Virtual LANs

Overview

❑ What is a LAN ?

❑ LAN Problems

❑ Introduction to VLAN: Types of Virtual LANs

❑ Access and Trunk Ports of L2 Switch

❑ VLAN Tagging Rules

❑ IEEE 802.1Q standard

❑ VLAN L2 Routing

❑ VLAN Benefits

VLAN- Logical Group of Computers that appear to be in the same LAN.
-Irrespective of configuration of physical network

What is a LAN?

| Server | Client 1 | Bridge | Client n | Router |

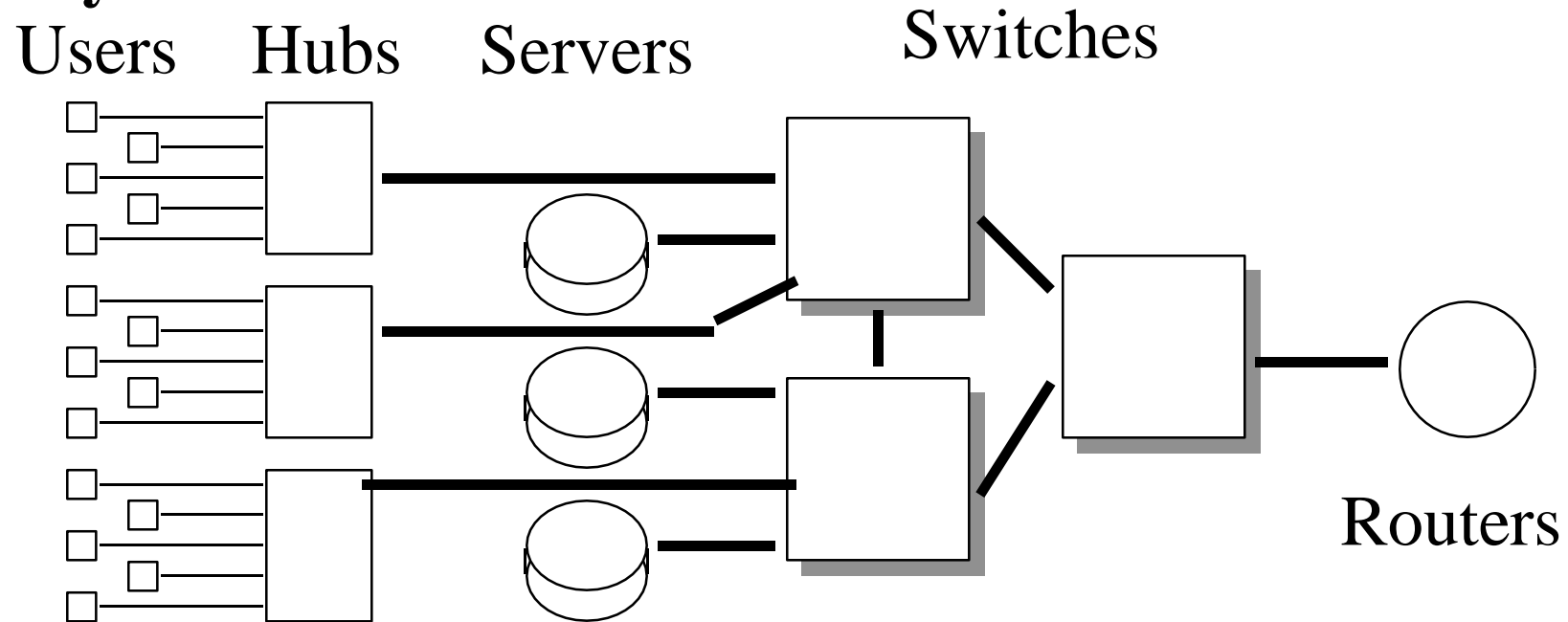⬭ LAN 1   ⬭ LAN 2

Router
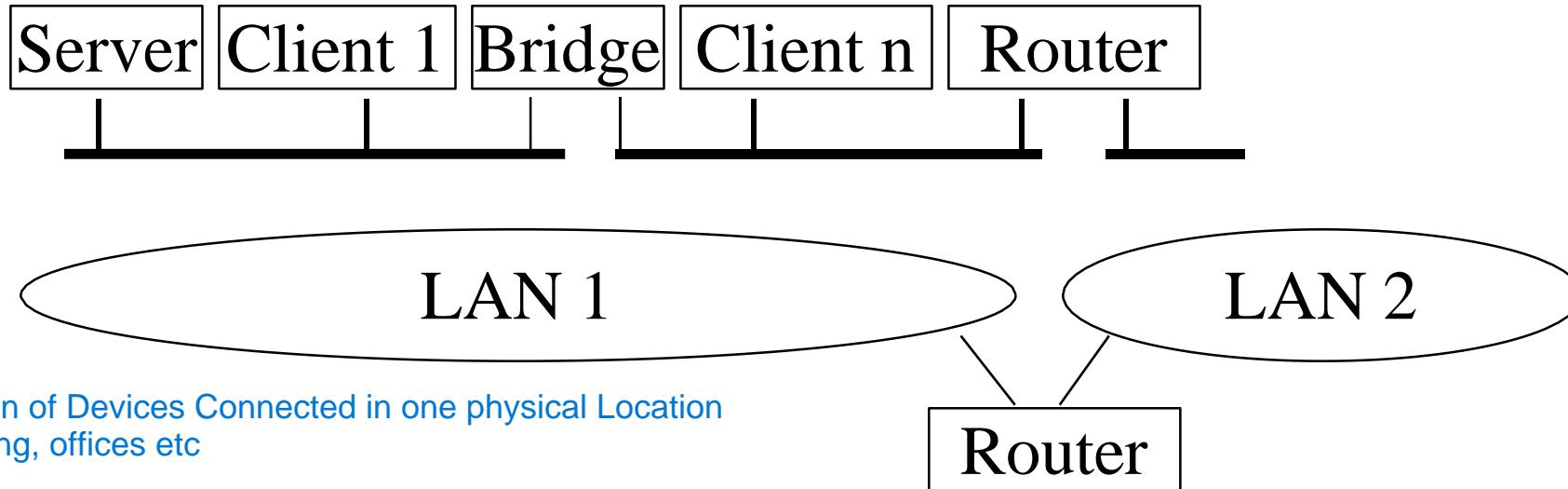
LAN- Collection of Devices Connected in one physical Location such as Building, offices etc

- ❑ LAN = Single broadcast domain = Subnet
- ❑ No routing between members of a LAN
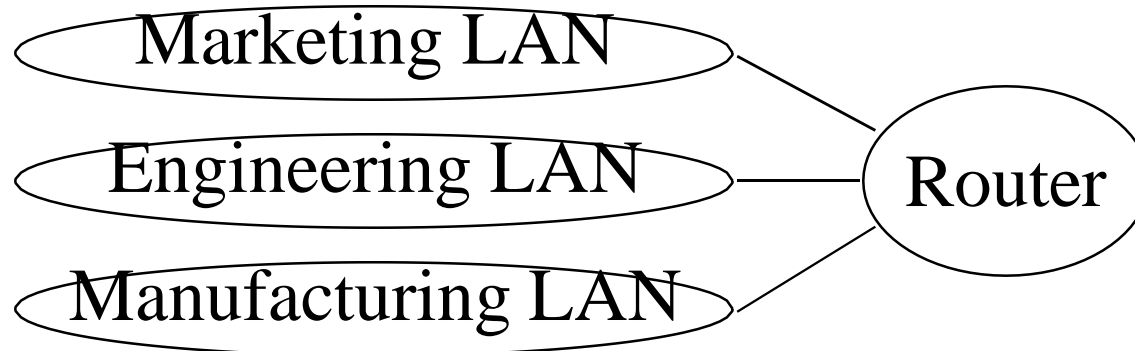- ❑ Routing required between LANs
- ❑ Immobility
- ❑ Security

