Virtual LANs

Raj Jain
Professor of Computer and Information Sciences

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/

MBone Instructions

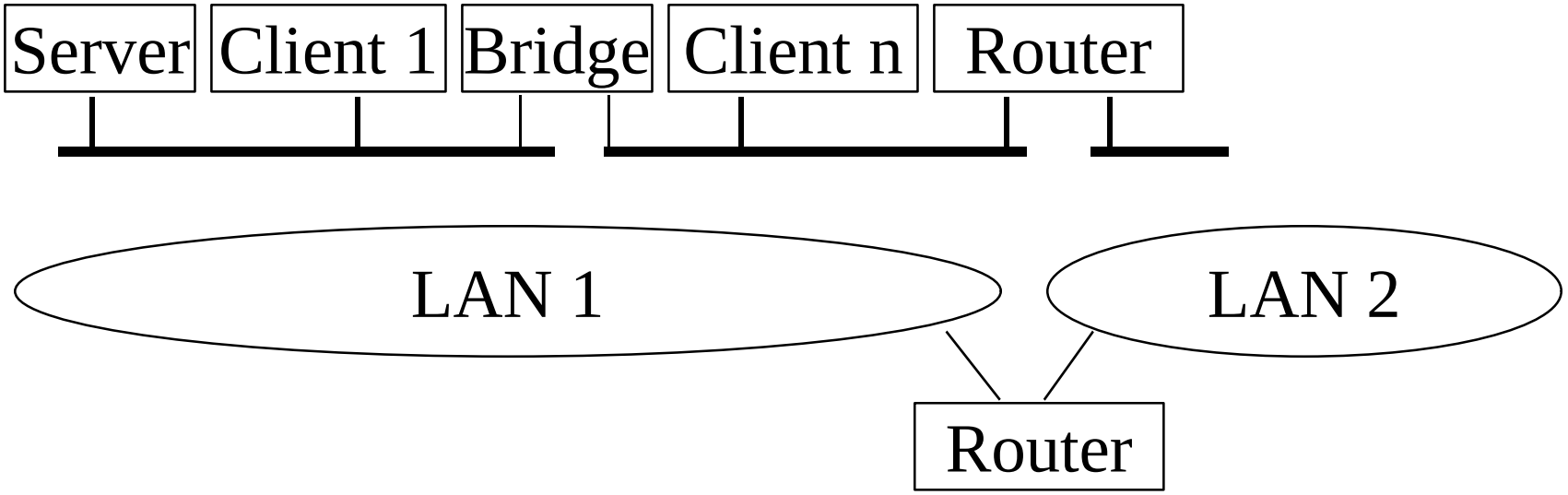
- Handouts for the class are available on-line: http://www.cis.ohio-state.edu/~jain/cis788-97/index.html or http://www.netlab.ohio-state.edu/~jain/cis788-97/index.html or ftp://netlab.ohio-state.edu/pub/jain/cis788-97/
- The schedule keeps changing. Please always check current schedule at: http://www.cis.ohio-state.edu/~jain/cis788-97/schedule.html

Instructions (Cont)

- Please email your positive and negative feedback about the quality of the reception as well as the content with a subject field of "Feedback" to mbone@netlab.ohio-state.edu
- If you are not able to receive the program due to some technical difficulties, please email "Feedback" to mbone@netlab.ohio-state.edu
- Please email technical questions with the subject field "Question" to mbone@netlab.ohio-state.edu. We will try to answer selected questions live.

- What is a LAN and what is a Virtual LAN?
- Types of Virtual LANs
- IEEE 802.1Q standard

