Computer Network And Network Design(CNND) ITC402

Subject Incharge

Ms. Jesleena Gonsalves

Assistant Professor

Room No. 326

email: jesleenagonsalves@sfit.ac.in

Whatsapp Group Invite Link -

Module 6

Network Design Concepts

Outline

- Virtual Local Area Networks (VLAN)
- Switching

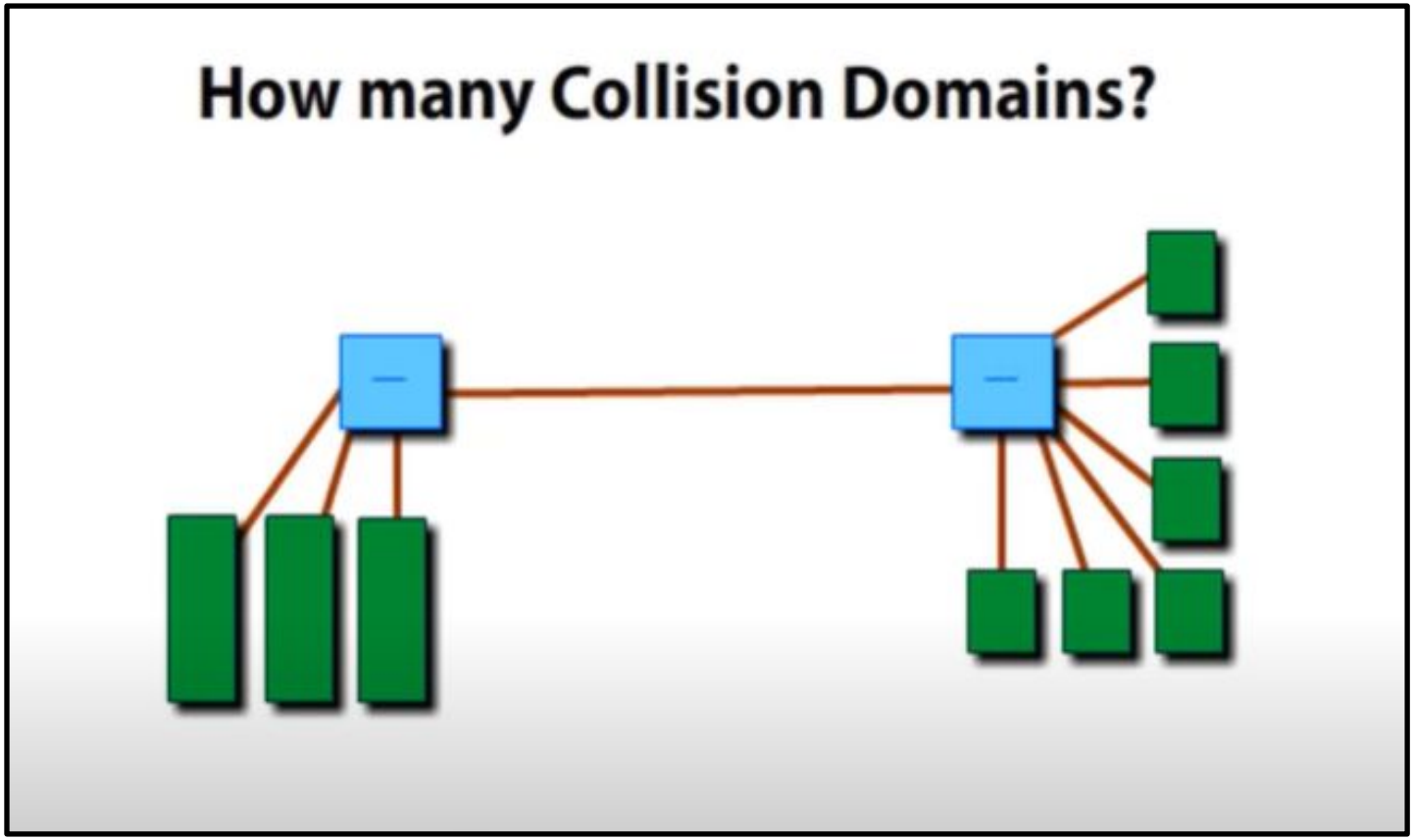
1. Collision Domain
2. Broadcast Domain

- Virtual Private Networks (VPN)

