# Layer 2 Engineering – VLANs

Network Infrastructure Workshop



Last updated October 2019

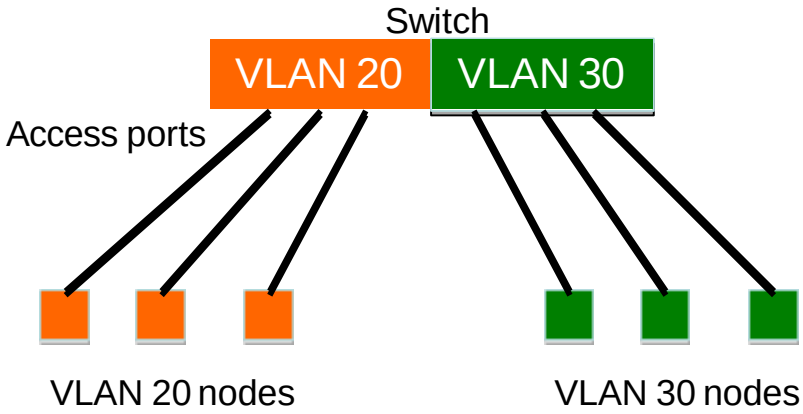
# Virtual LANs (VLANs)

- Allow us to split switches into separate (virtual) switches
- Only members of a VLAN can see that VLAN's traffic
  - Inter-vlan traffic must go through a router
- Allow us to reuse router interfaces to carry traffic for separate subnets
  - E.g. sub-interfaces in Cisco routers

# Local VLANs

- Two or more VLANs within a single switch
- The switch behaves as several virtual switches, sending traffic only within VLAN members
- ***Access ports***, where end nodes are connected, are configured as members of a VLAN
- By default, all ports of a switch are members of VLAN 1 or default VLAN (***VLAN ID*** = 1)
- Newly created VLANs must have a VLAN ID other than 1
  - Then add ports by moving them out of VLAN 1 into our new VLAN

# Local VLANs


Switch
VLAN 20
VLAN 30
Access ports
VLAN 20 nodes
VLAN 30 nodes

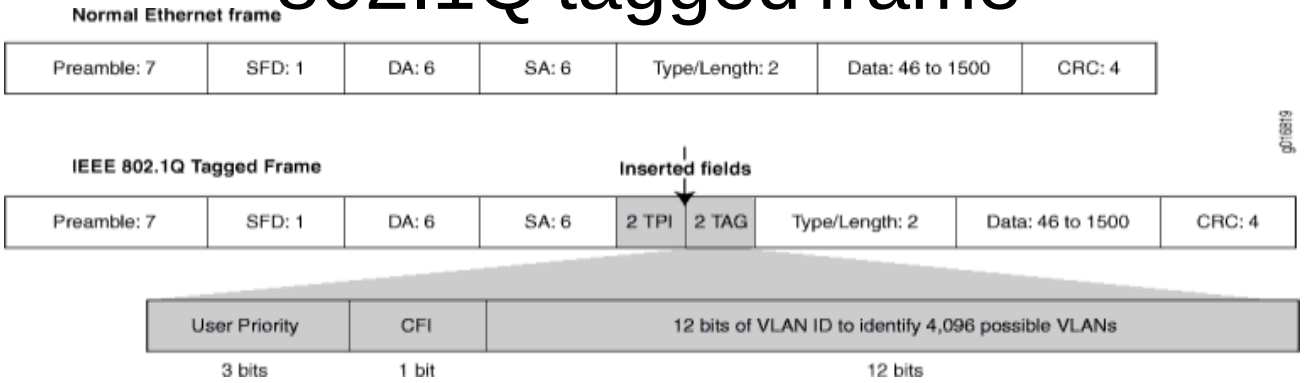
# VLANs across switches

- Two switches can exchange traffic from one or more VLANs
- Inter-switch links are configured as ***trunks***, carrying frames from all or a subset of a switch's VLANs
- Each frame carries a ***tag*** that identifies which VLAN it belongs to

# 802.1Q

- The IEEE standard that defines how ethernet frames should be ***tagged*** when moving across switch trunks
- This means that switches from *different vendors* are able to exchange VLAN traffic.