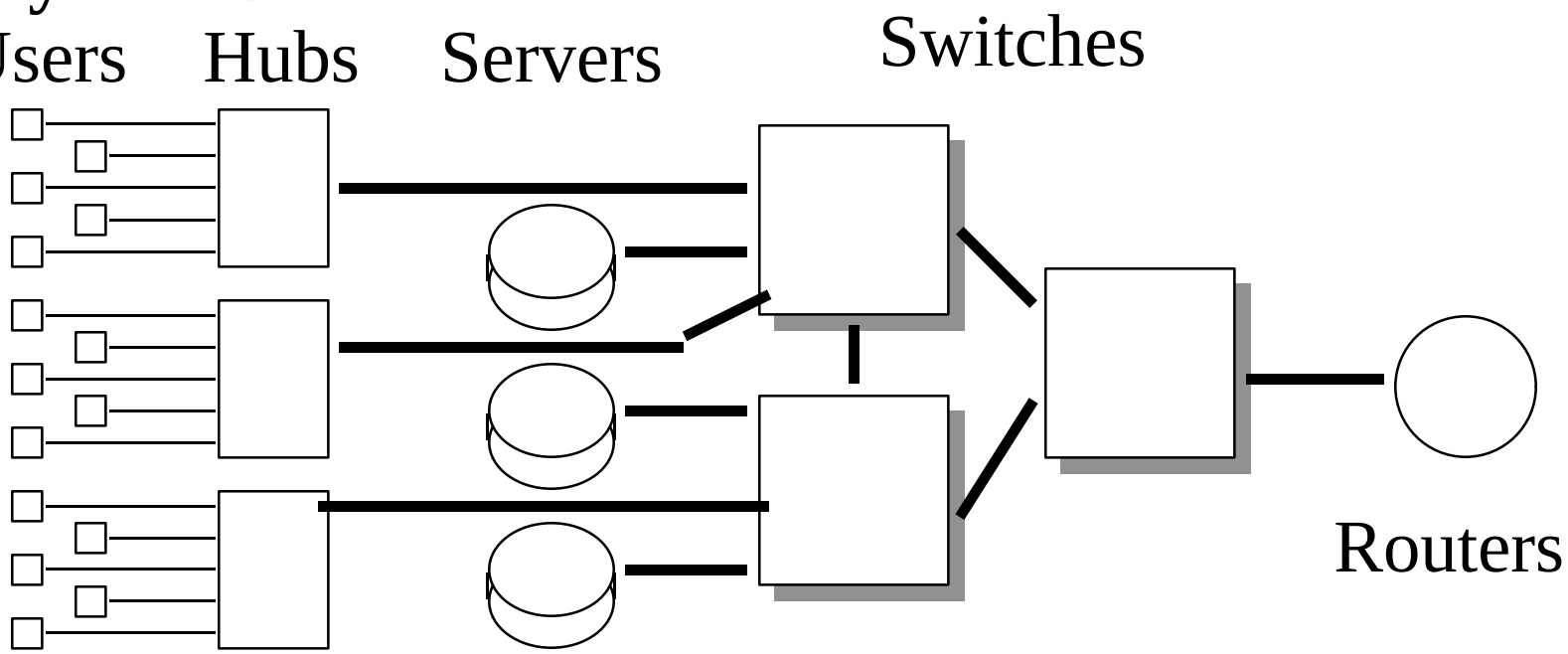
What is a LAN?



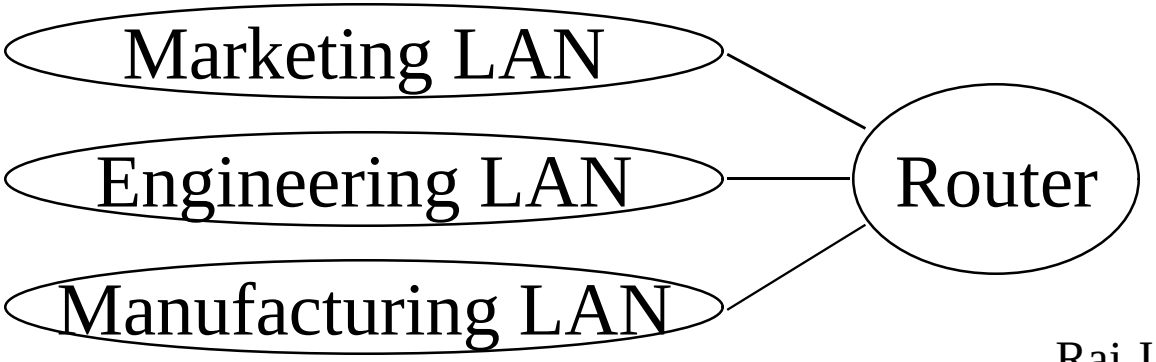
- LAN = Single broadcast domain = Subnet
- No routing between members of a LAN
- Routing required between LANs

What is a Virtual LAN

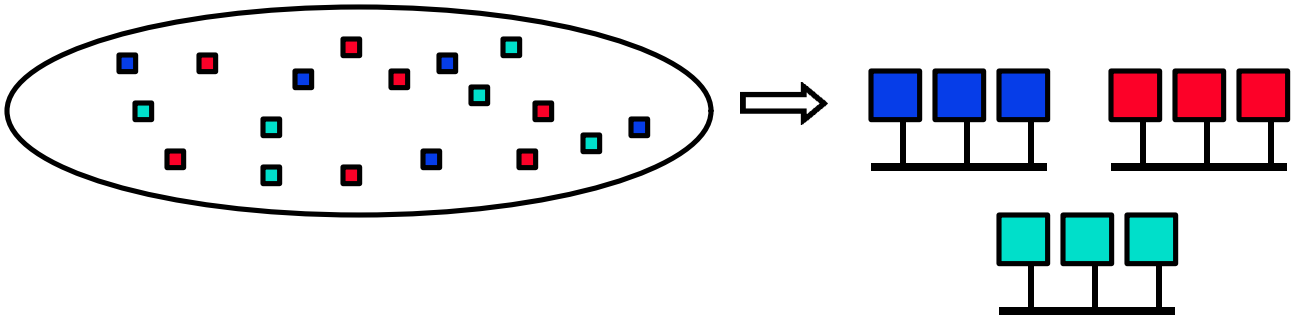
- **Physical View**



- **Logical View**



Virtual LAN



- Virtual LAN = Broadcasts and multicast goes only to the nodes in the virtual LAN
- LAN membership defined by the network manager ⇒ Virtual

VLAN: Why?