COLLISION DOMAIN

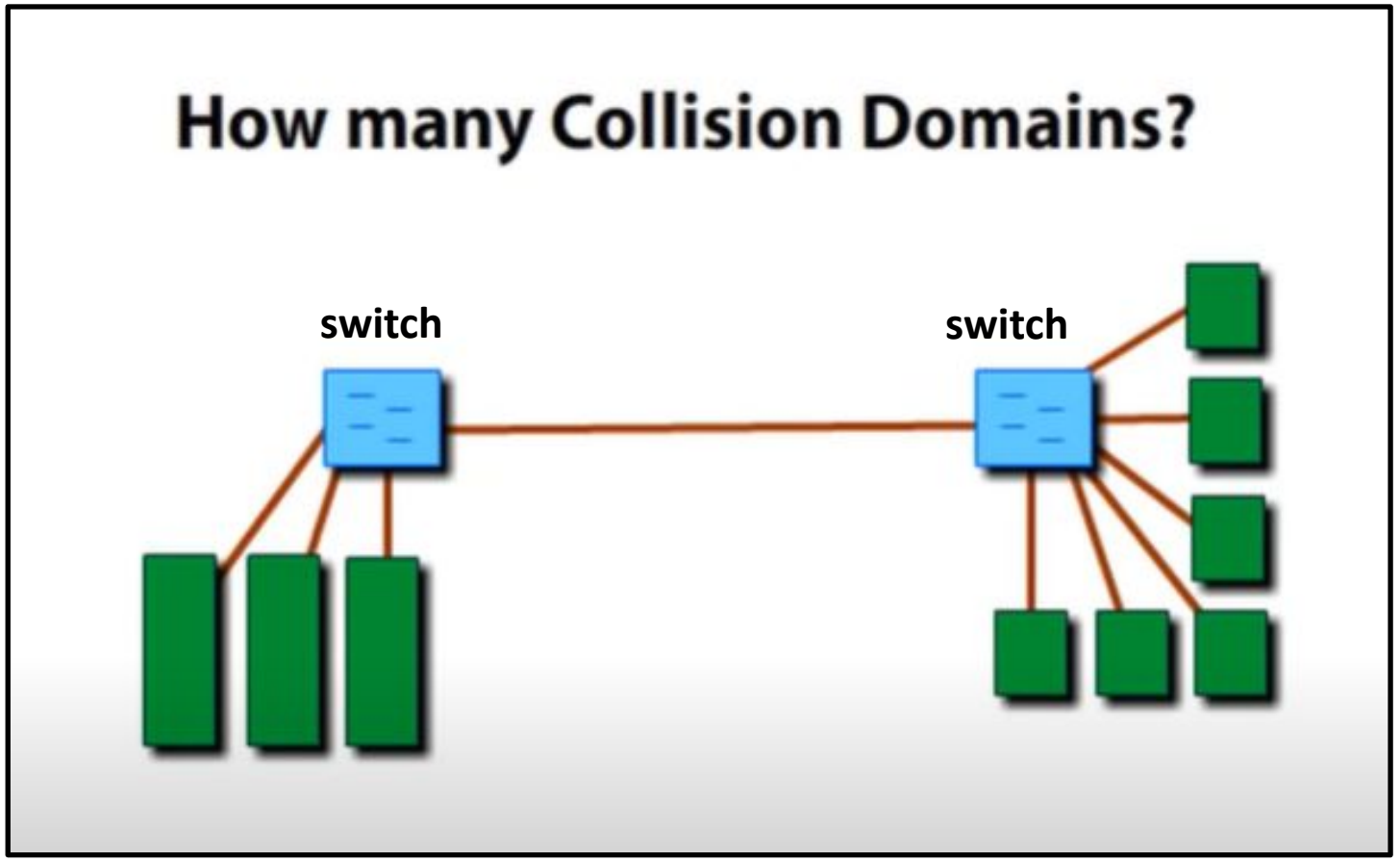
- **Collision domain:** part of a network where **packet collisions** can occur.
- A collision occurs when two devices send a packet at the same time on the shared network segment.
- The packets collide and both devices must send the packets again, which **reduces network efficiency**
- Collisions are common in a hub environment, because each port on a **hub** is in the **same collision domain.**
- By contrast, each port on a **bridge, a switch** or **a router** is in a **separate collision domain.**

