Internet Technology and Protocols

http://netgroup.uniroma2.it/ITP

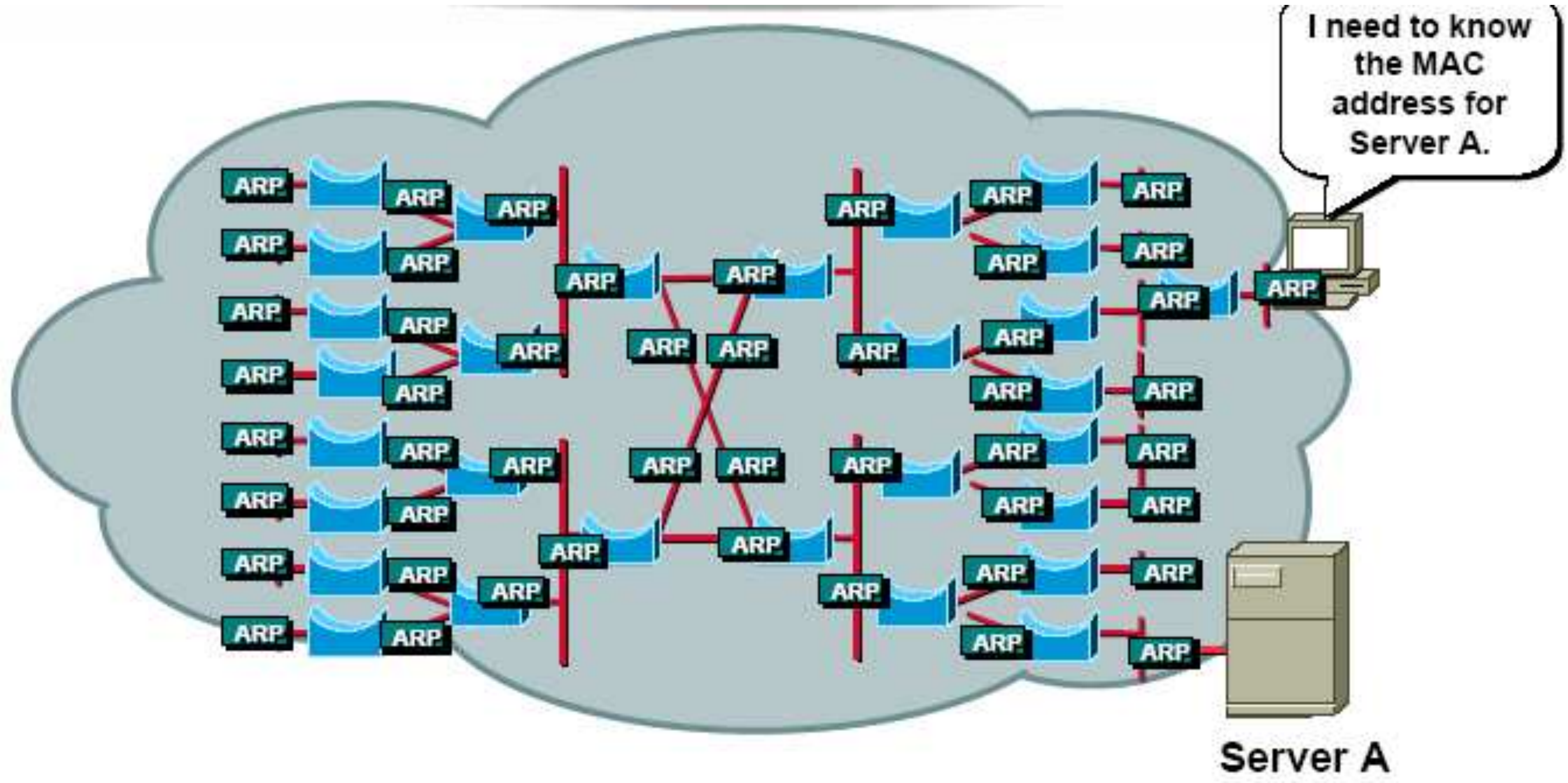
Prof. Stefano Salsano

http://netgroup.uniroma2.it/Stefano_Salsano/
e-mail: stefano.salsano@uniroma2.it

AA2019/20 – Slide deck #3 – v1

Virtual LANs

Broadcast issues

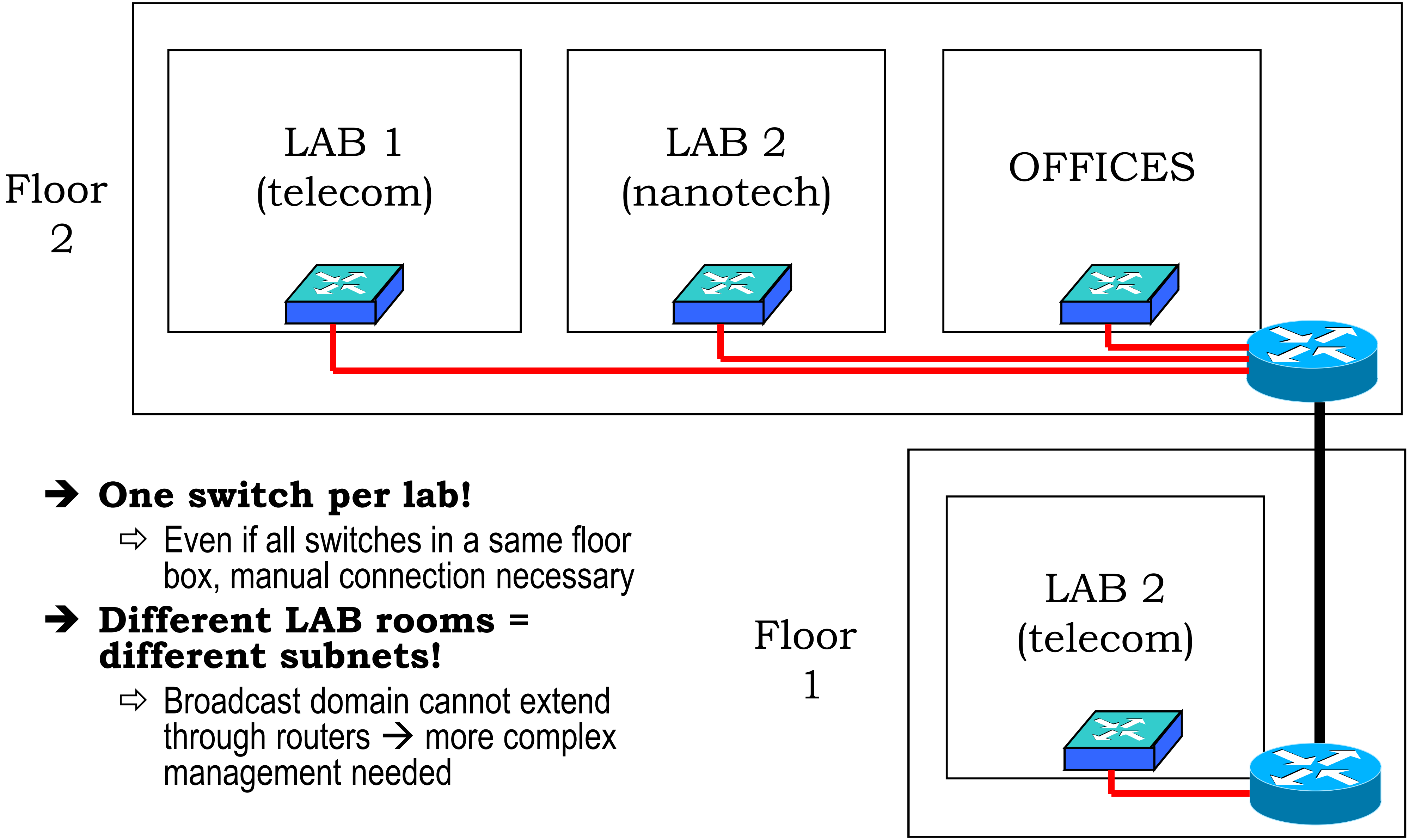


Switches: - did partition collision domains
- bud DID not partition broadcast domain

The “obvious” solution: IP subnets

- ➔**Partition network into several subnets**
  - ⇨Critical approach (especially in the past):