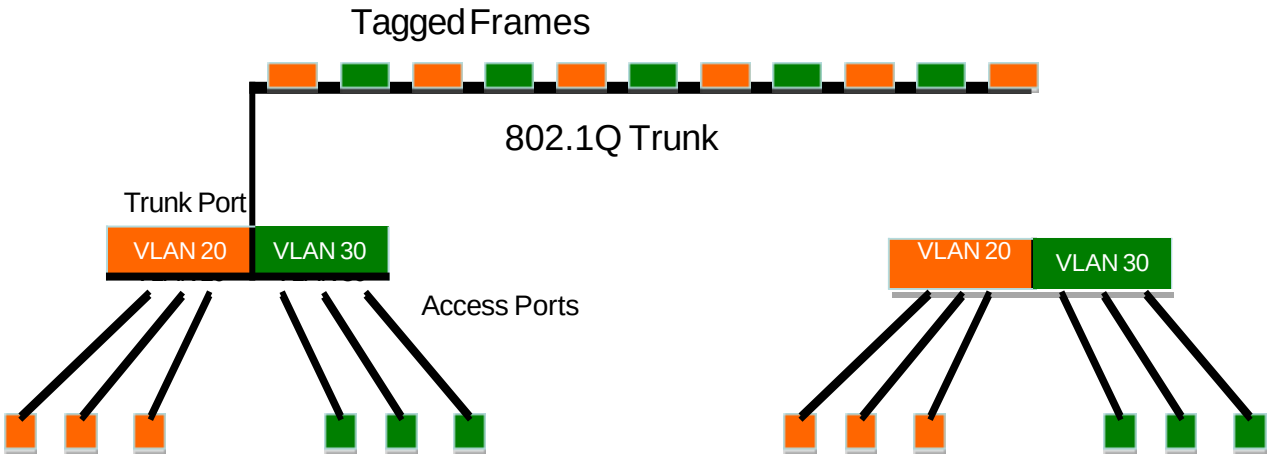
# 802.1Q tagged frame




Normal Ethernet Frame:
•Preamble (7 bytes): Synchronizes communication between devices.
•SFD (Start Frame Delimiter) (1 byte): Indicates the start of the frame.
•DA (Destination Address) (6 bytes): Address of the device the frame is sent to.
•SA (Source Address) (6 bytes): Address of the device sending the frame.
•Type/Length (2 bytes): Indicates either the type of payload (e.g., IPv4, IPv6) or the length of the payload.
•Data (46–1500 bytes): Actual payload (e.g., IP packet).
•CRC (4 bytes): Used for error detection.

IEEE 802.1Q Tagged Ethernet Frame:
TPID (Tag Protocol Identifier) (2 bytes): Identifies the frame as VLAN-tagged (value is 0x8100 for 802.1Q).

