



VLAN

Mario Baldi

Politecnico di Torino

<http://staff.polito.it/mario.baldi>

Pietro Nicoletti

Studio Reti

<http://www.studioreti.it>

Based on chapter 5 of:

M. Baldi, P. Nicoletti, "Switched LAN", McGraw-Hill, 2002, ISBN 88-386-3426-2

Copyright Notice

This set of transparencies, hereinafter referred to as slides, is protected by copyright laws and provisions of International Treaties. The title and copyright regarding the slides (including, but not limited to, each and every image, photography, animation, video, audio, music and text) are property of the authors specified on page 1.

The slides may be reproduced and used freely by research institutes, schools and Universities for non-profit, institutional purposes. In such cases, no authorization is requested.

Any total or partial use or reproduction (including, but not limited to, reproduction on magnetic media, computer networks, and printed reproduction) is forbidden, unless explicitly authorized by the authors by means of written license.

Information included in these slides is deemed as accurate at the date of publication. Such information is supplied for merely educational purposes and may not be used in designing systems, products, networks, etc. In any case, these slides are subject to changes without any previous notice. The authors do not assume any responsibility for the contents of these slides (including, but not limited to, accuracy, completeness, enforceability, updated-ness of information hereinafter provided).

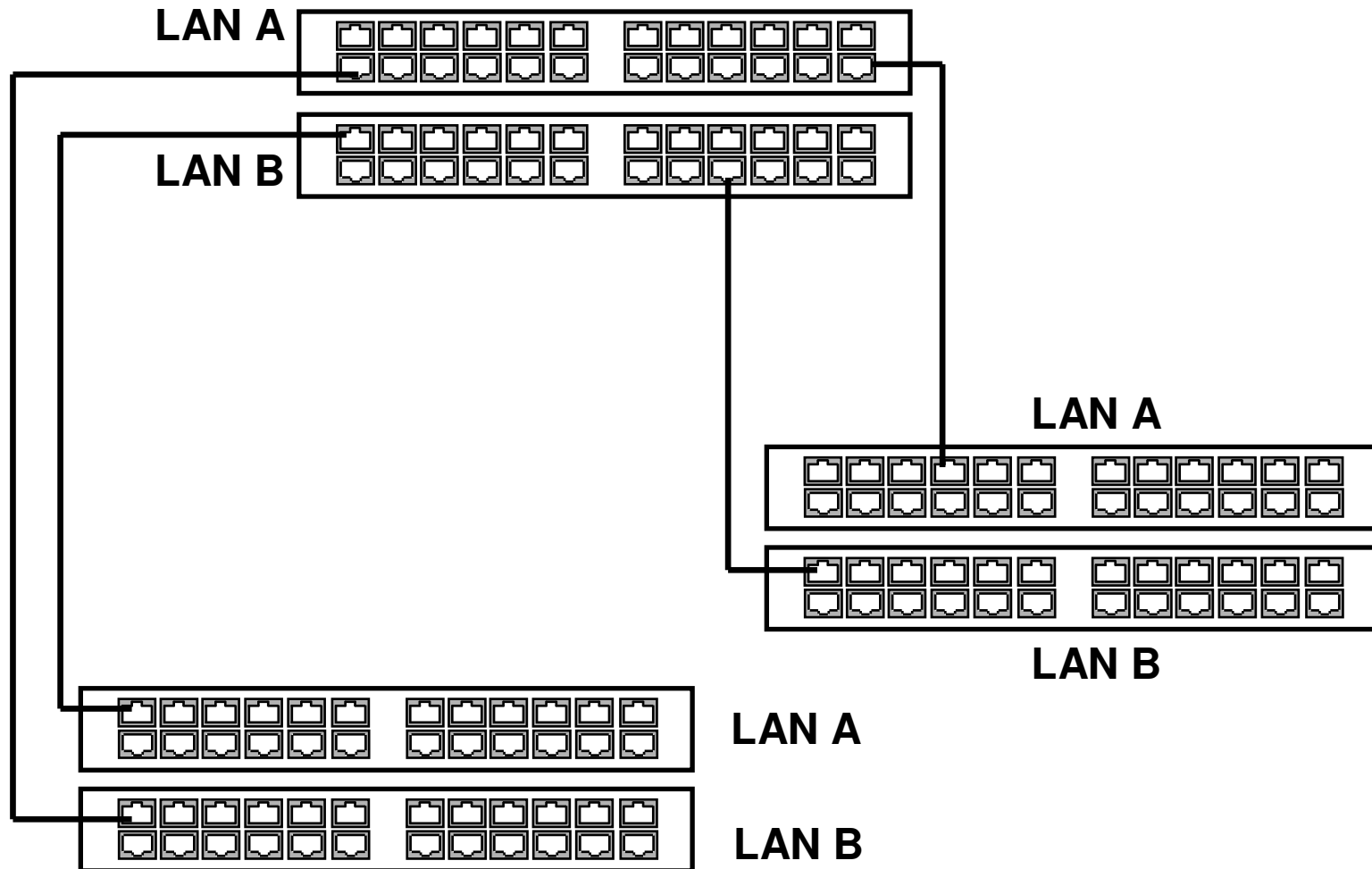
In any case, accordance with information hereinafter included must not be declared.

In any case, this copyright notice must never be removed and must be reported even in partial uses.

Parallel Independent Networks

- Need for separate networks within a building or campus
 - Privacy
 - Security
- Consequences
 - $n\text{Nets} = n \times (\text{links} + \text{net_devices})$
 - Waste of resources
 - Full separation
 - Traffic segregation

Parallel Network Example



Virtual LAN (VLAN)

- Extended (bridged) LANs, when too large, are affected by several issues
 - High levels of multicast/broadcast traffic
 - Multiple Logical IP Subnets (LISs)
 - Routing among them
 - Security and privacy
- With Virtual LANs
 - Eliminate the need for parallel (physical) networks
 - Only one physical infrastructure
 - Multiple (*virtually*) separate logical (*virtual*) networks can be setup
- A virtual LAN can span
 - A single switch
 - A whole extended LAN, i.e., multiple switches

Virtual LAN (VLAN)

- Ethernet frames do not move between different VLANs
 - Full separation
- Communication between different VLANs is provided by means of higher layer packets
 - E.g., IP: IP Routers route IP packets between VLANs
 - Possibly Layer 3 switches

VLAN Deployment Advantages

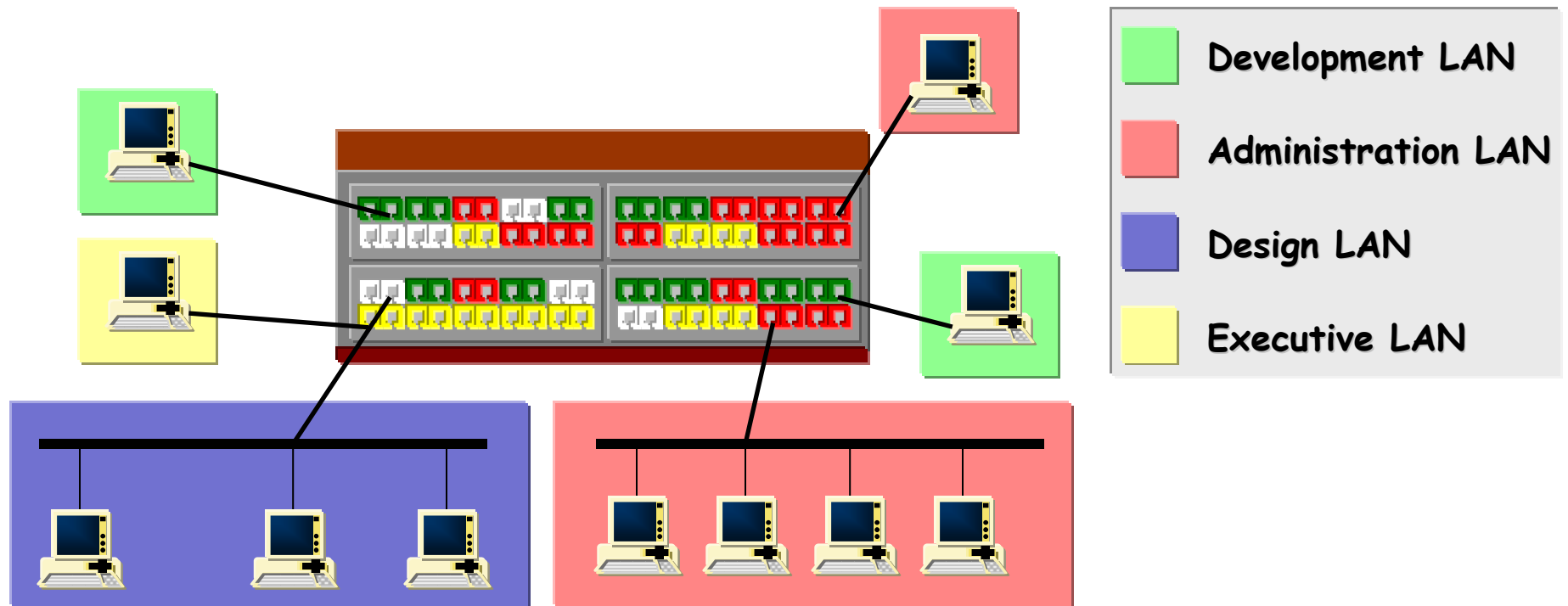
- Security
 - No direct, i.e. at the Ethernet frame level, communication between hosts in different VLANs
 - Communication can be granted (at a higher protocol layer) by routers with filtering functionalities
 - Layer 3 Switches
 - Firewalls
- Solve competence conflicts among different units/departments/functions of large organizations
 - Independent management/operation of VLANs
- Limit the scope of broadcast traffic

Intra-Switch and Inter-Switch VLANs

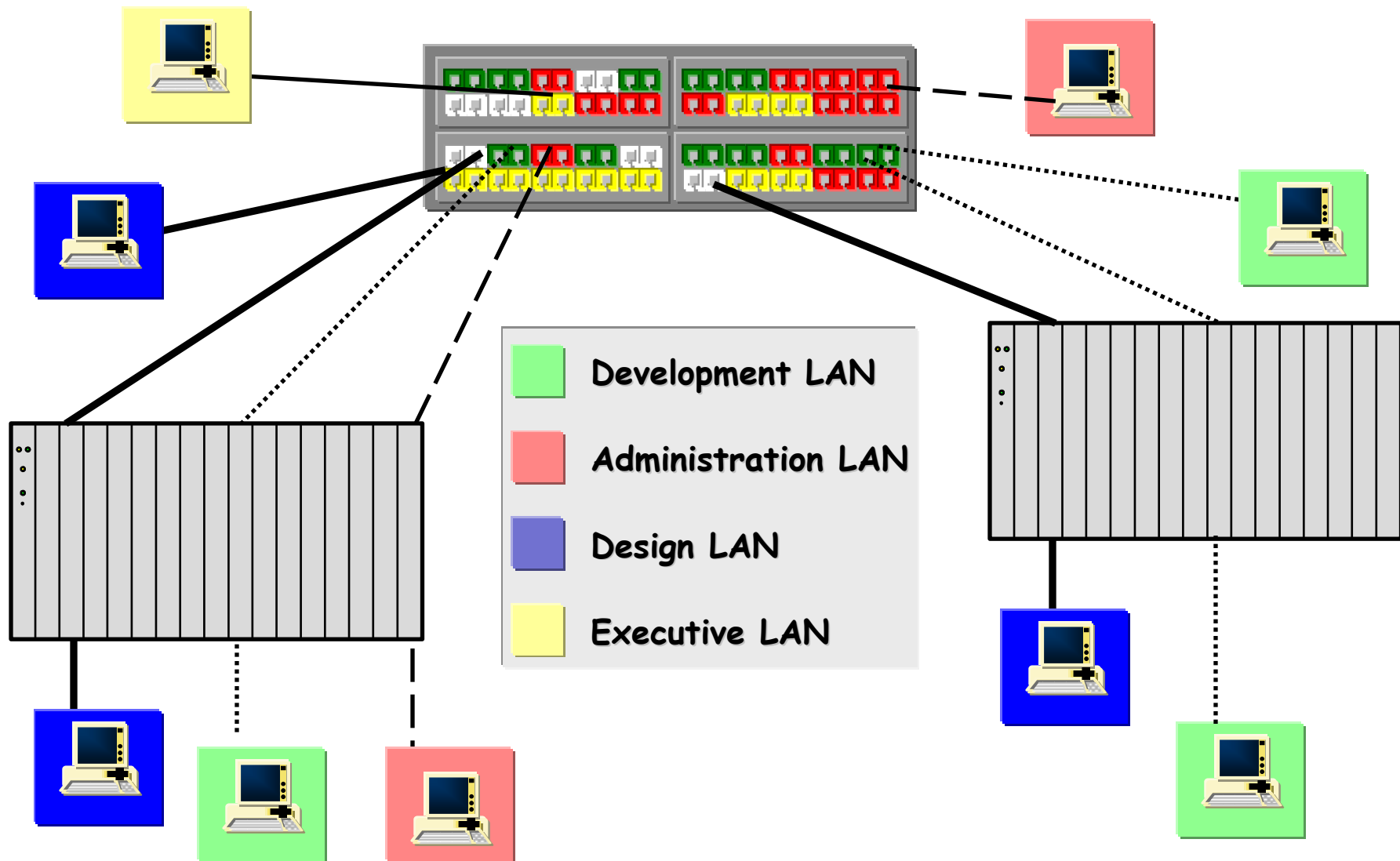
- First VLAN solutions were intra-switch
 - Simple
 - Only star topology networks with one switch at the core with hubs connected to it
 - Switch ports were grouped into a single broadcast domain
- Current products offer Inter-Switch VLAN solutions that can be deployed with both Full-Switching and Segment-Switching