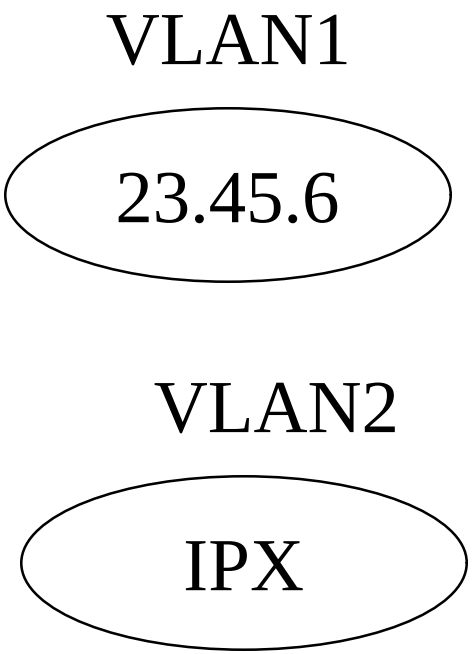
- Virtual is Better than Real
  - Location-independent
    ⇒ Marketing LAN can be all over the building
  - Users can move but not change LAN
  - Traffic between LANs is routed
    ⇒ Better to keep all traffic on one LAN
  - Switch when you can, route when you must
    ⇒ Do not VLAN over expensive WAN links
  - Better security

Types of Virtual LANs

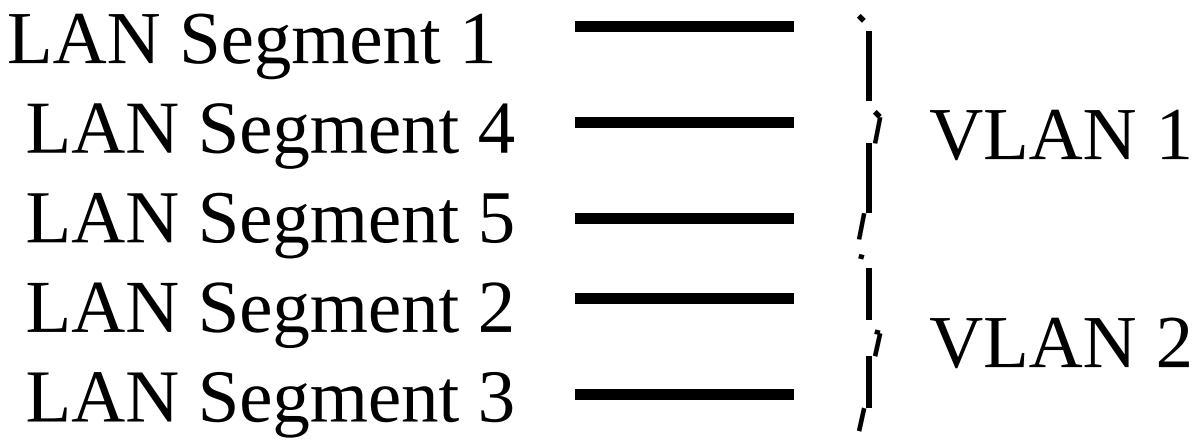
- Layer-1 VLAN = Group of Physical ports
- Layer-2 VLAN = Group of MAC addresses
- Layer-3 VLAN = IP subnet

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

VLAN1	VLAN2
A1B234565600	21B234565600
D34578923434	634578923434
1345678903333	8345678903333
3438473450555	9438473450555
4387434304343	5387434304343
4780357056135	6780357056135
4153953470641	9153953470641
3473436374133	0473436374133
3403847333412	8403847333412
3483434343143	8483434343143
4343134134234	0343134134234