COLLISION DOMAIN



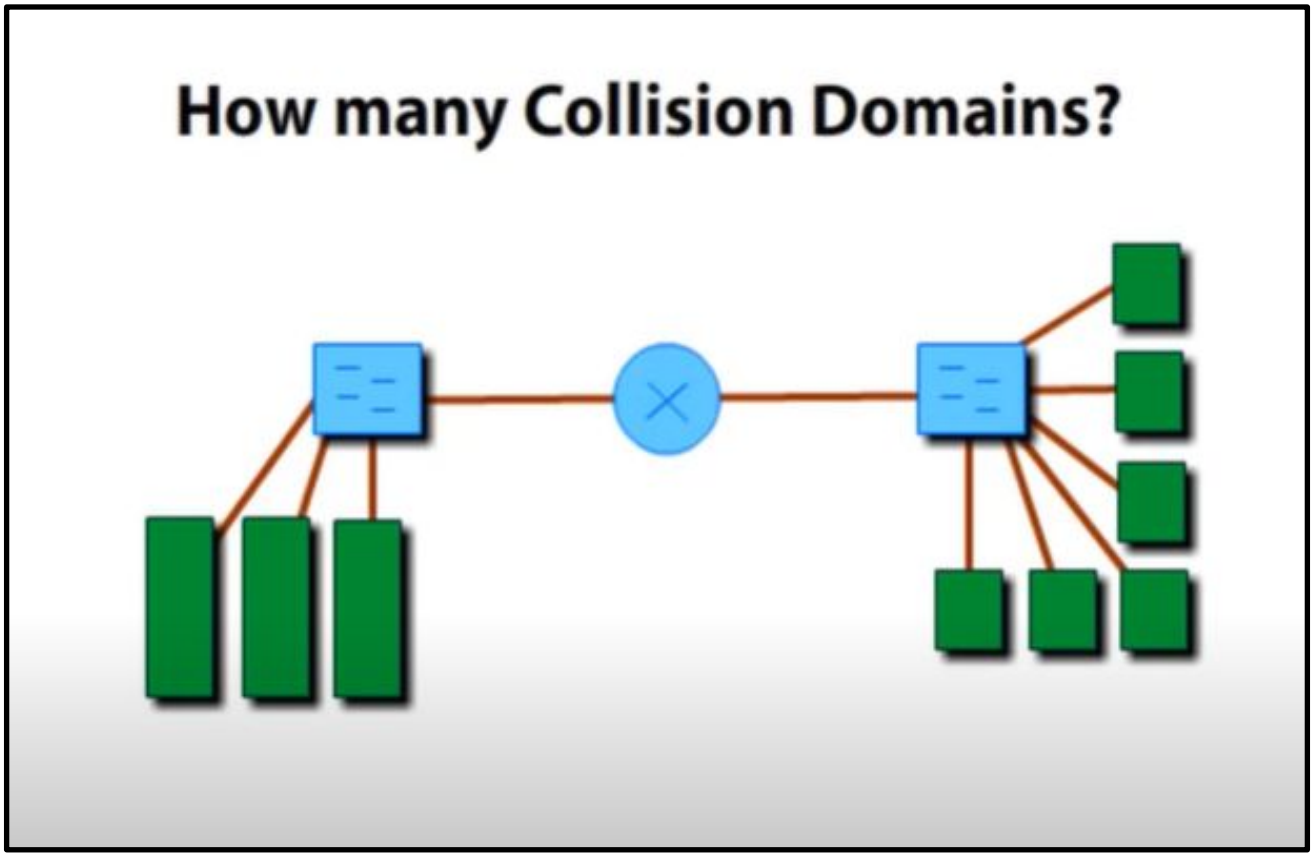
Answer: 1 collision domain

COLLISION DOMAIN



Answer: 10 collision domains

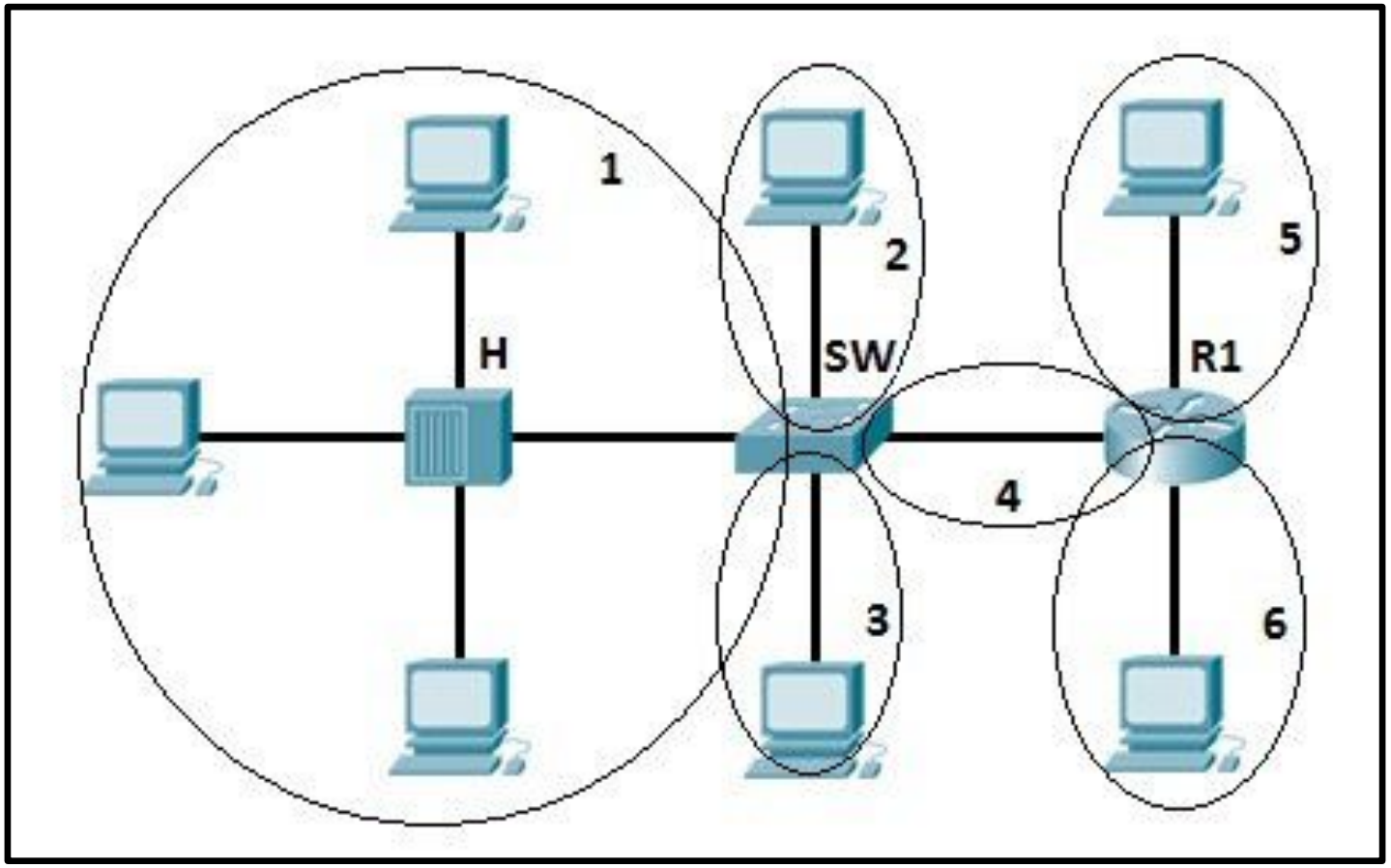
COLLISION DOMAIN



Answer: 11 collision domains

COLLISION DOMAIN

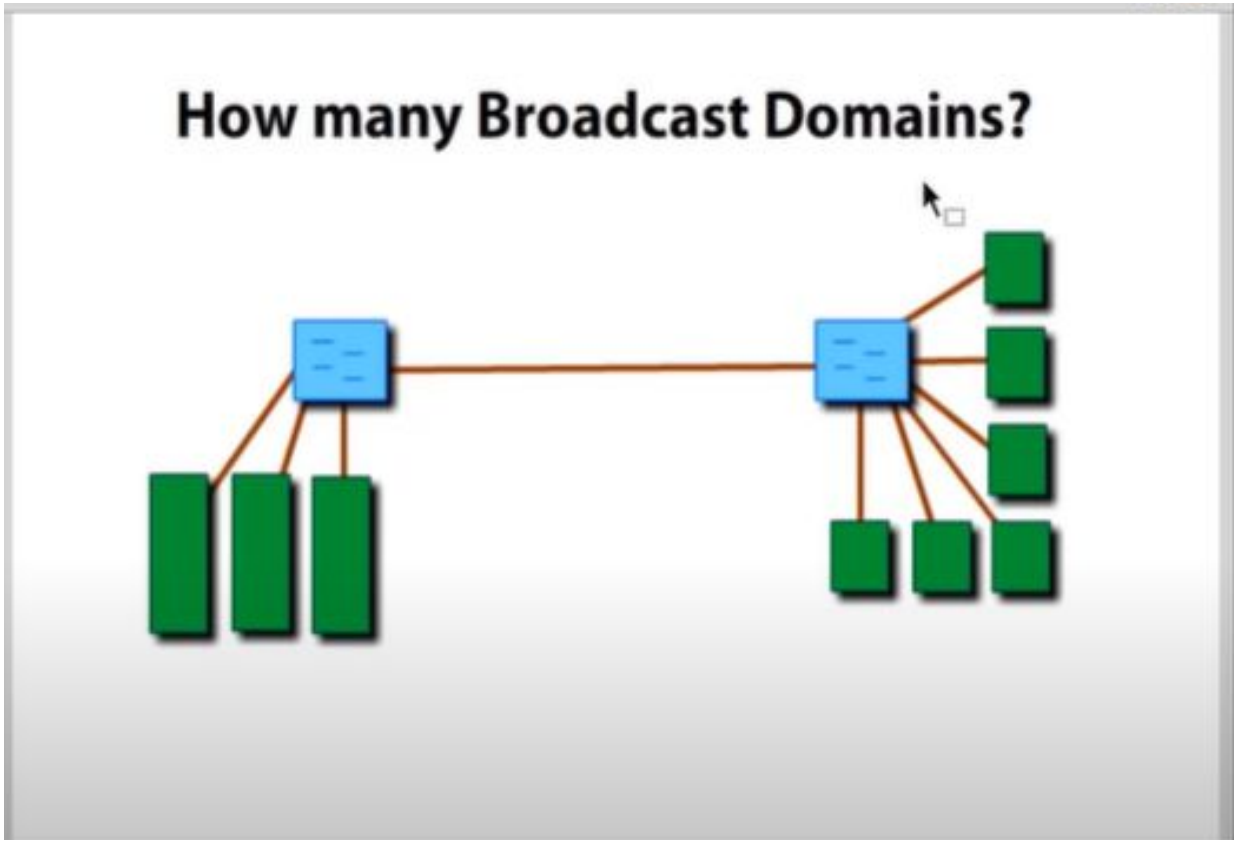
- Each port on a hub is in the same collision domain. Each port on a bridge, a switch or router is in a separate collision domain.



