CS3103: Computer Networks Practice

Packet Framing & Link-Layer Switching

VLAN

MPLS

Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

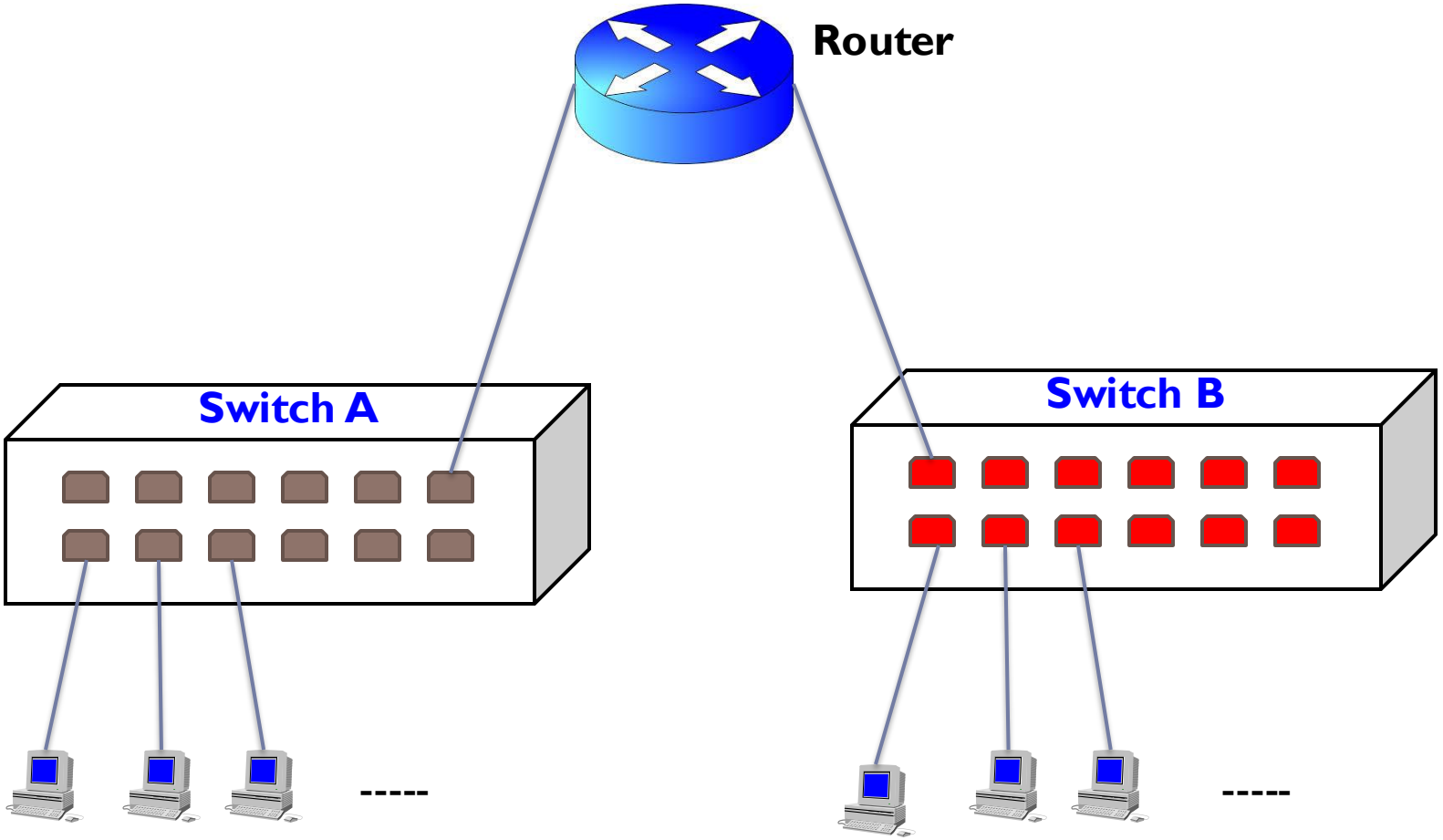
Packet Framing & Link-Layer Switching

Virtual LAN

- Motivation
- Typical LAN & VLAN
- VLAN Techniques
- VLAN implementation

Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

LAN/Subnet – An Example



Subnet - **Motivating Example**

- A company has been allocated an IP address block of 165.65.0.0/22 and wants to support six departments with following number of hosts

Subnet	# hosts
a. Mfg unit 1	200
b. R & D	70
c. Mfg unit 2	400
d. Admin	50
e. Marketing	28
f. Sales	26

What are possible network configurations?

Make it Simple - One Subnet

Total number of Hosts < 1,000, IP Addresses Available ~ 2^10 = 1024

Use one single subnet?

- Single broadcast domain to all hosts
- A host sees all traffic

Unable to meet common requirements:

- Separate network management traffic from end-user or server traffic.
- Isolate sensitive traffic from normal traffic
- Prioritize or implement Quality of Service (QoS) rules for specific services

Another Option: Multiple subnets (one subnet per department) => next slide

Subnet vs VLAN (VLAN – Motivation)

- A company has a 165.65.0.0/22 and wants to form subnets (LANs) for six departments

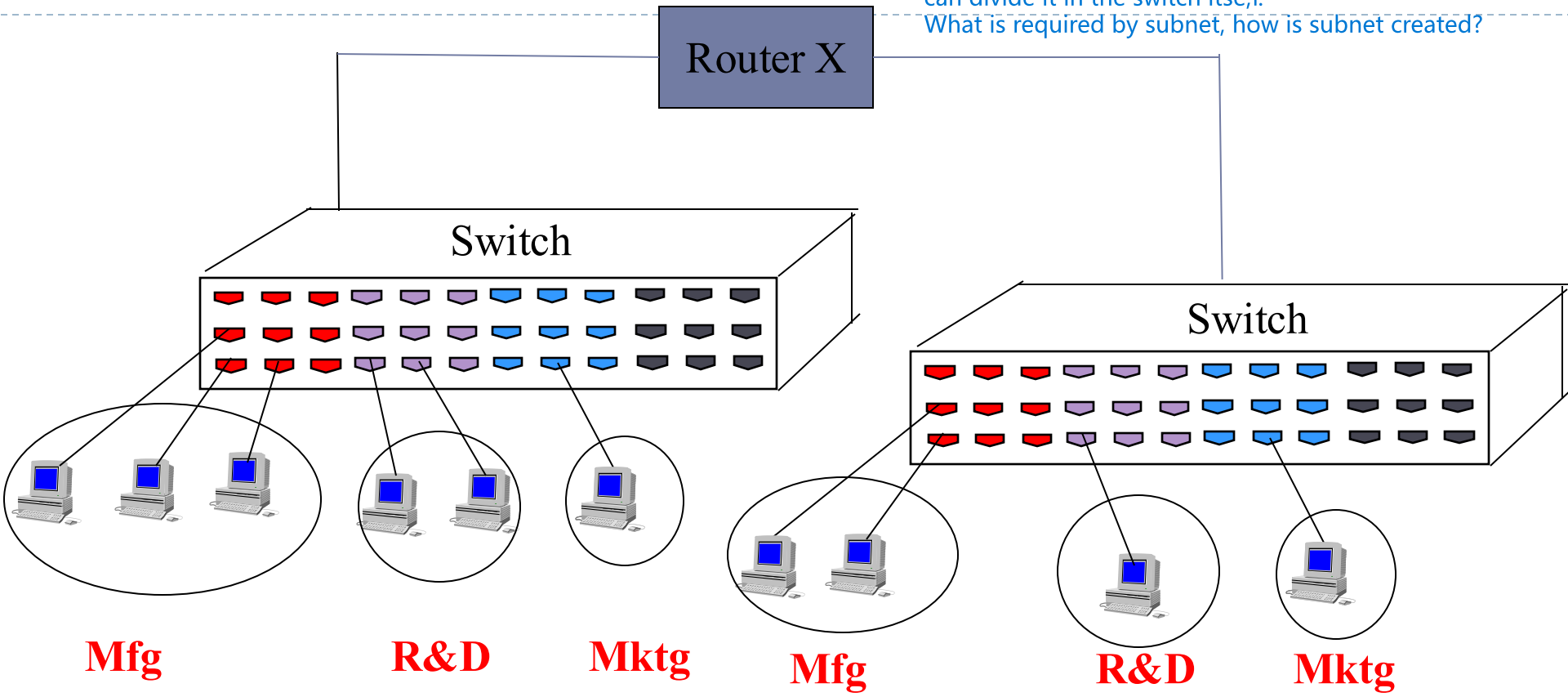
are there other ways to make subnets within subnets

Subnet	# hosts	**Subnet Id (A.B.C.D/n)**	**Broadcast Id**
a. Mfg unit 1	200	165.65.2.0/24	165.65.2.255
b. R & D	70	165.65.3.0/25	165.65.3.127
c. Mfg unit 2	400	165.65.0.0/23	165.65.1.255
d. Admin	50	165.65.3.128/26	165.65.3.191
e. Marketing	28	165.65.3.192/27	165.65.3.223
f. Sales	26	165.65.3.224/27	165.65.3.255

Q: What are the main deficiencies of LAN/Subnetting?