	VLAN	LAN
Cost	Low	High
Latency	Low	High
Efficiency	More Efficient	Less Efficient

What is a Virtual LAN

❑ **Physical View**

Users   Hubs   Servers   Switches

Routers

❑ **Logical View**

Marketing LAN

Engineering LAN

Manufacturing LAN

Router

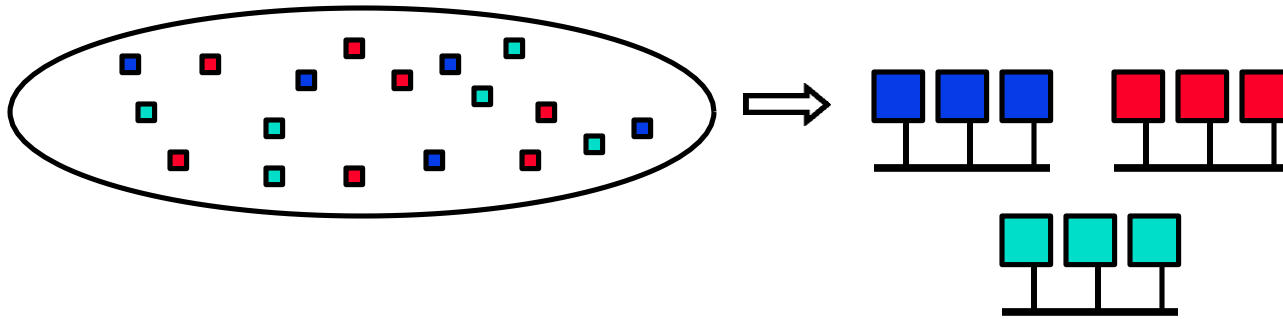# **Virtual LAN**

❑ Virtual LAN = Broadcasts and multicast goes only to the nodes in the virtual LAN

❑ LAN membership defined by the network manager $\Rightarrow$ Virtual
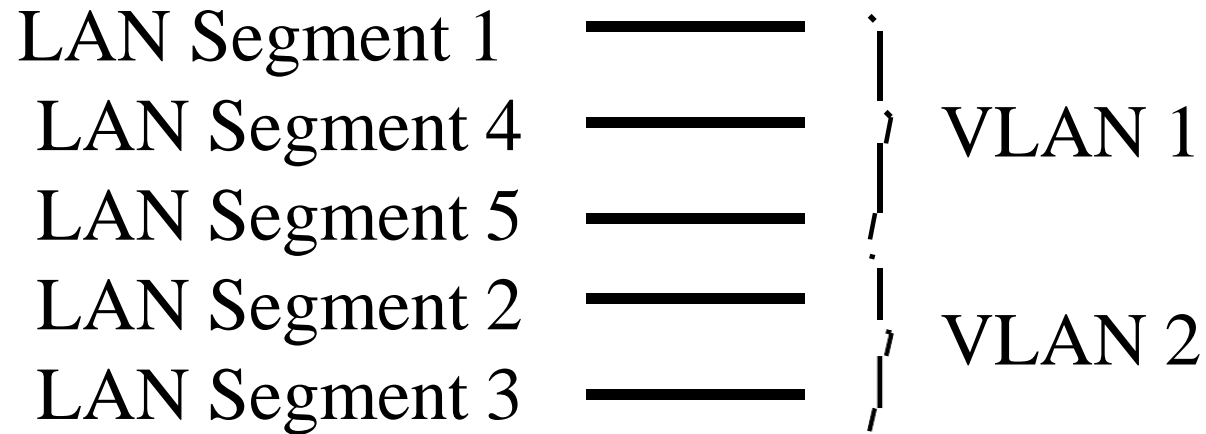
VLAN: Why?

