Introduction to Computer Networks

Virtual Bridged LANs (IEEE 802.1Q)

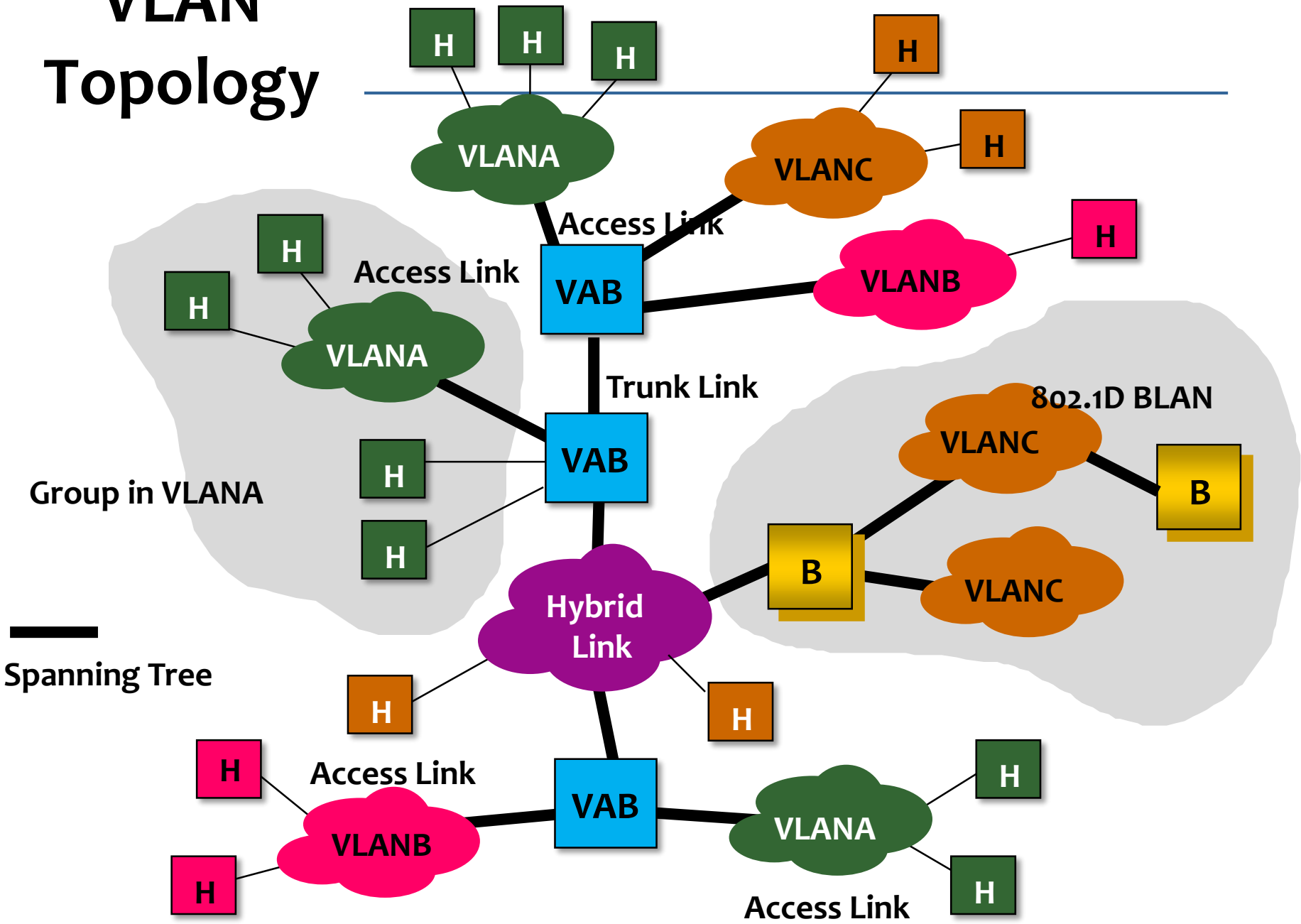
Outline

- Introduction
- Virtual LAN (VLAN) Architecture
- Port-based VLAN
- VLAN Tag
- Summary

VLAN Aims and Benefits

- Without VLAN, the layer 2 switches/bridges will forward received broadcast and multicast frames to all ports.
  不知道member在哪，所以广播
  - Bandwidth wasting issue
  - Security issue
- Easy administration of logical group of stations. Also moves, adds, and changes in members of theses groups.
- Traffic between VLANs is firewalled. The propagation of multicast and broadcast traffic between VLANs is limited.

VLAN Topology



VLAN Aims and Benefits

- Supported over shared and point-to-point media.
- Each VLAN is uniquely identified (VID).
- Maintain compatibility with existing bridges/ switches and stations.
- In the absence of VLAN configuration, switches/ bridges work in Plug-and-Play.

Overview of Virtual LAN

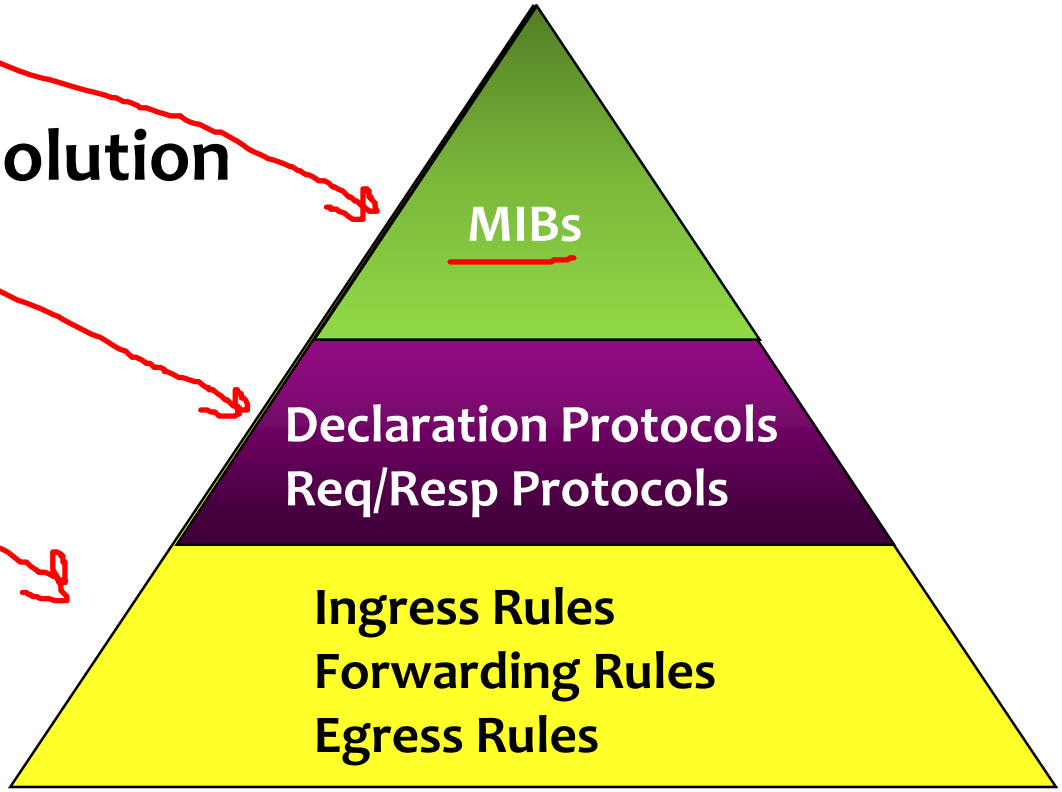
- **Virtual LAN Services** in Bridged LANs.
- **Forwarding Process** required to support VBLANs.
- **Filtering Database** needed to support VBLANs.
- **Protocols and Procedures** required to provide VLAN services and distribute the VLAN membership information.
- **Management services and Operations** required to configure and administer VBLANs.