# VLANs across switches



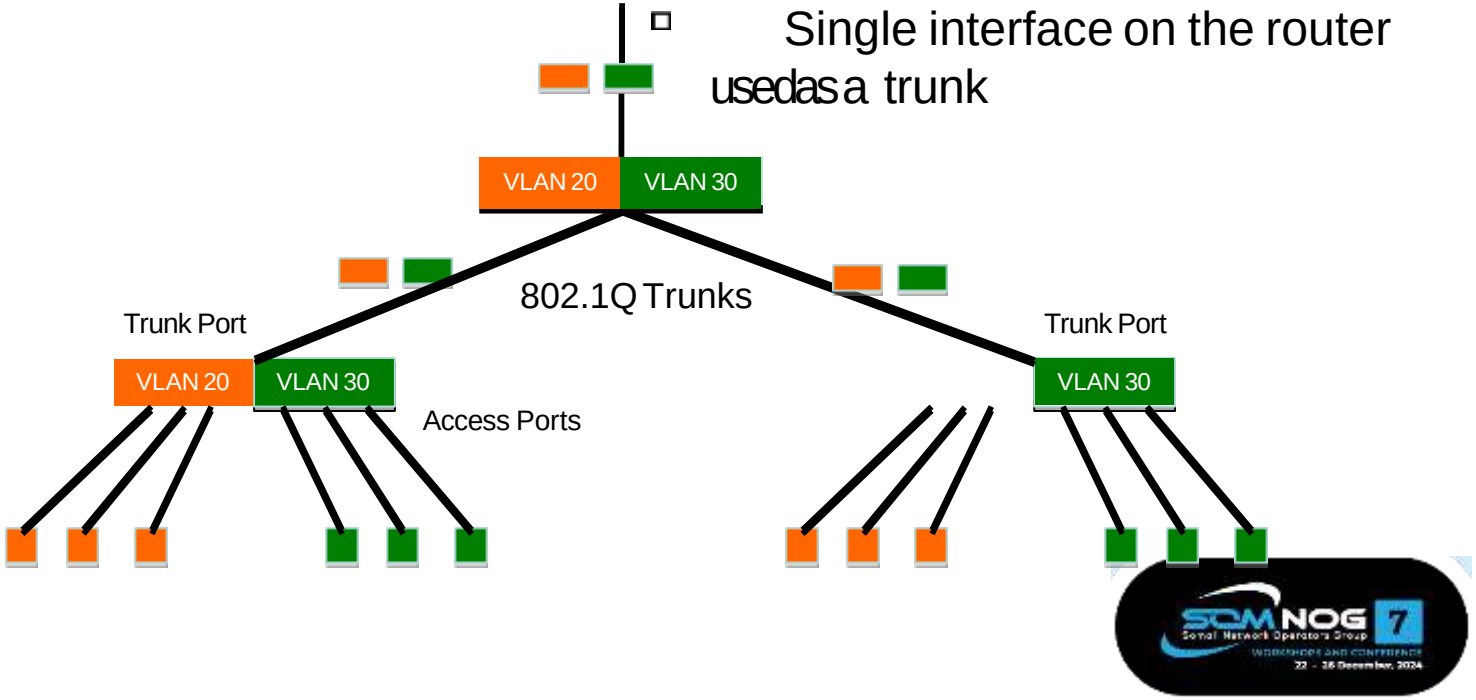

This is called “VLAN Trunking”

# Tagged vs. Untagged

- Frames sent out on access ports are not tagged
  - frames received on access ports are not expected to be tagged either
- You only need to tag frames in switch-to-switch links (trunks), when transporting multiple VLANs
- However, a trunk can transport both tagged and untagged frames
  - As long as the two switches agree on how to handle untagged frames

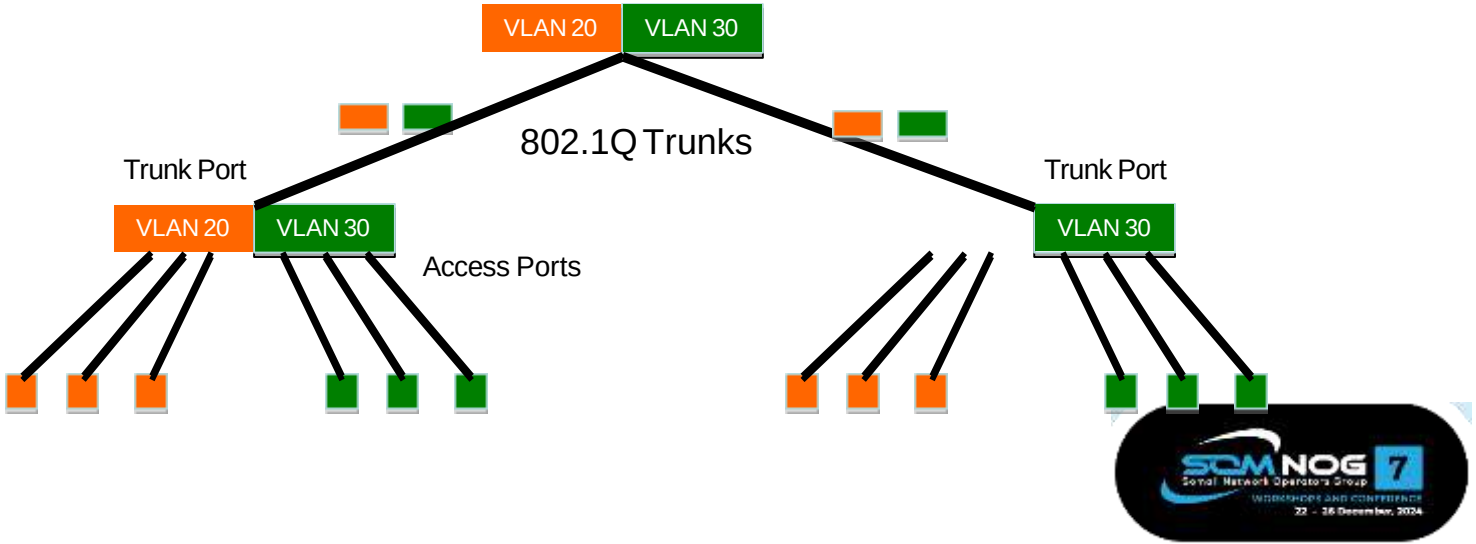
# Routing Inter-VLAN traffic

Traffic between VLANs must now go through a router.