❑ Virtual is Better than Real

  ○ Location-independent
    ⇒ Marketing LAN can be all over the building

  ○ Users can **move** but not change LAN

  ○ Traffic between LANs is routed
    ⇒ Better to keep all traffic on one LAN

  ○ Switch when you can, route when you must
    ⇒ Do not VLAN over expensive WAN links

  ○ Better security

Types of Virtual LANs

❑ Layer-1 VLAN = Group of Physical ports

❑ Layer-2 VLAN = Group of MAC addresses

❑ Layer-3 VLAN = IP subnet

Switch Port	VLAN 1	VLAN 2
A1	√	
A2		√
A3	√	
B1		√
B2	√	

VLAN1	VLAN2
A1B234565600	21B234565600
D34578923434	634578923434
1345678903333	8345678903333
3438473450555	9438473450555
4387434304343	5387434304343
4780357056135	6780357056135
4153953470641	9153953470641
3473436374133	0473436374133

VLAN1

23.45.6

VLAN2

IPX

Layer-1 VLANs

LAN Segment 1 ————⌉
LAN Segment 4 ————⎬ VLAN 1
LAN Segment 5 ————⌋

LAN Segment 2 ————⌉
LAN Segment 3 ————⎬ VLAN 2

❑ Also known as port switching

❑ Can be used to provide security and isolation

❑ Does not allow user mobility.

❑ Moved user has a new subnet $\Rightarrow$ new IP address
  $\Rightarrow$ May go through a router to access the old server

Layer-2 VLANs

❑ LANs defined by a list of MAC addresses

❑ Provides full user movement

❑ Clients and server always on the same LAN regardless of location

❑ Problem: Too many addresses need to be entered and managed

0234786890
Is that a marketing node?

Layer-2 VLANs (Cont)

❑ Notebook PCs change docking stations
$\Rightarrow$ MAC address changes

❑ Alternative: Membership implied by MAC protocol
type field. VLAN1 = IP, VLAN2 = , ...

0880 - IPv4
08DD - IPv6

Ethernet

Dest. Address	Src. Address	Protocol Type	

802.3

Dest. Address	Src. Address	Length	

	AA	AA	03	Protocol Type	

Layer-3 VLANs

Dest. Addr	Src. Addr	**Protocol Type**	

	IP Dest. Addr	**IP Source Addr**	

- ❑ Also known as **virtual subnet**
- ❑ VLAN membership implied by **MAC-layer protocol** type field and **subnet field** 123.34.*.*
- ❑ VLAN configuration is learned by the switches
- ❑ Stations do not belong to VLANs, packets do.
- ❑ Multiprotocol stations are put into multiple VLANs

Higher Layer VLANs

❑ Different VLANs for different applications:
  ○ FTP
  ○ Multimedia

❑ Service based VLANs: All workstations using Email server are on the EMAIL-VLAN, all workstations using employee database sever are on the HR-VLAN,..

❑ IP Multicast address based VLANs

❑ General policy based: VLAN membership can be based on a combination of incoming port, MAC address, subnet, or higher layer info, time of day.

VLAN Tagging

Dest. Addr	Src. Addr	VLAN Tag	Prot. Type

- ❏ First switch adds tag containing VLAN id to all incoming packets
- ❏ Intermediate switches do not recompute the VLAN id
- ❏ Last switch removes tags from all outgoing packets
- ❏ Tag is <u>not</u> swapped at every hop like labels

End Station — Switch — Bridged LAN — Switch — End Station
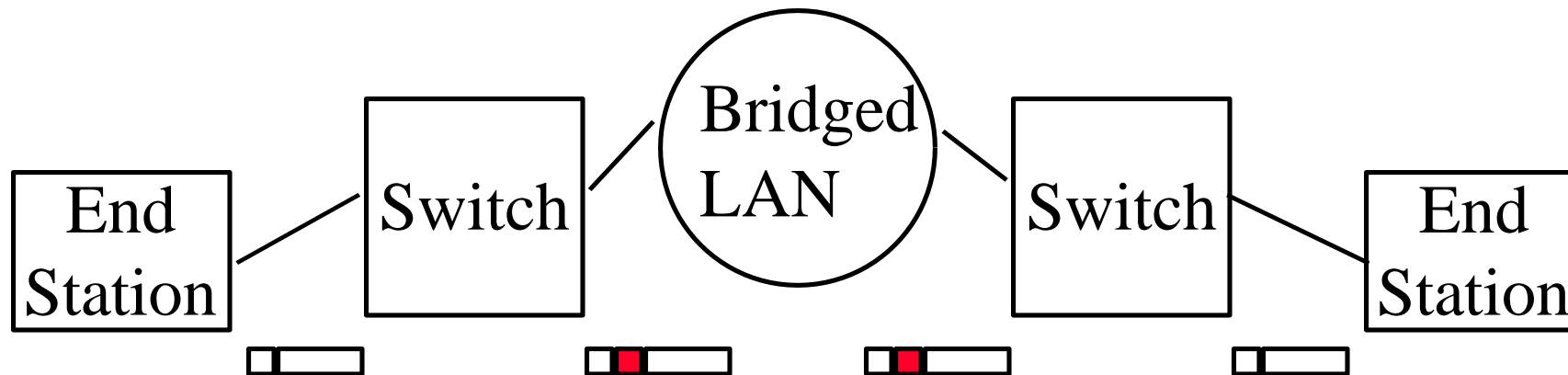
IEEE 802.1Q: Features