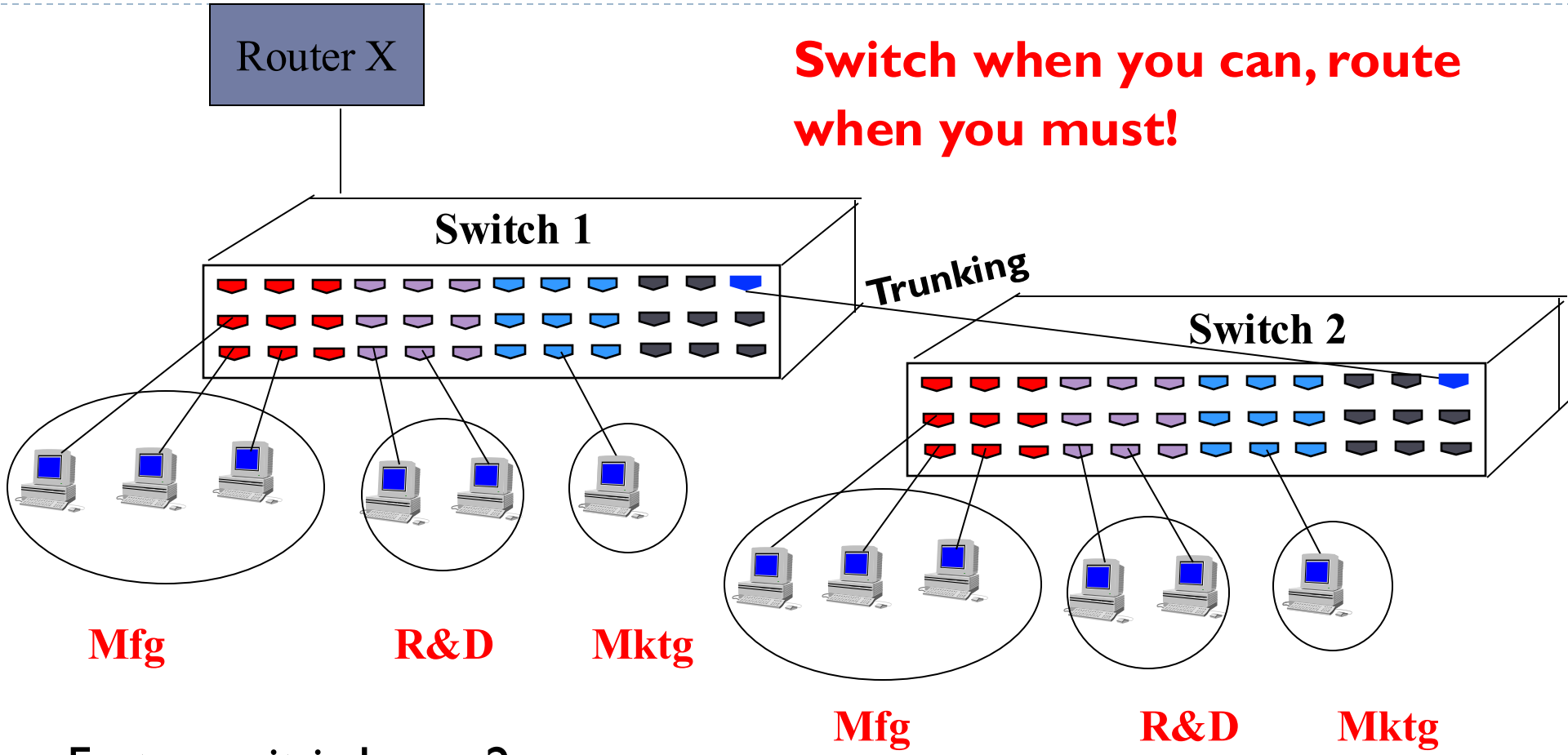
VLAN – An example

instead of requiring different switches for every subnet, can divide it in the switch itse;f.
What is required by subnet, how is subnet created?



- Segment without physically being in the same network (which is required by subnet). Easy to segment network
- Facilitate easy administration (policies for each department can be easily applied and managed.)
- Better security & improved performance
- Move anywhere easily and still be in the same VLAN

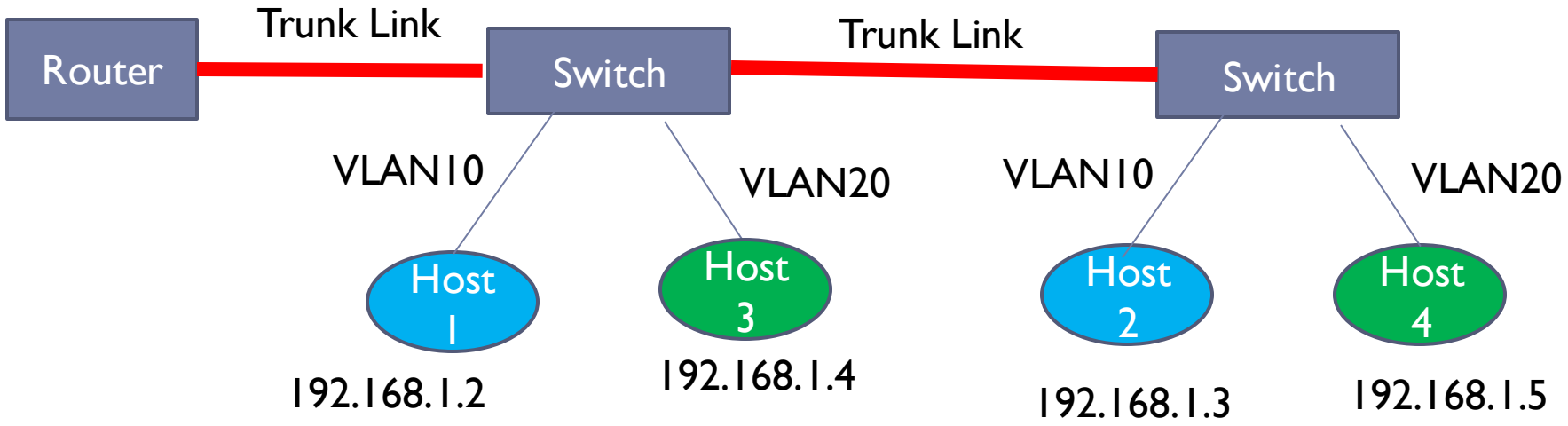
VLAN – An example [Trunking]



- Faster as it is Layer 2
- Switches bridge traffic within same VLAN (Broadcast frames are only switched on the same VLAN ID.)
- Switches DO NOT bridge traffic across different VLANs

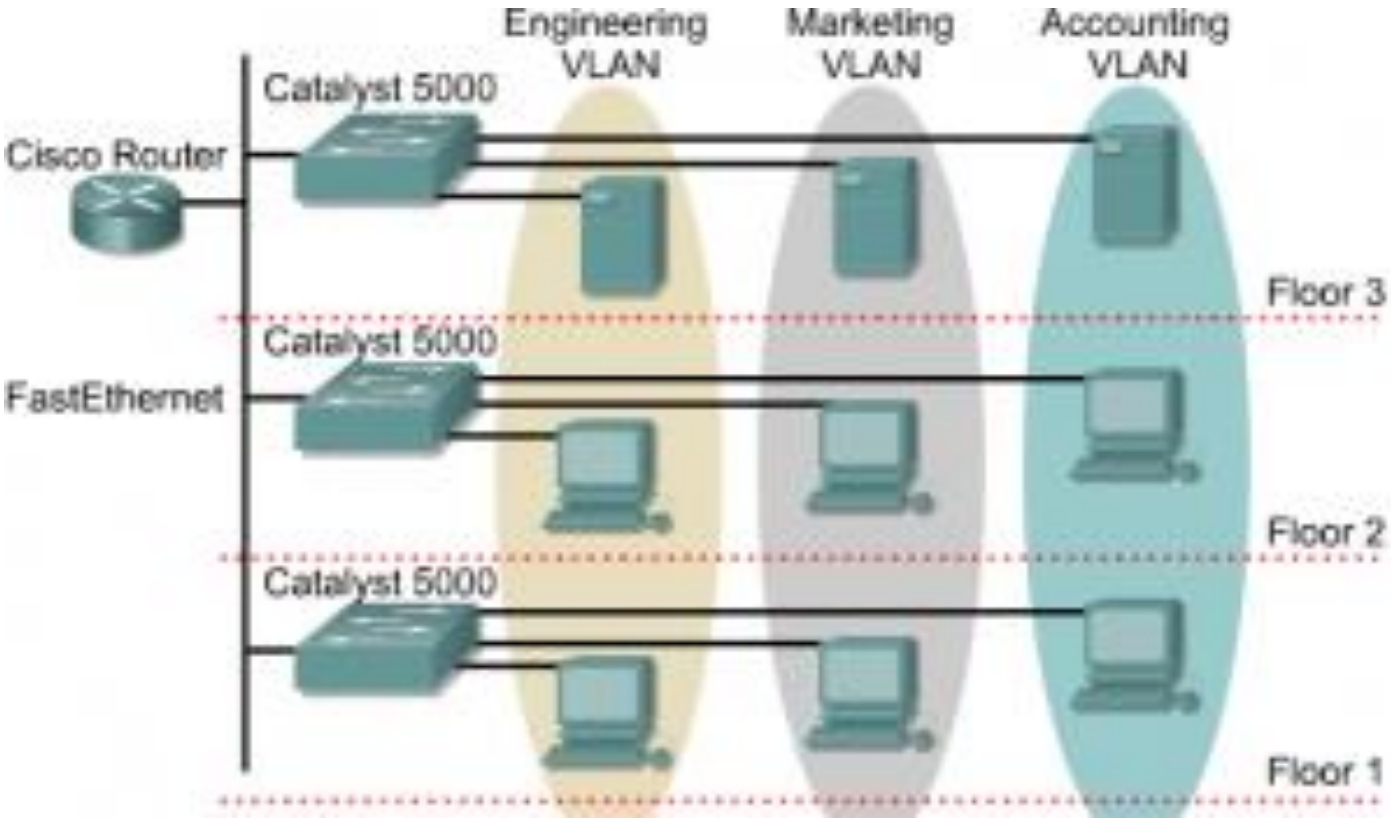
VLAN – Another View

This topology is also called "router on a stick"