Intra-Switch VLAN

Two or more switch ports can be grouped into a single broadcast domain



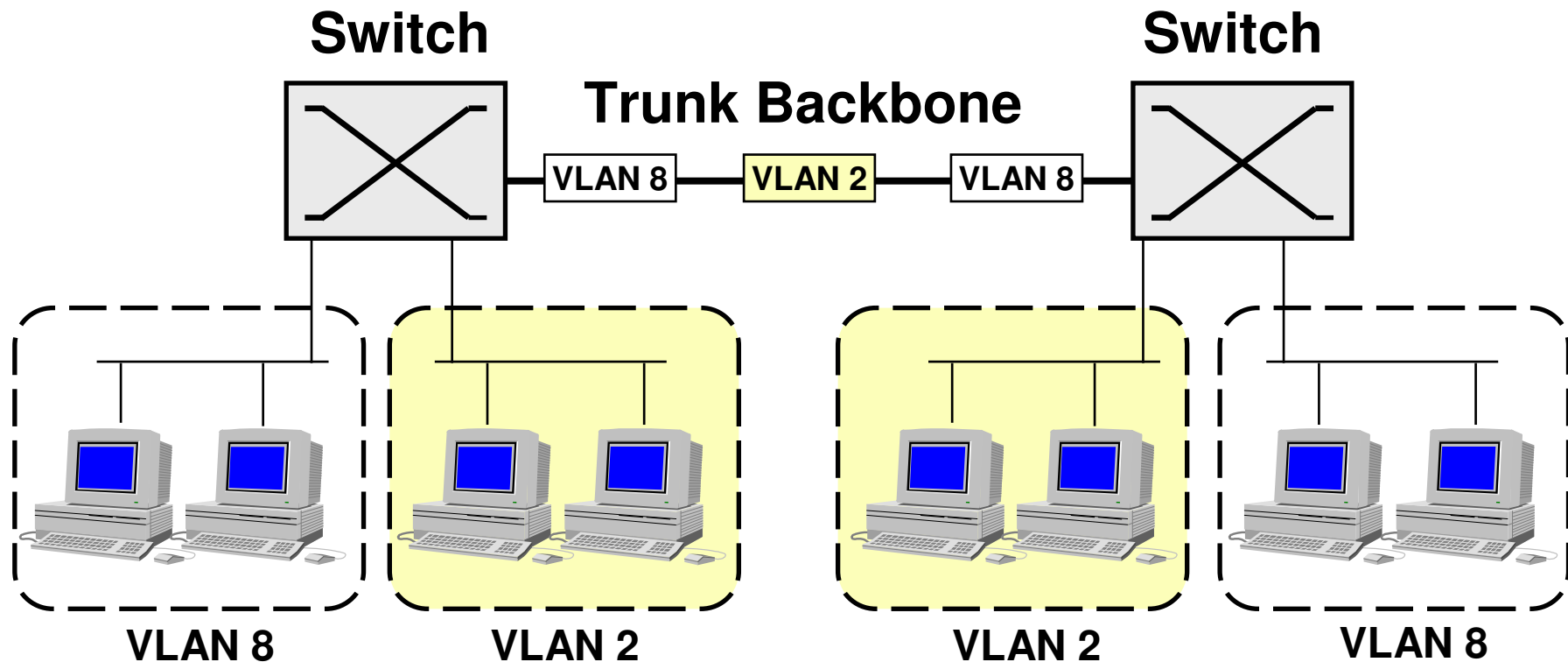
Intra-switch VLAN and Segmentable Hubs



Inter-Switch VLAN

One physical connection is deployed to build different LANs

- It is necessary to identify the LAN each packet belongs to



Tagging

■ Frame Tagging

■ Based on encapsulation

- An Ethernet (Token Ring or FDDI) frame is encapsulated into another Ethernet frame

■ Proprietary solutions

- E.g., ISL (Inter-Switch Link) by Cisco

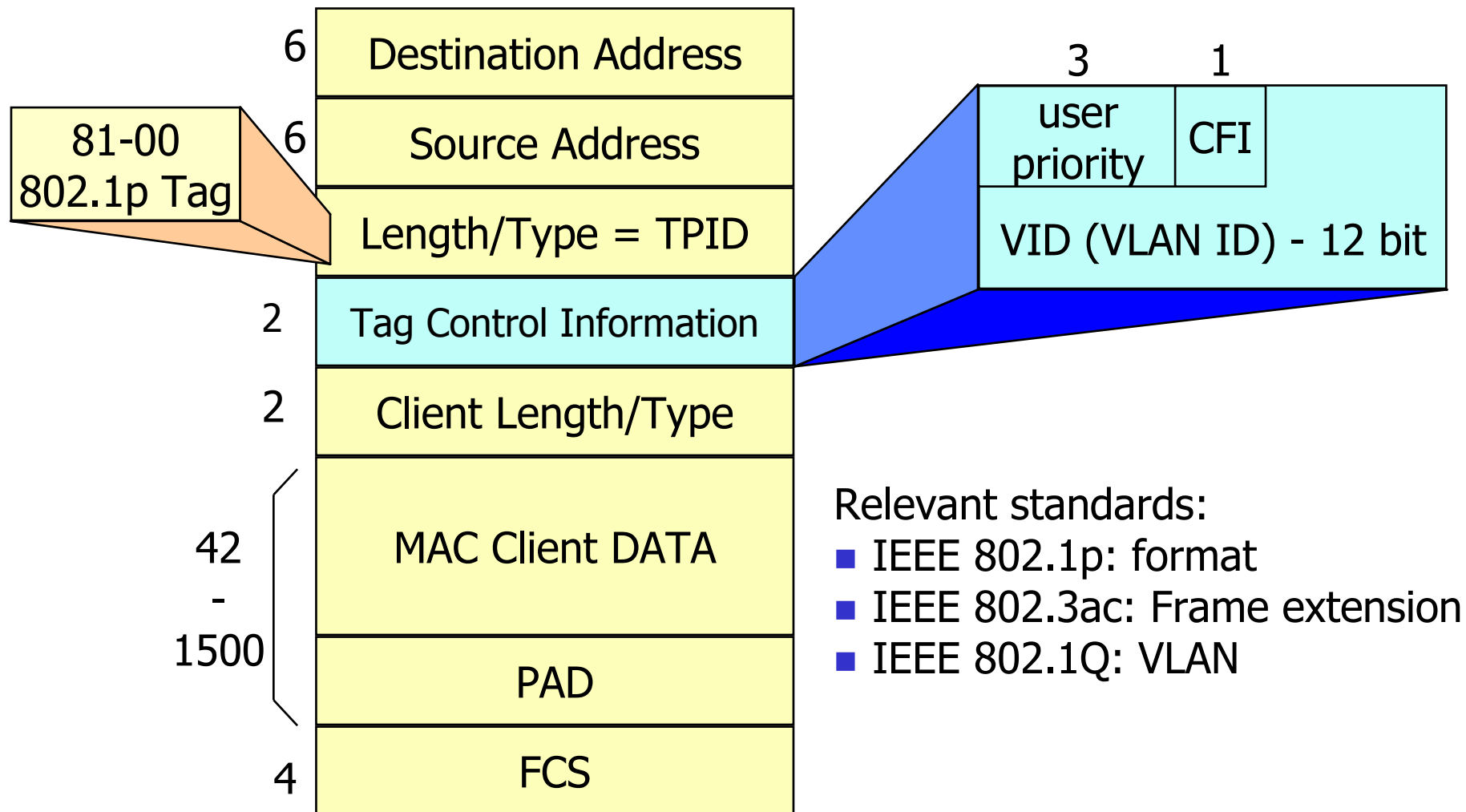
■ Packet Tagging

■ An additional header is added to the MAC header

■ Standardized by IEEE 802.1Q

- VLAN-ID

IEEE 802.1Q Tag Encoding



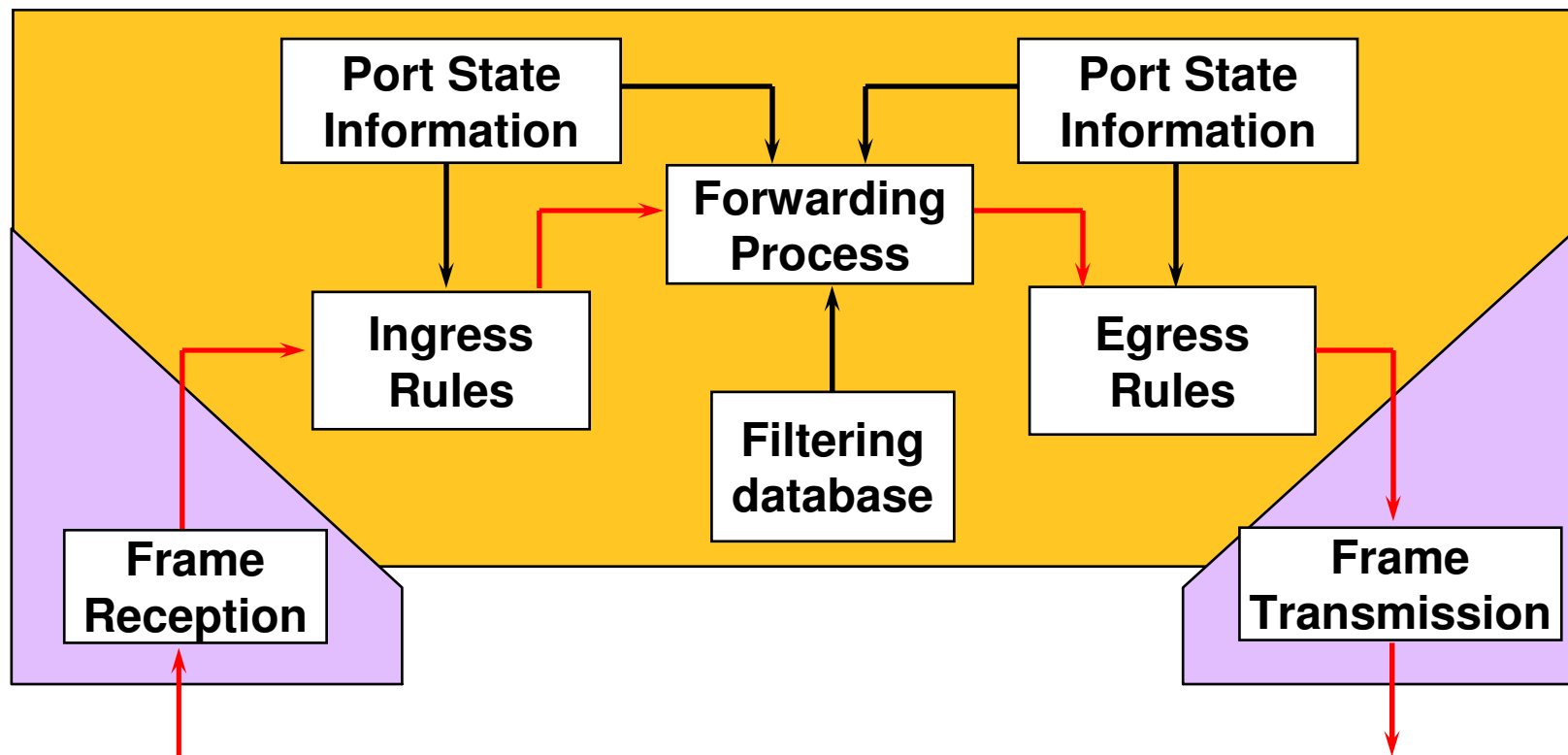
Relevant standards:

- IEEE 802.1p: format
- IEEE 802.3ac: Frame extension
- IEEE 802.1Q: VLAN

Relevant Standards

- IEEE 802.1Q defines VLAN functionalities and specifications
- IEEE 802.3ac defines a new Ethernet frame format to include the Tag header carrying the VLAN ID
- IEEE 802.1p defines:
 - Tag header format
 - Packet priority field, whose use is specified by IEEE 802.1p
 - VLAN ID field
 - GVRP for propagating VLAN related information among switches
 - Based on the more general GARP defined in IEEE 802.1p
 - GARP = Generic Attribute Registration Protocol
 - GVRP = GARP VLAN Registration Protocol

IEEE 802.1Q Bridge Relay Function

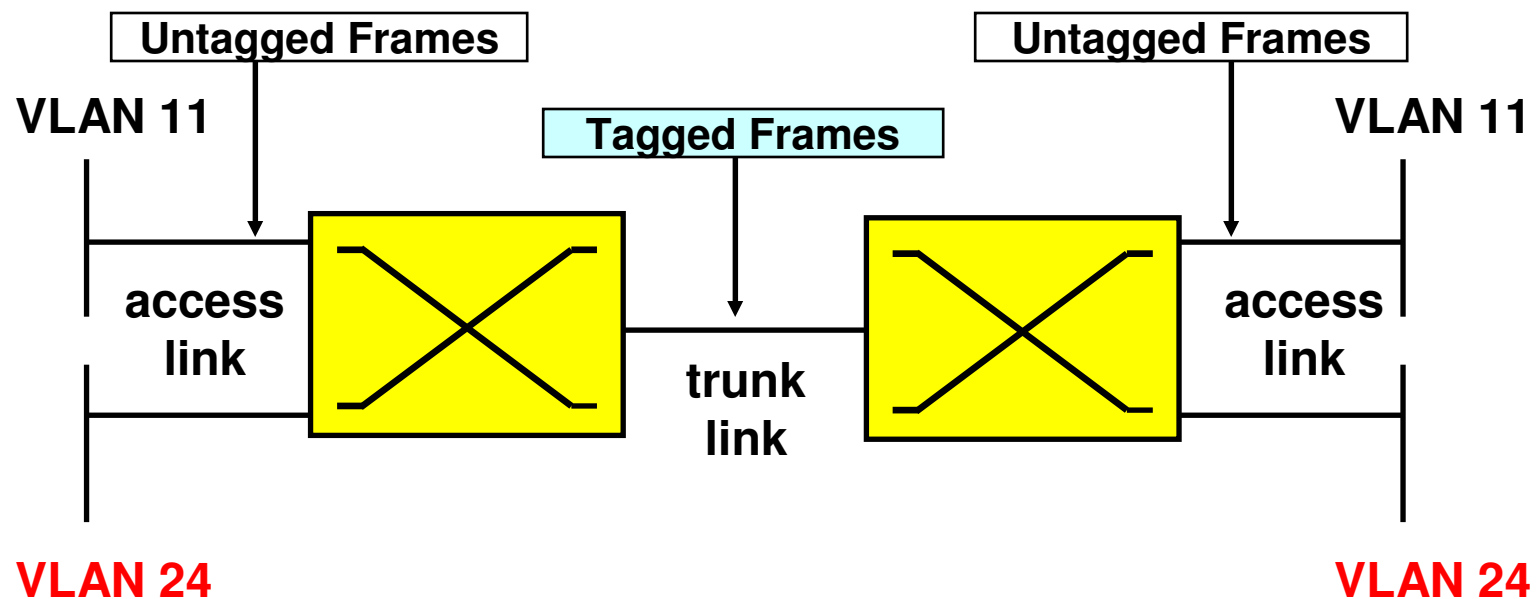


IEEE 802.1Q Specifics

- Per port based VLAN assignment
- Unique spanning tree
- Multiple filtering database identified by FID (Filtering Identifier)
 - Can exist only one entry per MAC address on filtering database
 - A MAC Address may be present in different filtering database

Port-based VLAN

- VLANs are setup on a per-port basis
- Each port can be configured as wither access port or trunk port



Device and Link Type

- Equipment:
 - VLAN-Aware manage tagged and untagged frames
 - VLAN-Unaware don't manage tagged frames
- Access link:
 - Receive and transmit Untagged frames
 - default port configuration on the switch
- Trunk link:
 - Receive and transmit Tagged frames

VLAN Configuration on Switches

3 typical steps:

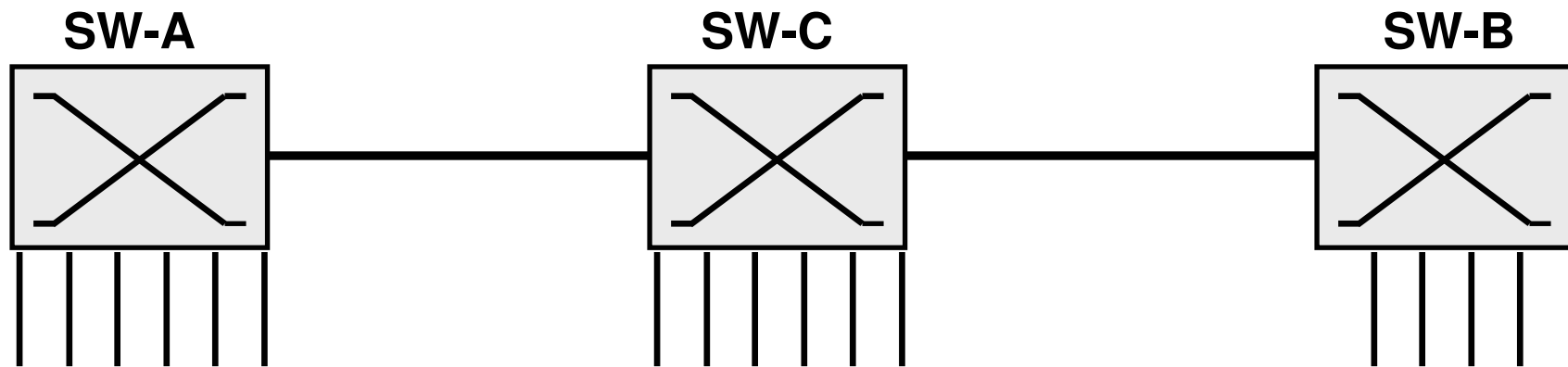
- VLAN creation on the switch;
- VLAN port association;
- Trunk ports definition

By default a port is considered of access type and associated to a default VLAN

- The switch has a VLAN-unaware behaviour.

VLAN Configuration Example

Network topology:

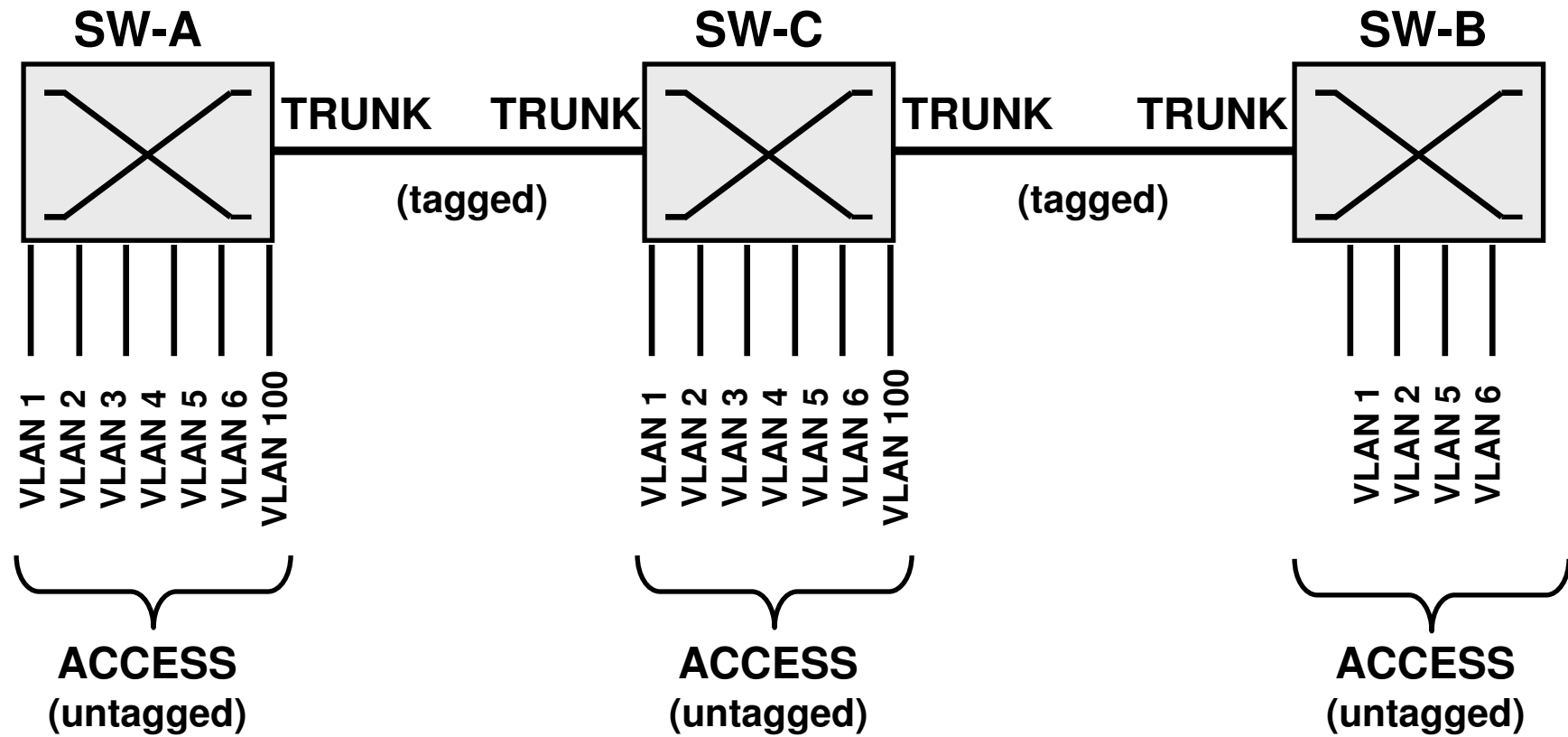


Port Information Before VLAN Configuration

```
SW-C#sho vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Fa0/25, Fa0/26, Fa0/27, Fa0/28, Fa0/29, Fa0/30, Fa0/31, Fa0/32, Fa0/33, Fa0/34, Fa0/35, Fa0/36, Fa0/37, Fa0/38, Fa0/39, Fa0/40, Fa0/41, Fa0/42, Fa0/43, Fa0/44, Fa0/45, Fa0/46, Fa0/47, Fa0/48, Gi0/1, Gi0/2

VLAN Scenario to be Realized



VLAN Creation



```
SW-C#vlan database
Switch(vlan)#vlan 2 name Administration
VLAN 2 added:
    Name: Amministrazione
Switch(vlan)#vlan 3 name Sales
VLAN 3 added:
    Name: Vendite
Switch(vlan)#vlan 4 name test-1
VLAN 4 added:
    Name: prova-1
Switch(vlan)#vlan 5 name test-2
VLAN 5 added:
    Name: prova-2
Switch(vlan)#vlan 6 name test-3
VLAN 6 added:
    Name: prova-3
Switch(vlan)#vlan 100 name Production
VLAN 100 added:
    Name: Produzione
SW-C(vlan)#exit
APPLY completed.
Exiting....
SW-C#
```

Port Association to VLAN

```
SW-C(config)#int fastEthernet 0/12
SW-C(config-if)#switchport access vlan 100
Switch(config-if)#exit
.....
SW-C(config)#int fastEthernet 0/16
SW-C(config-if)#switchport access vlan 2
SW-C(config-if)#exit
.....
SW-C(config)#int fastEthernet 0/20
SW-C(config-if)#switchport access vlan 3
SW-C(config-if)#exit
.....
SW-C(config)#int fastEthernet 0/24
SW-C(config-if)#switchport access vlan 4
SW-C(config-if)#exit
.....
SW-C(config)#int fastEthernet 0/28
SW-C(config-if)#switchport access vlan 5
SW-C(config-if)#exit
.....
SW-C(config)#int fastEthernet 0/32
SW-C(config-if)#switchport access vlan 6
SW-C(config-if)#exit
.....
```

Port and VLAN Information After Switch Configuration



```
SW-C#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/36, Fa0/37, Fa0/38, Fa0/39, Fa0/40, Fa0/41, Fa0/42, Fa0/43, Fa0/44, Fa0/45, Fa0/46, Fa0/47, Fa0/48, Gi0/1, Gi0/2
2	Administration	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19
3	Sales	active	Fa0/20, Fa0/21, Fa0/22, Fa0/23
4	test-1	active	Fa0/24, Fa0/25, Fa0/26, Fa0/27
5	test-2	active	Fa0/28, Fa0/29, Fa0/30, Fa0/31
6	test-3	active	Fa0/32, Fa0/33, Fa0/34, Fa0/35
100	Production	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15