Outline

- Introduction
- Virtual LAN (VLAN) Architecture
- Port-based VLAN
- VLAN Tag
- Summary

VLAN Architecture

- Based on a 3-level model:
- Configuration
- Distribution/Resolution
- Relay



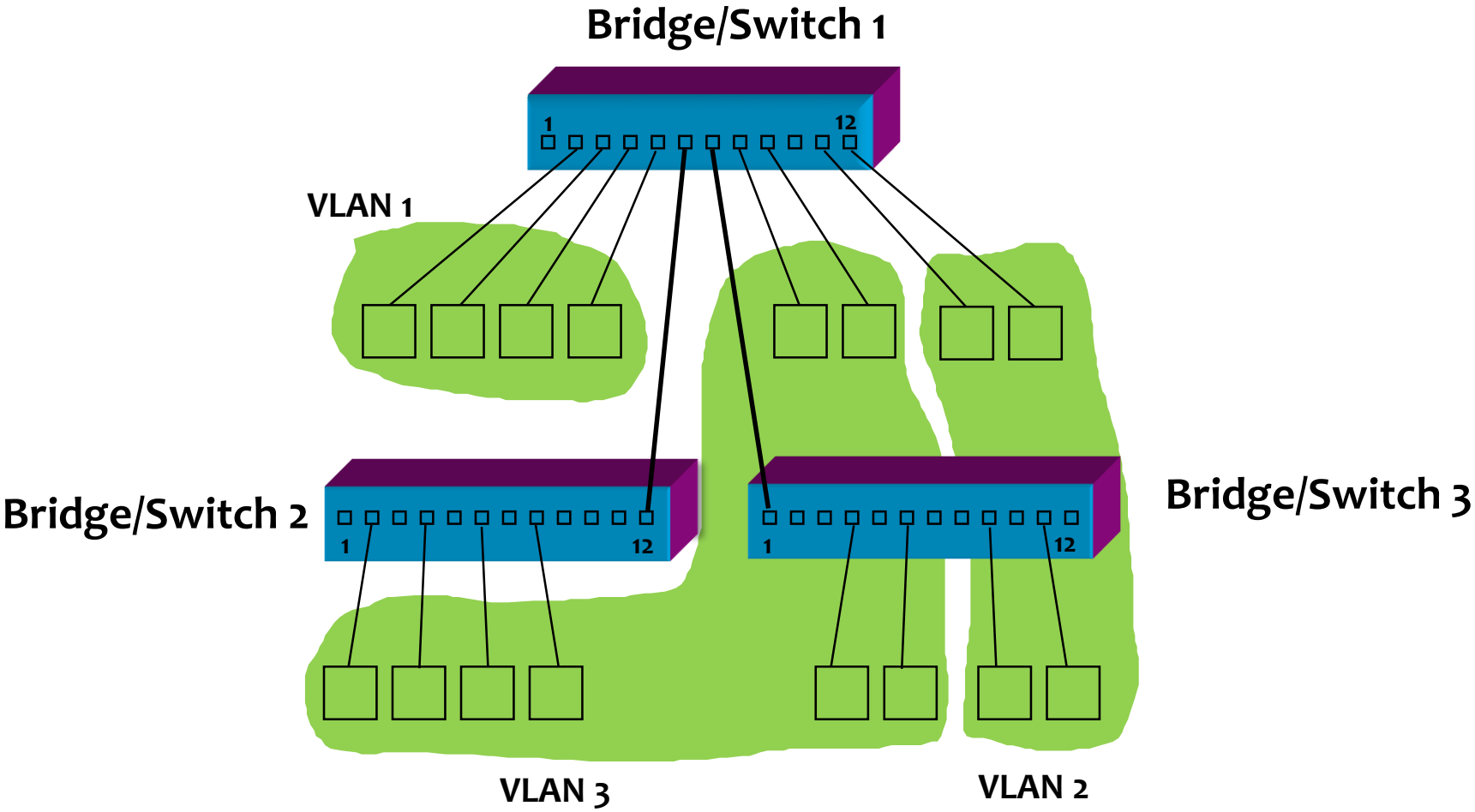
Configuration

- The VLAN configuration is specified in the first place.
- Assignment of VLAN configuration.

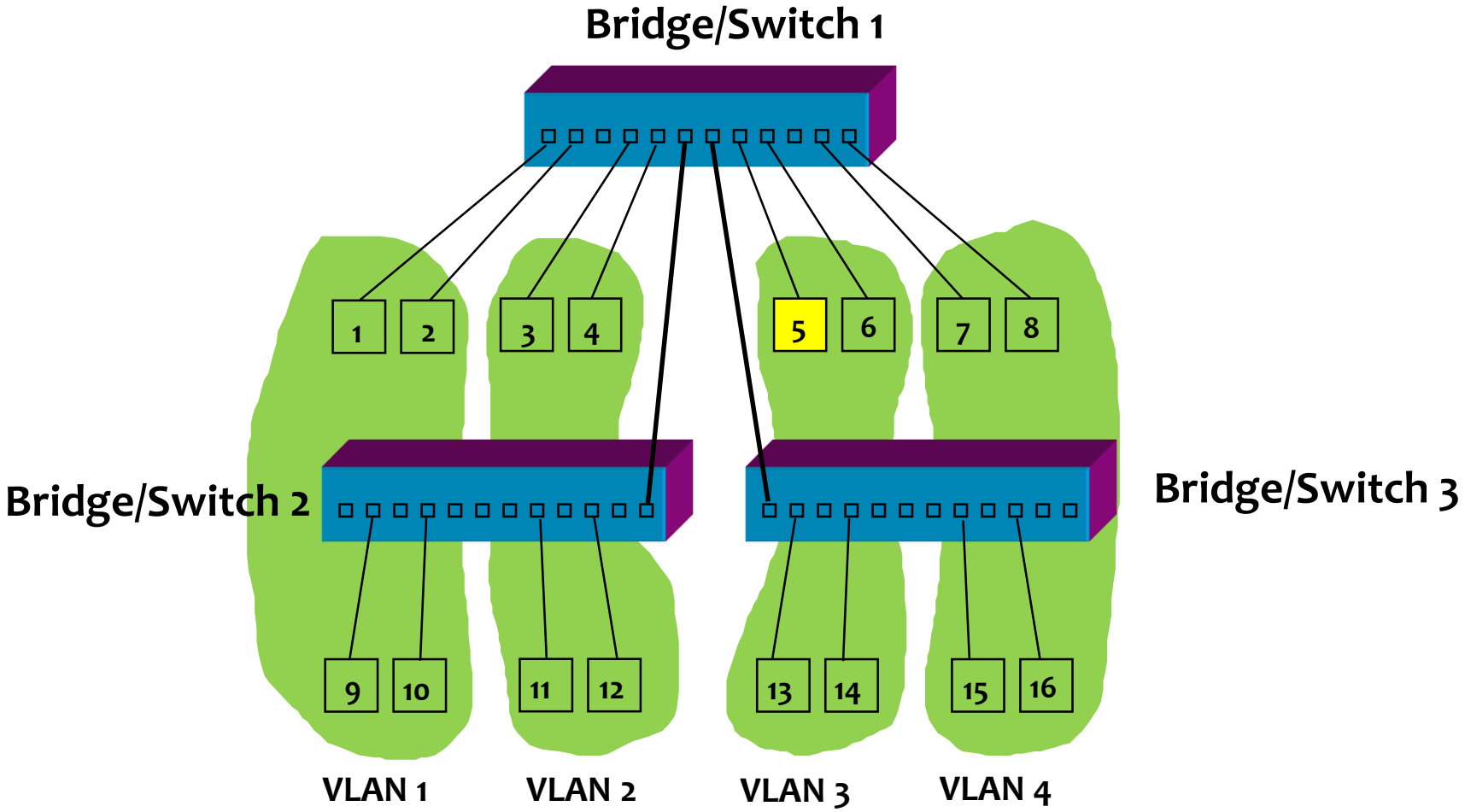
Virtual LANs Technologies

- Port-based VLAN
- MAC-based VLAN
- IP-subnet based VLAN
- Layer-3 Protocol based VLAN