Trunking is used for VLAN communication between switches

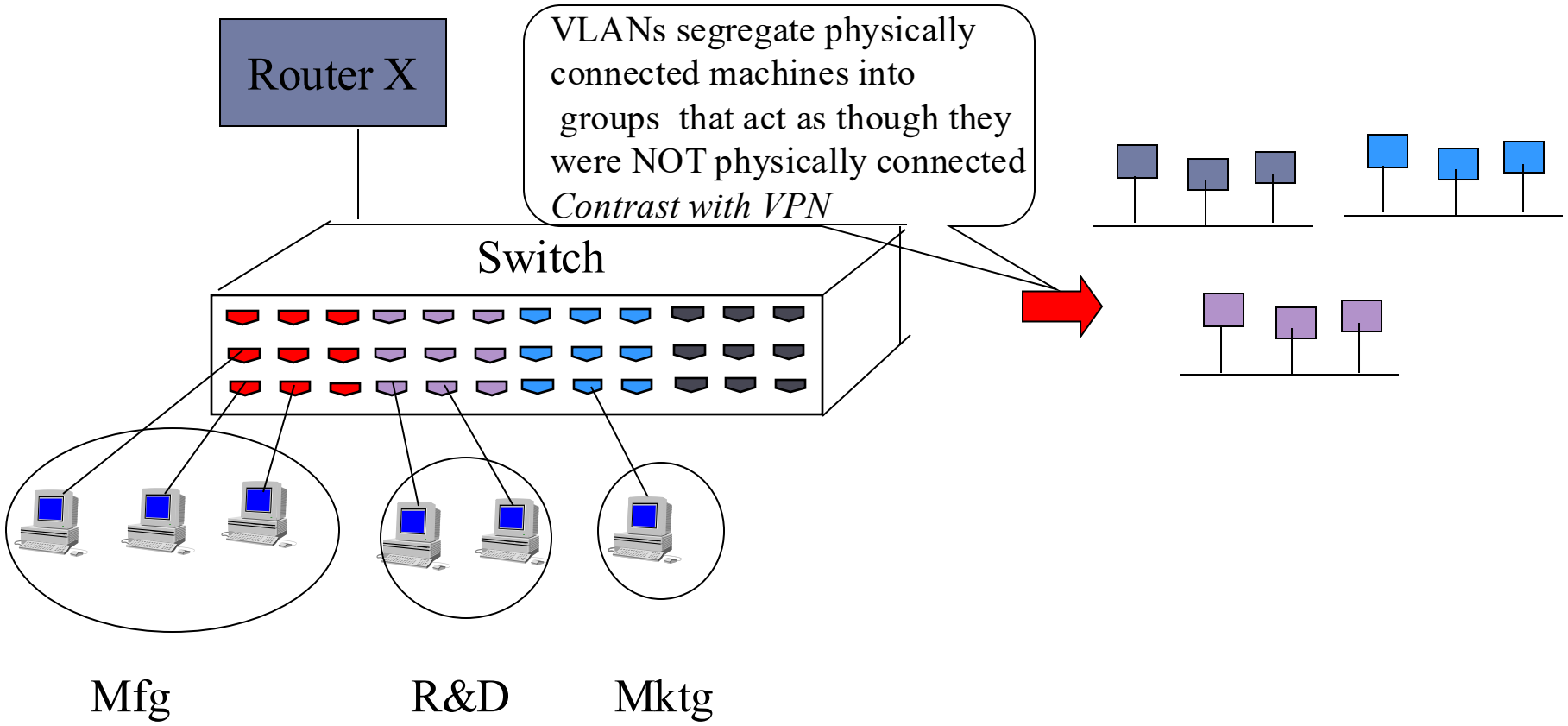
VLAN – Another View



"router on a stick" architecture

- Routers in VLAN topologies provide:
  - security
  - traffic flow management
  - broadcast filtering

VLAN – Another View (in Single Switch)



LAN vs VLAN

LAN or Subnet:

1. LAN is a broadcast domain under a single switch
2. Grouped based on the switch/hub (physically)
3. Traffic between LANs is routed using a router.

VLAN:

1. VLAN is a broadcast domain created by one or more switches.
2. Grouped based on logical function, department or application
   - 20% to 40% of work force moves every year
   - Recabling / readdressing and reconfiguration
3. Traffic can be routed between VLANS with a router

VLAN – VLAN Table & Switching

- Switches maintain a separate bridging table or VLAN table for each VLAN :-

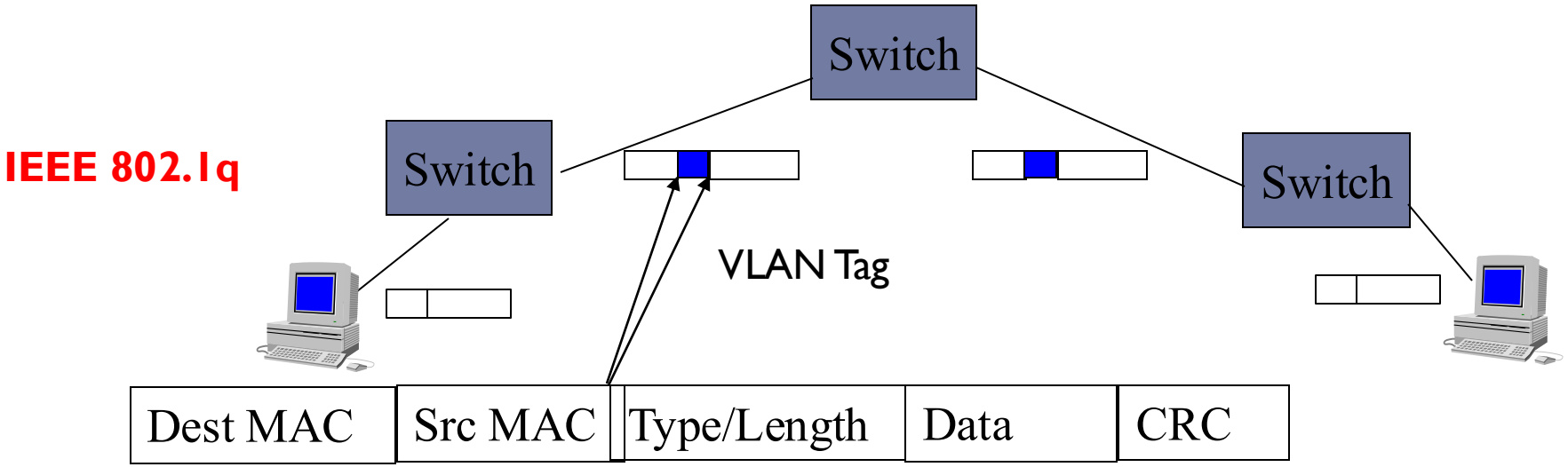
  tuple(VLAN id, Switch Interface or port).

- VLANs can logically segment users into different subnets (broadcast domains). Broadcast frames are only switched on the same VLAN ID.
- Users can be logically grouped via software based on:
  - port number
  - MAC address
  - protocol being used
  - application being used
  - User Identity and Role based

VLAN across backbone

- Two techniques
  - Frame Filtering
    - Examines particular information about each frame (MAC address or layer 3 protocol type)
  - Frame Tagging
    - Places a unique identifier in the header of each frame as it is forwarded throughout the network backbone.
    - **Popular tagging standard 802.1Q**: VLAN traffic between switches (trunks) is tagged (802.1q) to identify VLAN membership

VLAN Frame Tagging



Ethernet II or DIX frame format

- First switch (Ingress Switch) adds tag containing VLAN id to all incoming packets
- Intermediate switches do not recompute the VLAN id
- Last switch (Egress Switch) removes tags from all outgoing packets

Q: Identify the difference between DIX, 802.3 and Ethernet II Frame formats

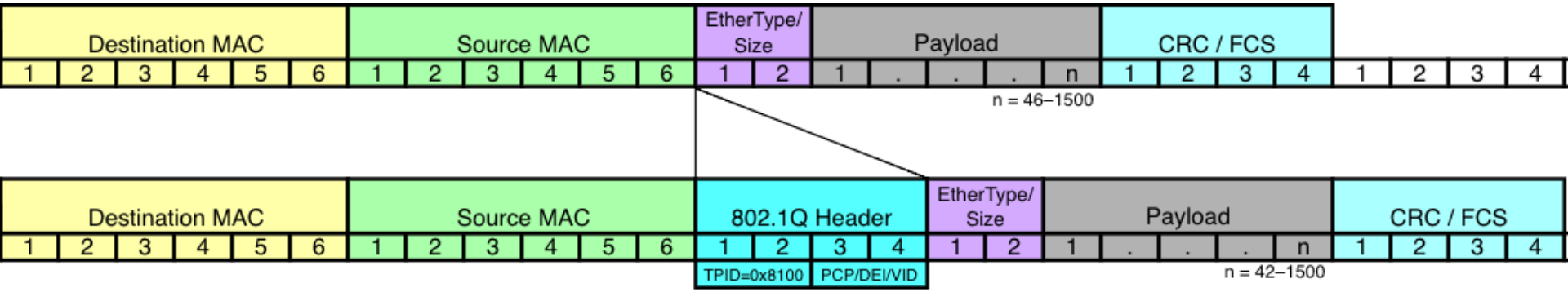
https://pollev.com/banand

Make sure you

LOGIN using your NUSNET ID.