- ☑ Allows up to 4095 VLANs (**0 to 4095 =4096**): 4094
- ☑ Allows port based, MAC address based, and higher-layer VLANs
- ❏ Upward compatible with existing VLAN-unware hubs and bridges
- ☑ Supports both shared-media and switched LANs
- ❏ Allows mixing legacy bridges and VLAN-aware bridges
- ❏ Retains plug and play mode of current LAN bridges

Features (Cont)

- Extends 802.1p priority mechanism to priority based on VLAN membership
- Allows priority associated with each VLAN
- VLAN-based priority takes precedence over other priority considerations
- Allows signaling priority information on non-priority (CSMA/CD) LANs
- Allows both local/universal MAC addresses
- Operation with/without explicit VLAN header in the frame

Features (Cont)

- ✅ Supports static and dynamic configurations for each VLAN

- ❑ Allows intermixing different IEEE 802 MACs and FDDI

- ❑ Allows signaling source routing information on CSMA/CD LANs

- ❑ Each VLAN is a subset of a "single" physical spanning tree
  Does not preclude future extensions to multiple spanning trees

Features (Cont)
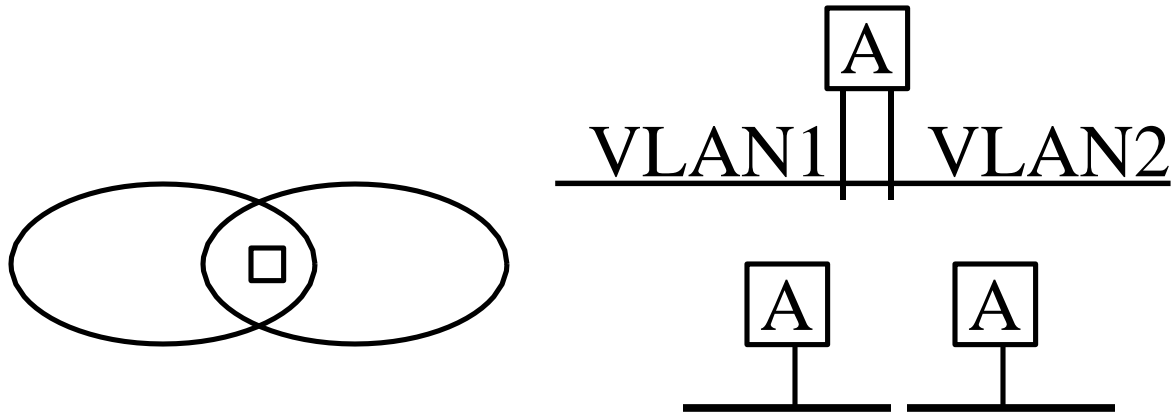
☑ Overlapping VLANs:

- ○ Multiple stations with same individual address
- ○ One station with multiple interfaces using the same address
- ○ Restriction: One station or interface per VLAN