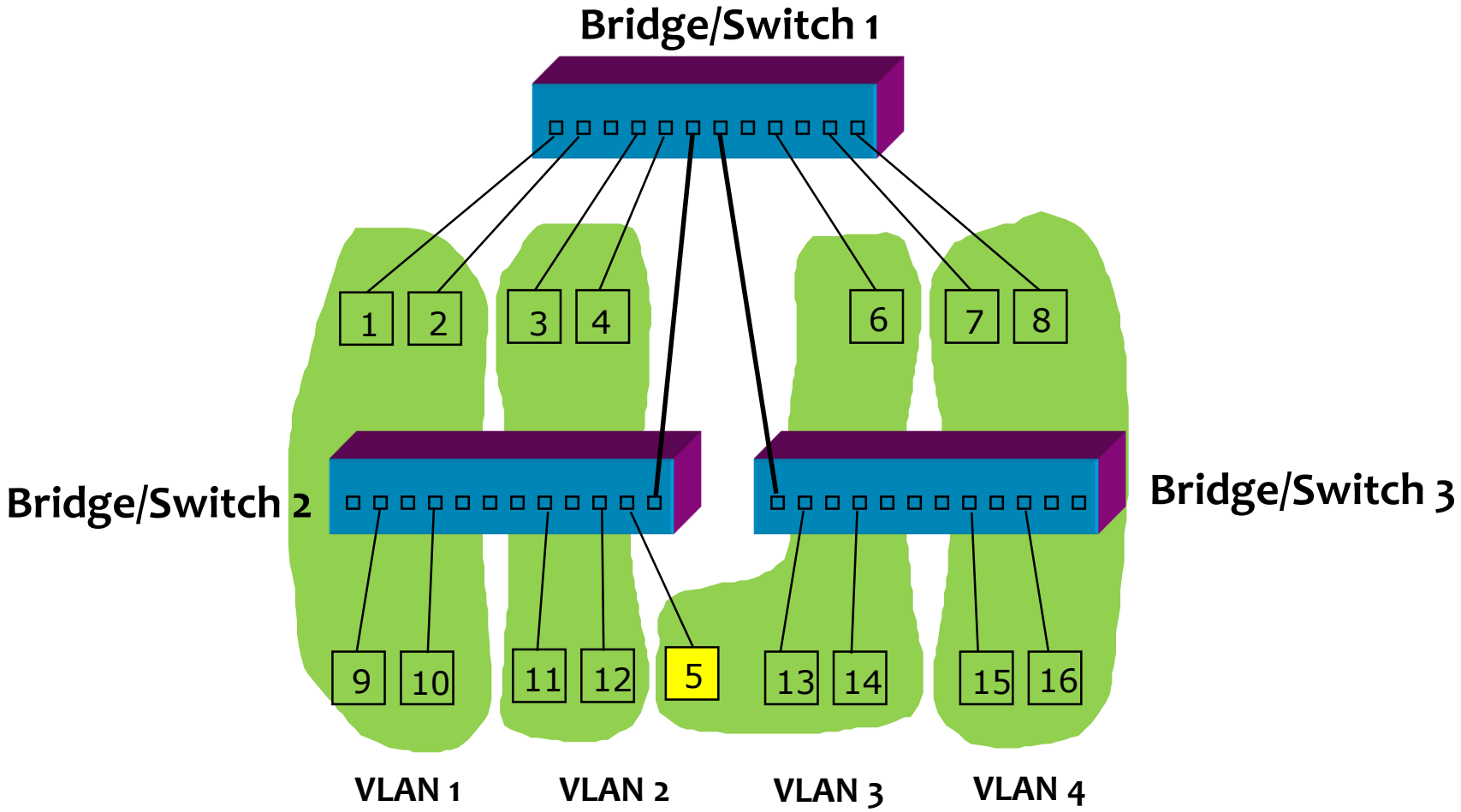
Port-based Virtual LANs



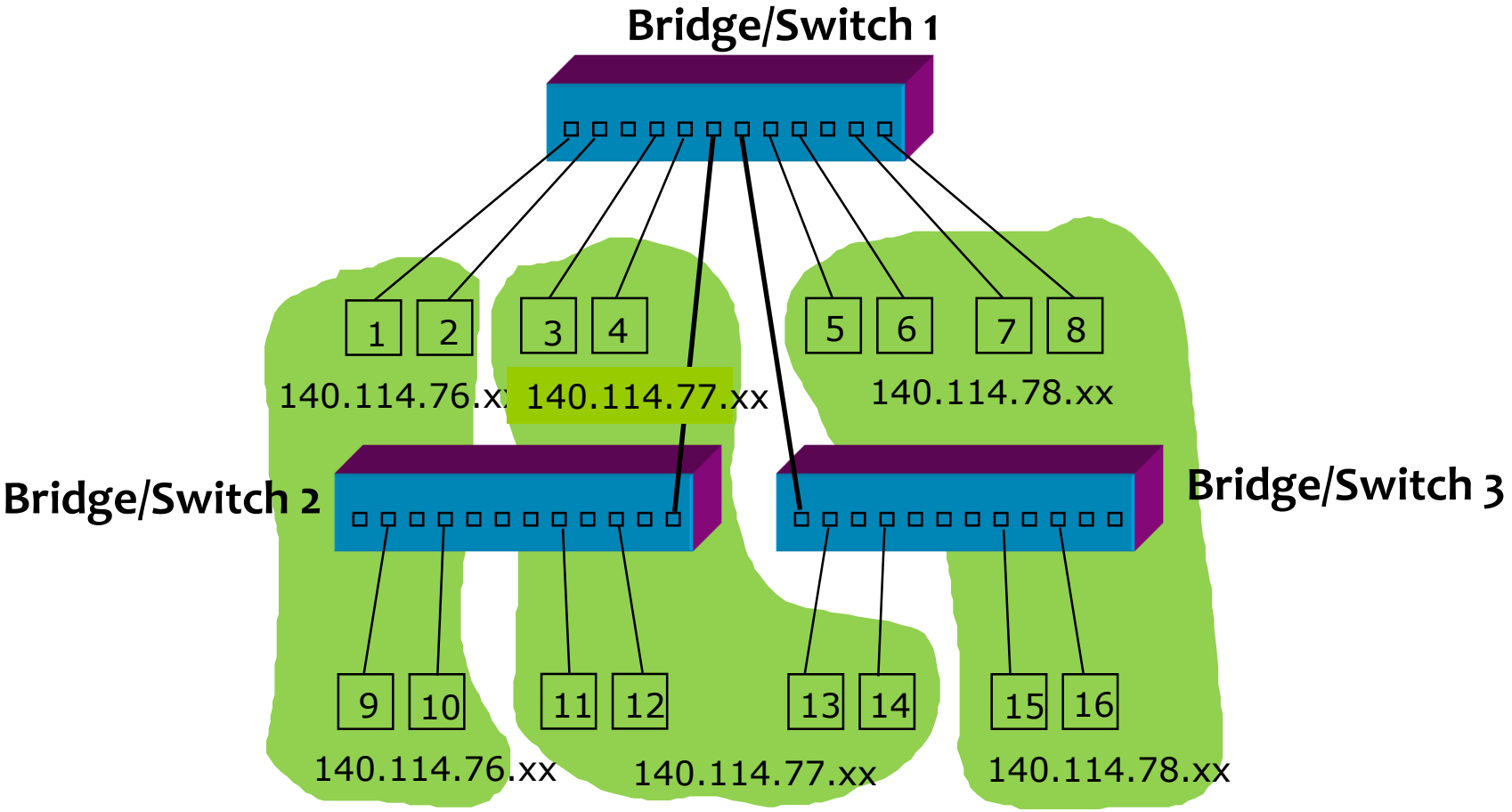
MAC-based Virtual LANs



MAC-based Virtual LANs -- MAC_5 moves

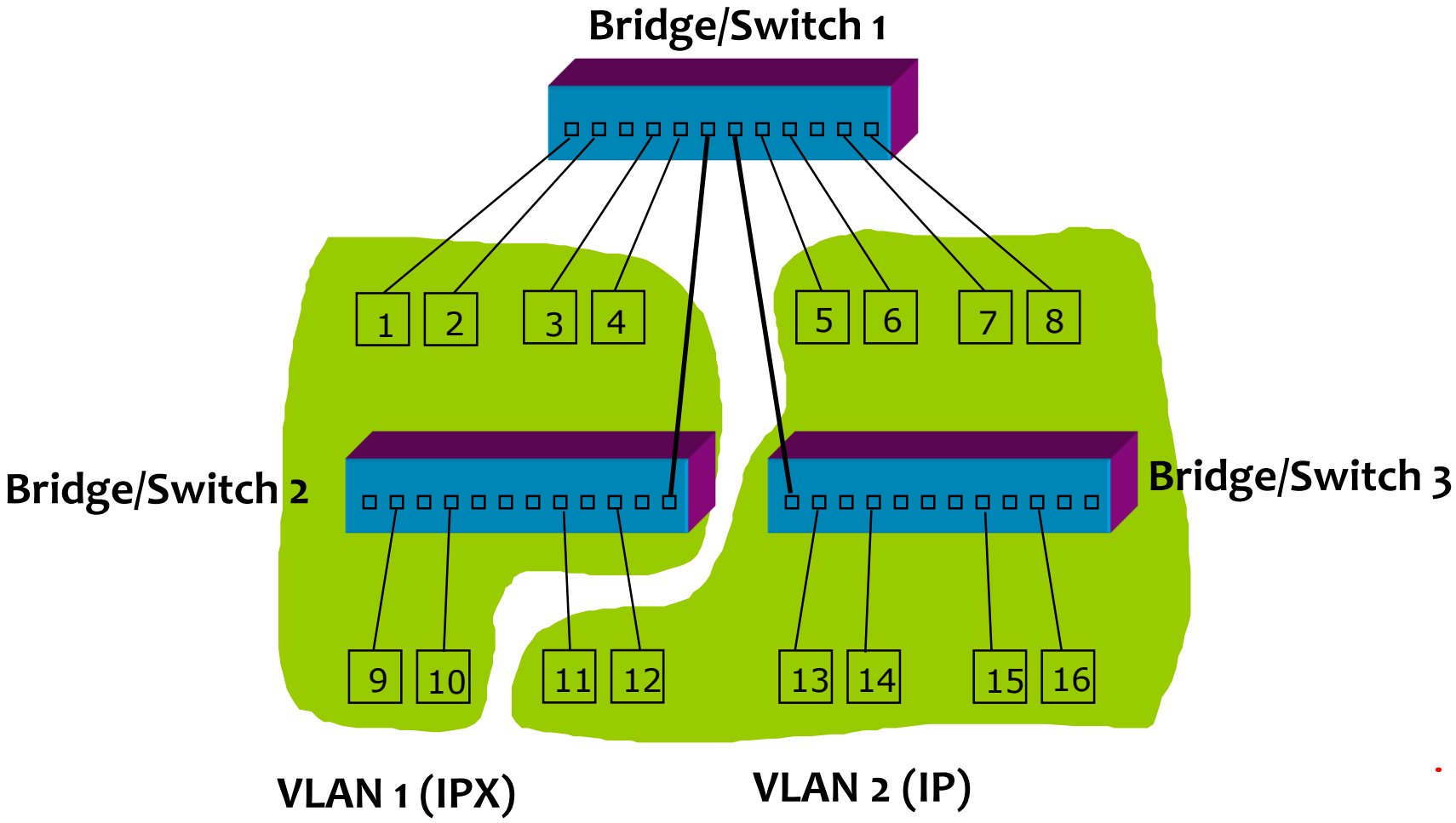


IP Subnet-based Virtual LANs



VLAN 1 = IP subnet 140.114.76
VLAN 2 = IP subnet 140.114.77
VLAN 3 = IP subnet 140.114.78