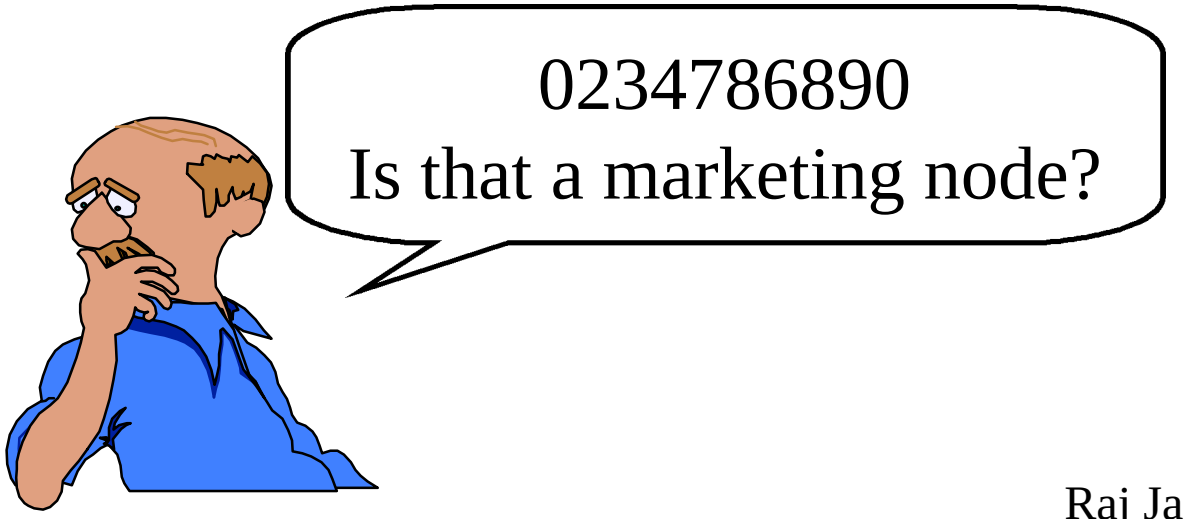
Layer-1 VLANs



- Also known as port switching
- Can be used to provide security and isolation
- Does not allow user mobility.
- Moved user has a new subnet ⇒ new IP address
  ⇒ 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

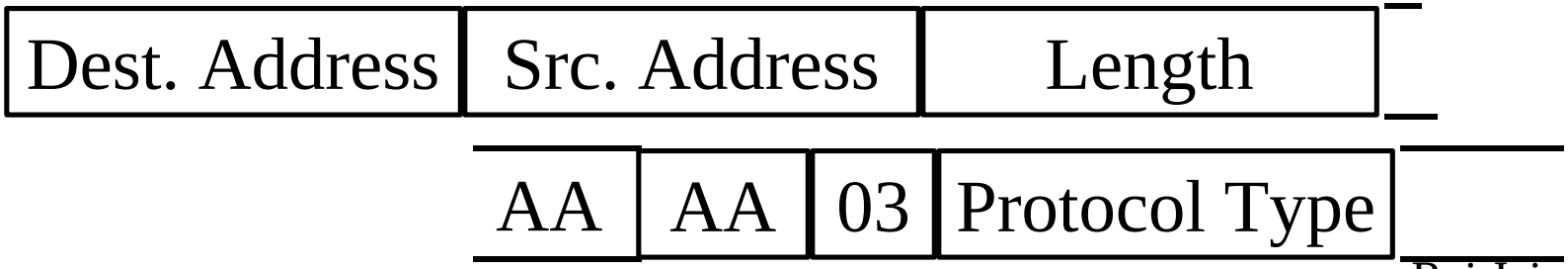


Layer-2 VLANs (Cont)

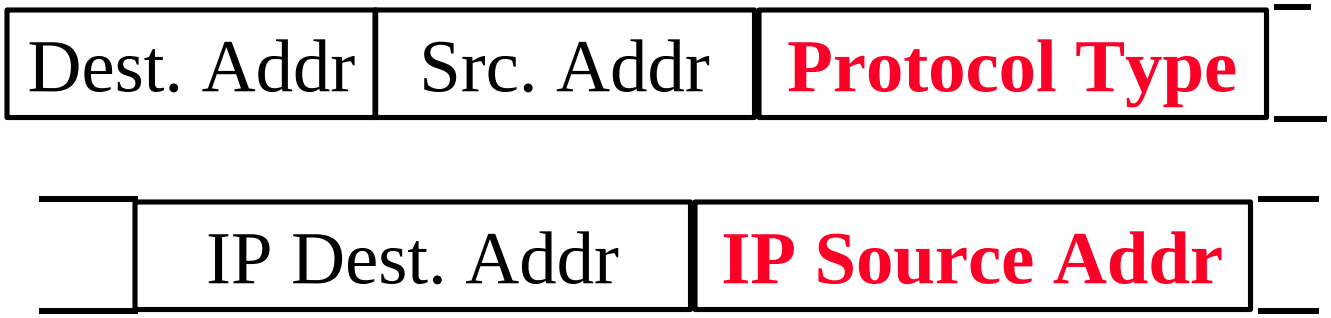
- Notebook PCs change docking stations
  ⇒ MAC address changes
- Alternative: Membership implied by MAC protocol type field. VLAN1 = IP, VLAN2 = LAT, ...