(Counts towards participation Marks)

VLAN Frame Tagging – 802.1q

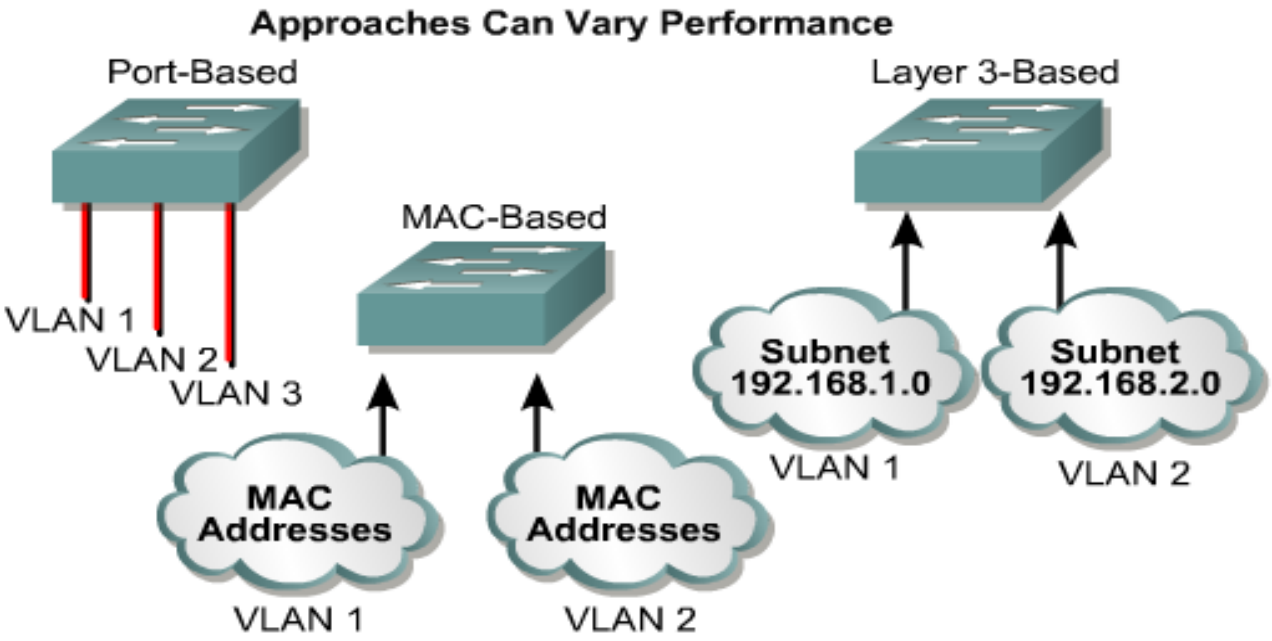


1. *Tag Protocol Identifier (TPID)* -> 0x8100 indicates IEEE 802.1Q-tagged frame
2. Priority code point (PCP) -> 3-bit Frame Priority.
   - PCP: 1 (background), 0 (best effort, default), 2 (excellent effort), 3 (critical application), 4 (video), 5 (voice), 6 (internetwork control), 7 (network control).
3. Drop eligible indicator (DEI) > 1-bit flag. 1 (eligible to drop), 0 (non-eligible). May be used separately or in conjunction with PCP
4. VID – VLAN ID [12 bits]

Q: Double Tagging is Possible. When double tagging is required?

VLAN implementation

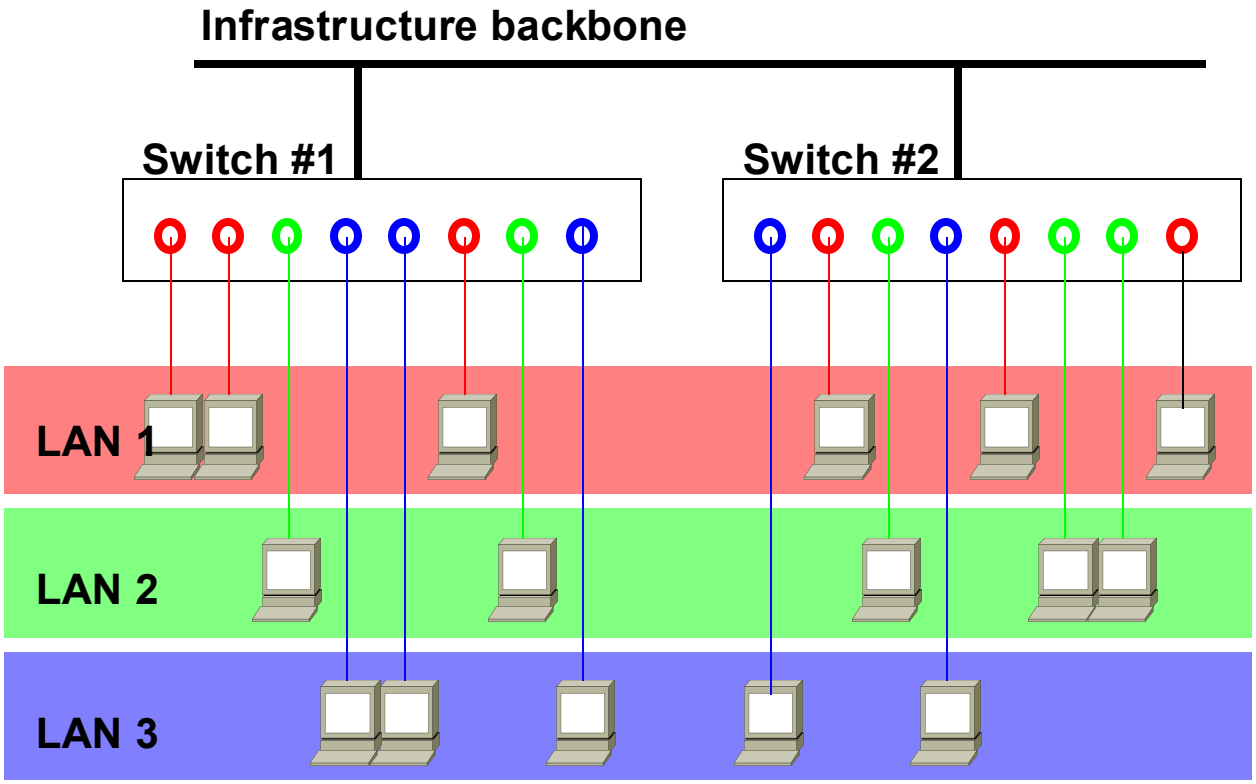
- Created by software running on Layer 2 switches
- Two methods for implementing VLANs
  - Static: Port-Centric or Port-Based
  - Dynamic: MAC Address Based; Layer 3 Protocol Based; User Indeitity and Role based



Network address driven or Layer 3 protocol based approach is not used that much these days due to DHCP

- Port driven
- MAC address driven
- Network address driven

Port Based VLAN (Static-VLAN)

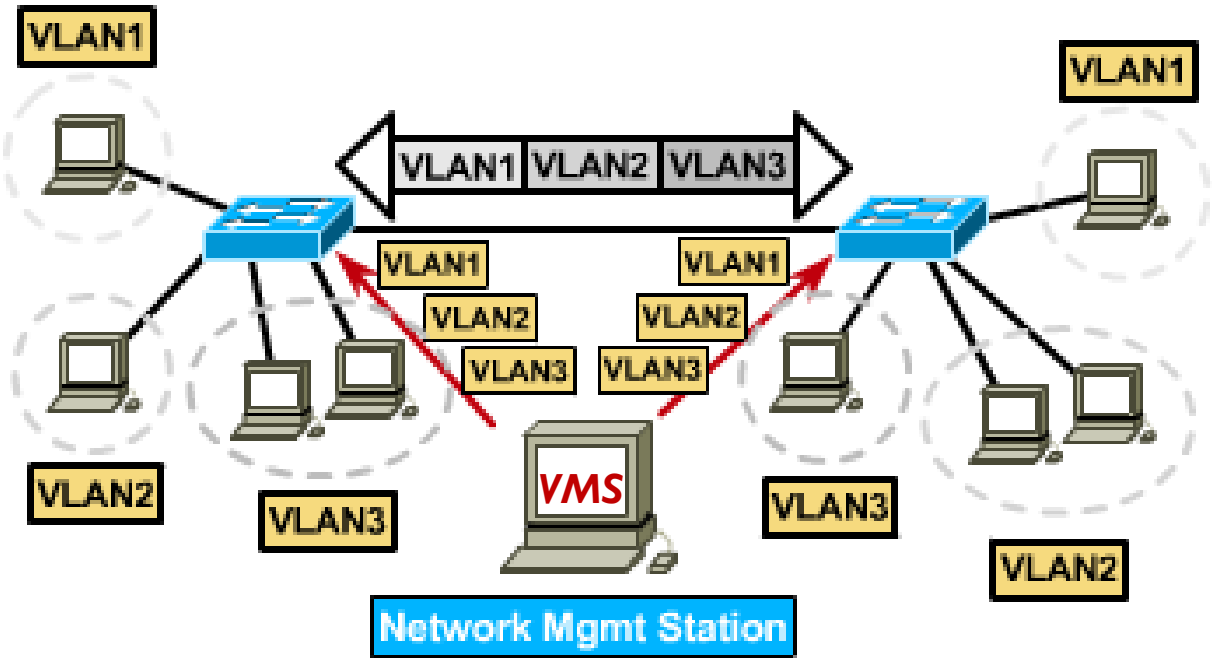


VLAN Table

Port	VLAN
1	3
2	1
3	2
4	3
5	1
6	2
7	2
8	1

- Physical ports on a switch are administratively assigned to a VLAN (independent of the user or system attached to the port)
- Also known as **port switching**
- Provides security and isolation
- User mobility may require configuration