    - →routers were slow
    - →Need to replace switches with routers
  - ⇨No more a problem of efficiency, today
    - →layer 3 switches = hardware-based routers, very fast!
  - ⇨However…

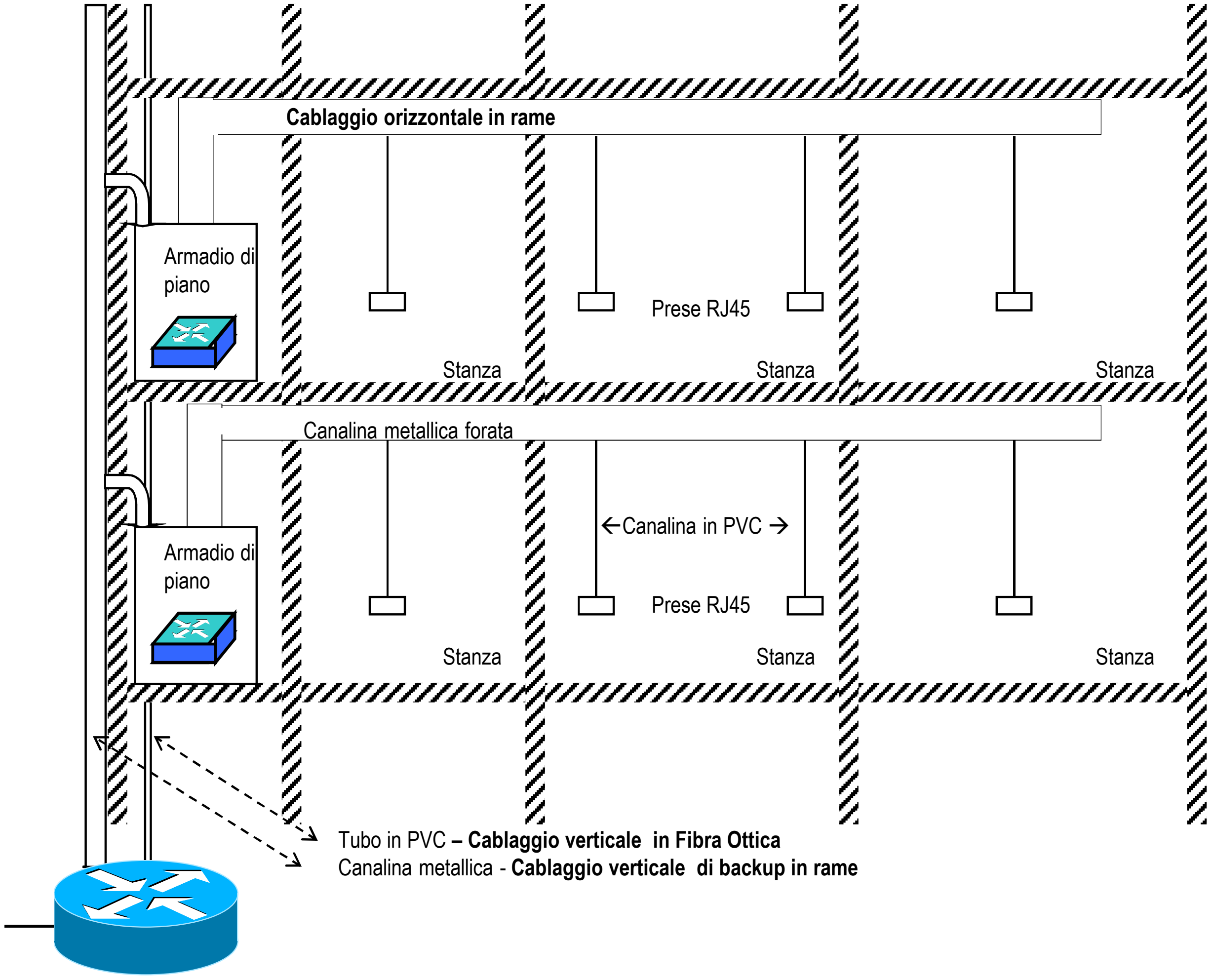
Cons of physical IP subnets



- ➔ **One switch per lab!**
  - ⇨ Even if all switches in a same floor box, manual connection necessary
- ➔ **Different LAB rooms = different subnets!**
  - ⇨ Broadcast domain cannot extend through routers → more complex management needed