Ethernet

802.3



Layer-3 VLANs



- 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

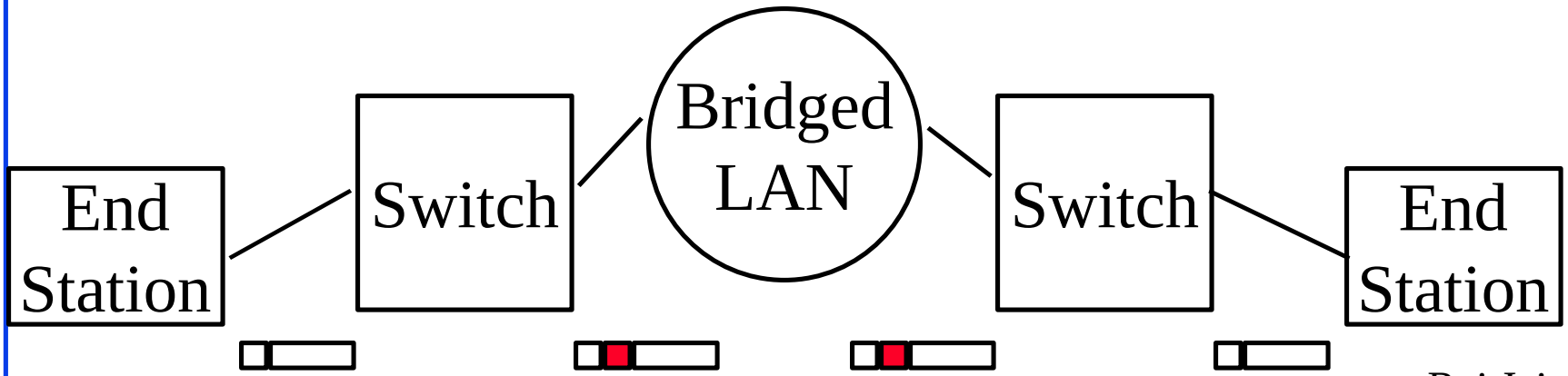
Higher Layer VLANs

- 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 not swapped at every hop like VC Id or labels



Synonyms

- Tag
- Label
- Mark
- Sticker
- Brand

IEEE 802.1Q: Features

- Allows up to 4095 VLANs
- 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

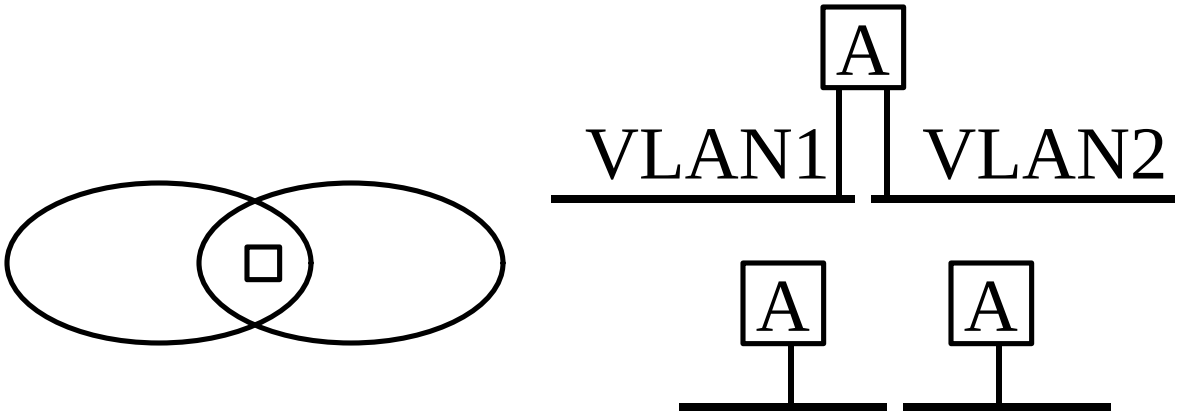
Features (Cont)

- 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)