Trunk Port Static Configuration

- Trunk port static configuration without implementation of GVRP protocol

```
SW-C(config)#interface GigabitEthernet 0/1
SW-C(config-if)#switchport mode trunk
SW-C(config-if)#switchport trunk allowed vlan add 1,2,5,6
SW-C(config-if)#exit
SW-C(config)#interface GigabitEthernet 0/2
SW-C(config-if)#switchport mode trunk
SW-C(config-if)#switchport trunk allowed vlan all
```

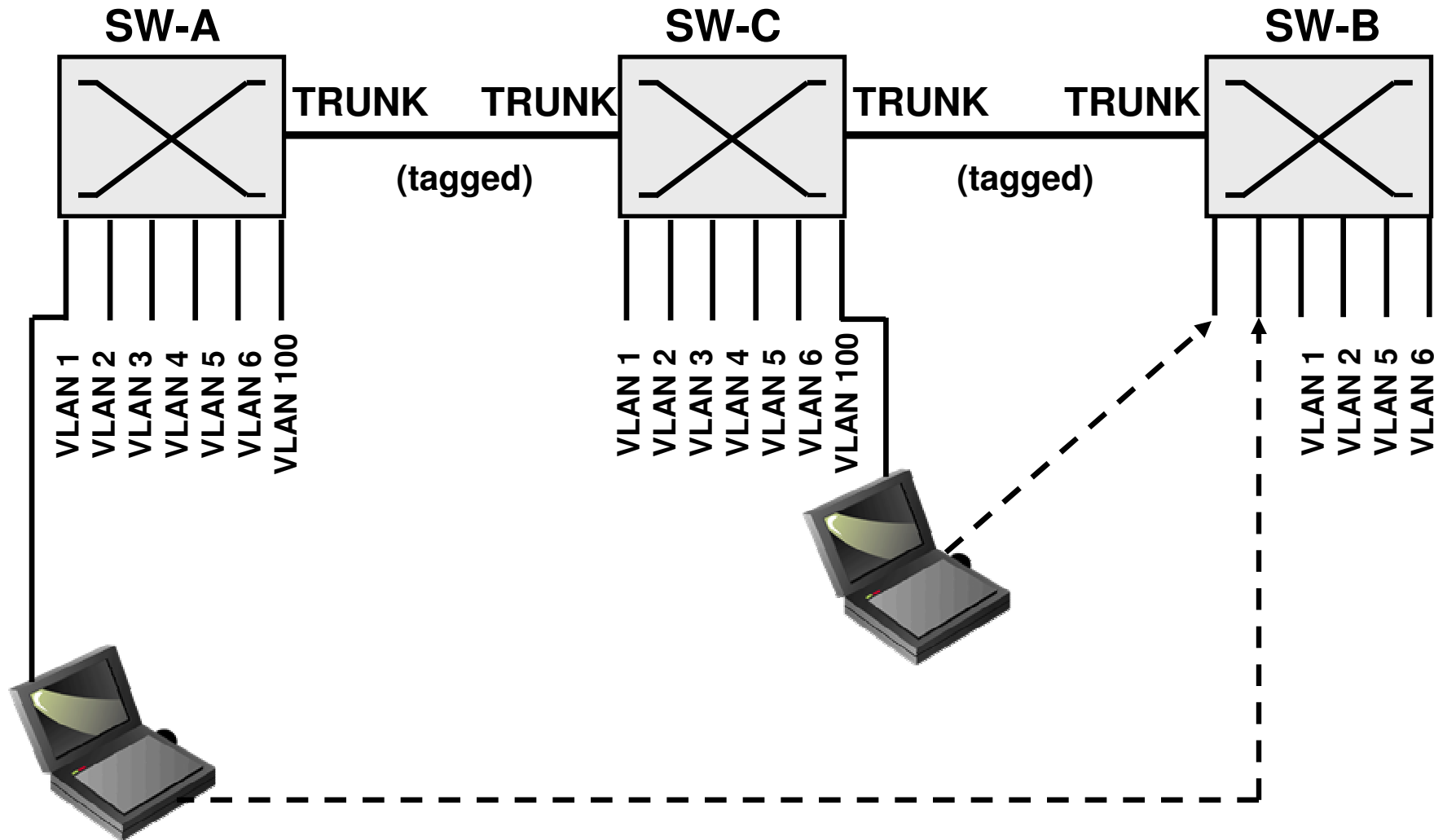

Mobility

Port-based VLAN assignment does not support mobility

- The VLAN a station belongs to depends on the port it is connected to
- If a host is moved to another port does not necessarily keep being assigned to the same VLAN
 - Proper configuration or network administrator intervention might be required

Possible solution: “anarchic” VLAN

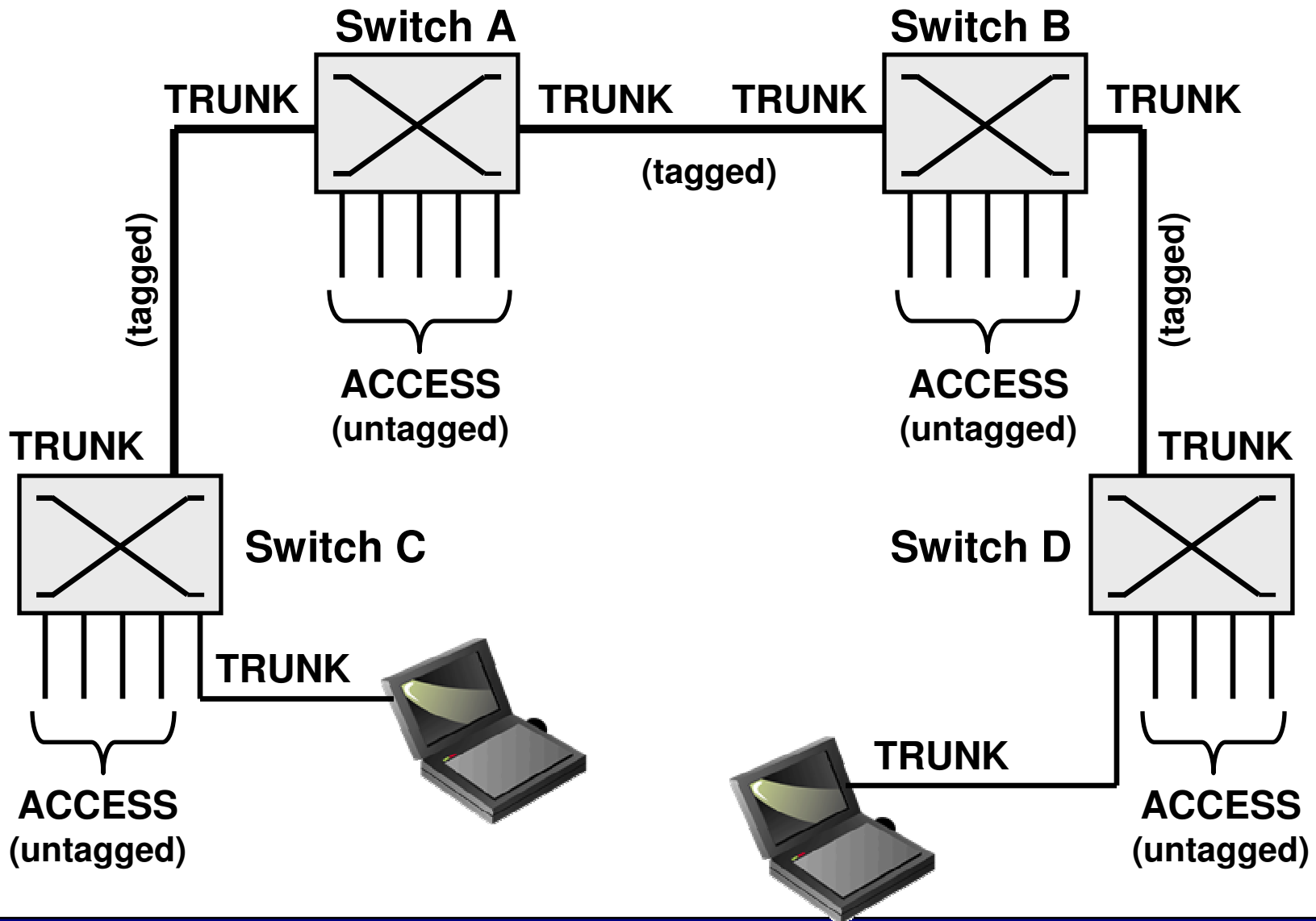
Mobility support example



Mobility Support

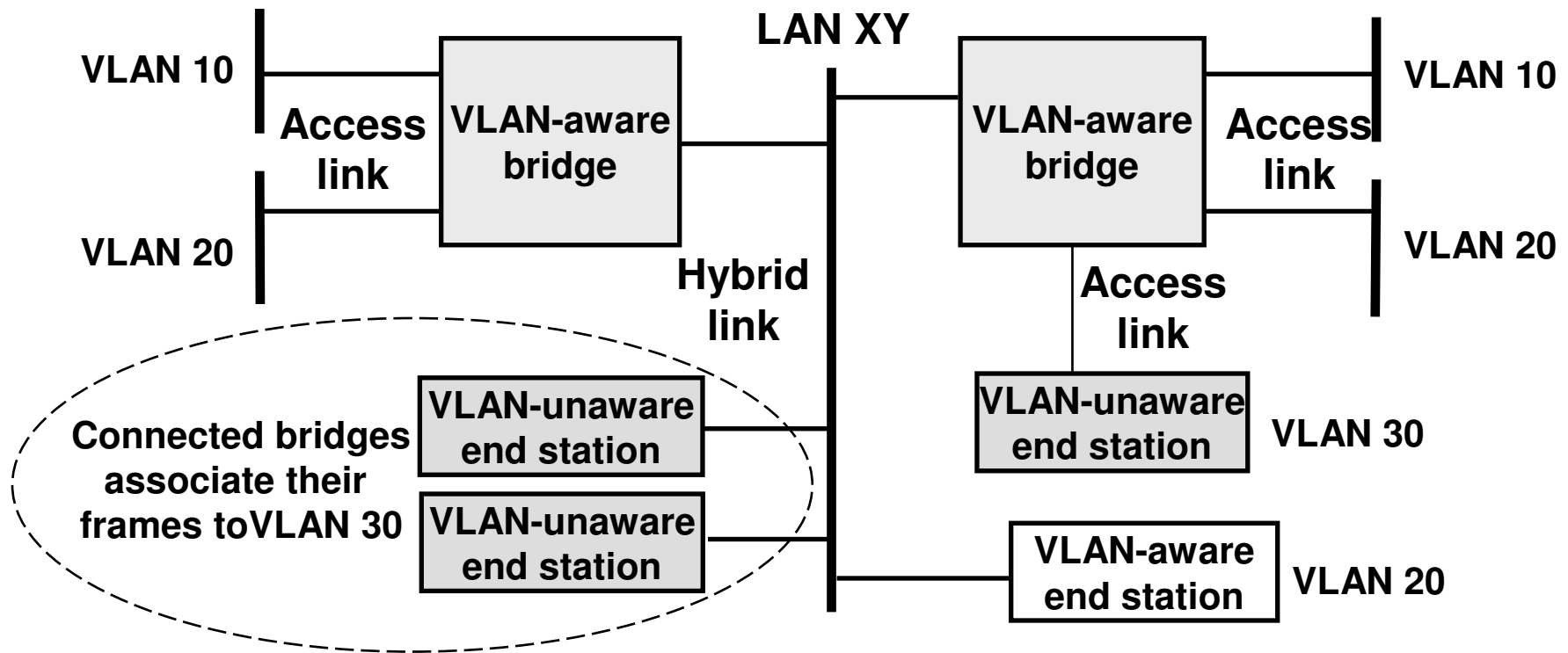
- Hosts with VLAN aware interfaces supporting IEEE 802.1Q tagging
- *Trunk* configuration of host interfaces
- Applicable to both shared (HUB-based) and switched LANs
- Hosts (users) determine the VLAN they belong to
- Hybrid solution:
 - (Large number of) Access ports for non-mobile hosts
 - (Small number of) Trunk ports for mobile hosts

Hybrid Solution with Access and Trunk Ports



Hybrid Link

Both tagged and untagged frames travel on a hybrid link and the switch ports connected to it



GVRP: GARP VLAN Registration Protocol

- A specialization of GARP: Generic Attribute Registration Protocol
- Used to register or unregister VLAN related attributes
 - A switch registers the VLANs it “knows” with the switch on the other side of a trunk link.
 - Remote switch learns the VLANs whose packets should be forwarded on the trunk link
- Alternative to static definition of VLANs to be forwarded on a *Trunk Link*
- Switch using GVRP are said GVRP-Aware
- GVRP operates on the STP active topology