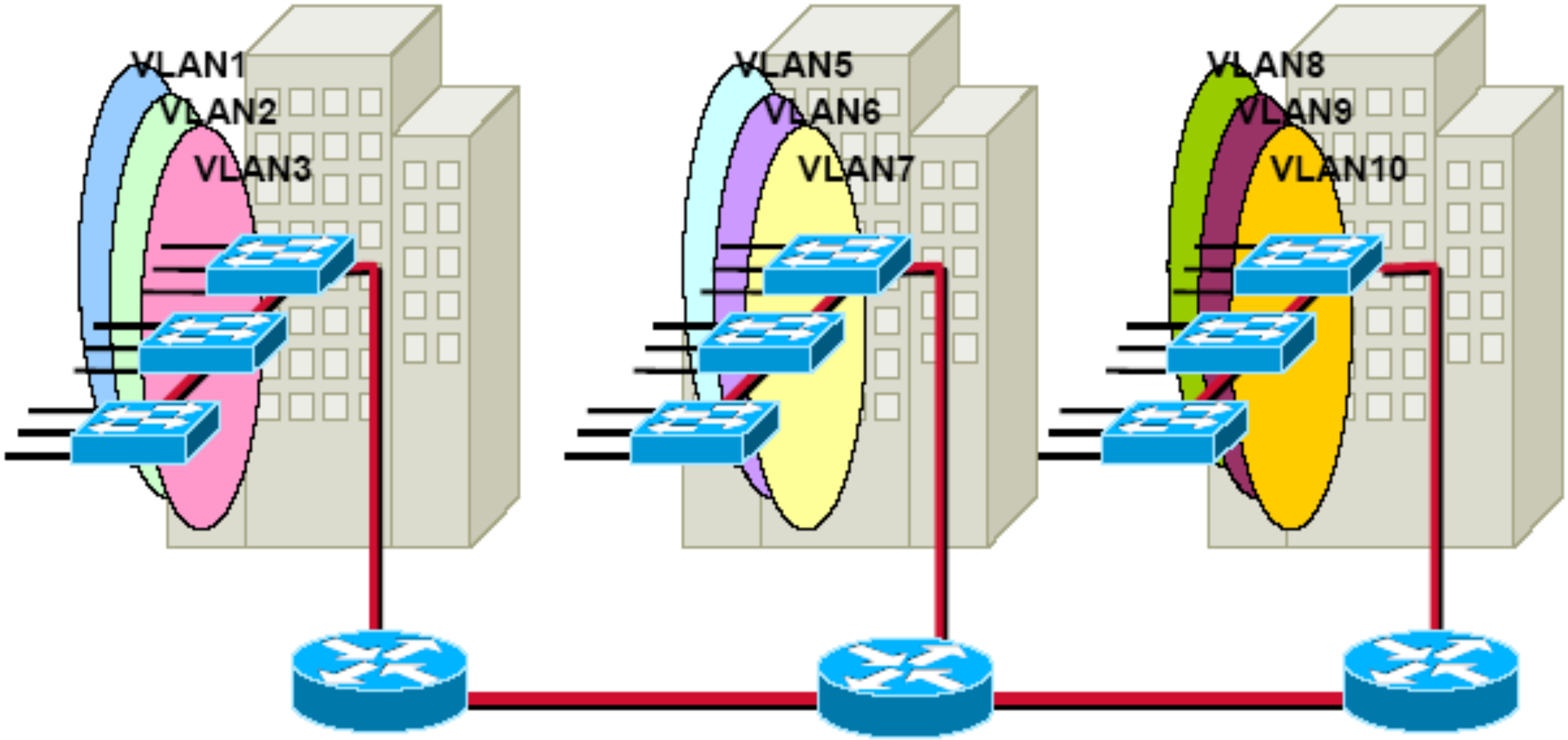
Physical Network Design vs Logical Network Design

- ➔ **Standard design for physical network**



Tubo in PVC – **Cablaggio verticale in Fibra Ottica**
Canalina metallica - **Cablaggio verticale di backup in rame**

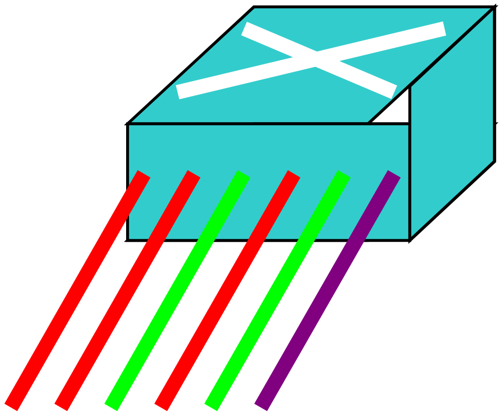
Solution: Virtual LAN (VLAN)



- ➔ VLAN = area which limits the broadcast domain
  - ⇨ **Benefits**
    - → **Broadcast confinement – solves scalability issues of large flat networks**
    - → **Isolation of failures and network impairments**
    - → **Security (more later)**
- ➔ Multiple VLANs may coexist over a same <u>Switched</u> LAN