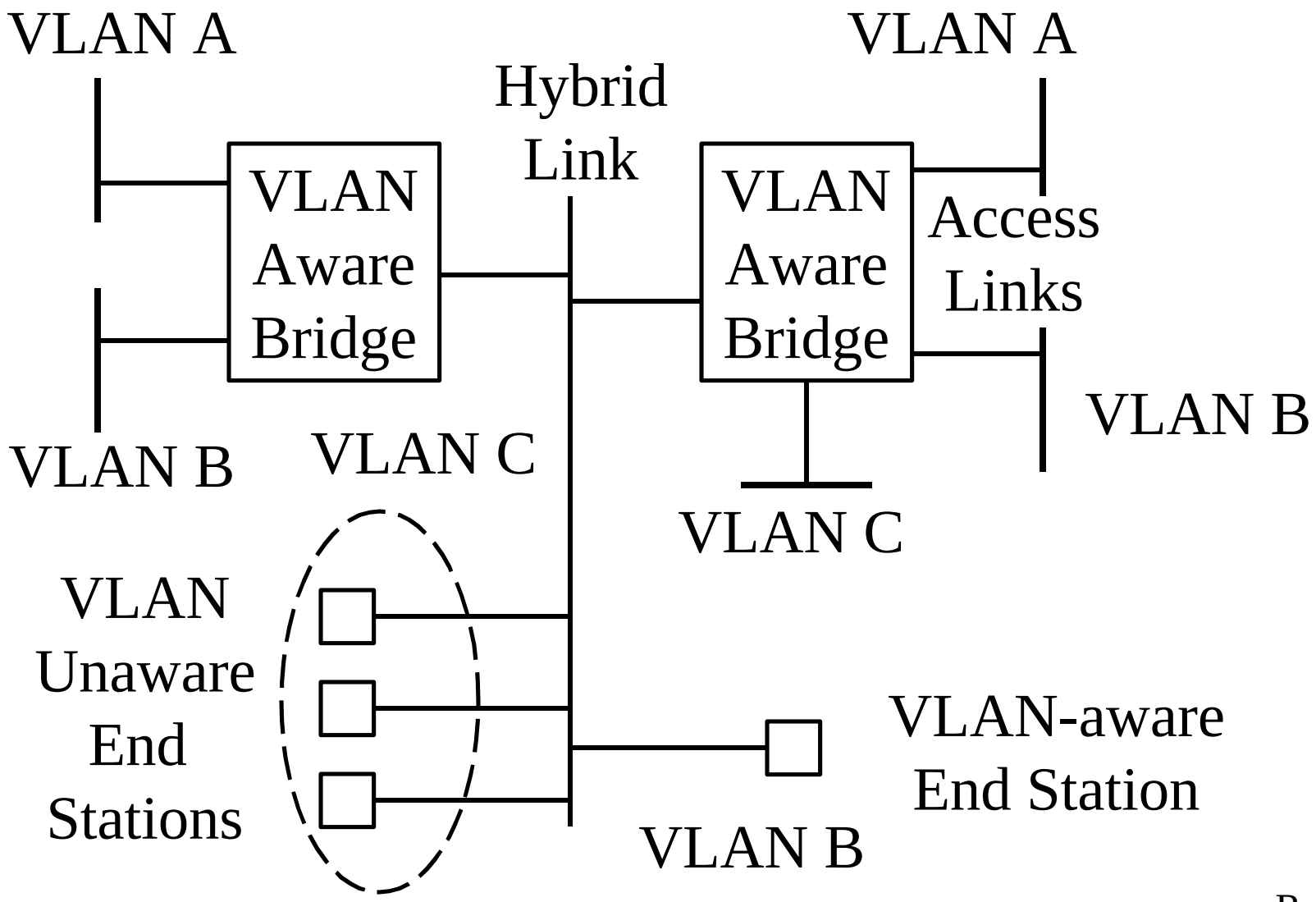
- Supports static and dynamic configurations for each VLAN
- Allows intermixing different IEEE 802 MACs and FDDI
- Allows signaling source routing information on CSMA/CD LANs
- Each VLAN is a subset of a "single" physical spanning tree
  Does not preclude future extensions to multiple spanning trees

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

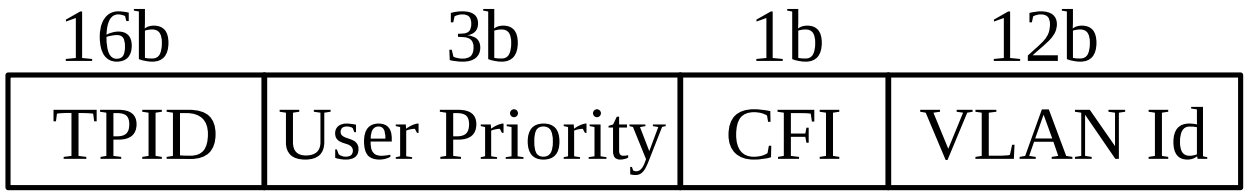


Tagging Rules (Cont)

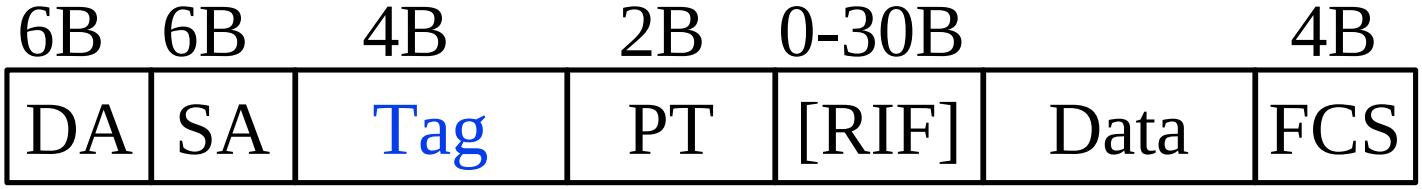
- On a given LAN segment for a given VLAN, all frames should be either implicitly or explicitly tagged.
- Different VLANs on the same segment may use different options.
- Access Link: Contain VLAN unaware devices
  All frames on access links are untagged
- Hybrid Link: Contains both VLAN-aware and VLAN-unaware devices
  - All frames for some VLANs are tagged
  - All frames for other VLANs are untagged