BROADCAST DOMAIN

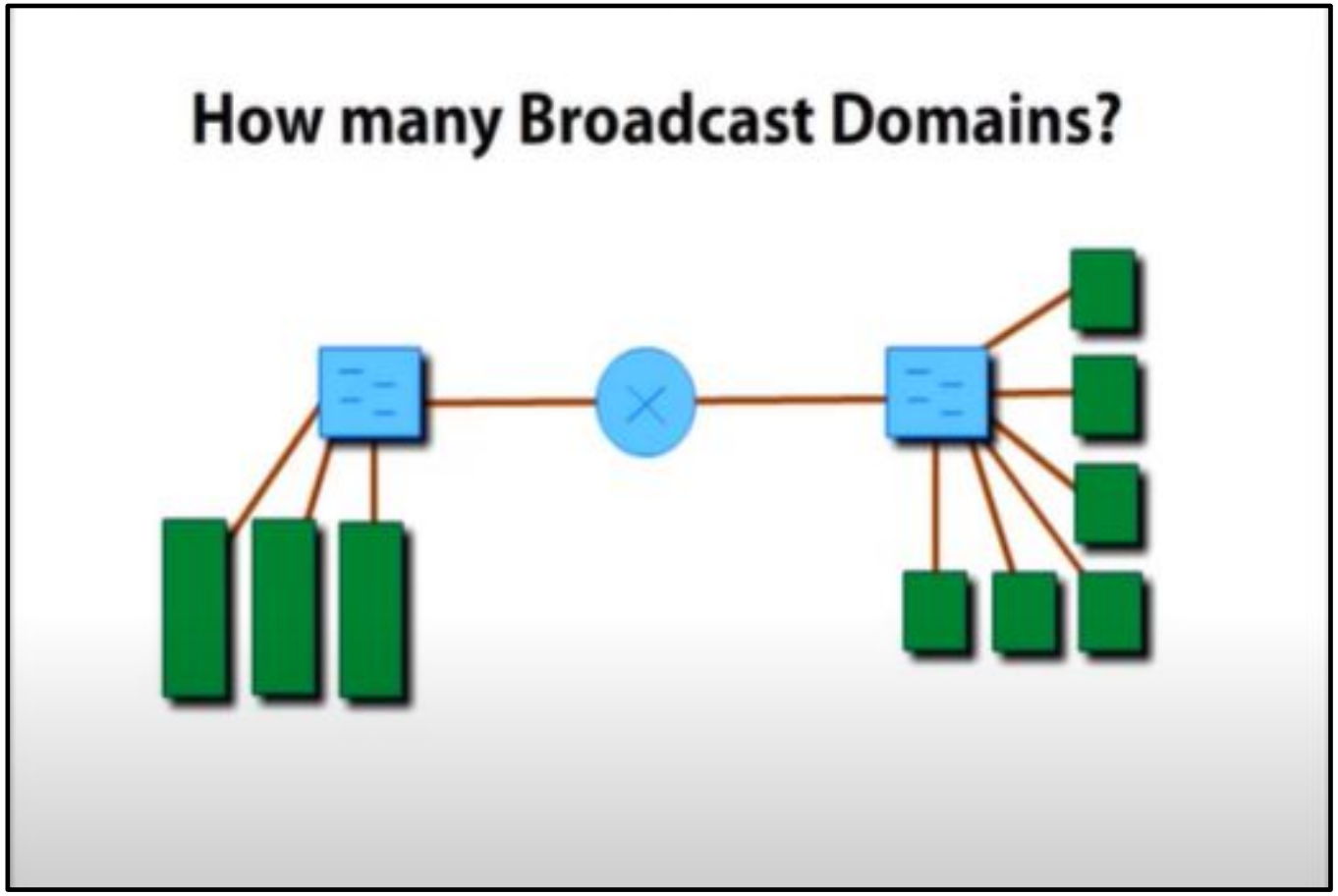
- Broadcast domain: **domain in which a broadcast is forwarded.**
- A broadcast domain contains **all devices** that can reach each other at the **data link layer** (OSI layer 2) by using broadcast messages.
- All **ports on a hub** or **a bridge/switch** are by default in the **same broadcast domain.**
- All **ports on a router** are in the **different broadcast domains.**
- **Routers don't forward broadcasts** from one domain to another.