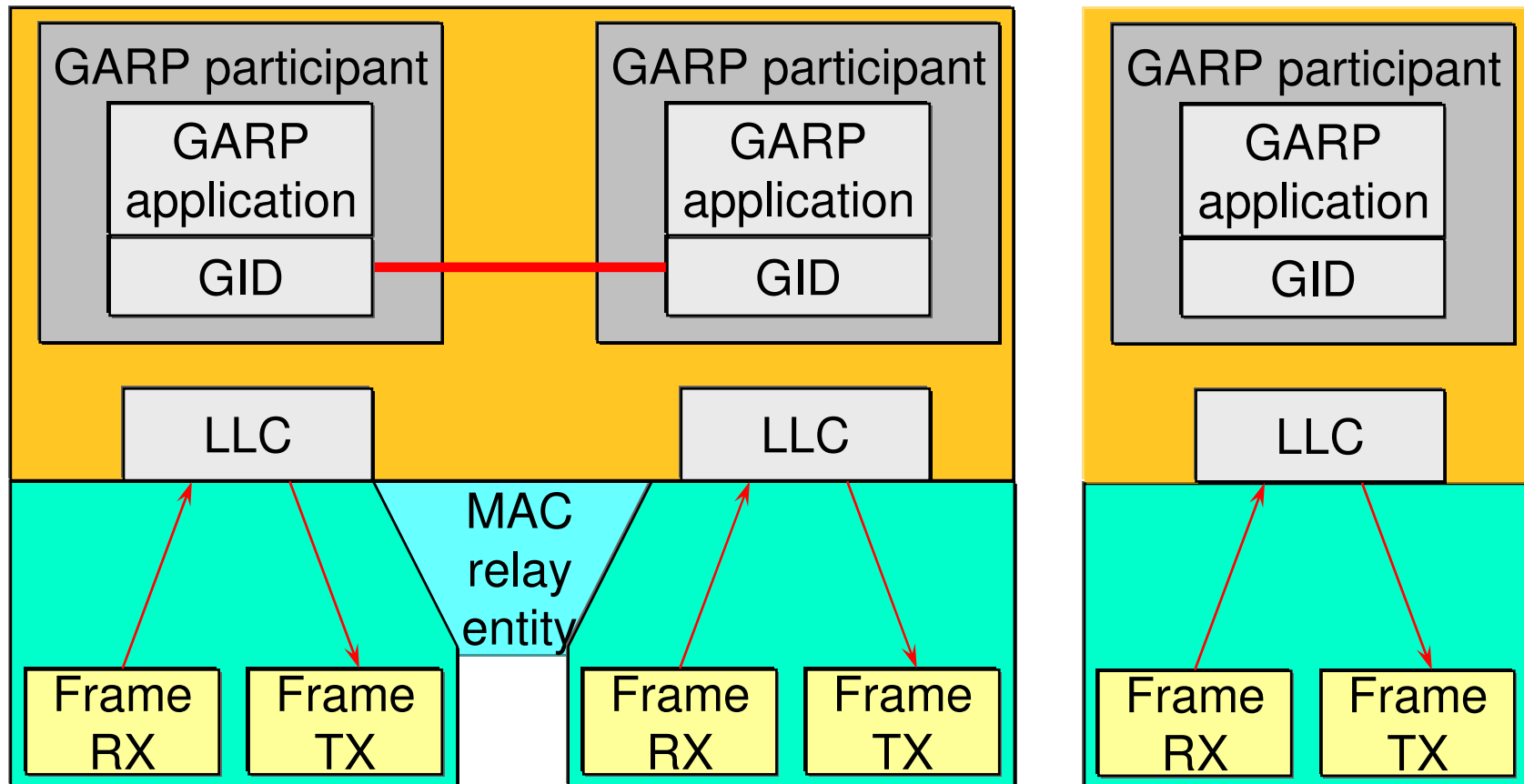
GARP: Generic Attribute Registration Protocol

- Registers or unregisters various types of attributes into an entity within a switch called GID
- GID (GARP Information Distribution)
 - Collection of state machines defining the current status of attribute registrations and declarations
- Attribute registration relates to a port receiving a GARP PDU with the corresponding declaration
 - Also a port set in Blocking state by STP
- GIP (GARP Information Propagation)
 - Entity in charge of propagating information among GARP Participants
 - Inside a single bridge
 - Among different bridges (based on LLC type 1)

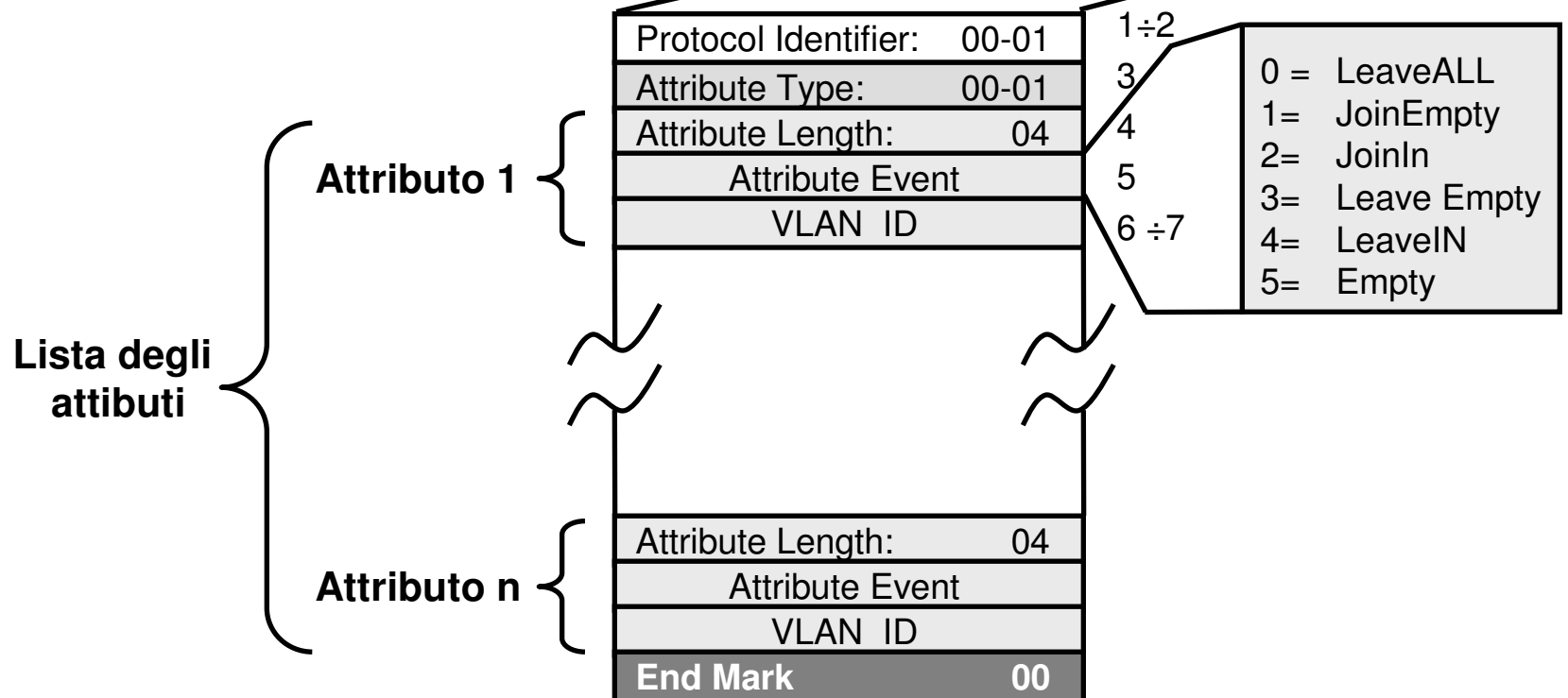
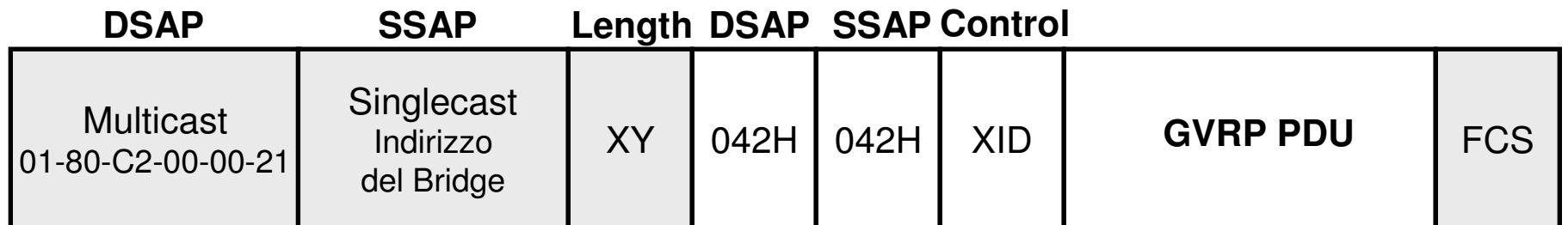
GARP: Architecture and Entities

Bridge

End Station



GVRP Packet Format

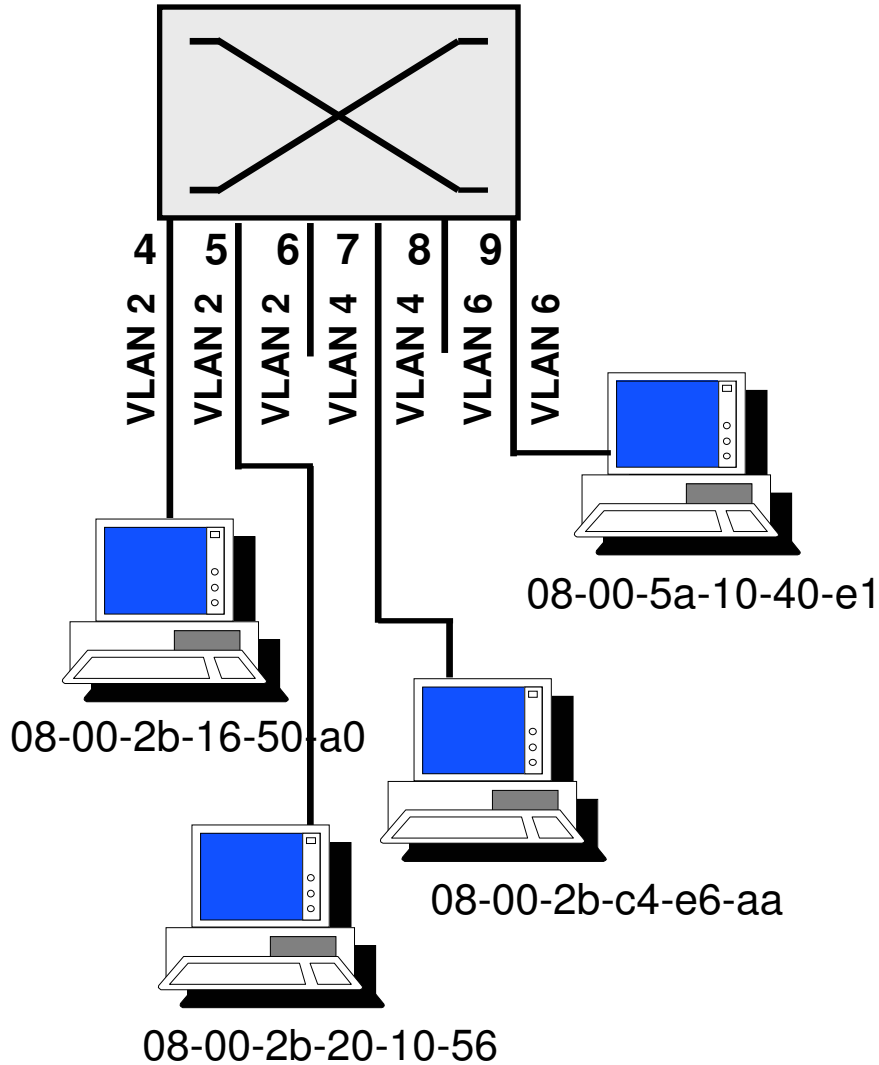


SVL and IVL Bridge/Switch

- SVL (*Shared VLAN*) Bridge
 - Single forwarding table (filtering database)
 - Shared by all VLANs
- IVL (*Independent VLAN*) Bridge
 - A forwarding table is maintained for each VLAN
 - Identified by a FID (Filtering Identifier)