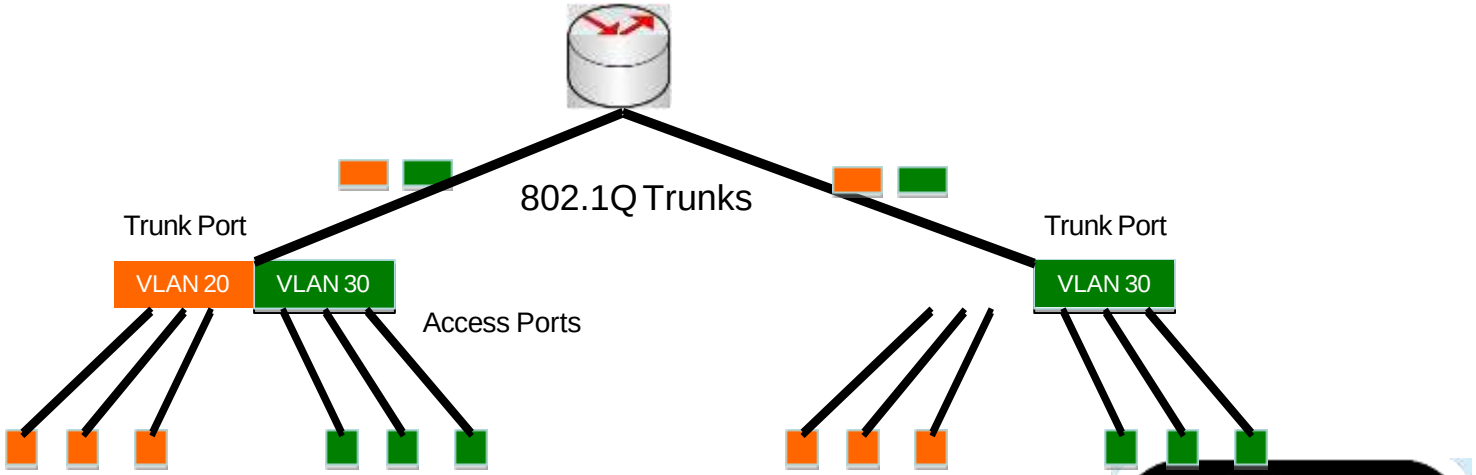
# Routing Inter-VLAN traffic (2)

- Separate interfaces for each VLAN



# Routing Inter-VLAN traffic (3)

Can use a 802.1Q compliant Layer-3 switch to do switching as well routing



# VLANs increase complexity

- You can no longer “just replace” a switch
  - Now you have VLAN configuration to maintain
  - Field technicians need more skills
- You have to make sure that all the switch-to-switch trunks are configured to carry frames of all the necessary VLANs
  - Need to keep in mind when adding/removing VLANs

# Good reasons to use VLANs

- You want multiple subnets in a building, and carry them over a single fibre to your core router
- You want to segment your network into multiple subnets, without buying more switches
  - Separate broadcast domains for wired, wireless, phones, device management etc.
- Separate control traffic from user traffic
  - Restrict who can access your switch management address

# Bad reasons to use VLANs

- Because you can, and you feel cool 
- Because they will completely secure your hosts (or so you think)
- Because they allow you to extend the same IP network over multiple separate buildings
  - This is actually very common, but a bad idea

# Do not build “VLAN spaghetti”

- Extending a VLAN to multiple buildings across trunk ports
- Bad idea because:
  - Broadcast traffic is carried across all trunks from one end of the network to another
  - Broadcast storm can spread across the extent of the VLAN, and affect all VLANS!
  - Maintenance and troubleshooting nightmare

# Cisco configuration

- Configure access port
  - ```
    interface
    GigabitEthernet1/0/3
    switchport mode access
    switchport access vlan 10
    ```
- Configure trunk port
  - ```
    interface
    GigabitEthernet1/0/1
    switchport mode trunk
    switchport trunk allowed vlan 10,20,30
    ```

# Cisco mis-features

- *Disable* VLAN Trunking Protocol (VTP)
  - `vtp mode off`
    *or*
    `vtp mode transparent`

- *Disable* Dynamic Trunking Protocol (DTP)
  - `interface range Gi 1 - 8`
    `switchport mode [trunk|access]`
    `switchport nonegotiate`

# Questions?