BROADCAST DOMAIN



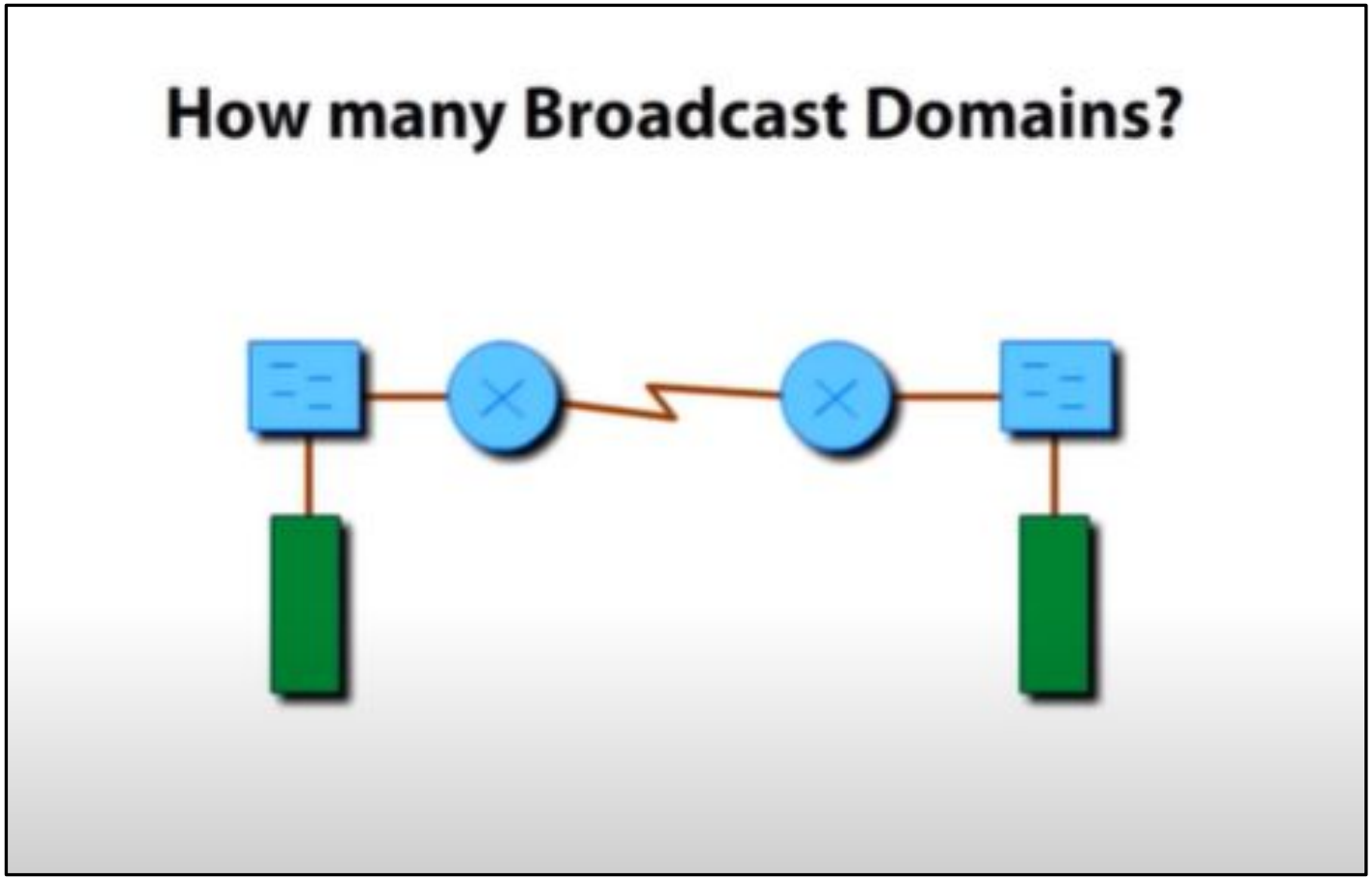
Answer: 1 broadcast domain

BROADCAST DOMAIN



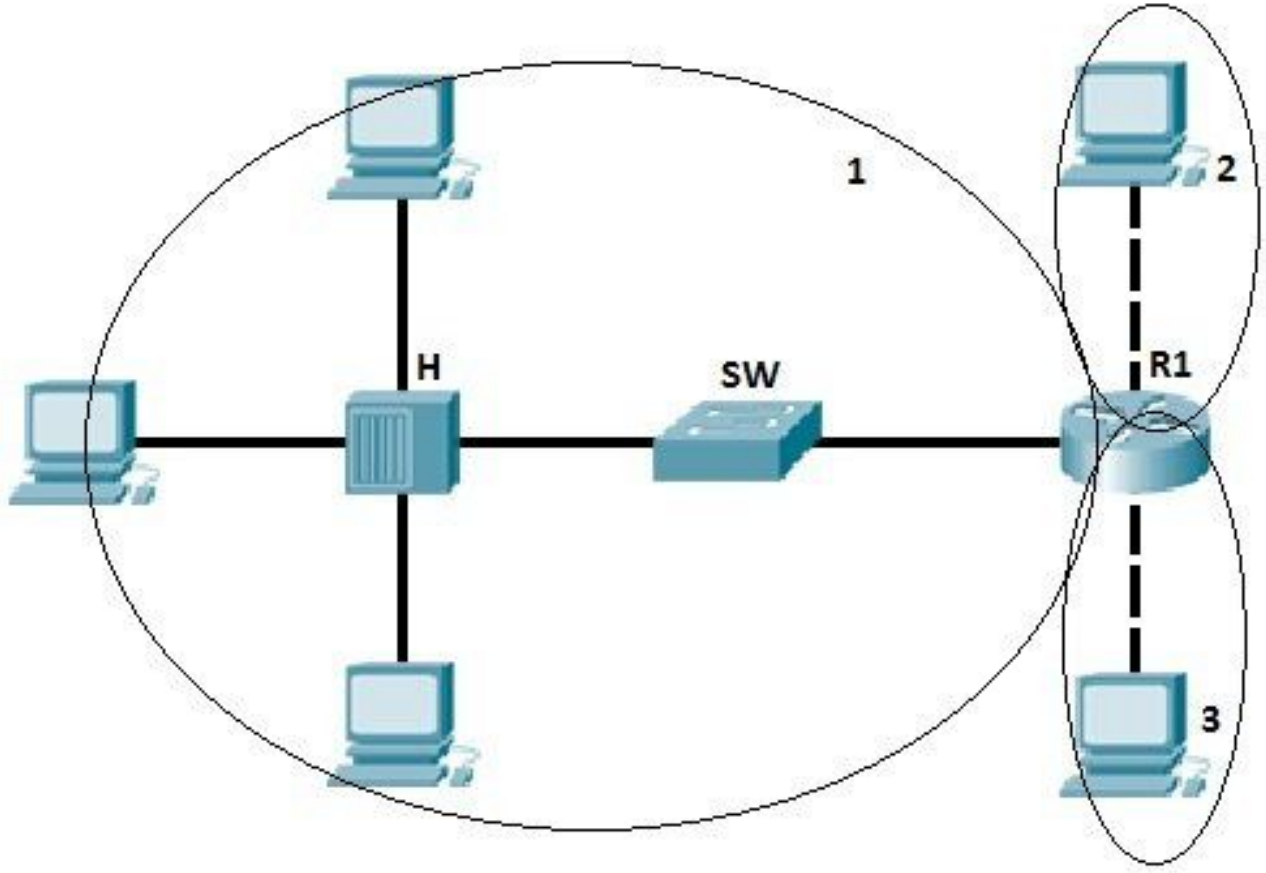
Answer: 2 broadcast domains

BROADCAST DOMAIN



Answer: 3 broadcast domains

BROADCAST DOMAIN



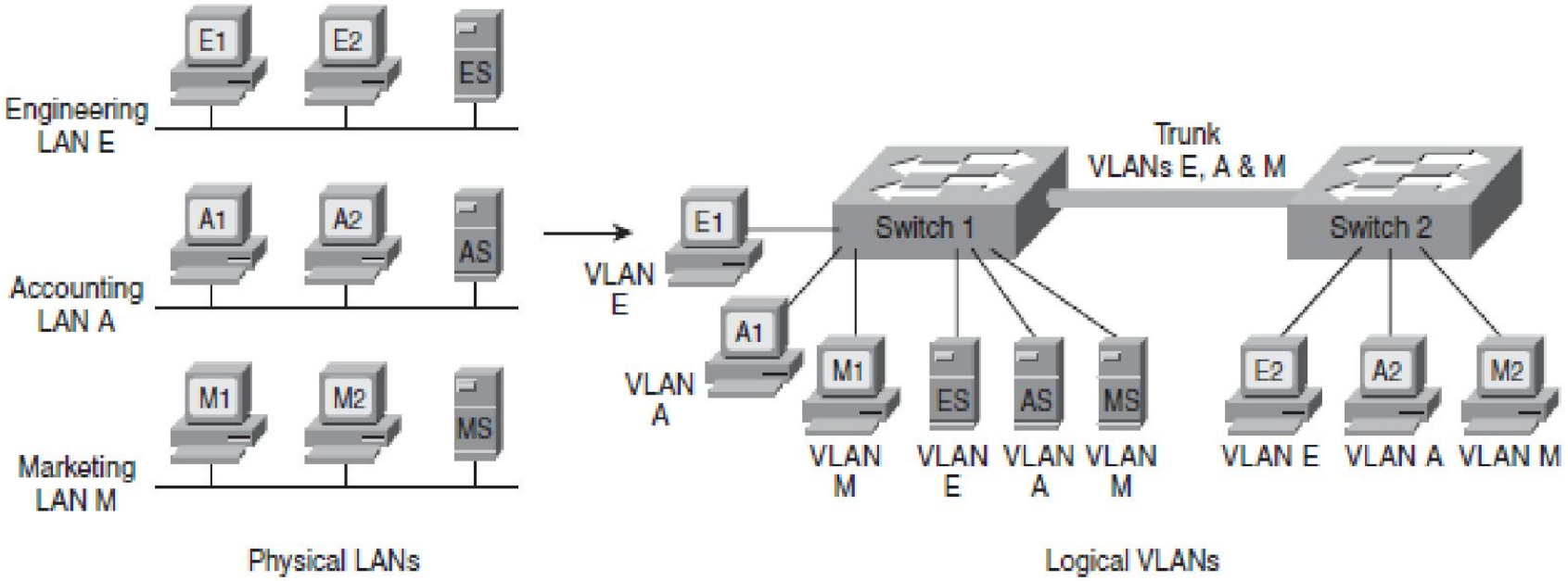
COMPARE

Collision Domain		Broadcast Domain	
Hubs	Bridges Switches Routers	Hubs Bridges Switches	Routers
All ports in same collision domain	Every port is in different collision domain	All ports in same broadcast domain	Every port is in different broadcast domain
Form large collision domains	Divides collision domains	Form large broadcast domains	Divides broadcast domains
Cause more collisions	Avoid collisions	Hubs and bridges cause Broadcast storms Switches along with VLAN can divide broadcast domains	Routers don't forward broadcasts
Affects network performance adversely	Improves network performance by dividing collision domains	Affects network performance adversely	Improves network performance by dividing broadcast domains

VLAN

- Broadcast domain is a set of devices that receive each others broadcasts (typically LANs)
- Hubs, bridges, switches forwards the broadcasts, only router blocks it.
- Concept of Virtual LAN allows separating broadcast domains with the help of switches
- What is VLAN?
  - **Group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.**
- VLANs are based on logical instead of physical connections
- They are extremely flexible.