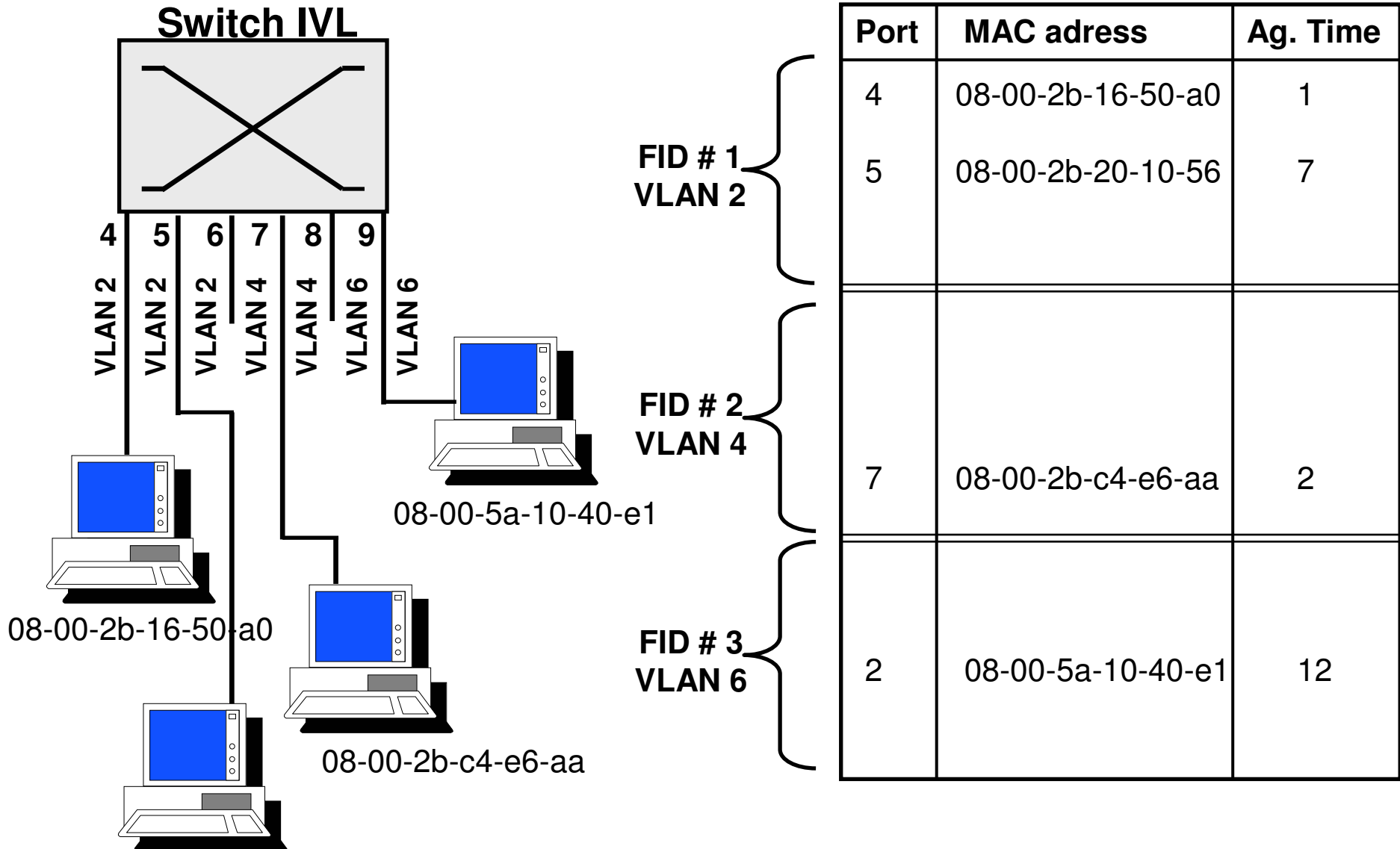
SVL Bridge/Switch

Switch SVL



Port	MAC adress	Ag. Time	VLAN
4	08-00-2b-16-50-a0	1	2
7	08-00-2b-c4-e6-aa	2	4
5	08-00-2b-20-10-56	7	2
2	08-00-5a-10-40-e1	12	6

IVL Bridge/Switch



Host Belonging to Multiple VLANs

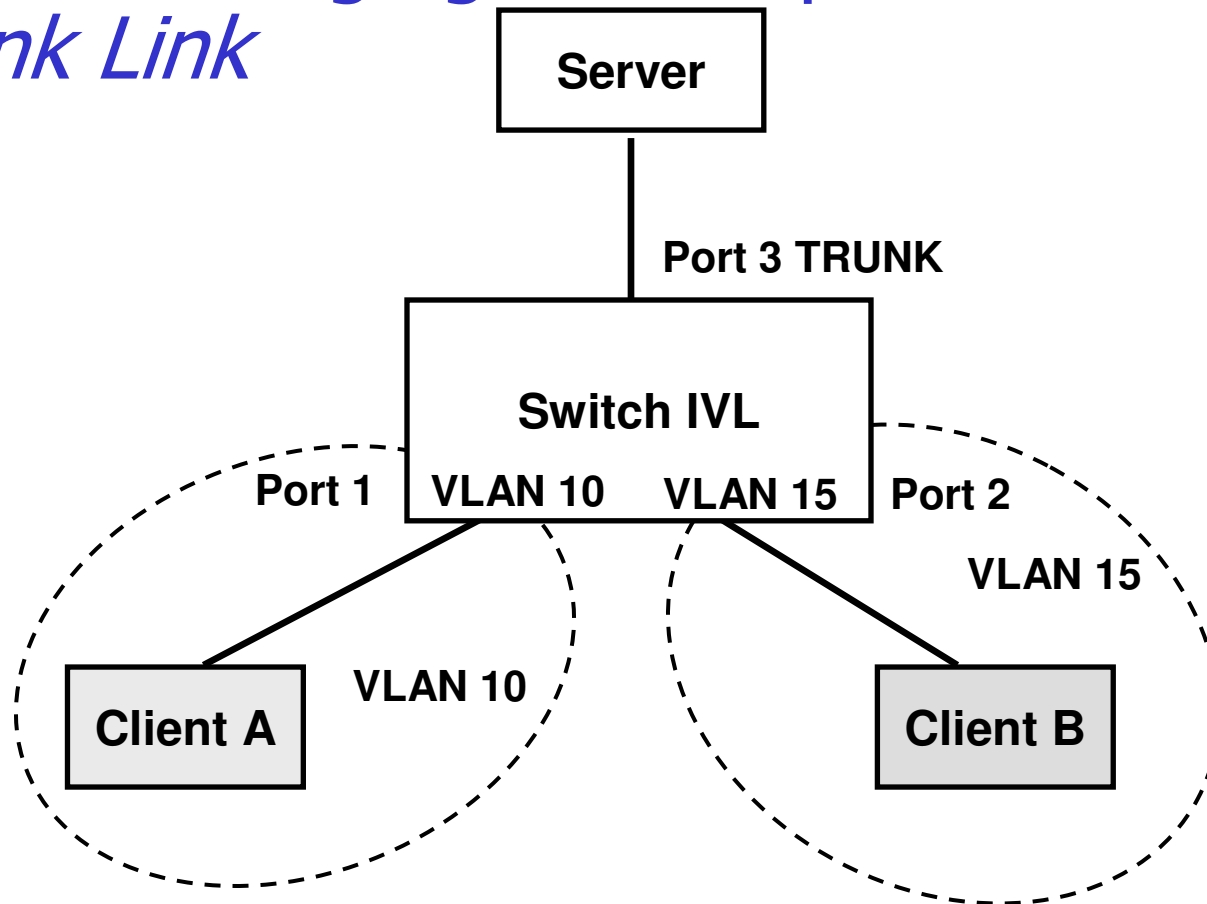
■ IVL Switch

- If host (e.g., a server) interface is VLAN-Aware (i.e., it supports IEEE 802.1q tagged frames), host and switch port are configured in *Trunk mode*
- Some products (e.g., Cisco switches) support *Multi VLAN* access ports

■ SVL Switch

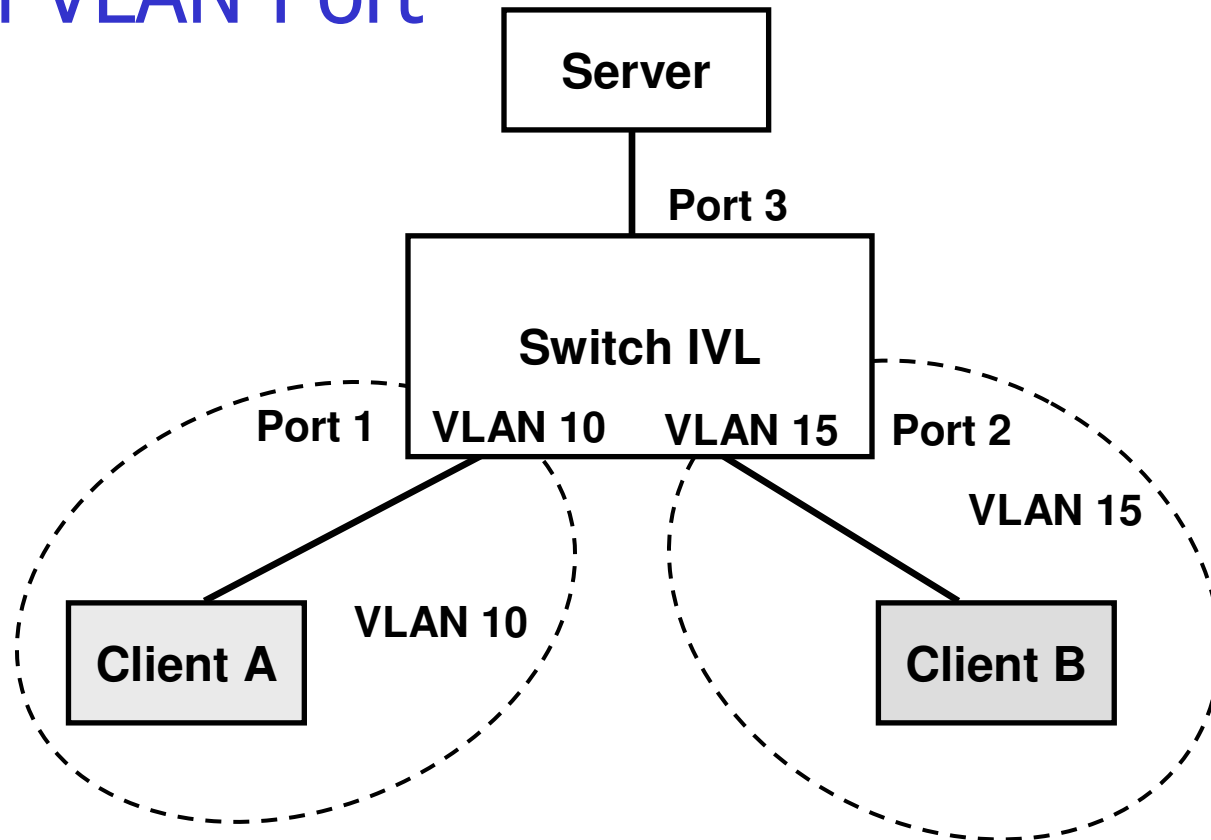
- Host is connected to Access port
- Sophisticated VLAN configuration