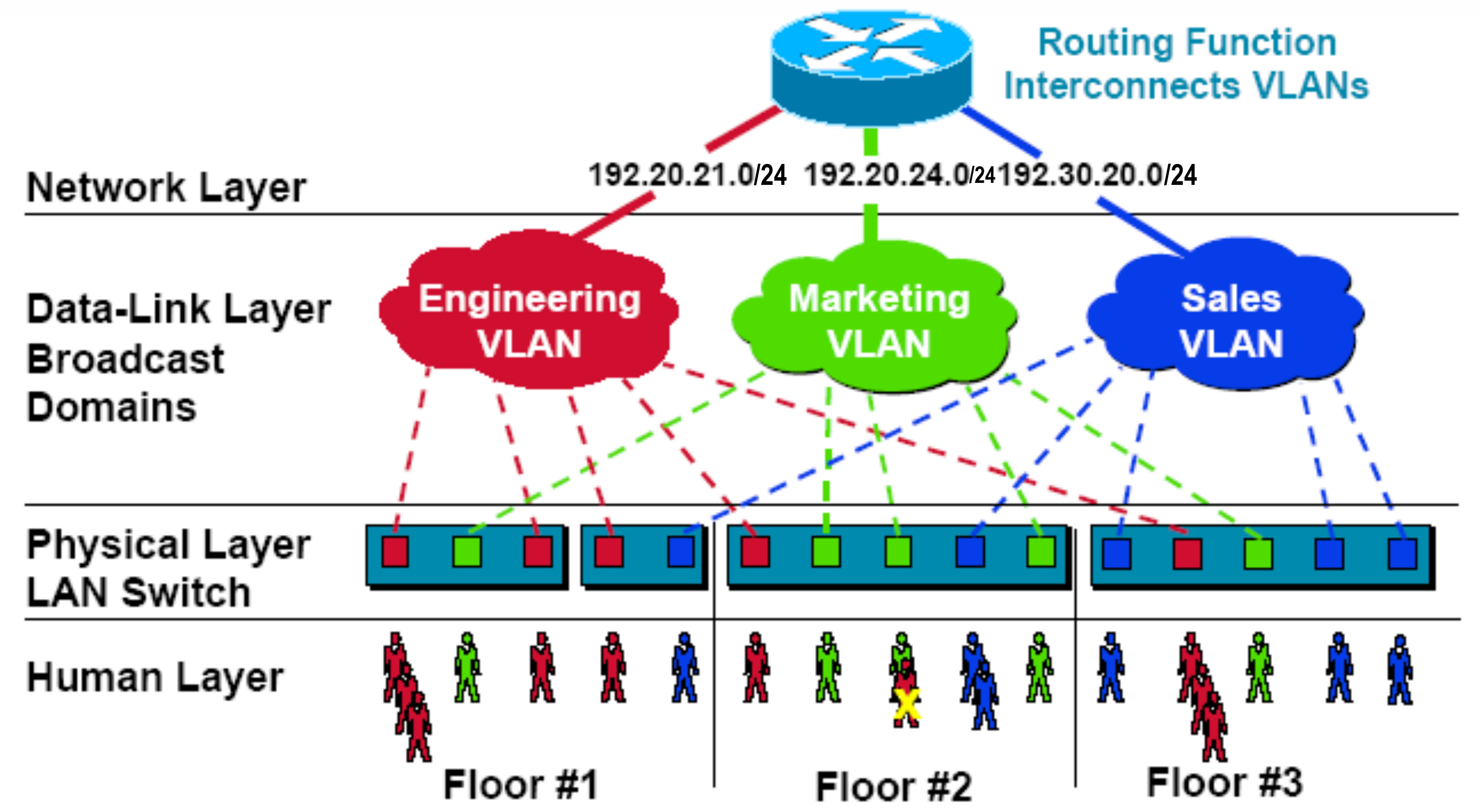
VLAN Membership

- **Per Port**
  - THE typical VLAN approach
  - The IEEE 802.1Q approach
- **Per User**
    - Via MAC address
    - Via VLAN tag
  - Results: anarchic VLAN
    - but too easy to break into ☹
- **Per Protocol**
  - New feature in IEEE 802.1v
- **Combination (cross-layer)**
  - Supported as proprietary extensions
    - Via IP subnet address
    - ….
  - Classification hierarchy may be defined
    - E.g. per IP subnet;
    - if not IP → per protocol;
    - if not in the set of classified protocols → per MAC;
    - if not in MAC list per port.



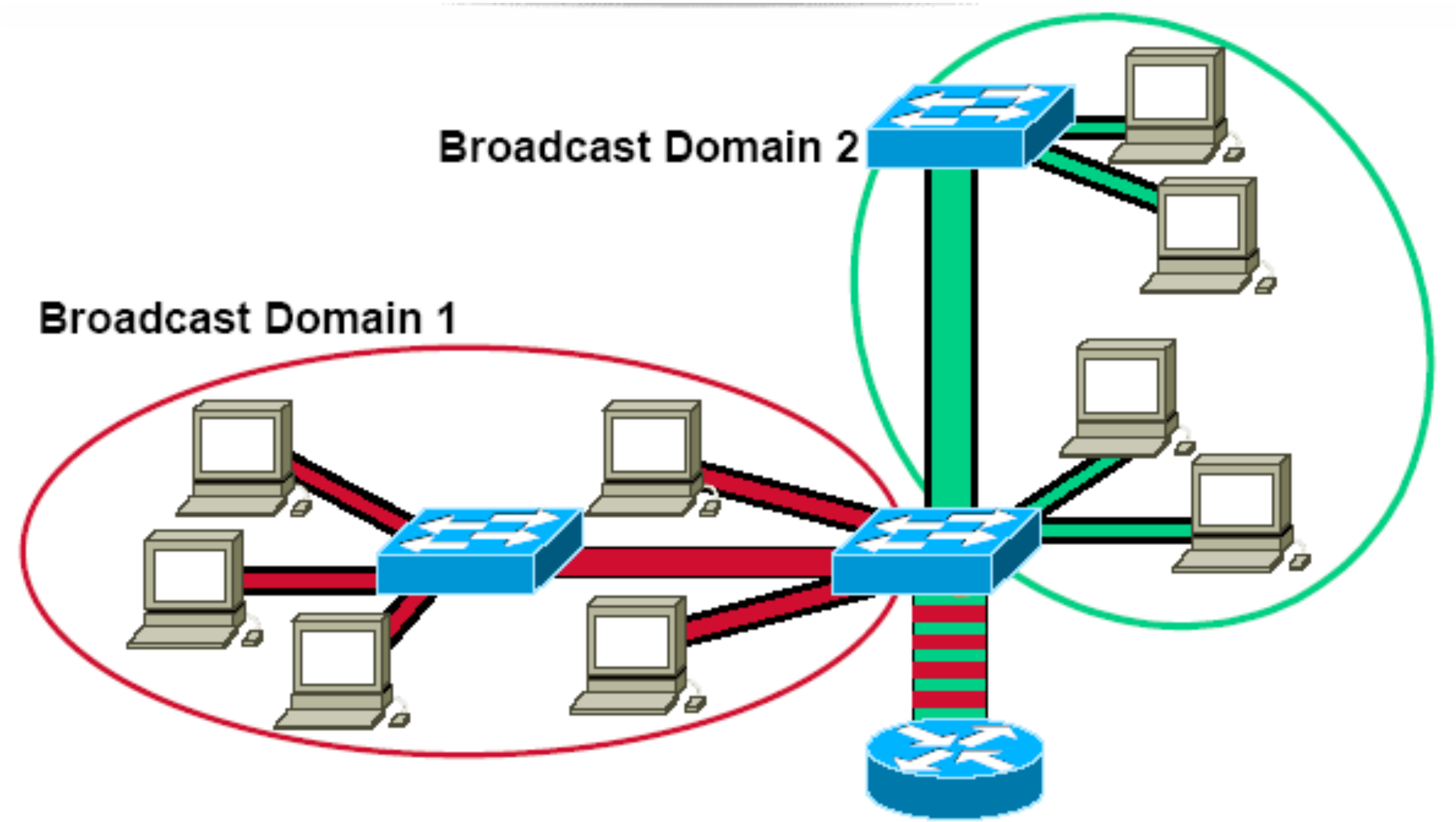
Physical vs logical view
(i.e. why VLANS instead of IP network)