Port-Centric VLAN (Static-VLAN)



- The default VLAN for every port in the switch is the management VLAN.
- The management VLAN is always **VLAN 1** and may not be deleted. All ports on the switch may be reassigned to alternate VLANs.
- static VLANs are configured using ***VLAN management software (VMS) or manually using the CLI***
- Benefits
  - secure, easy to configure and monitor
- Problem
  - user movements in the network should be controlled

https://pollev.com/banand

Make sure you
LOGIN using
your
NUSNET ID.

(Counts towards
participation Marks)

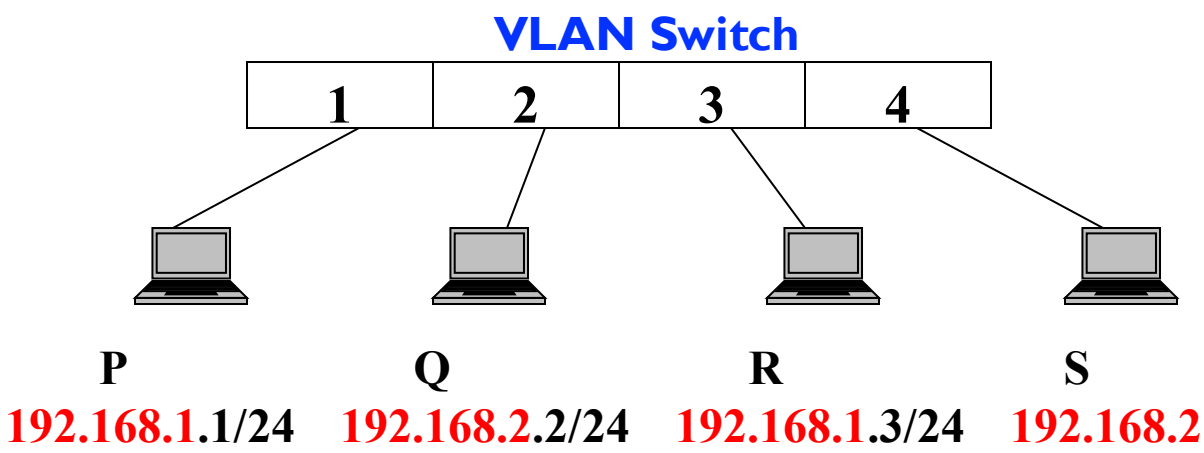
Packet Framing & Link-Layer Switching

Virtual LAN - Continued

Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

Example

- Port 1 and 2 belong to Vlan-1, port 3 and 4 belong to Vlan-2. IP address and netmask of P, Q, R and S are shown as below: (Note: there is no router)



VLAN Table

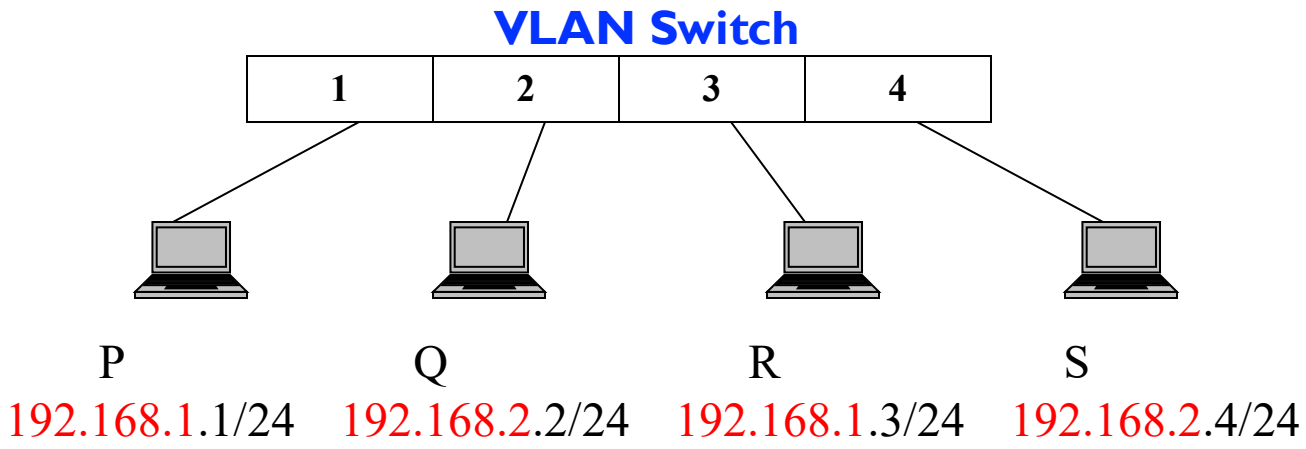
Port	VLAN
1	1
2	1
3	2
4	2

State true or false.

Host Q can ping Host S : _____

Example

- Port 1 and 2 belong to Vlan-1, port 3 and 4 belong to Vlan-2. IP address and netmask of P, Q, R and S are shown as below: (Note: there is no router)



VLAN Table

Port	VLAN
1	1
2	1
3	2
4	2

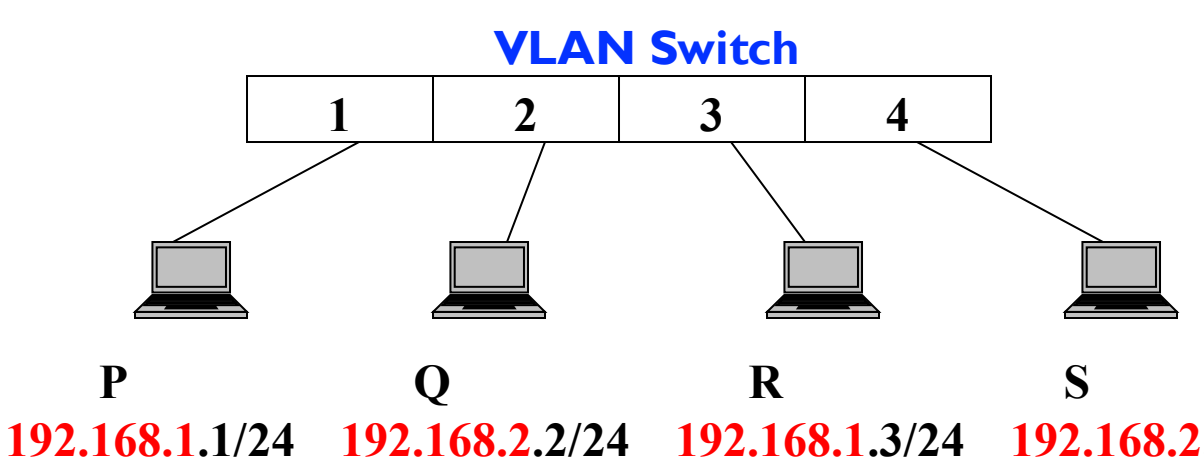
State true or false.

Host P can ping Host Q : no p and q same vlan BUT DIFFERENT SUBNET SO ARP WILL HAVE AN ISSUE SO CANNOT, PING IS FROM LAYER 3 SO ARP BROADCAST WILL NOT REACH ~~NODE Q FOR ARP B~~BROADCAST TO REACH, SAME VLAN SAME SUBNET

Suppose we swap the VLAN assignment of port 2 and 3, how does the answers to above queries changes? ➔ NEXT SLIDE

Example

- Port 1 and 3 belong to Vlan-1, port 2 and 4 belong to Vlan-2. IP address and netmask of P, Q, R and S are shown as below: (Note: there is no router)



VLAN Table

Port	VLAN
1	1
2	2
3	1
4	2

State true or false.

Host Q can ping Host S : _____

Configuring a Static VLAN Using CLI

- Create a VLAN entry in the VLAN database
  - *Switch#* vlan database
  - *Switch(vlan)#* vlan vlan_number
  - *Switch(vlan)#* exit
- Assign VLAN to a port
  - *Switch(config)#* interface fastethernet 0/9
  - *Switch(config-if)#* switchport access vlan vlan_number

```
SydneySwitch#configure terminal
SydneySwitch(config)#interface fastethernet 0/3
SydneySwitch(config-if)#switchport access vlan 2
SydneySwitch(config-if)#
```

- Show Commands
  - *Switch#* show vlan
  - *Switch#* show vlan brief
  - *Switch#* show vlan id id_number

Configuring a Static VLAN Using CLI

- To remove port fa 0/2 from vlan2
  - *Switch(config)#* interface fastethernet 0/2
  - *Switch(config-if)#* no switchport access vlan 2
  - *Switch(config-if)#* end

- To delete vlan 2
  - *Switch#* vlan database
  - *Switch(vlan)#* no vlan 2
  - *Switch(vlan)#* exit

VLAN Trunk Ports

- A trunk is a point-to-point link between two switches or between switches and routers. Trunks carry the traffic of multiple (all) VLANs found in a switch to another switch.