Tagging Rules
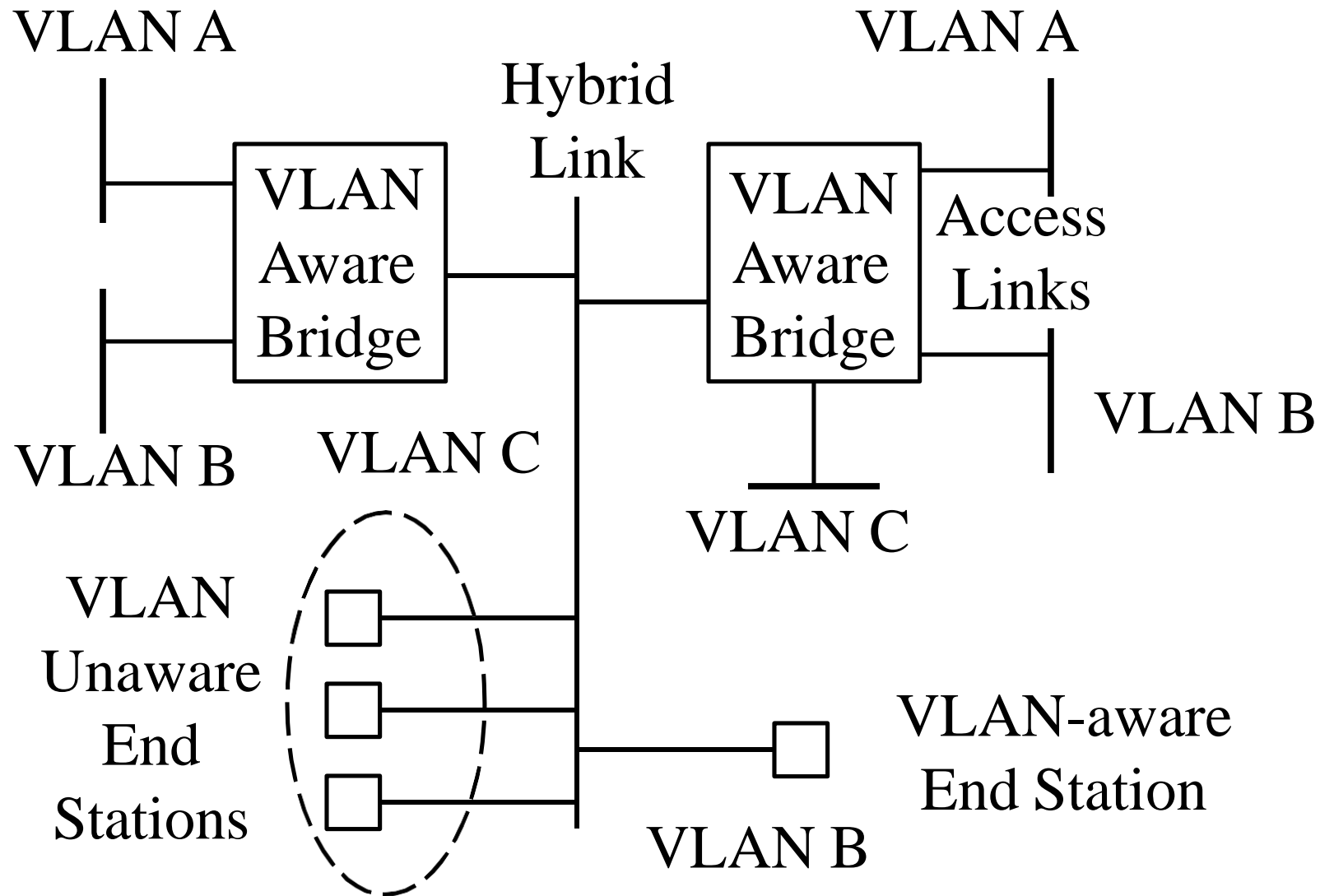
Tagging Rules (Cont)

❑ On a given LAN segment for a given VLAN, all frames should be either implicitly or explicitly tagged.

❑ Different VLANs on the same segment may use different options.