- ➔ **Layer 3 subnets ought to be physically separated**
- ➔ **BUT many VLANs may overlap**
- ➔ **on the same, unique physical network structure!**
  - ⇨ Robust, failure-proof, single managed



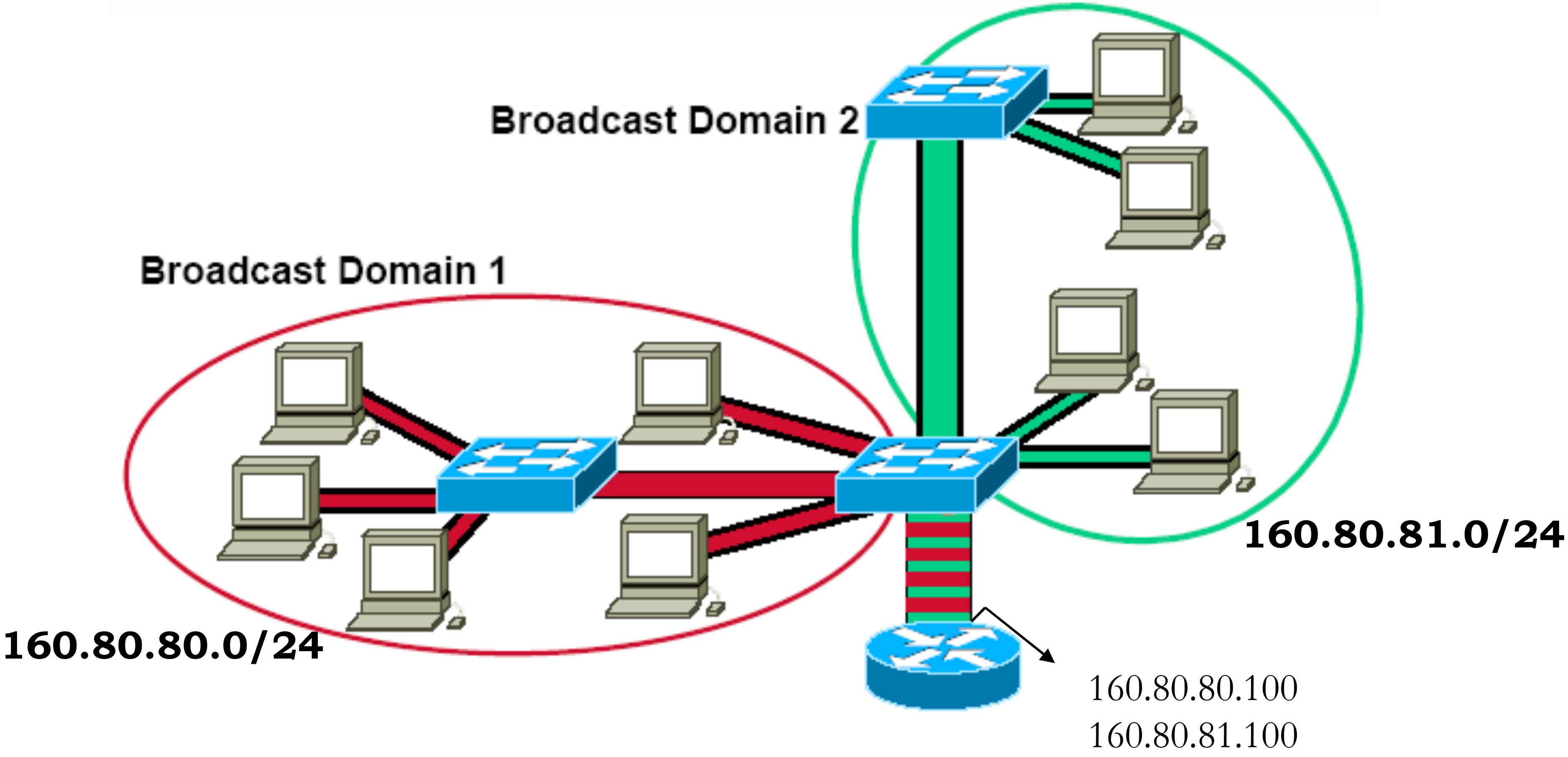
All users attached to same switch port must be in the same VLAN.