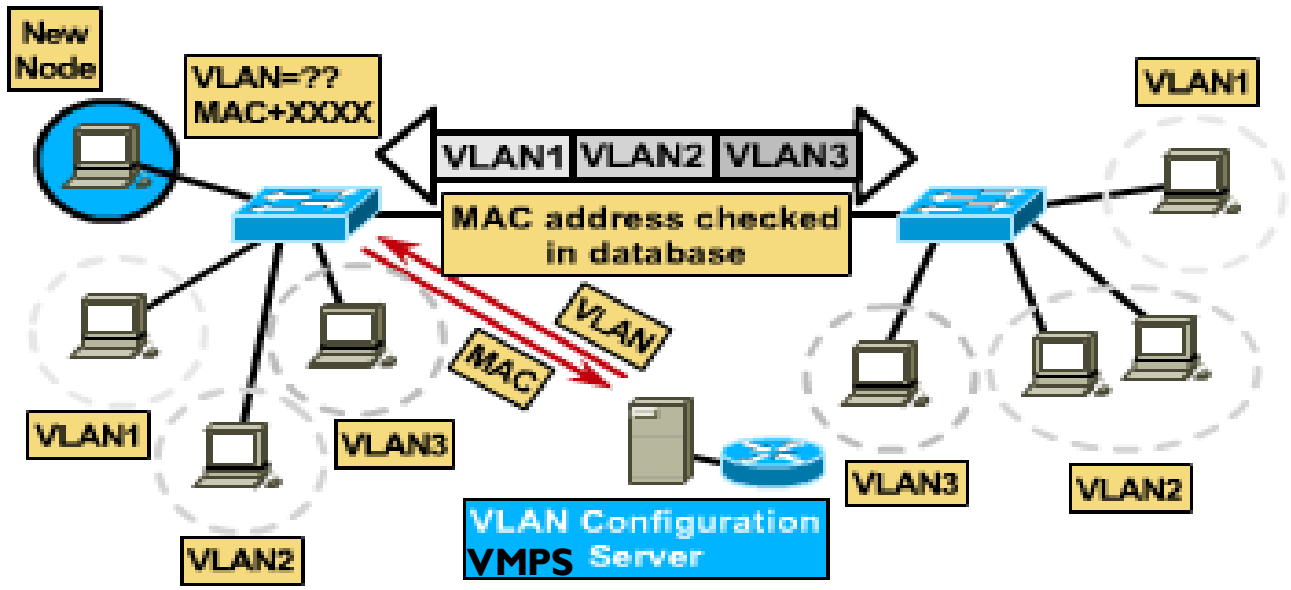
- Configure the port as a VLAN trunk
  - *Switch(config-if)#* switchport mode trunk
  - *Switch(config-if)#* switchport trunk encapsulation dot1q *---for "802.1Q trunk port, supporting 802.1Q encapsulation"*

Dynamic VLAN (**MAC Address Based**)

- LANs defined by a list of MAC addresses.
- Provides full user movement.
  - Clients & server always on the same VLAN regardless of location.
- Requires computers to be pre-registered.
- Problem: Too many addresses need to be entered and managed.

Mac Address	VLAN
08-00-39-00-2F-C3	1
08-00-5A-21-A7-22	2
08-00- 28-00-38-A9	2
08-00-10-99-AC-54	1

Dynamic VLAN (**MAC Address Based**)



- Switch ports can automatically determine a user's VLAN assignment based on **MAC / physical address.**
- As a device enters the network, the switch that it is connected to, queries [(using, VLAN Query Protocol (VQP)] a database on the **VLAN Configuration Server** [**VMPS server** (VLAN Membership Policy Server)]. for VLAN membership. That is, When a new device is connected to a port, the switch dynamically configures the port with the right VLAN
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port.
- Dynamic VLAN memberships [a table mapping MAC to VLAN] are created through ***VLAN management software (VMS) or manually using the CLI.*** [pre-registeration of MAC addresses].

Managing MAC Based VLANs Network Wide

Eg. CISCO Switches

- **VLAN Trunking Protocol (VTP)** is a Layer 2 client/server messaging protocol (CISCO proprietary) that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain.
- **A VTP domain** (also called a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and that are interconnected with trunks.
- A switch in can be in **VTP Server** or **VTP Client** or **VTP Transparent** mode.
  - In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters, such as VTP version and VTP pruning, for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches and synchronize their VLAN based on advertisements received over trunk links.
  - VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
  - VTP transparent switches do not participate in VTP, but do forward VTP advertisements received through their trunk ports.

Dynamic VLAN (**Layer-3 Based)**

- VLAN membership implied by MAC-layer **protocol type field** and **subnet field** (eg., 123.34.*.*).
- VLAN configuration is learned by the switches.
- Stations do not belong to VLANs, packets do.
- Multiprotocol stations are put into multiple VLANs.
- Generally slower than MAC or Port based VLAN.

Destination MAC	Source MAC	**Type**	Destination IP	**Source IP**

Dynamic VLAN (**Layer-3 Based)**

Protocol	VLAN
IP	1
IPv6	2

IP Subnet	VLAN
23.2.24	1
26.21.35	2

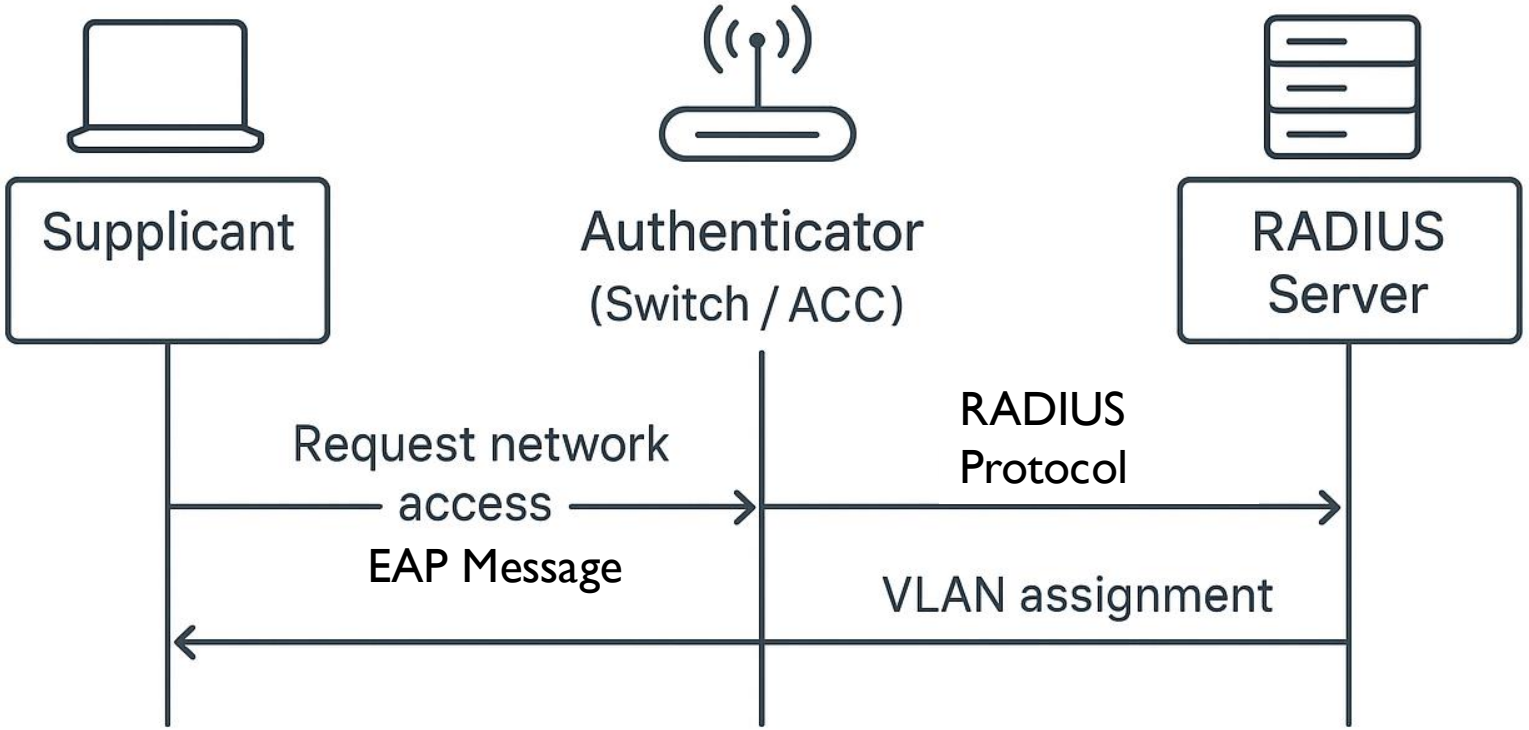
- VLAN membership is based on Layer 3 information, this has nothing to do with network routing and should not be confused with router functions.
- In this method, IP addresses are used only as a mapping to determine membership in VLAN's. No other processing of IP addresses is done.