❑ **Access Link**: Contain VLAN unaware devices All frames on access links are untagged

❑ **Hybrid Link**: Contains both VLAN-aware and VLAN-unaware devices

○ All frames for some VLANs are tagged

○ All frames for other VLANs are untagged

Tagged Frame Format

❑ **Tag Header:**

16b	3b	1b	12b
TPID	User Priority	CFI	VLAN Id

❑ **Ethernet Frame:**

6B	6B	4B	2B	0-30B		4B
DA	SA	Tag	PT	[RIF]	Data	FCS

❑ **802.3 Frame:**

6B	6B	4B	2B	0-30B		42-1470B	4B
DA	SA	Tag	Length	[RIF]	LLC	Data	FCS

Frame Format (Cont)

❑ TPID = Tag Protocol ID

❑ CFI/DEI = Canonical Format Indicator
  = Bit order of address info in TR/FDDI frames
  = Presence/absence of RIF in 802.3/Ethernet frames

❑ RIF = Routing Information Field

  ○ New routing type: 01 = Transparent frame
    ⇒No routing info.

❑ DA = Destination Address, SA = Source Address
  PT = Protocol Type, LLC = Logical Link Control
  FCS = Frame Check Sequence

❑ Largest data size = 1470 on 802.3

Communication Between VLANs

- Need routers
- Can use 1-armed VLAN-aware router
- VLAN-aware switches can route between VLANs
- Such switches can be placed in the core, in the edges, or everywhere

VLAN Aware Switch

VLAN Aware/Unaware Core

VLAN Aware Router
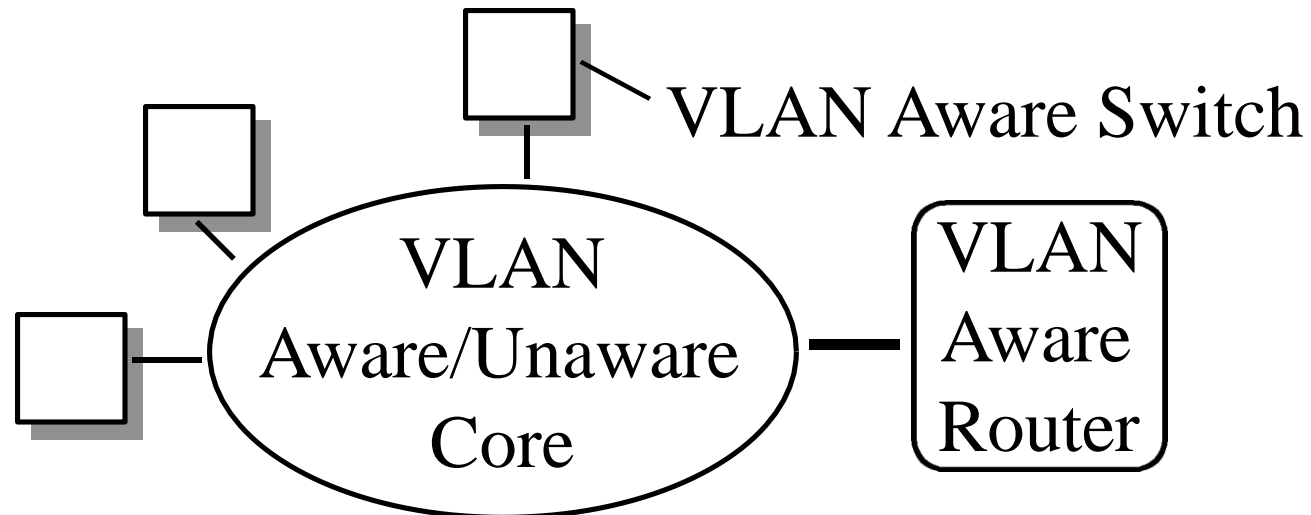
VLAN Benefits

- Segmentation,
- Resolve Thrashing,
- Reduced Broadcast Domain
- Mobility

Summary

- Virtual LANs $\Rightarrow$ Location independent LAN Groups
- Layer-1, Layer-2, Layer-3, higher layer VLANs
- IEEE 802.1Q allows both explicit and implicit tagging
- Need routing between VLANs

References

- Computer Networking: A Top Down Approach 6th edition Jim Kurose, Keith Ross Addison-Wesley March 2012.

- Switching, Routing, and Wireless Essentials Companion Guide, Cisco

- Draft Standard for Virtual Local Area Networks, IEEE P802.1Q/D6, May 16, 1997.

- Data Communications and Networking, Forouzan