Server Belonging to Multiple VLANs with *Trunk Link*



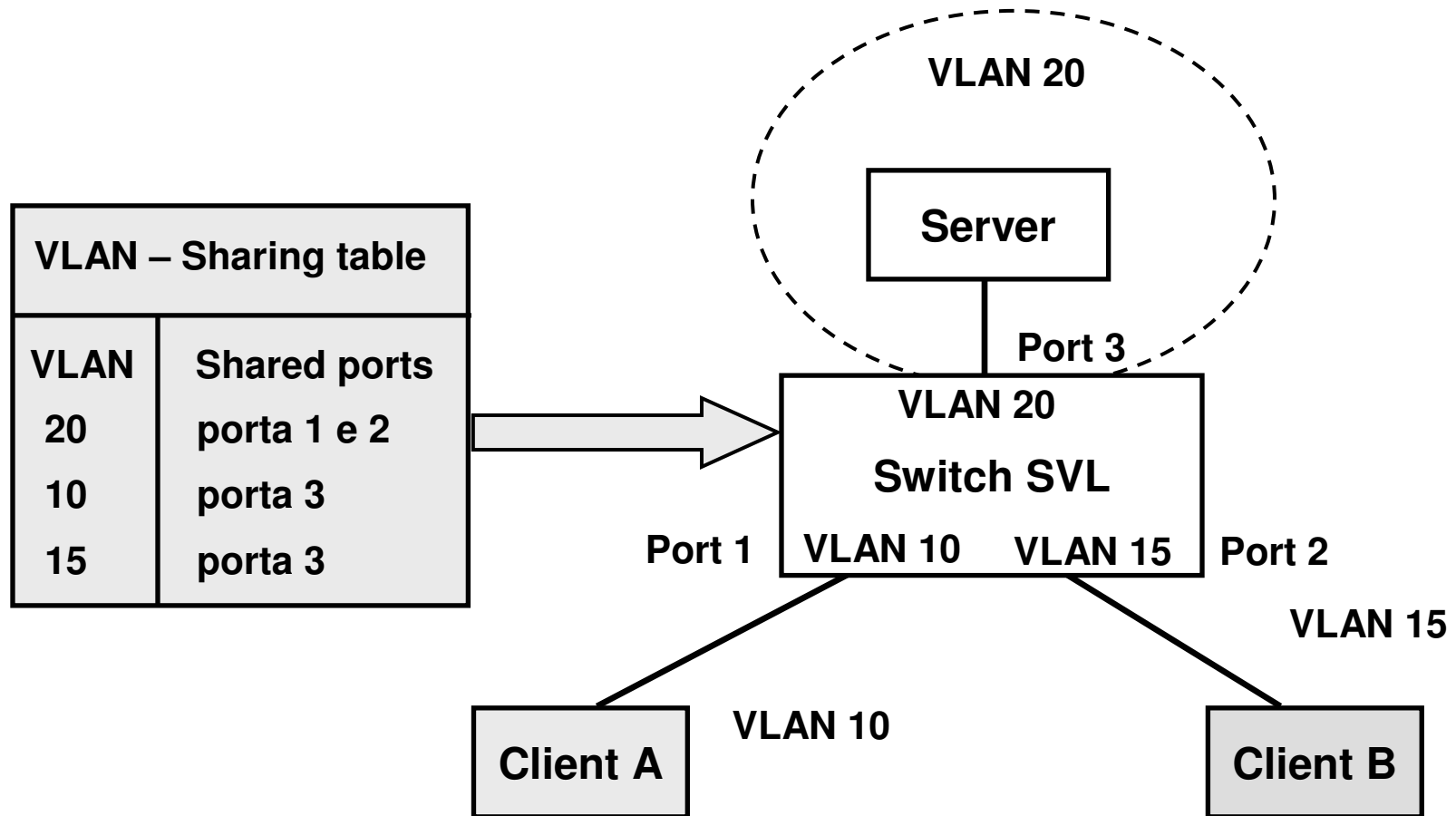
```
Switch(config)#int fastEthernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10,15
Switch(config-if)#end
```

Server Belonging to Multiple VLANs with Multi VLAN Port



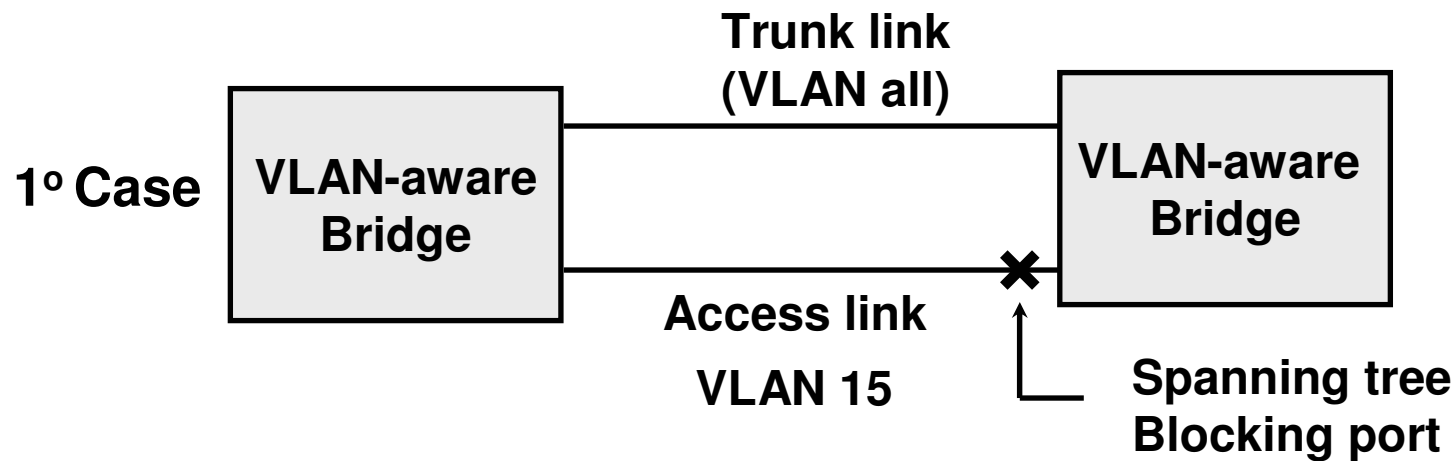
```
Switch(config)#int fastEthernet 0/3
Switch(config-if)#switchport mode multi
Switch(config-if)#switchport multi vlan add 10
Switch(config-if)#switchport multi vlan add 15
Switch(config-if)#end
```

Server Belonging to Multiple VLANs with SVL Switch

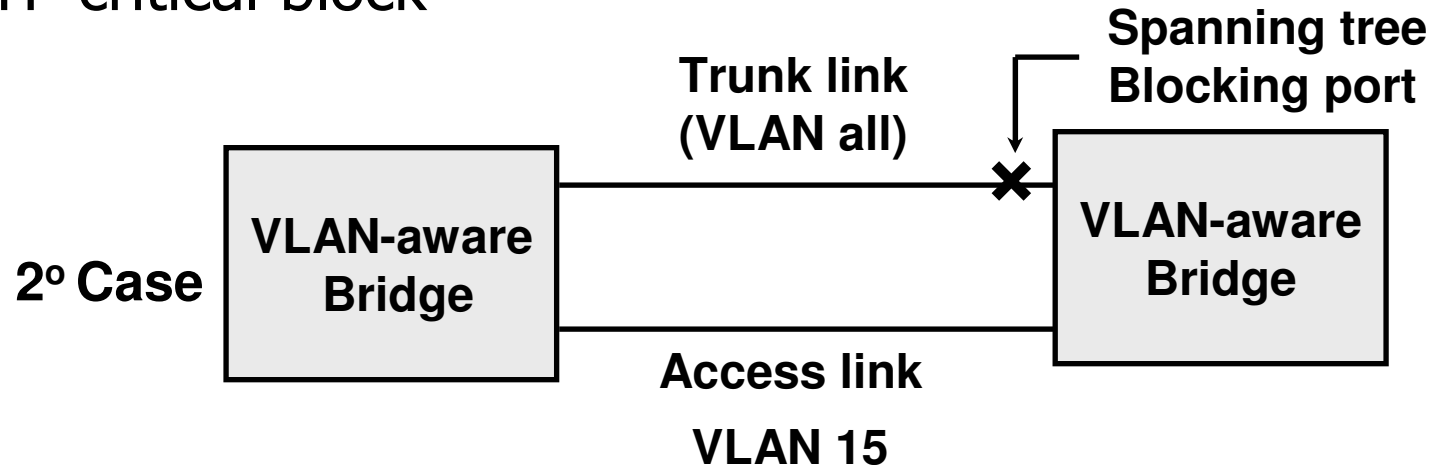


Spanning tree problem with 802.1Q

STP not critical block

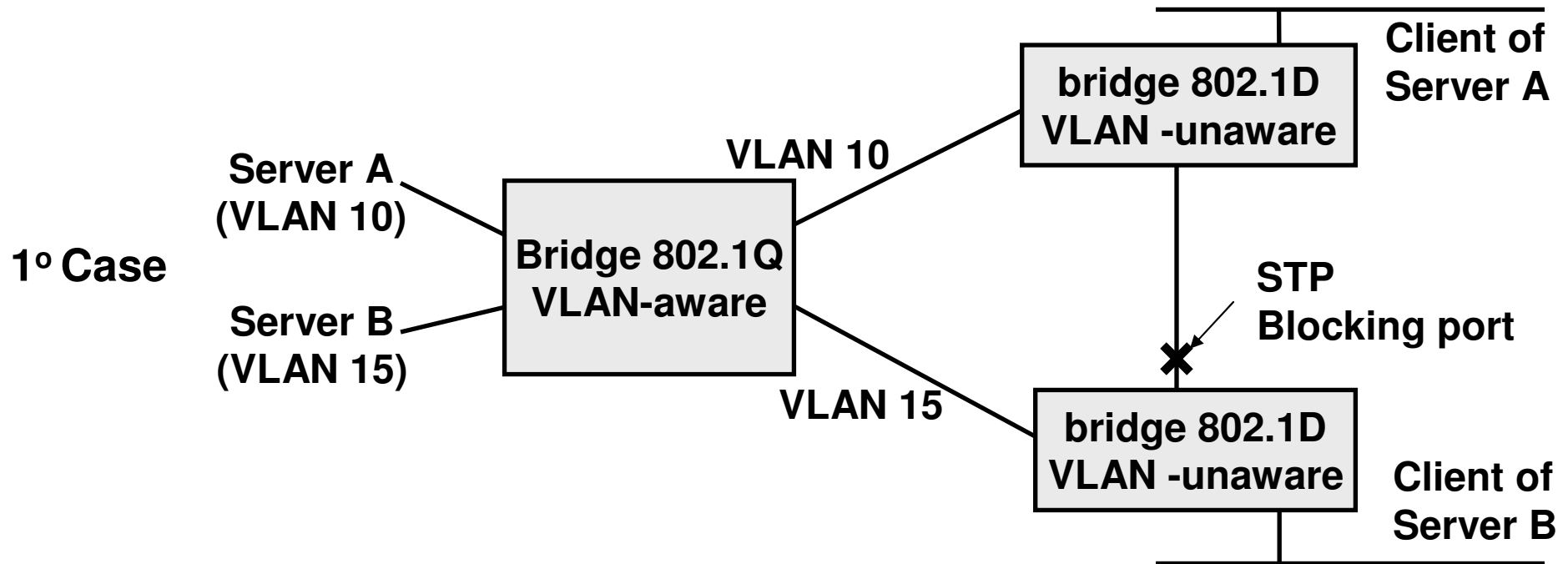


STP critical block



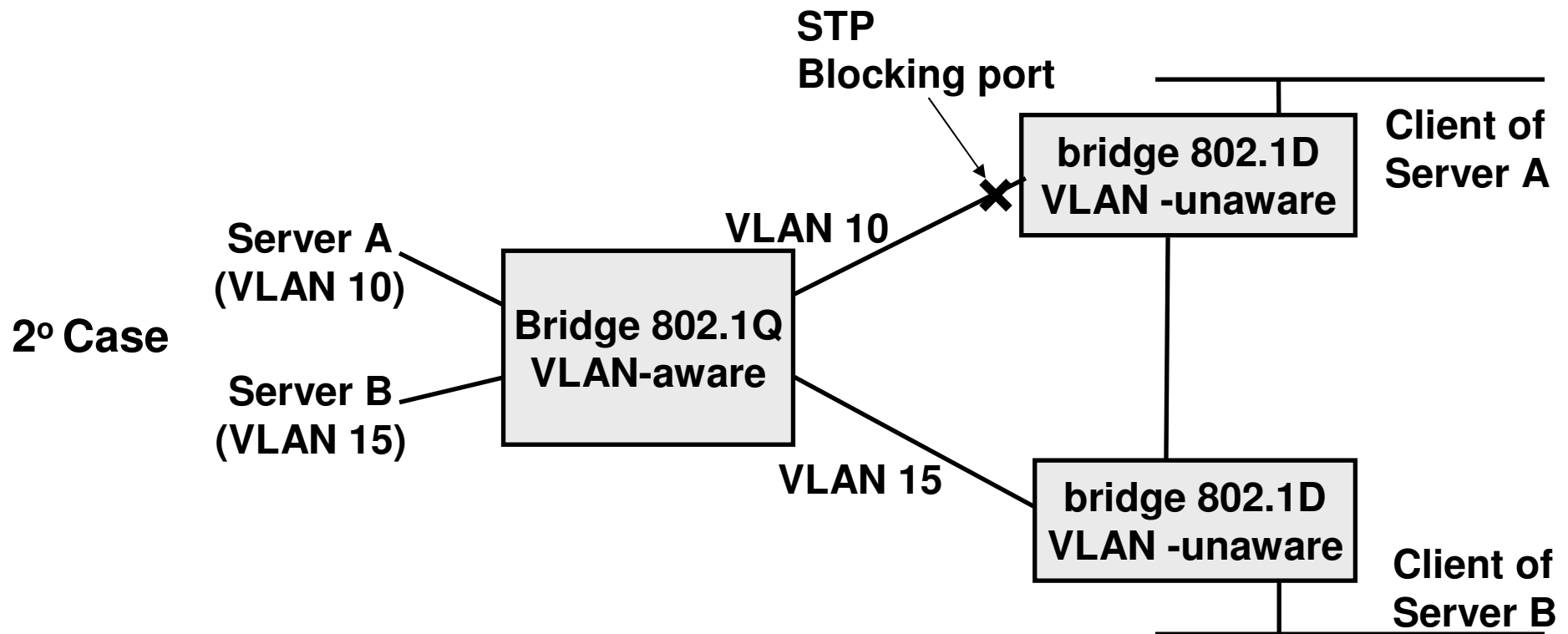
Problems between VLAN-Aware and VLAN-Unaware bridge