Tagged Frame Format

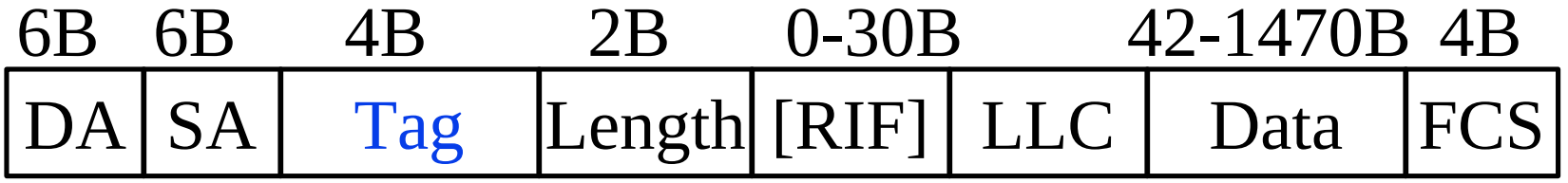
- **Tag Header:**



- **Ethernet Frame:**



- **802.3 Frame:**

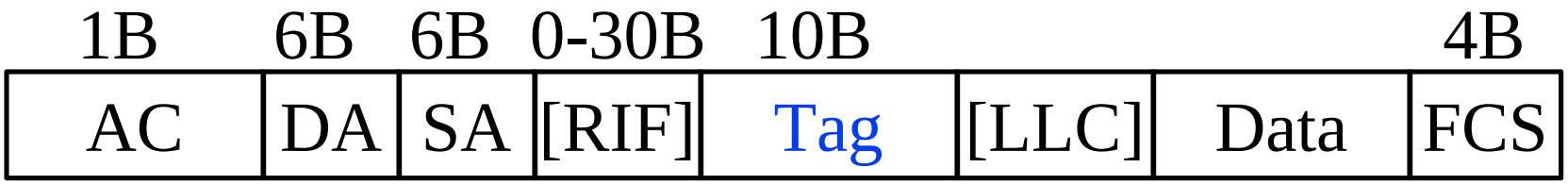


Frame Format (Cont)

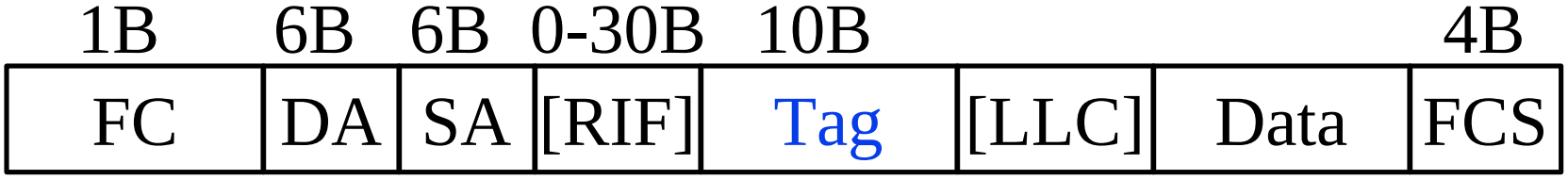
- TPID = Tag Protocol ID
- CFI = Canonical Format Indicator
  = Bit order of address info in TR/FDDI frames
  = Presence/absence of RIF in 802.3/Ethernet frames
- RIF = Routing Information Field
  - New routing type: 01 = Transparent frame
    ⇒ No routing info.
- DA = Destination Address, SA = Source Address
  PT = Protocol Type, LLC = Logical Link Control
  FCS = Frame Check Sequence
- Largest data size = 1470 on 802.3

Frame Format (Cont)

- **Token Ring:**



- **FDDI:**



GVRP

- GARP VLAN registration protocol
- GARP = Generic attribute registration protocol
- Register VLAN Ids and port filtering modes
- Both end-stations and bridges can be GARP participants
- GARP Participants issue/revoke membership declaration $\Rightarrow$ Creates entries in the databases
- VLAN-aware bridges propagate VLAN membership changes on all active ports

GVRP (Cont)

- VLAN-aware end stations can "source prune" traffic for VLANs that have no other members
- Initially, all ports on all bridges are set to a default "Port VLAN ID"