Layer-3 Protocol based Virtual LANs



Distribution

- Distribute VLAN membership information for Bridges to determine on which VLAN a given packet should be forwarded.
- Various possibilities exist for achieving this:
  - Declaration Protocols for distributing VLAN associations.
    - GARP (Generic Attributes Registration Protocol) is used to distribute membership information among Bridges.
  - Request/Response protocols to request a specific VLAN association (SNMP).

Relay

- The procedure to tag frames, modify tagged frames, and untag frames.
- VLAN frame format to carry VLAN IDs (VIDs).
- Ingress rules
  - Mapping received frames to VLANs
- Forwarding rules
  - Where received frames should be forwarded
- Egress rules
  - Mapping frames for output ports and format (tagged or untagged):

Relay

- The Port-based approach specifies ingress, forwarding and egress rules based on VLAN membership, which allow bridges to:
  - Classify all received untagged frames as belonging to particular VLAN (PVID, Port VID).
  - Recognize the VID associated with received tagged frames.
  - Make use of this VID to forwarding/filtering.
  - Transmit frames in tagged or untagged format, as defined for a given Port/VLAN pairing.

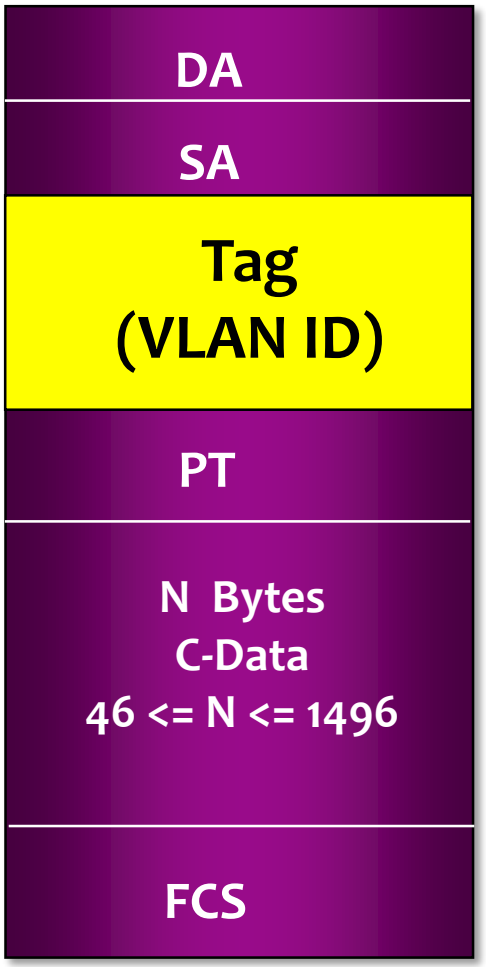
Frame Tagging

Implicit tagging

- A frame is classified to a particular VLAN based on the data content of the frame (MAC address, Layer 3 Protocol ID, etc) and/or the receiving Port.

Explicit tagging

- A frame carries an explicit ID of the VLAN to which it belongs.



Ingress Rules/Egress Rules

- Each frame received is classified as belonging to exactly one VLAN by associating a VID with it.
- The classification is achieved as follows
  - Explicit Tagging : the VID value it carries
  - Implicit Tagging : the PVID associated with the port it is received.
- Frames shall be filtered if outgoing port is not present in the Member Set of the VLAN

Outline

- Introduction
- Virtual LAN (VLAN) Architecture
- Port-based VLAN
- VLAN Tag
- Summary

Port-Based VLAN Definitions

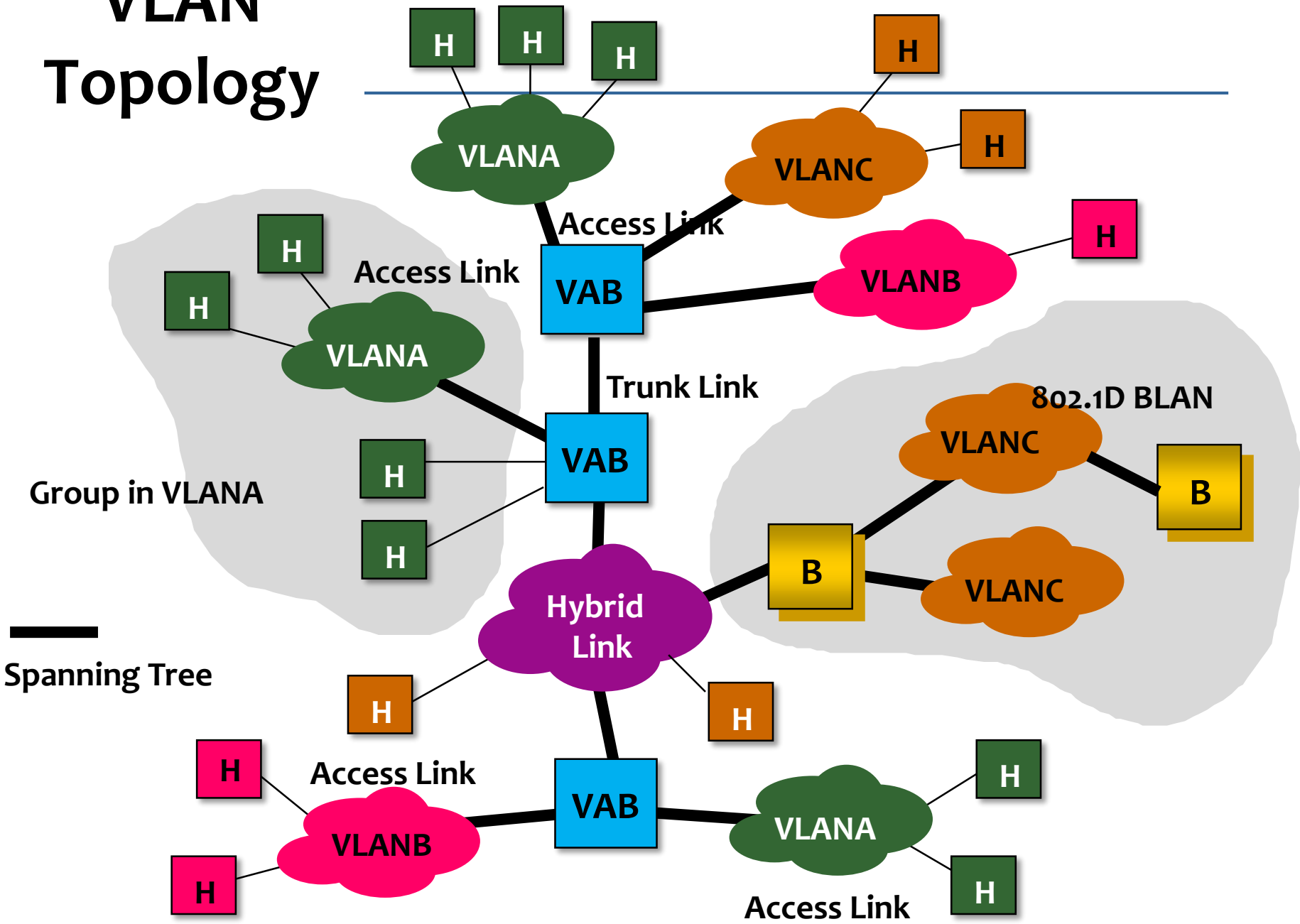
- VLAN aware devices understand VLAN membership and VLAN frame format.
- VLAN unaware devices.
- An Access Link is a LAN segment used to multiplex one or more VLAN unaware devices into a port of a VLAN Bridge.
  - All frames on an access link are implicitly tagged.
  - No VLAN tagged frames on an access link.
  - Viewed as being on the edge of the network.
  - Can be attached to other 802.1D-conforment Bridges (BLAN).