VLAN



Note:

- Members of each department can be physically located anywhere, yet still be logically connected with their own workgroup
- VLANs A, E and M will be forming separate broadcast domains

VLAN

- VLANs can span multiple switches.
- The link between the two switches that carries traffic from all three VLANs is called a **trunk.**

VLAN Membership

- **A switch port that is not a trunk can belong to only one VLAN at a time.**
- **It is possible to statically or dynamically configure which VLAN a port belongs to**
  - **Static port membership**: the network administrator configures which VLAN the port belongs to
  - **Dynamic port membership**: switch dynamically assigns proper VLAN to the devices, but need to maintain separate server (VMPS)

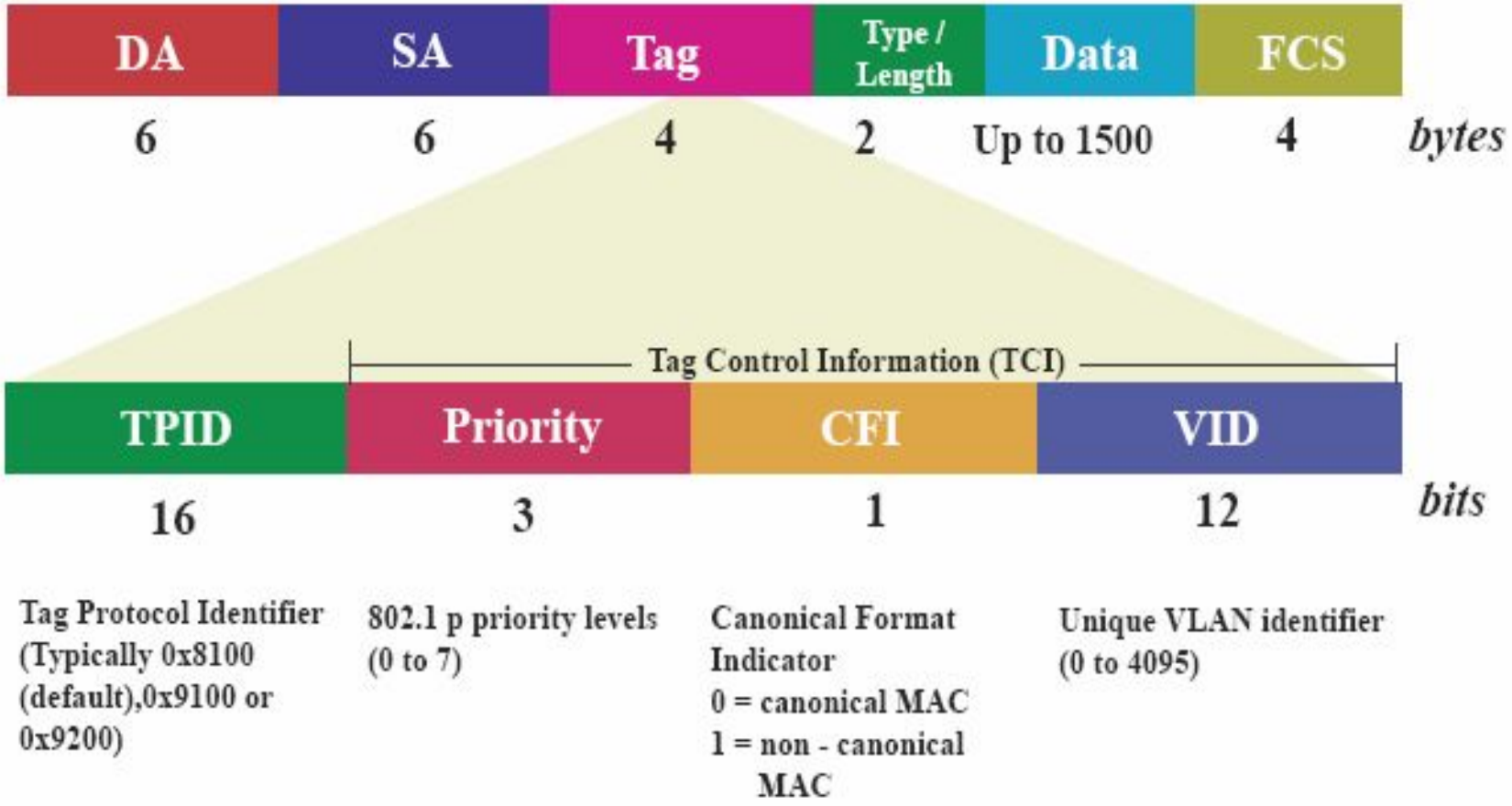
VLAN

- **Trunks**
  - a port that carries data from multiple VLANs
  - A trunk port can be on a switch, a router or a server
  - Protocols used:
    - Inter-switch Link (ISL) – Cisco proprietary
    - IEEE 802.1Q
- **IEEE 802.1Q**
  - trunking information is encoded within a Tag field inserted inside the frame header.
  - Trunks using the 802.1Q protocol supports native VLAN
  - Traffic for the native VLAN is not tagged, it is carried across the trunk unchanged.

