VLANs** are called `trunk ports`.
  - **Trunk ports** send and receive `802.1Q frames`. These frames are `tagged` with the VLAN ID.
  - **Access ports** send and receive `802.1 frames`. These frames are `untagged`.

PC2 sends a packet to **PC4**.
Drag and drop the correct Ethernet protocol and VLAN tag of the frame at each link.