Definitions

- A Trunk Link is a LAN segment used to multiplex VLANs between VLAN Bridges.
  - All devices connect to a Trunk Link must be VLAN aware.
  - All frames (including end station frames) on a Trunk Link are explicitly tagged with a VLAN ID.

- A Hybrid Link is a LAN segment that has both VLAN aware and unaware devices.
  - There can be a mix of Tagged Frames and Untagged Frames but they must be from different VLANs.

VLAN Topology



Rules for Tagging Frames on a Hybrid link

- For each VLAN, all frames traversing a particular hybrid link must be tagged the same way:
  - All implicitly tagged or
  - All carrying the same explicit tag.
- There can be a mix of implicitly and explicit tagged frames but they must be for different VLANs.
- For the hybrid link in the example
  - All frames for VLANs A and B are explicit tagged
  - All frames for VLAN C are implicitly tagged.

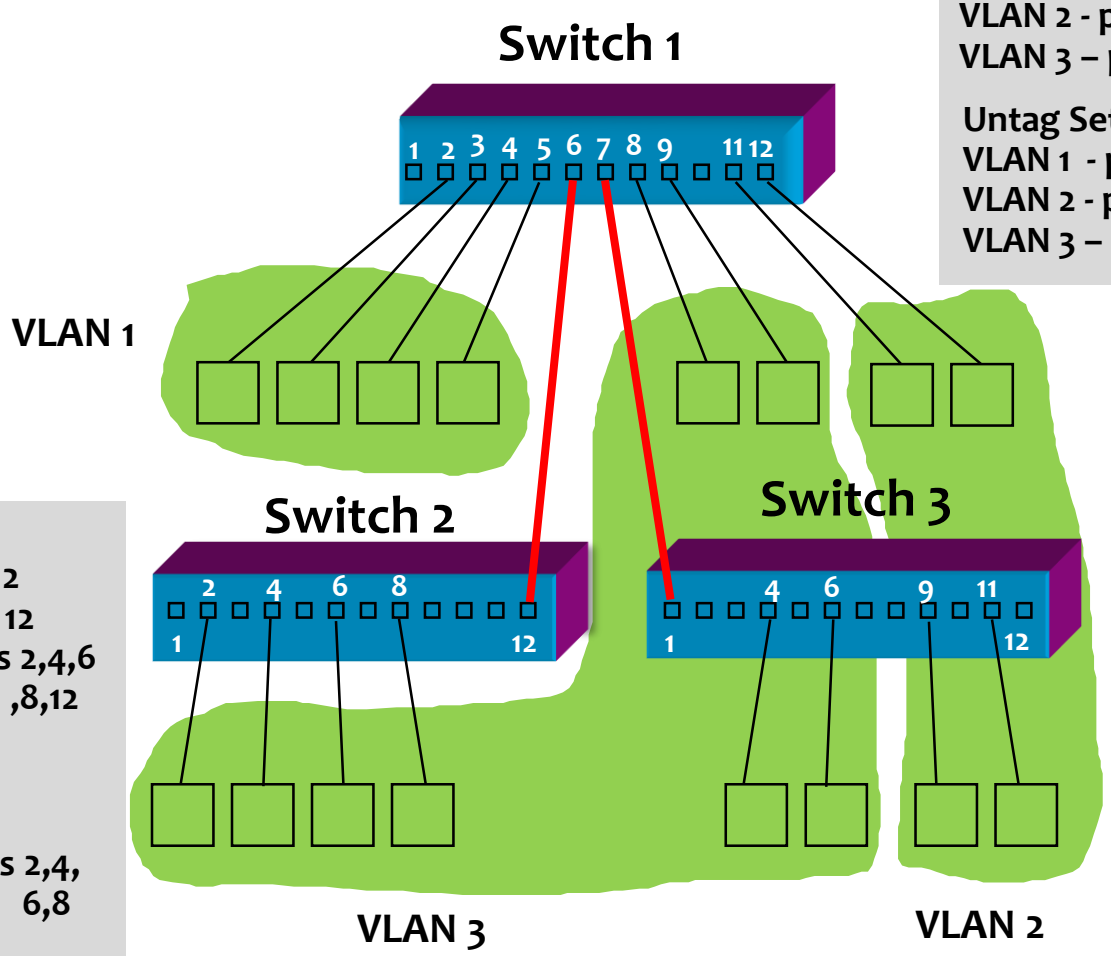
Spanning Tree and VLAN

- Eliminate loops in a bridged LAN.
- Provide the routing path for any pair of nodes.
- All VLANs are aligned along the spanning tree.
- A VLAN is defined by a subset of the spanning tree.
- Each VLAN may be overlaid on different segments or entirely separate from each other.
- The topology of each VLAN is dynamic.

Bridge Operation for VLAN

- A Bridge filters frames to ensure that traffic destined for a given VLAN is forwarded only on segments (ports) that form a path to members of that VLAN.
- For each VLAN, the bridge needs to keep:
  - Member set (Port IDs)
  - Untagged set (Port IDs)

Examples of Member set and Untagged set



Member Set：
VLAN 1 - ports 2, 3, 4, 5
VLAN 2 - ports 7, 11, 12
VLAN 3 – ports 6, 7, 8, 9

Untag Set：
VLAN 1 - ports 2,3,4,5
VLAN 2 - ports 11, 12
VLAN 3 – ports 8, 9

Member Set：
VLAN 1 - port 12
VLAN 2 – port 12
VLAN 3 – ports 2,4,6 ,8,12

Untag Set：
VLAN 1 -
VLAN 2 -
VLAN 3 – ports 2,4, 6,8

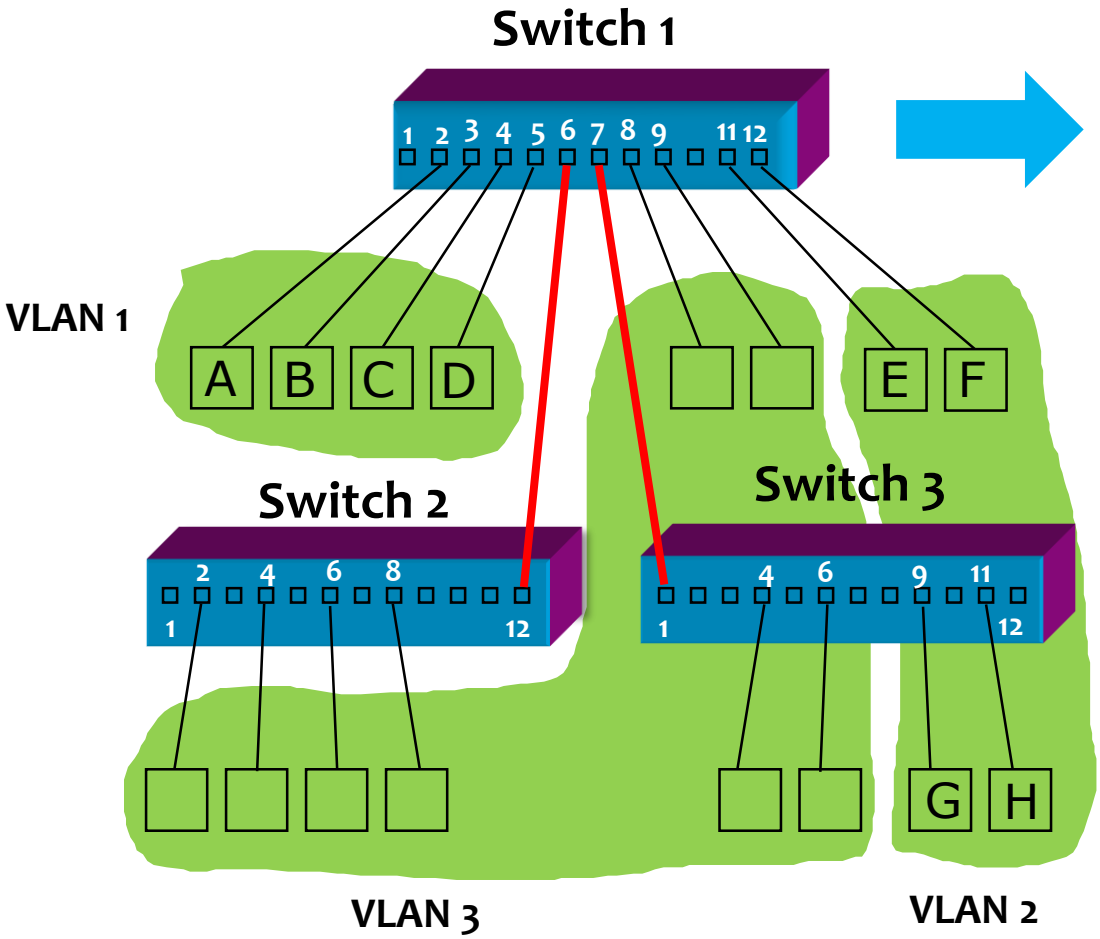
Member Set：
VLAN 1 - port 1
VLAN 2 – ports 1 9, 11
VLAN 3 – ports 1, 4, 6

Untag Set：
VLAN 1 -
VLAN 2 - ports 9, 11
VLAN 3 – ports 4, 6

VLAN Addressing Learning

- **Shared VLAN Learning (SVL)**
  - The addresses learned by each VLAN are shared for all VLANs
- **Independent VLAN Learning (IVL)**
  - The addresses learned from each VLAN are NOT shared
- In most cases, SVL or IVL produces the same result.
- But in some special cases, we need to specify the learning mode of bridge.