VLANs and IP subnets / 1



- ➔ **1 VLAN = 1 IP subnet**
  - ⇨ Routers are needed to move frames from different VLANs
  - ⇨ Even if STAs are in the same physical network
- ➔ **Inter-VLAN connectivity through router: improves security**
  - ⇨ May apply packet filtering mechanisms such as ACL, etc

VLANs and IP subnets /2

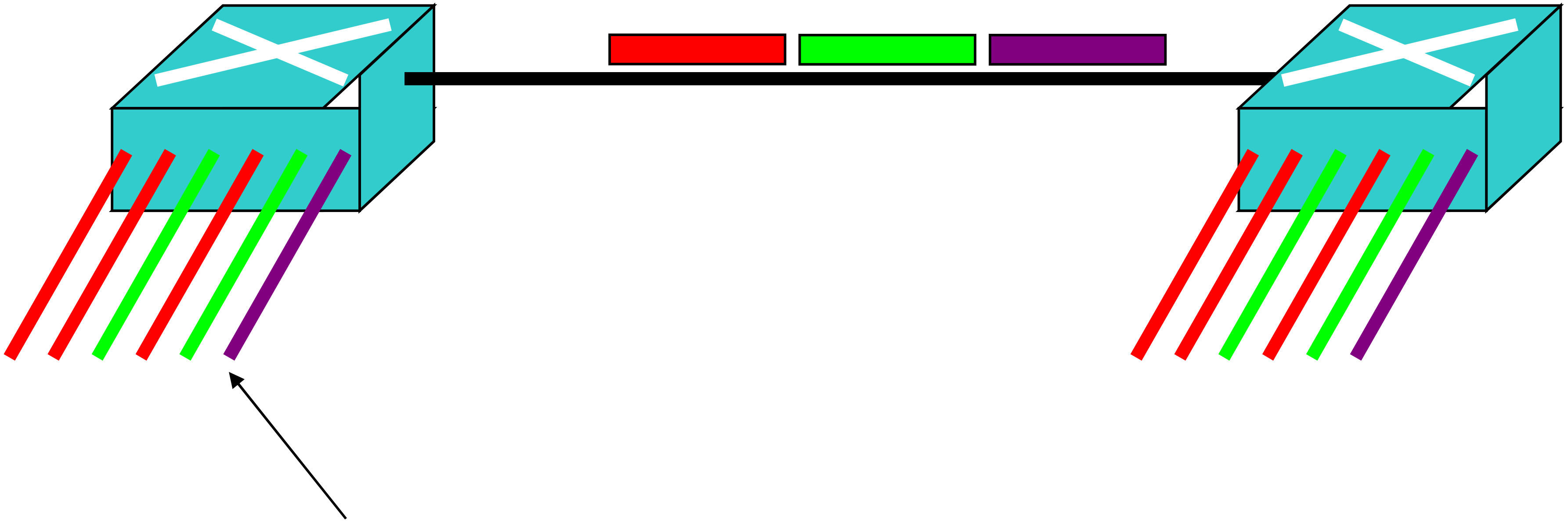


- ➔ **Routers for VLAN interconnection may have as little as just one physical interface**
  - ⇨ Also called, in jargon, “one-armed routers”
- ➔ **Multiple IP addresses on the single interface**

VLAN tagging

Port types

TRUNK port: transmits and receives tagged frames i.e. with explicit VLAN membership indication

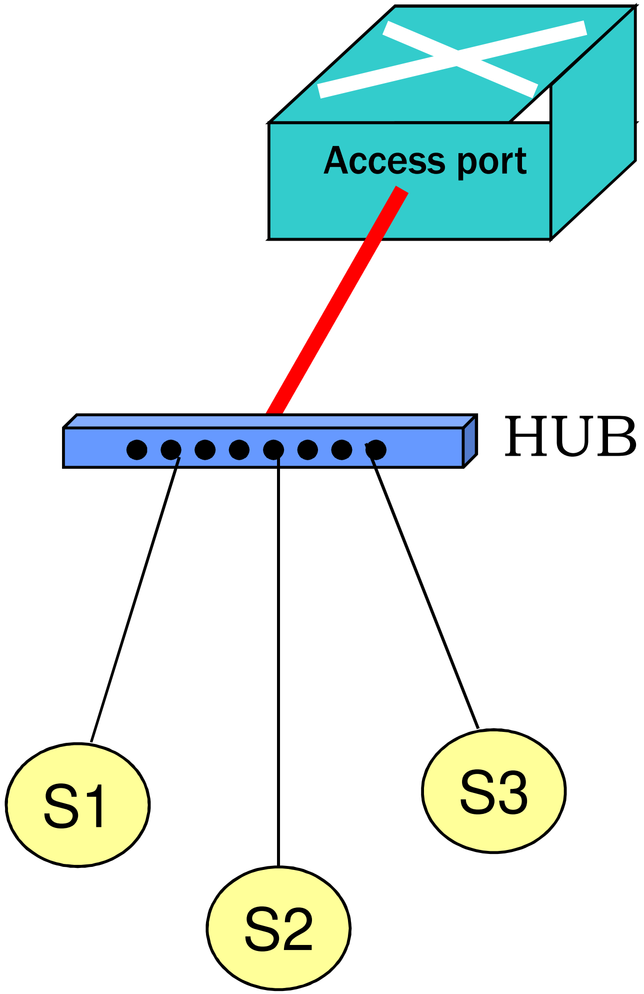


ACCESS port: transmits and receives untagged frames i.e. with no VLAN membership indication