Dynamic VLAN (**Identity and Role based**)

1. **Device/User connects** to Wi-Fi (SSID) or LAN. Device requests network access.
2. Authenticator **blocks normal traffic** but allows EAP messages.
3. Authenticator **forwards EAP messages** to RADIUS (often integrated with LDAP/Active Directory).
4. **RADIUS authenticates** the user and sends **Access-Accept** with VLAN ID (or tunnel), QoS, Policies, etc
5. Authenticator grants network access and applies VLAN assignment.

- **EAP** - Extensible Authentication Protocol. Defines message format not authentication. The actual authentication is done by a specific EAP method (like EAP-TLS, EAP-PEAP, etc).
- **802.1X -** is a standard for **port-based network access control**. It's used to secure networks by controlling **who can connect to a switch port or wireless access point**.
- **RADIUS -** Remote Authentication Dial-In User Service Protocol. Standardised way for **AAA—Authentication, Authorization, and Accounting.** Works over UDP, typically ports 1812 for authentication and 1813 for accounting

802.1X + RADIUS + Dynamic VLAN



802.1X = controls port/network access
RADIUS = authentication server backend
EAP = method used within 802.1X to authenticate users

EAP methods

FYORP

Common EAP Methods

Method	Description	Use Case
EAP-TLS	Uses client/server **certificates**	Very secure, common in enterprises
EAP-PEAP	Encrypted tunnel, uses **server certificate** and **user/password** inside	Popular in corporate Wi-Fi
EAP-TTLS	Like PEAP, supports legacy auth methods inside a secure tunnel	Flexible for mixed environments
EAP-MD5	Simple username/password	Not recommended; weak security

Future – Role-based/Identify Aware VLAN

FYORP

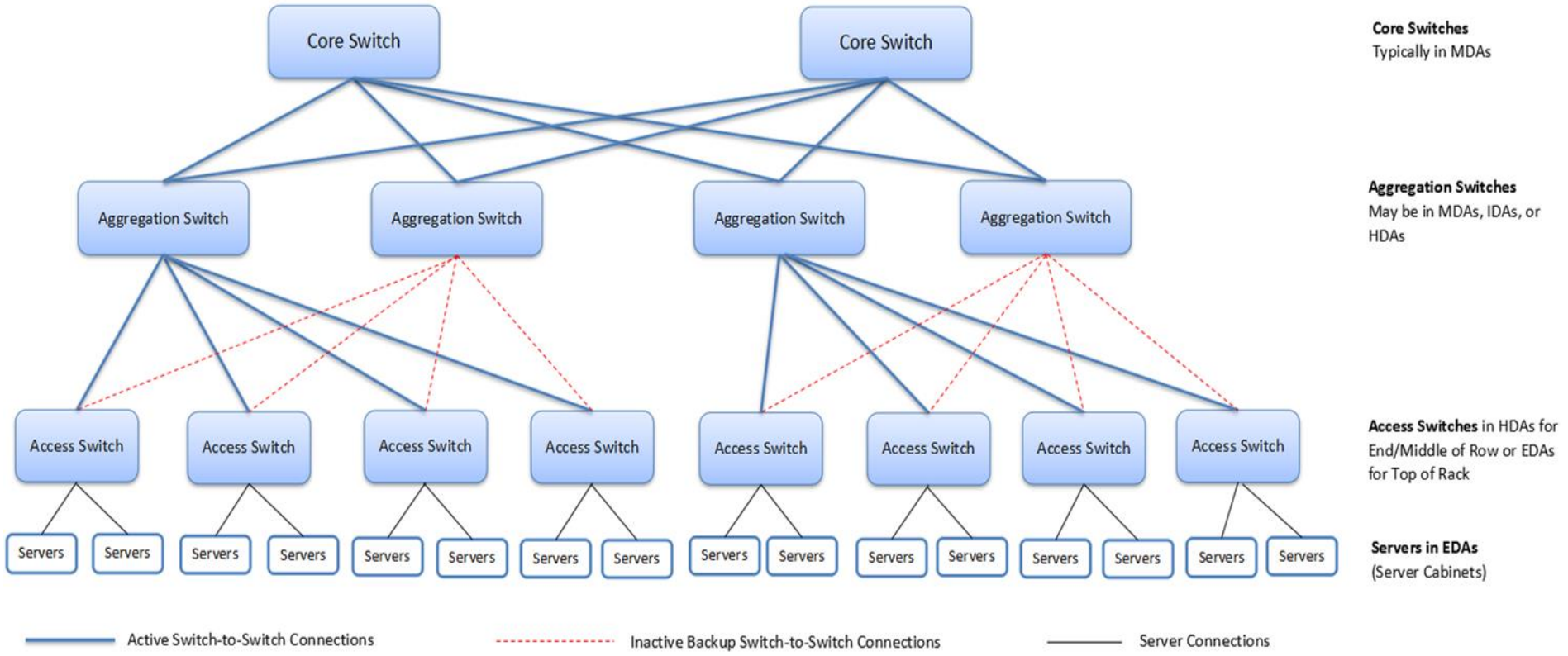
- **Reduced VLAN Sprawl:** No need for separate VLANs per team/project; simpler management.
- **Identity-Aware Access:** Policies based on user/device role, not IP/location.
- **Granular Security:** Fine-grained access to apps/services; supports context (device, time, location).
- **Enhanced Segmentation:** Micro-segmentation; limits lateral threat movement.
- **Simplified Policy Management:** Centralized enforcement across wired, wireless, cloud.
- **Scalable:** Onboard users/devices without creating VLANs.
- **Improved Compliance:** Better logging and auditing of access.
- **Future-Ready:** Supports Zero Trust, SDN, cloud, and automated policies.

Questions to Ponder

- What is the highest VLAN number (maximum value for VLANs)? Or What is the maximum VLANs per VTP domain?
- What is VxLAN? Discuss one use case of VxLAN?
  - Refer RFC 7348
- What is SDN (Software Defined Networking)?
- What is leaf-spine architecture? Compare 3-Tier Architecture vs. Leaf Spine Architecture

Some related materials follows ….

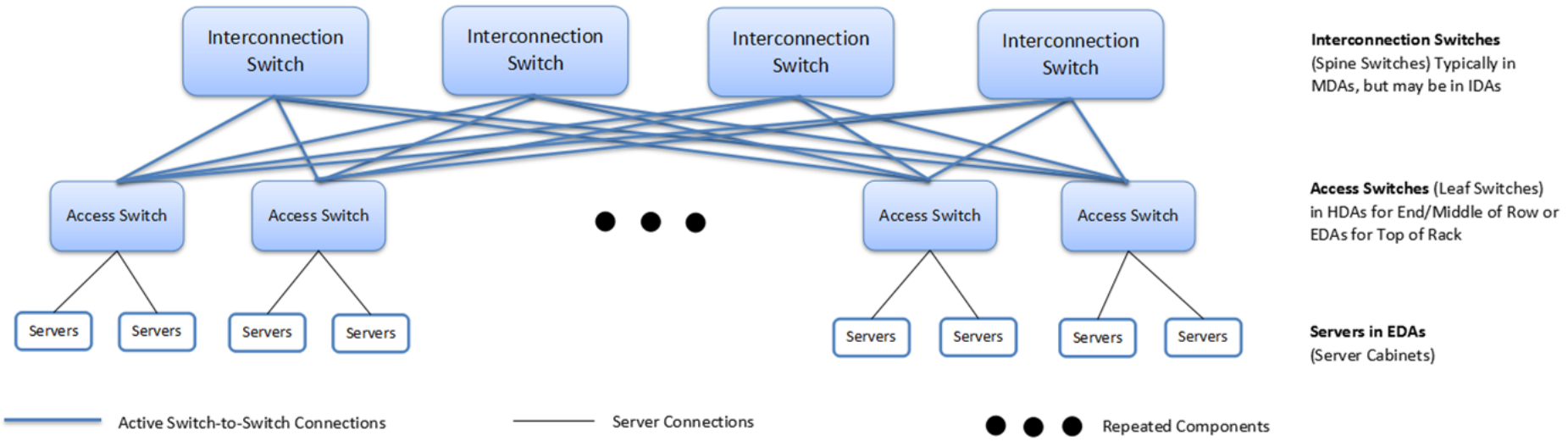
Traditional 3-tier Architecture



Switches are interconnected by pathways for redundancy which can create loops in the network. As part of the design, a protocol (Spanning Tree) that prevents looped paths is implemented.

Two-tier Leaf-spine or fat-tree Architecture

- Emerging architecture



Requirements to apply leaf-spine topology:

- Each leaf connects to all spines in the network.
- The spines are not interconnected with each other.
- The leafs are not interconnected with each other for data-plane purposes. (The leafs may be interconnected for control-plane operations such as forming a server-facing vLAG.)

Packet Framing & Link-Layer Switching

MPLS

- Motivation
- MPLS Techniques

Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

Multiprotocol Label Switching (MPLS)

- Directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

layer 2 so much faster

  - IP Routed to Label Switched
  - Each packet entering an MPLS network is labelled with a locally significant MPLS label. As the packet passes through the MPLS network, label is replaced with another label or stripped off.
  - Multi-Protocol Label Switching (MPLS) converts routed network to something closer to a switched network and offers information transfer speeds that are not available in a traditional IP-routed network. Instead of forwarding packets on a hop-by-hop basis, paths are established for particular source-destination pairs.