Examples of SVL and IVL



FD of VLAN 1

MAC Addr	Port	Time (S)
A	2	20
B	3	18
C	4	25
D	5	4

MAC Addr	Port	Time (S)
E	11	20
F	12	18
G	7	25
H	7	4

FD of VLAN 2

IVL Example -- Multiple Independent VLANs

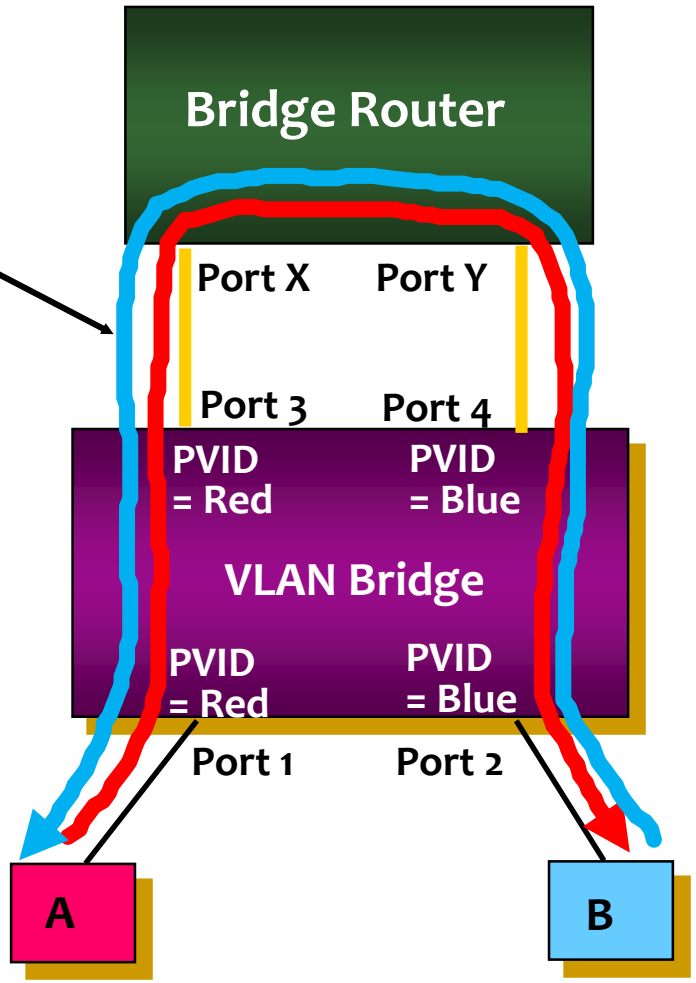
- Server (Bridge-Router, or Connector) connecting multiple independent VLANs.
- Connector and stations are VLAN unaware (untag).
- Connector did not turn on spanning tree algorithm.
- VLAN Red (A) <--> VLAN Blue (B) should be delivered to Connector (firewalled).
- The Filtering databases should be independent (IVL).
- Otherwise, MAC A(B) will be learned from different ports 1,4 (2,3) alternatively.
- Then, the frames from A (B) to B(A) will be delivered in a wrong way.

IVL Example -- Multiple Independent VLANs

Correct paths
For A->B and B->A

Member Set：
Red - Ports 1,3
Blue - Ports 2,4

Untag Set：
Red - Ports 1,3
Blue - Ports 2,4



Filtering DB

MAC	Port
A	X
B	Y

VLAN Red

MAC	Port
A	1
B	3

VLAN Blue

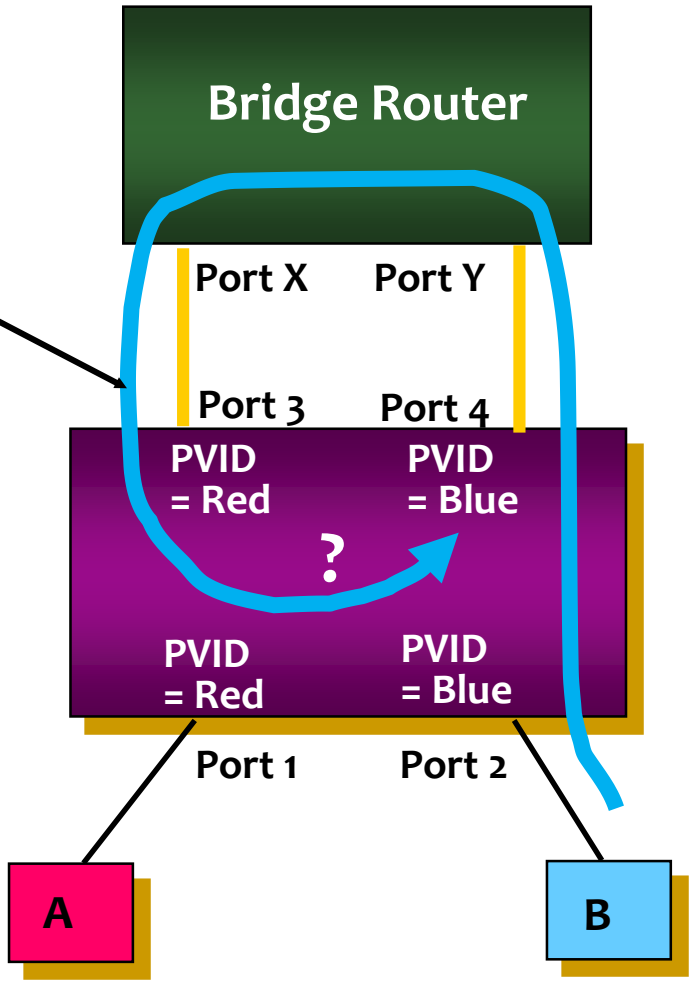
MAC	Port
A	4
B	2

If SVL is used for this case

Incorrect path
For B --->A

Member Set：
Red - Ports 1,3
Blue - Ports 2,4

Untag Set：
Red - Ports 1,3
Blue - Ports 2,4



Filtering DB

MAC	Port
A	X
B	Y

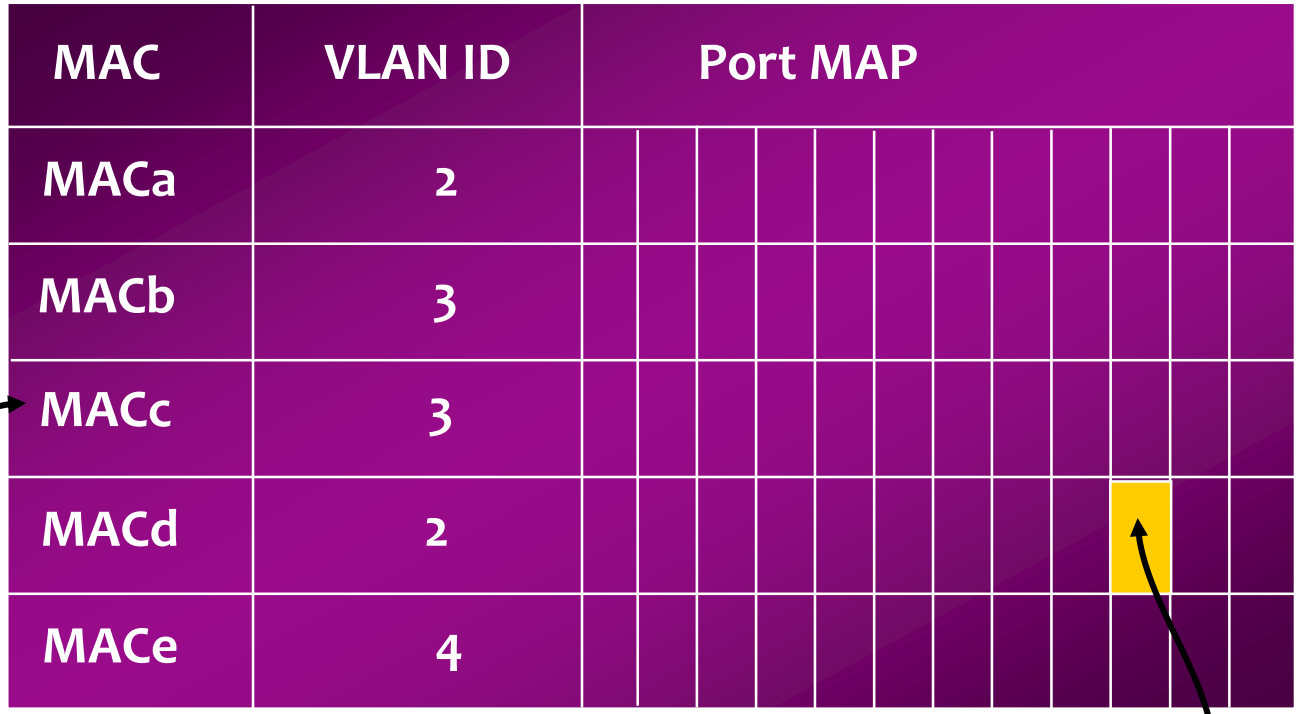
SVL (Red, Blue)