VLAN IEEE 802.1Q

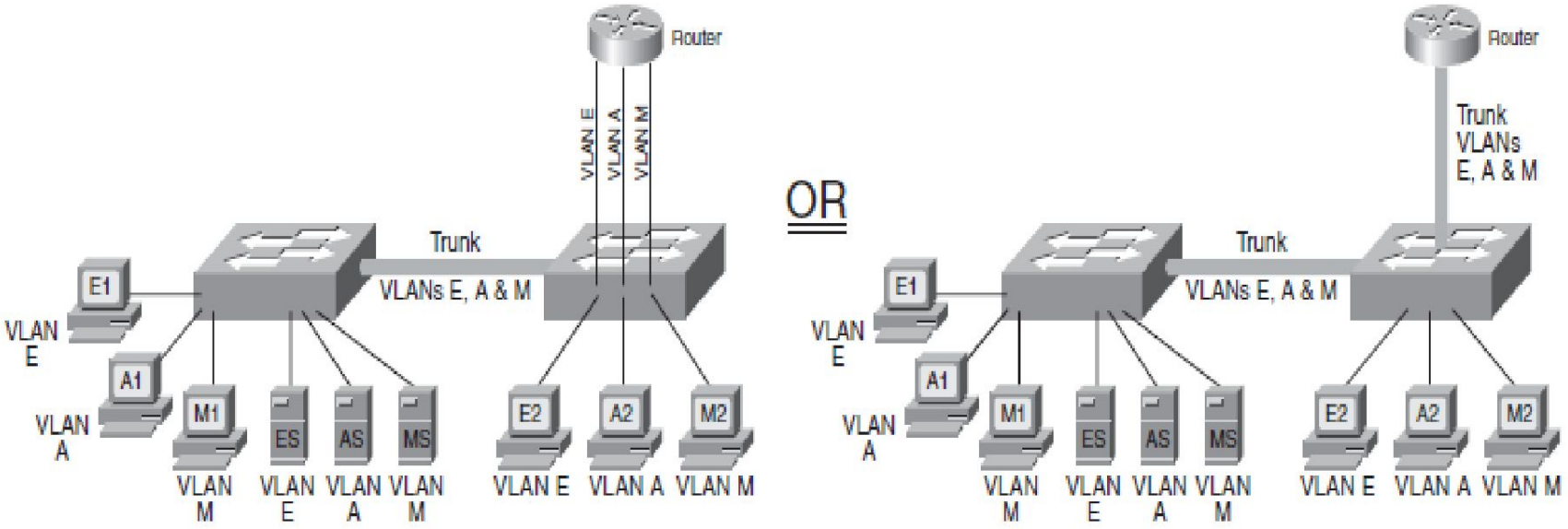
- End-user stations that don't understand trunking can communicate with other devices directly over an 802.1Q trunk as long as they are on the native VLAN.
- The native VLAN must be defined to be the same VLAN on both sides of the trunk.
- Within the Tag field,
  - The 802.1Q VLAN ID field is 12 bits long, allowing up to 4096 VLANs to be defined
  - also includes a 3-bit 802.1p user priority field, these bits are used as class of service (CoS) bits for QoS marking

VLAN



INTER VLAN ROUTING

- Devices on different VLAN require a Layer 3 mechanism (a router or a Layer 3 switch) to communicate with each other.



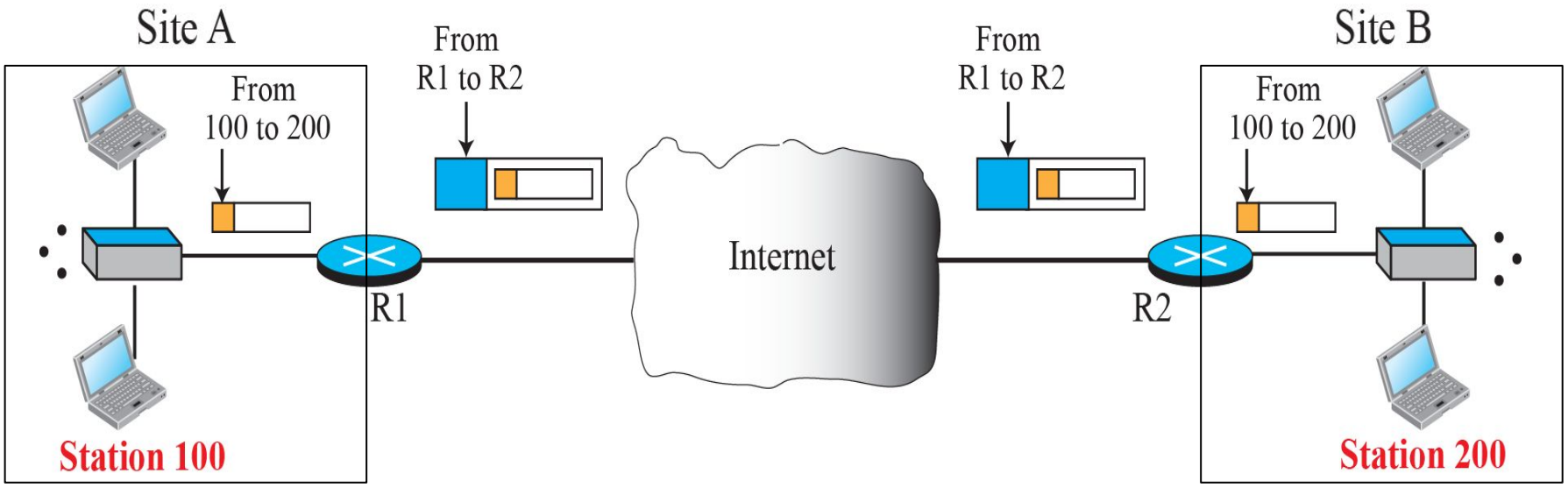
INTER VLAN ROUTING

- A Layer 3 device can be connected to a switched network in two ways:
  - by using multiple physical interfaces
  - through a single interface configured as a trunk.
- The diagram on the left illustrates a router with three physical connections to the switch
- each physical connection carries traffic from only one VLAN.
- The diagram on the right illustrates a router with one physical connection to the switch.
- The interfaces on the switch and the router have been configured as trunks; therefore, multiple logical connections exist between the two devices.
- Each interface between the switch and the Layer 3 device, whether physical interfaces or logical interfaces within a trunk, is in a separate VLAN and therefore in a separate subnet for IP networks.

Virtual Private Networks (VPN)

- VPN is a network that is private but virtual.
- It is private because it guarantees privacy like inside the organization.
- It is virtual because it does not use real private WANs.
- It use public network such as internet to connect privately.
- The network is physically public but virtually private.

Virtual Private Networks (VPN)



Virtual Private Networks (VPN)

- Figure shows the idea of a virtual private network.
- Routers R1 and R2 use VPN technology to guarantee privacy for the organization.
- VPN technology uses the IPSec protocol in the tunnel mode.
- A private datagram, including the header, is encapsulated in an packet.
- The router at the border of the sending site uses its own IP address and the address of the router at the destination site in the new datagram. The public network (Internet) is responsible for carrying the packet from R1 to R2.
- Outsiders cannot decipher the contents of the packet or the source and destination addresses.

REFERENCES

- https://www.youtube.com/watch?v=A9lMH0ye1HU\
- https://www.youtube.com/watch?v=CWy3x3Wux6o

Thank you ...