MPLS Applications

- Traffic Engineering (TE)
- Virtual Private Networking (VPN)
- Quality of Service (QoS)
- Any Transport over MPLS (AToM)

Multiprotocol Label Switching (MPLS)

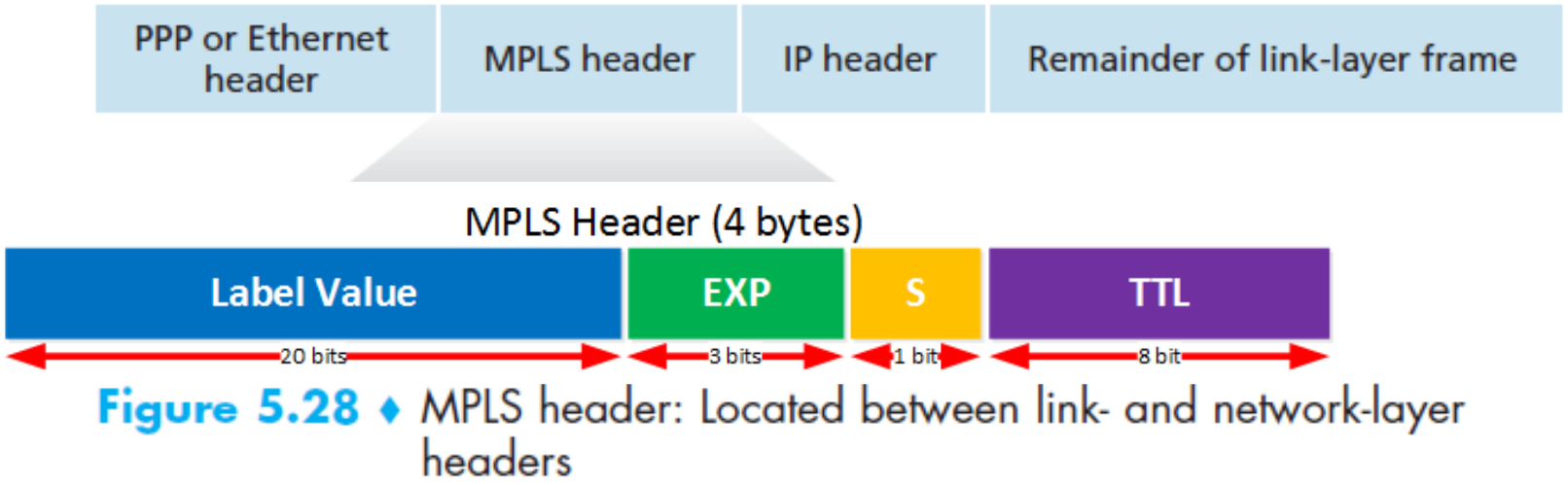


Figure 5.28 ♦ MPLS header: Located between link- and network-layer headers

•**Label value**: MPLS label / id
•**EXP**: Three experimental bits. These are used for QoS, normally the IP precedence value of the IP packet will be copied here.
•**S**: this is the "bottom of stack" bit. With MPLS it's possible to add more than one label, you'll see why in some of the MPLS VPN lessons. **When this bit is set to one, it's the last MPLS header.** When it's set to zero then there is one or more MPLS headers left.
•**TTL**: the time to live field

Multiprotocol Label Switching (MPLS)

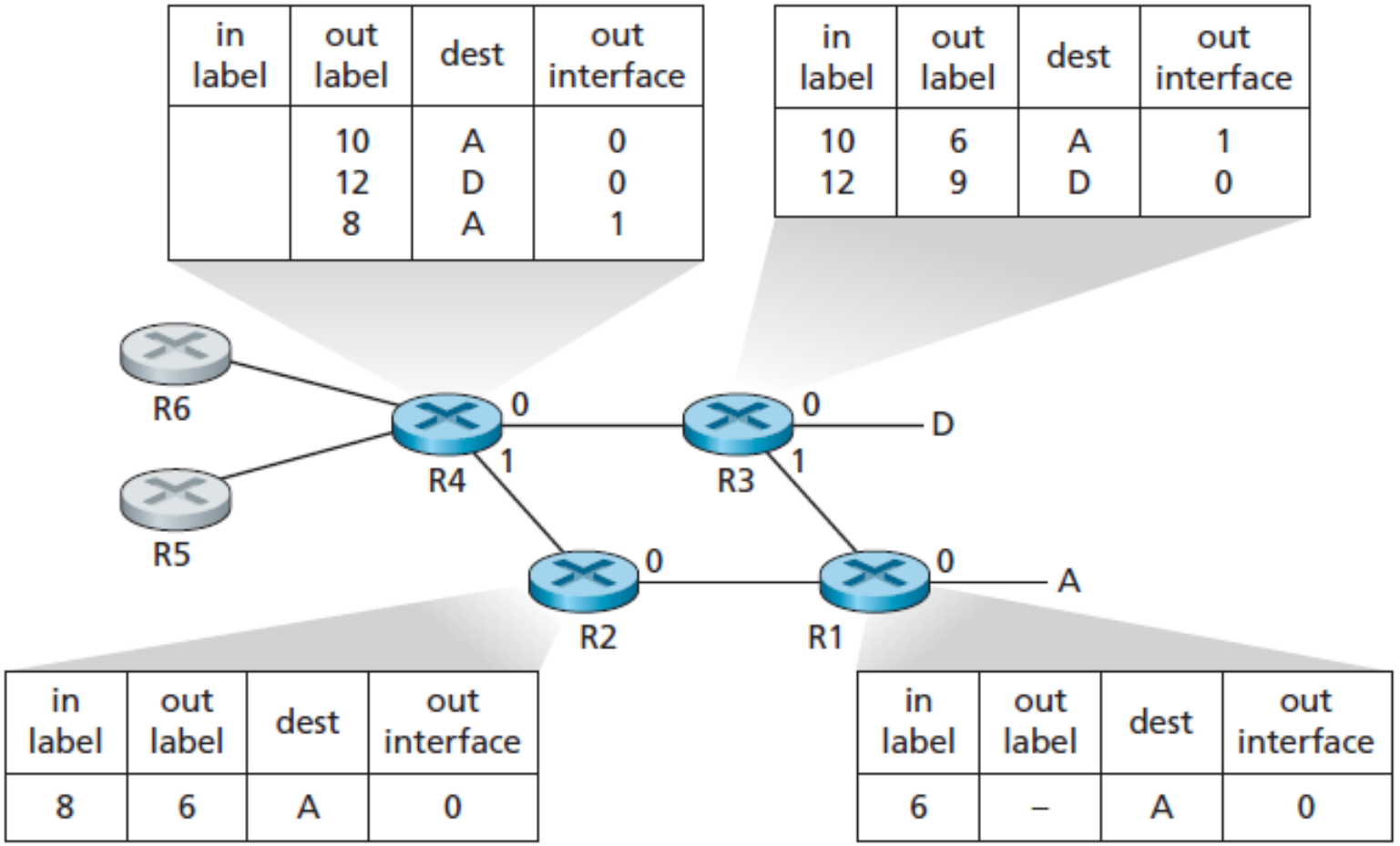


Figure 5.29 ♦ MPLS-enhanced forwarding

How MPLS paths are established?

FYORP

- Known as, Label-switched paths (LSPs)
- LDP – Label Distribution Protocol
  - LDP is a protocol that automatically generates and exchanges labels between routers. Each router will locally generate labels for its prefixes and will then advertise the label values to its neighbours.
  - How LDP works? Read more @ https://networklessons.com/mpls/mpls-ldp-label-distribution-protocol

Questions to Ponder

- What is SD-WAN? Is it a good alternative for MPLS? Why?

Let us debate

- Assume yourself as a **Network Architect** and debate on the following question @ Discord

NW Segmentation: VLAN vs SDN

In light of evolving cybersecurity threats, increasing network complexity, and the need for scalability, should organizations primarily adopt software-defined networking (SDN) with Zero Trust architectures for network segmentation, move towards traditional methods like VLANs and MPLS, or pursue a hybrid approach that leverages the strengths of multiple segmentation strategies? How should factors such as security, cost, complexity, compliance, and legacy system integration influence this decision?

Activities ….. Next Week

- Lab Sessions Starts from Tomorrow @ **COM1-B1-02 (Data Comm Lab 1)**
- Read the "Labs Intro" and familiarise yourself with the Lab Setting.
- Read the "Lab Sheet" at least once before you come to each Lab session.
- Learning Activities (Every Week) –
  - In-class online quiz **[PIs login to Pollev**, before answering questions]
  - Discord discussion forum for clarifications & to discuss new topics

THE END

Lab TAs

	10am-12pm	12pm-2pm	2pm-4pm	4pm-6pm
WED	KWAN FAI YEW	**ADITI** CHADHA	XIE WENHAO	ZHU YONGZE
THURS	**ADITI** CHADHA	**ADITI** CHADHA	AJAY	AJAY
FRI	KWAN FAI YEW	HAZIM	HAZIM	ZHU YONGZE

Find their Discord ID and emails in Lecture-1 slides & Canvas->CS3103->Home.

Tasks: Handle Lab Sessions & Grading Your Assignments
Head TA (Aditi Chadha) – Pre-lab quiz, Lab Sheets

Attendance

- https://inetapps.nus.edu.sg/ctr/