MAC	Port
A	4
B	3

The Filtering Databases for VLAN

- Static Filtering Entry
- Static VLAN Registration Entry
- Dynamic Filtering Entry
- Dynamic VLAN Registration Entry

Static Filtering Entry

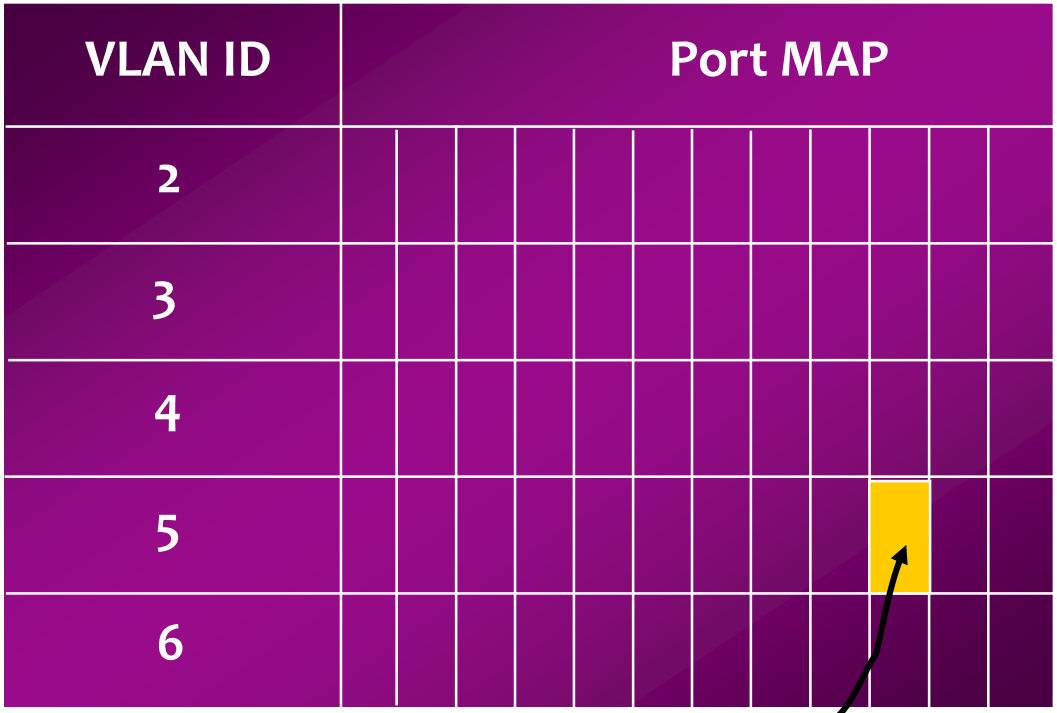


Individual MAC,
Group MAC,
All Group MAC,
All Unregistered Group MAC

Control Element

Forward, Filter,
According to dynamic FD

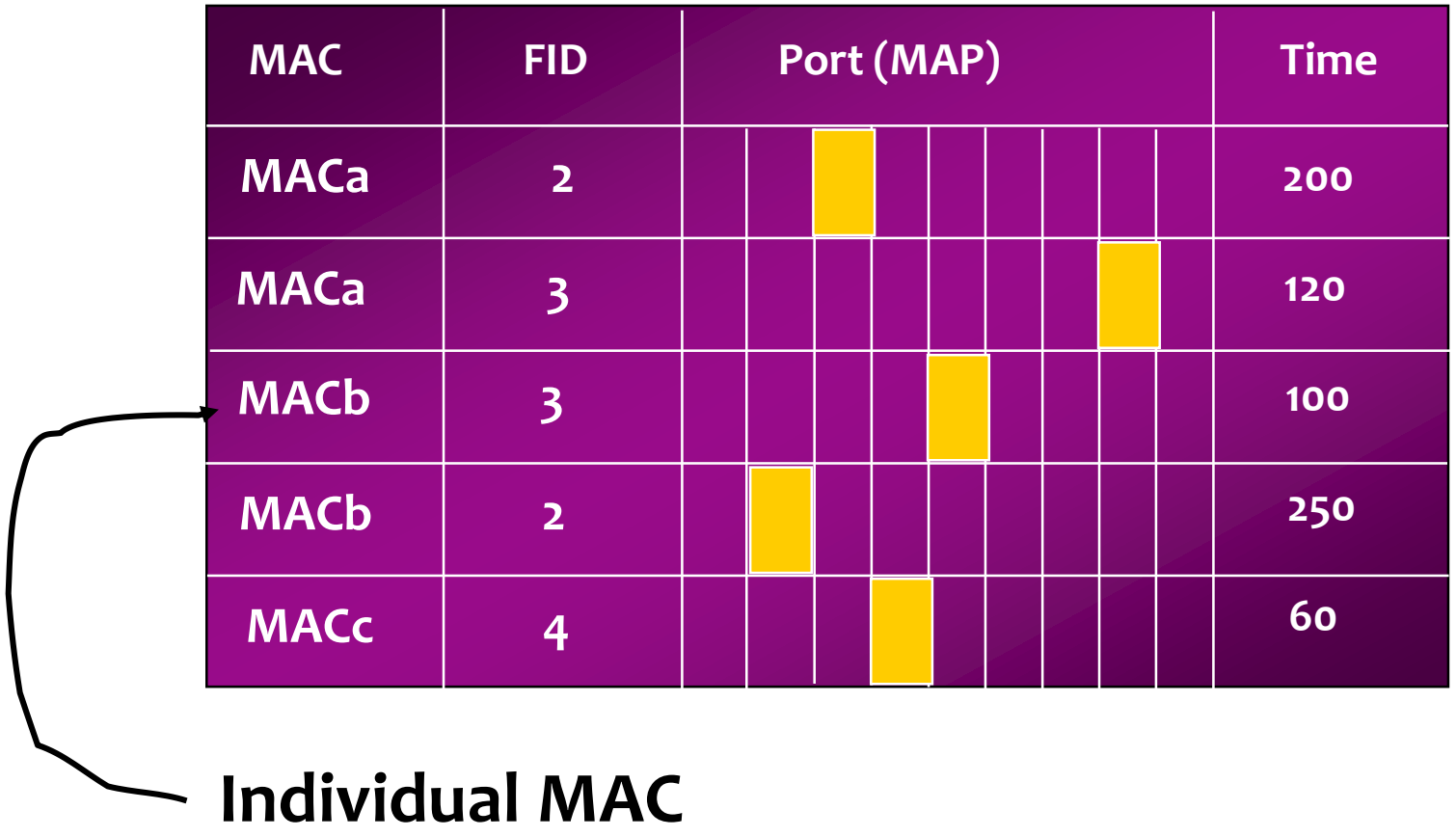
Static VLAN Registration Entry



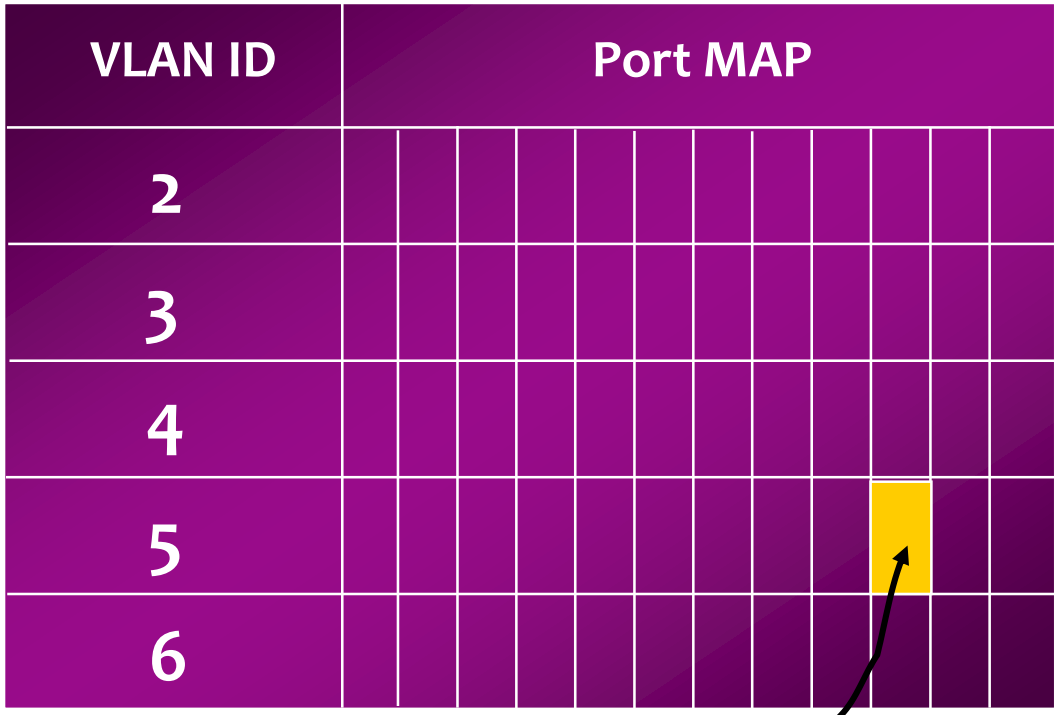
Control Element

GVRP Registrar Administrative Control :
Registration Fixed, Forbidden, Normal.
Tagged/Untagged