GMRP in VLANs

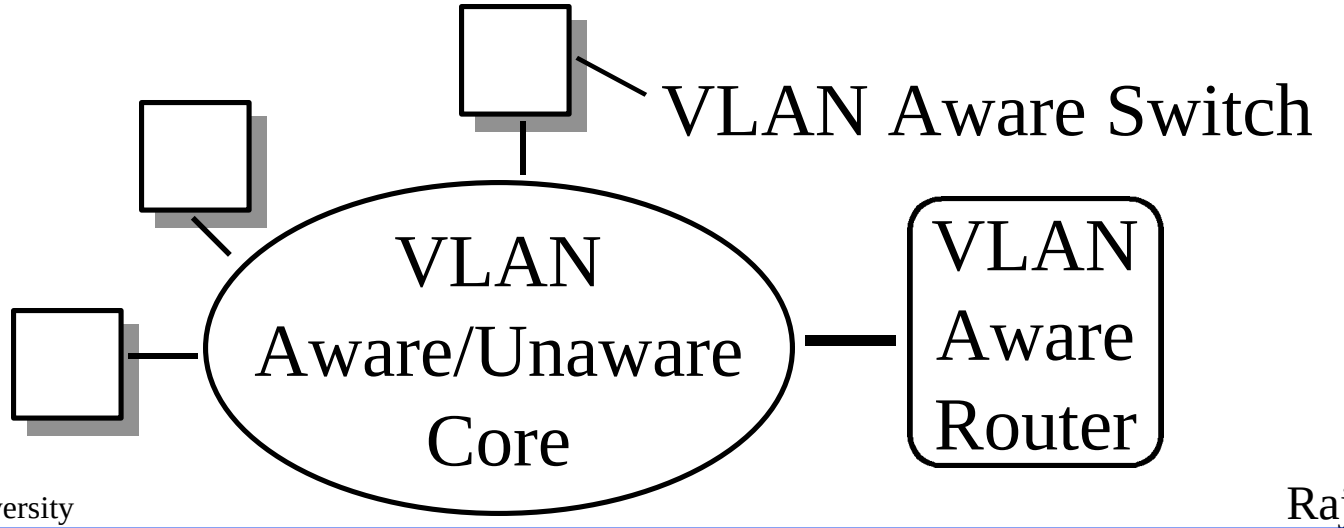
- Original GMRP is designed for one LAN
  ⇒ One one context or base spanning tree context
- With VLANs, multicast addresses are registered a particular VLAN context
  ⇒ Filtering behavior in a VLAN does not affect other VLANs

VLAN Filtering Database

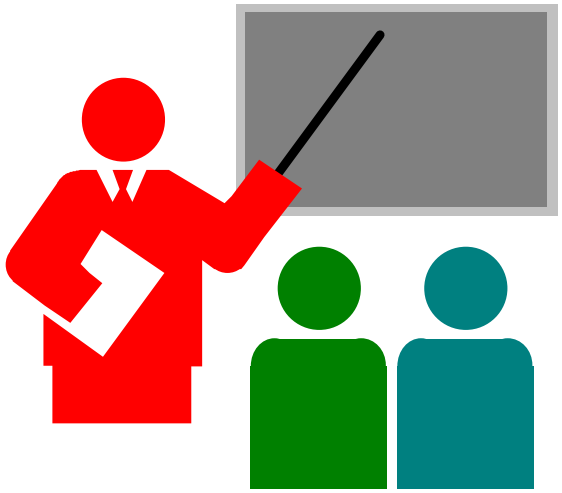
- Two Types of Entries:
  - VLAN Registration entries
  - Group Registration entries
- Both types can static or dynamic
  - Static VLAN Entries: via Management
  - Dynamic Filtering Entry:
    - via learning or registration
    - Learnt entries are aged out
- Port Map for each VLAN: Whether frames should be tagged or untagged

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



Summary



- Virtual LANs ⇒ 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

- For a detailed list of references, see http://www.cis.ohio-state.edu/~jain/refs/lsw_refs.htm
- Email list: p8021-request@hepnrc.hep.net
  Mail archive: http://www.hep.net/mail/p8021.html
- Draft Standard for Virtual Local Area Networks, IEEE P802.1Q/D6, May 16, 1997.

Other Related Standards

- Traffic Class Expediting and Dynamic Multicast Filtering, IEEE P802.1p/D6, April 28, 1997.
- 802.1D MAC bridges
- 802.1G Remote MAC Bridging
- 802.1H Ethernet V2.0 and 802 bridging

Current Schedule

7/17/97 Priority and Multicasting on LANs

7/22/97 No Class

7/24/97 Virtual LANs

7/29/97 Gigabit Ethernet

7/31/97 Quiz 2 (No MBone transmission)

8/5/97 Residential broadband: Cable Modems, xDSL

8/7/97 Multimedia: Compression Standards

8/12/97 Multimedia over IP: RSVP, RTP

8/14/97 Wireless LANs and WANs

8/19/97 Quiz 3 (No MBone transmission)

Credits

This MBone transmission was made possible by:

- Mark Fullmer, OSU/UTS
- Mike Iverson, OSU/UTS
- Mike Douglas, OSU/UTS
- Jayaraman Iyer, OSU/CIS
- Sohail Munir, OSU/CIS