HYBRID ports: may handle both tagged and untagged frames

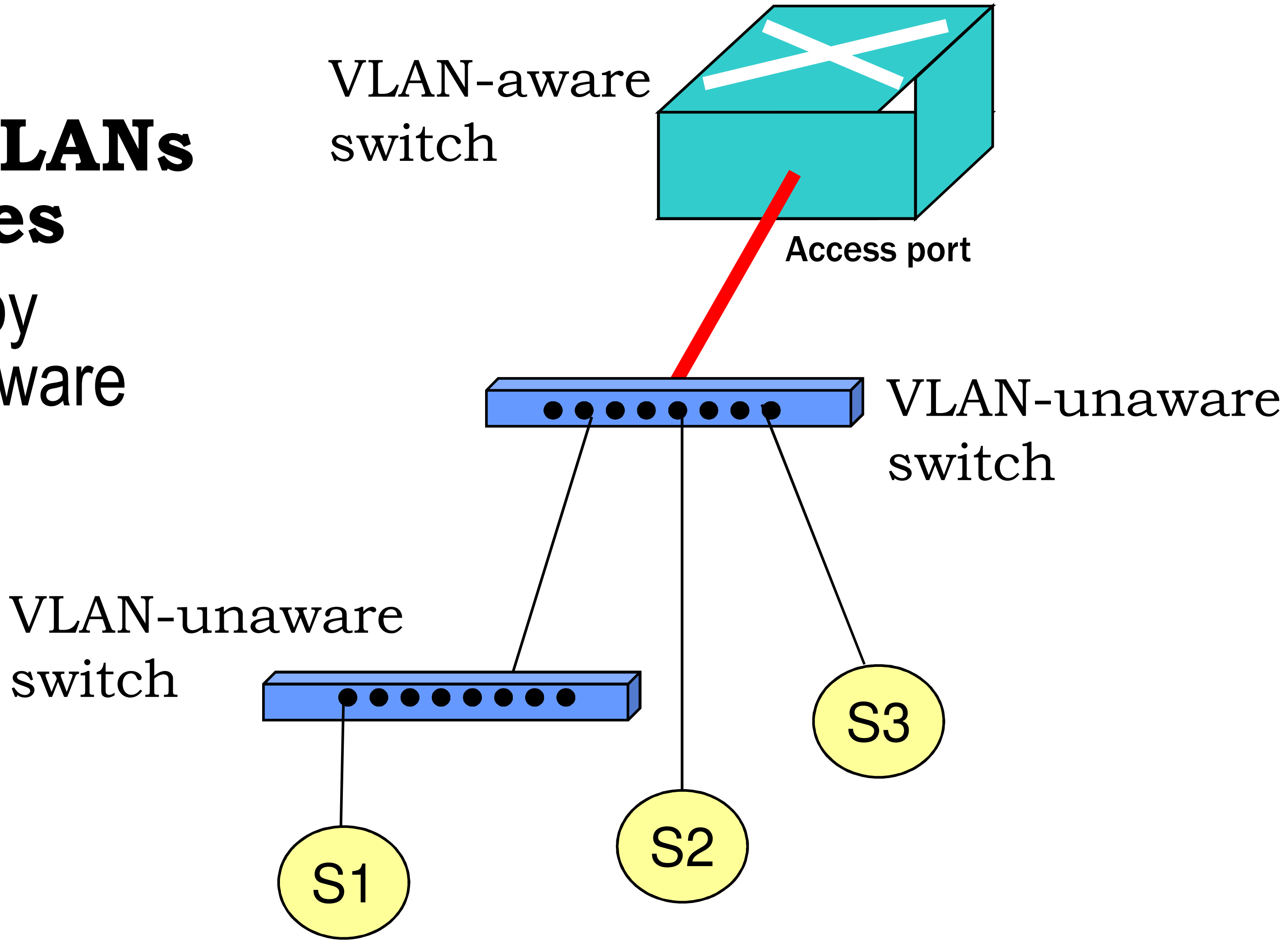
Access links

- ➔ **A link connected to an access port**
  - ⇨ Typically the PC-to-switch link
  - ⇨ or small-hub-to-switch link
- ➔ **Connected STAs belong to only 1 VLAN**
- ➔ **Connected STAs DO NOT NEED TO KNOW they are on a VLAN**
  - ⇨ They just assume to be on a dedicated IP subnet
- ➔ **TX/RX frames:**
  - ⇨ standard Ethernet (no QTAG prefix)



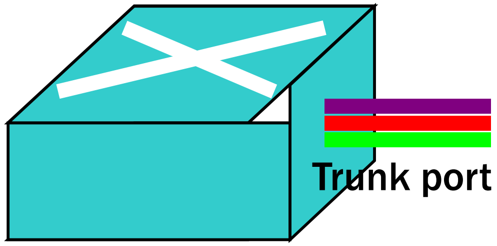
Access links (legacy regions)