STP critical block



Problems between VLAN-Aware and VLAN-Unaware bridge

Block which does not allow the connection from clients A to server A



IEEE 802.1v STANDARD

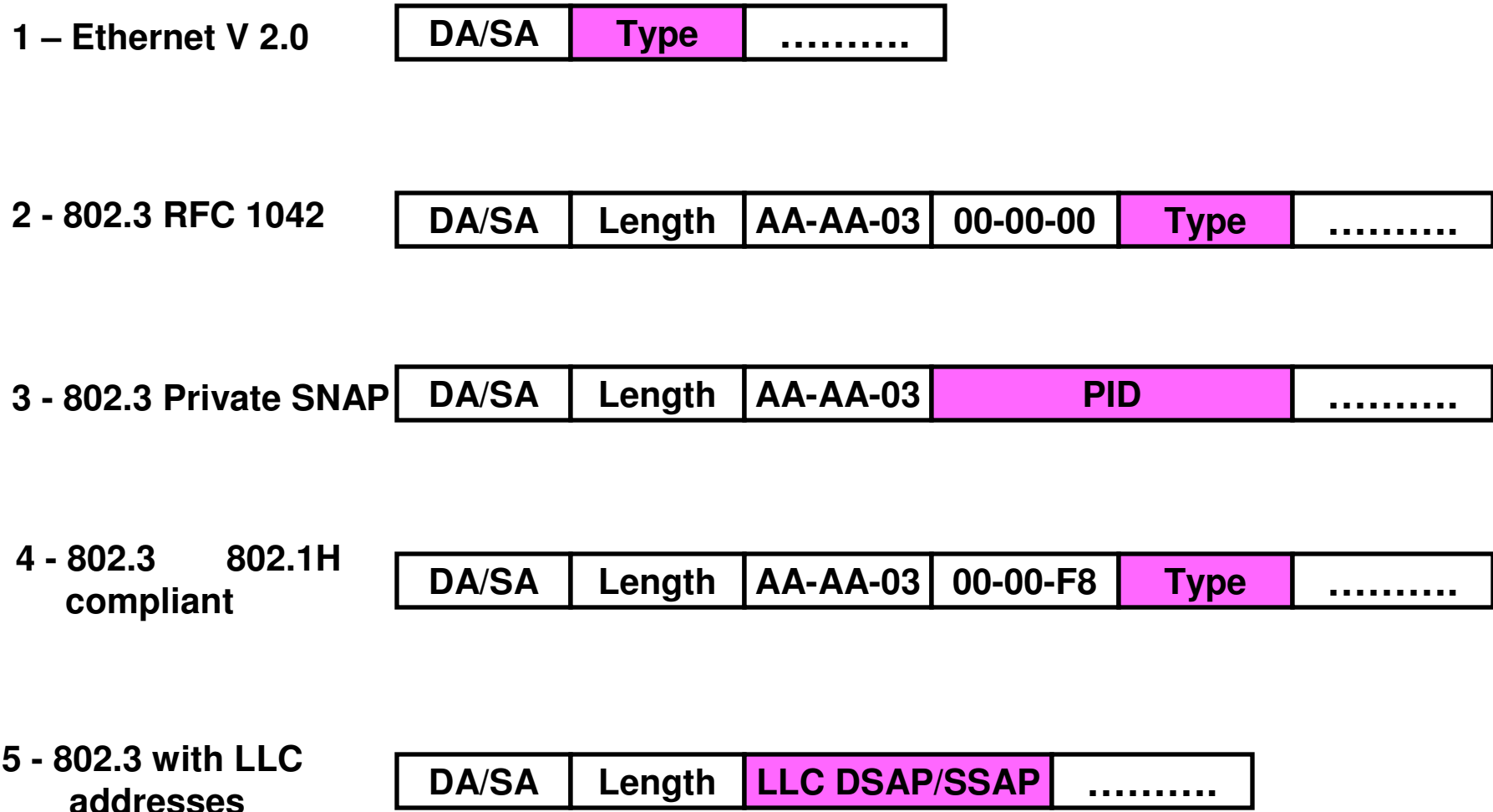
- Per protocol based VLAN assignments
 - VLAN Port-and-Protocol-based classification
- Possible associations:
 - One VLAN on the switch port (per port VLAN)
 - More VLANs on the same port based on protocols classified (per protocol VLAN)
- Packets classification :
 - On a basis protocol if they transport one of the protocols a VLAN association was defined for
 - The other ones, not classified by protocol, assumes VLAN assigned to the port the (per port VLAN)

Protocol classification

This fields according to the frame format are taken:

- Ethernet V 2.0
- IEEE 802.3 RFC 1042 compliant
- IEEE 802.3 IEEE 802.1H compliant
- IEEE 802.3 with Private SNAP
- All the other cases of IEEE 802.3 formats

Classification fields



Rudiments on which 802.1v bases his functions

- Protocol Group Database
 - Code of the classifiable protocols
 - *Group ID* (identifier)
- Group ID are associated with VLAN in a flexible manner:
 - A VLAN for every Group ID
 - Several Group ID to the same VLAN
- Several VLAN ID (VID) for ports receiving untagged traffic
 - Port-and-Protocol-based classification

Multiple VID on the switch ports assignation example

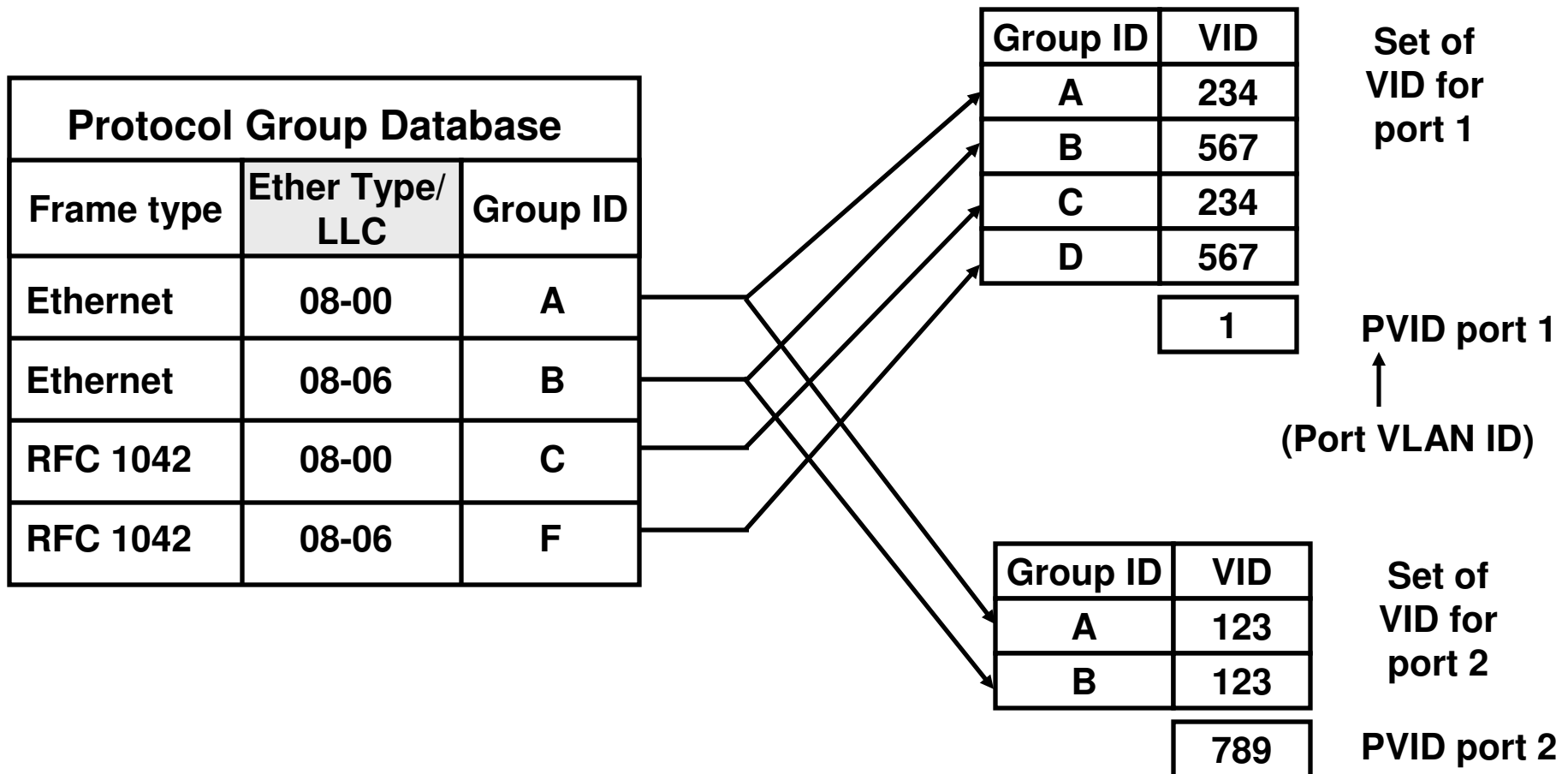


Ethernet

DA/SA	Type
-------	------	-------

802.3 RFC 1042

DA/SA	Length	AA-AA-03	00-00-00	Type
-------	--------	----------	----------	------	-------



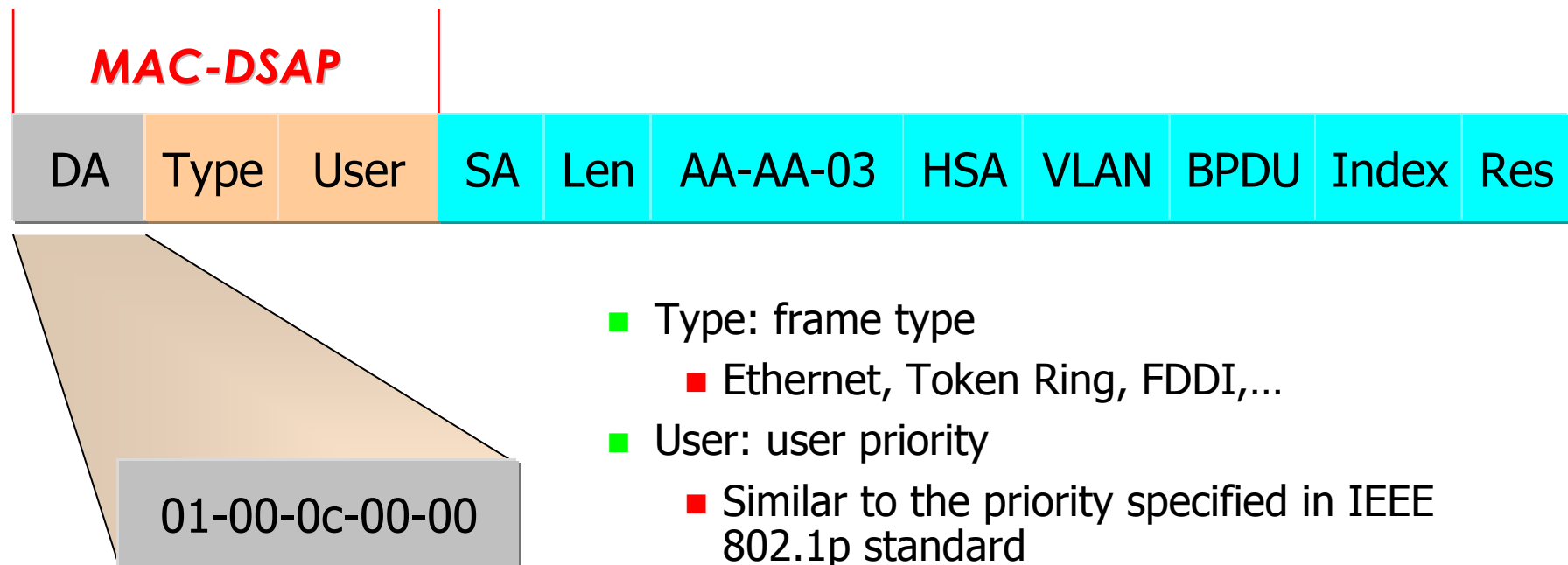
Cisco Inter Switch Link (ISL)

- The original frame is encapsulated within a ISL header and a new FCS
 - two level tagging method
- allows the support of 1024 VLAN
- Multiple Spanning Tree (one per VLAN)
- Realized in ASIC to ensure wire speed performances



ISL header format

- The 40 first bits of MAC DA identify a multicast destination address
- The other 8 bits are used as type and user field



- Type: frame type
 - Ethernet, Token Ring, FDDI,...
- User: user priority
 - Similar to the priority specified in IEEE 802.1p standard

ISL per VLAN Spanning tree