Dynamic Filtering Entry (By Learning Process)



Dynamic VLAN Registration Entry



Control Element

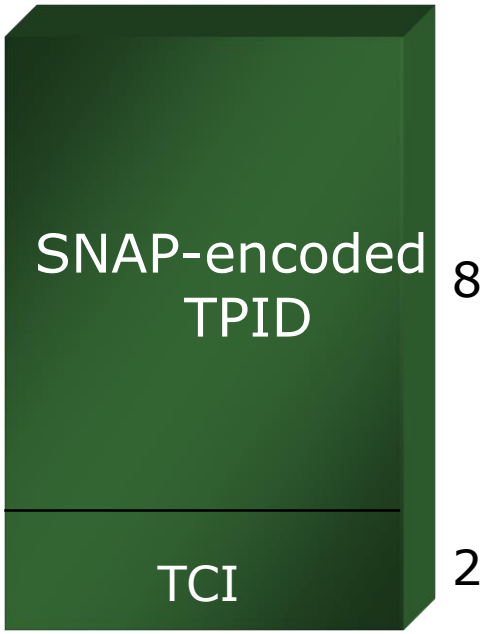
VID is registered on this port ?

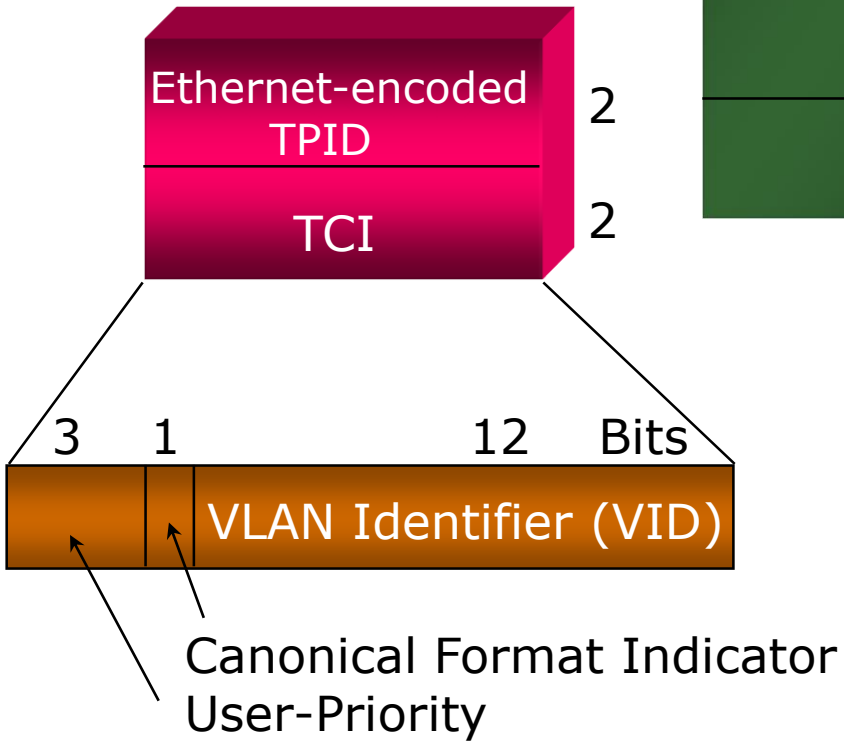
Outline

- Introduction
- Virtual LAN (VLAN) Architecture
- Port-based VLAN
- VLAN Tag
- Summary

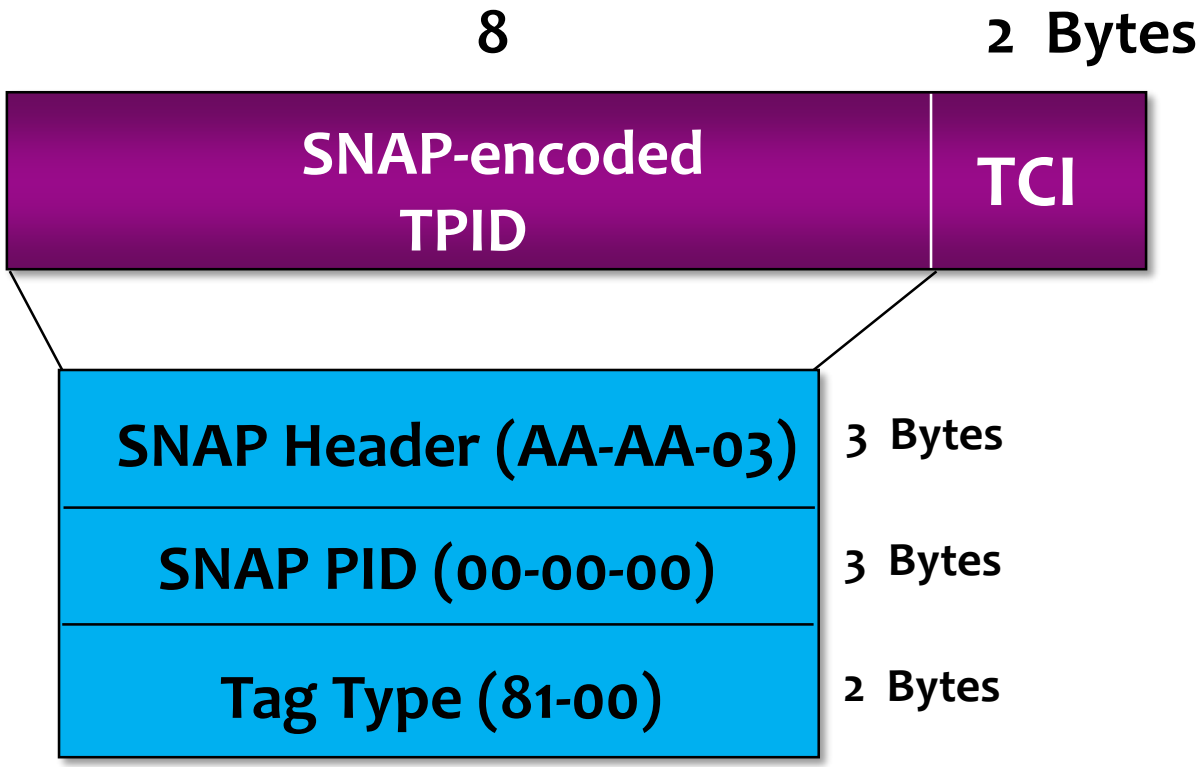
VLAN Tag Structure

- Tag Protocol Identifier (TPID)
- Tag Control Information (TCI)
  - User-Priority
  - Canonical Format Indicator
  - VID





Tag Format (SNAP-encoded)



SNAP: SubNetwork Access Protocol

The SubNetwork Access Protocol (SNAP) is an a standard for the transmission of IP datagrams over IEEE 802 networks. In other words, IP datagrams could be sent on IEEE 802 networks encapsulated within the 802.2 LLC and SNAP data link layers and the 802.3, 802.4 or 802.5 physical network layers.

Summary

- VLAN is designed to logical group of stations.
- The members of a VLAN can be removed and added dynamically.
- Without VLAN, the broadcast and multicast frames will be forwarded to all ports.
  - Bandwidth wasting issue
  - Security issue
- With VLAN, the propagation of multicast and broadcast frames between VLANs is limited.

Summary

- Directly communications between different VLANs is not allowed. The communication should be directed to a router.
- IEEE 802.1Q defines port-based VLAN
- Three-phase model
  - VLAN configuration
  - Declaration/Distribution VLAN membership
  - Frame Relay
- VLAN ID is 12 bits (4096 VLANs)

Summary

- Three types of link:
  - Access Link: all frames are untagged
  - Trunk Link: all frames are tagged
  - Hybrid Link: a mix of tagged frames and untagged frames but they must be from different VLANs.
- For each VLAN, the bridge needs to keep:
  - Member set (Port IDs)
  - Untagged set (Port IDs)