- ➔ **May be switched LANs themselves**
  - ⇨ Made up by VLAN-unaware switches



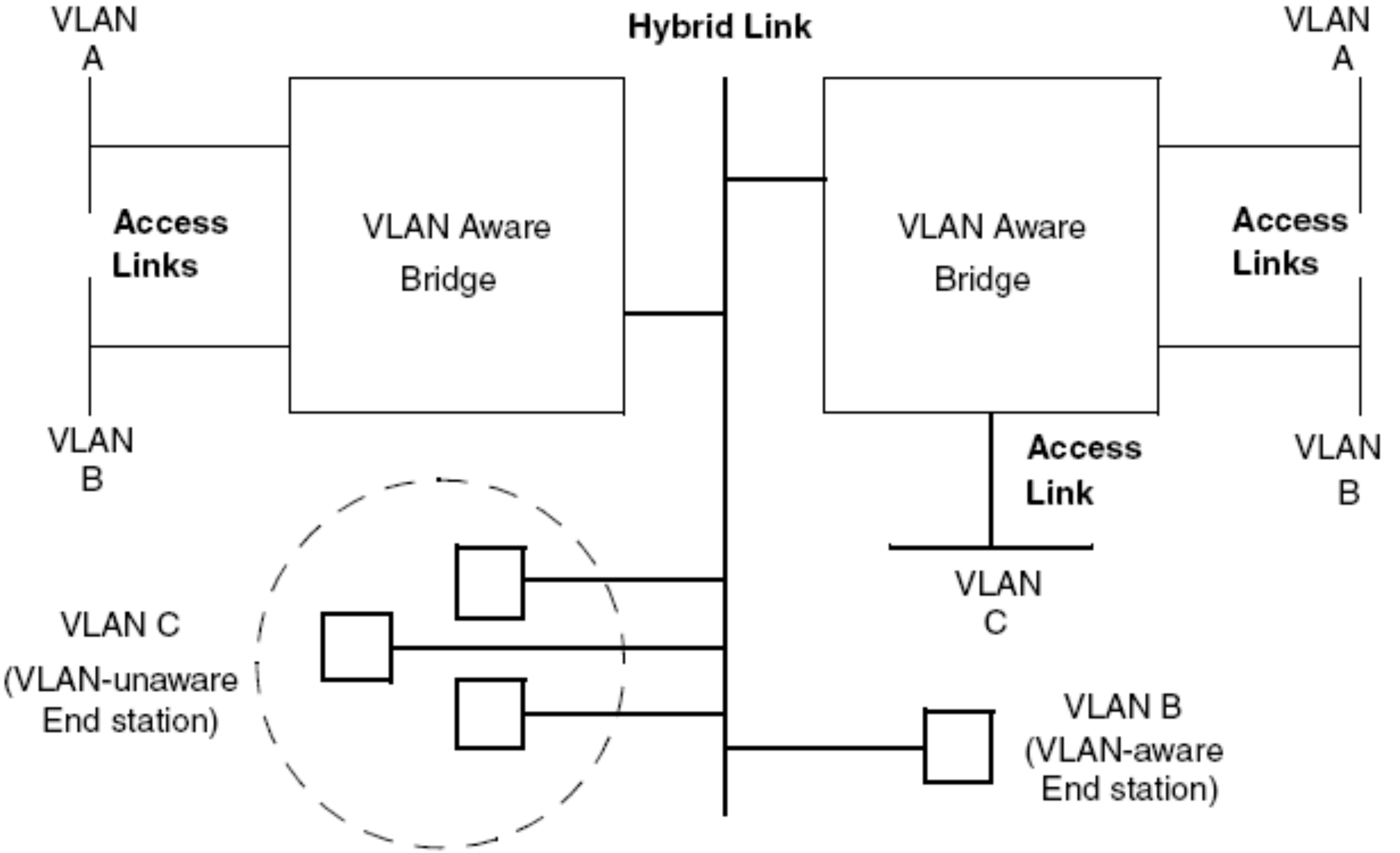
Trunk links

- **A link connected to a trunk port**
  - Typically switch-to-switch or switch-to-router links
  - frequently server-to-switch link
  - If PC-to-switch link:
    - → Anarchic VLANs considered



- **Support tagged Ethernet frames**
  - Explicit tagging mechanism to differentiate them
- **Does not belong to a VLAN but transport VLAN frames**
  - Either from all VLANs
  - Or just from selected VLANs
- **However, may belong to a VLAN**
  - Case of hybrid link
  - Untagged frames assumed to belong to a VLAN

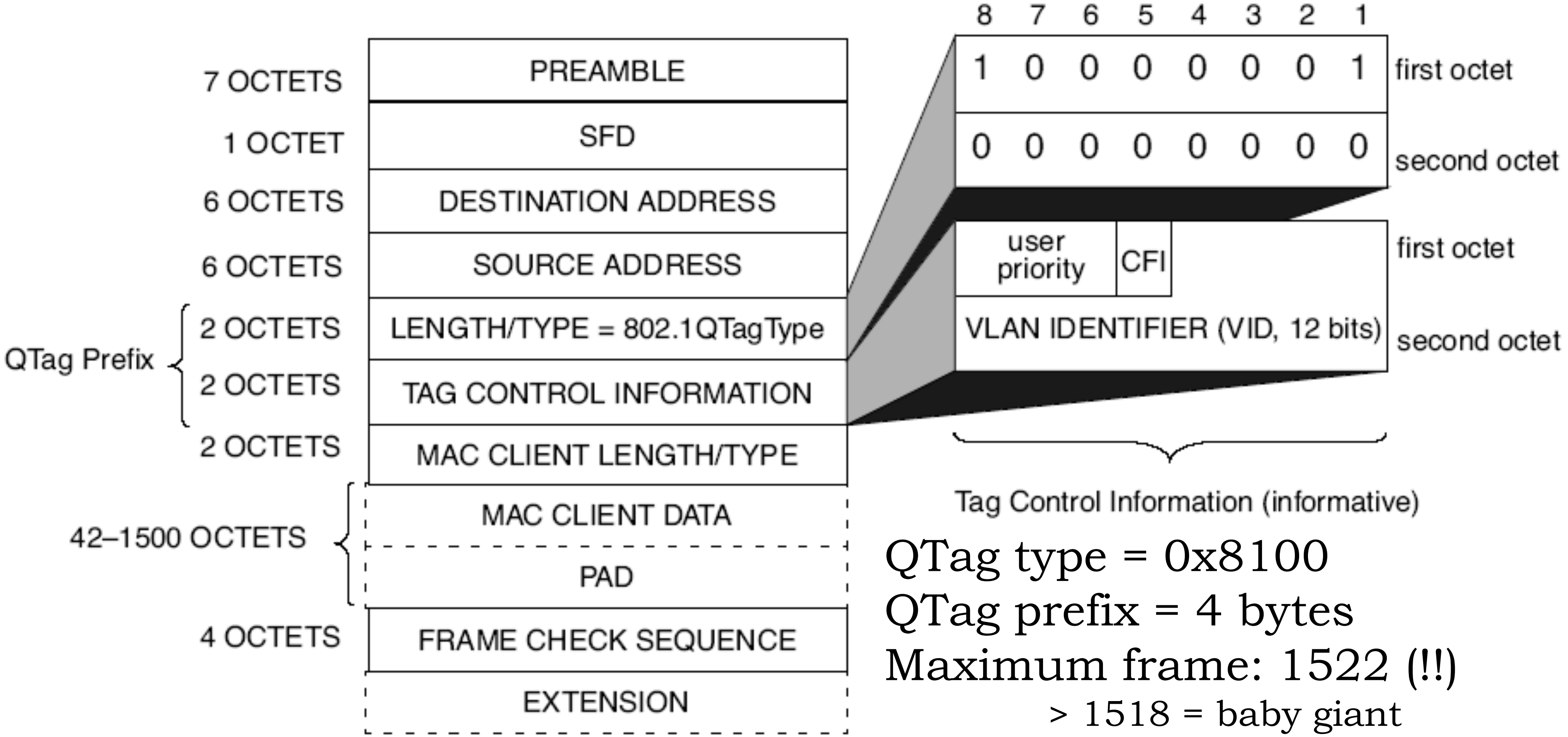
Hybrid links



➔ **Support both tagged and untagged Ethernet frames**

- ⇨ Untagged frames belong to the same VLAN (in the example, VLAN C)
- ⇨ Modern understanding and implementations: all links are of hybrid type…

Ethernet Frame format for VLAN (802.3ac, 1998)



QTag type = 0x8100

QTag prefix = 4 bytes

Maximum frame: 1522 (!!)

> 1518 = baby giant

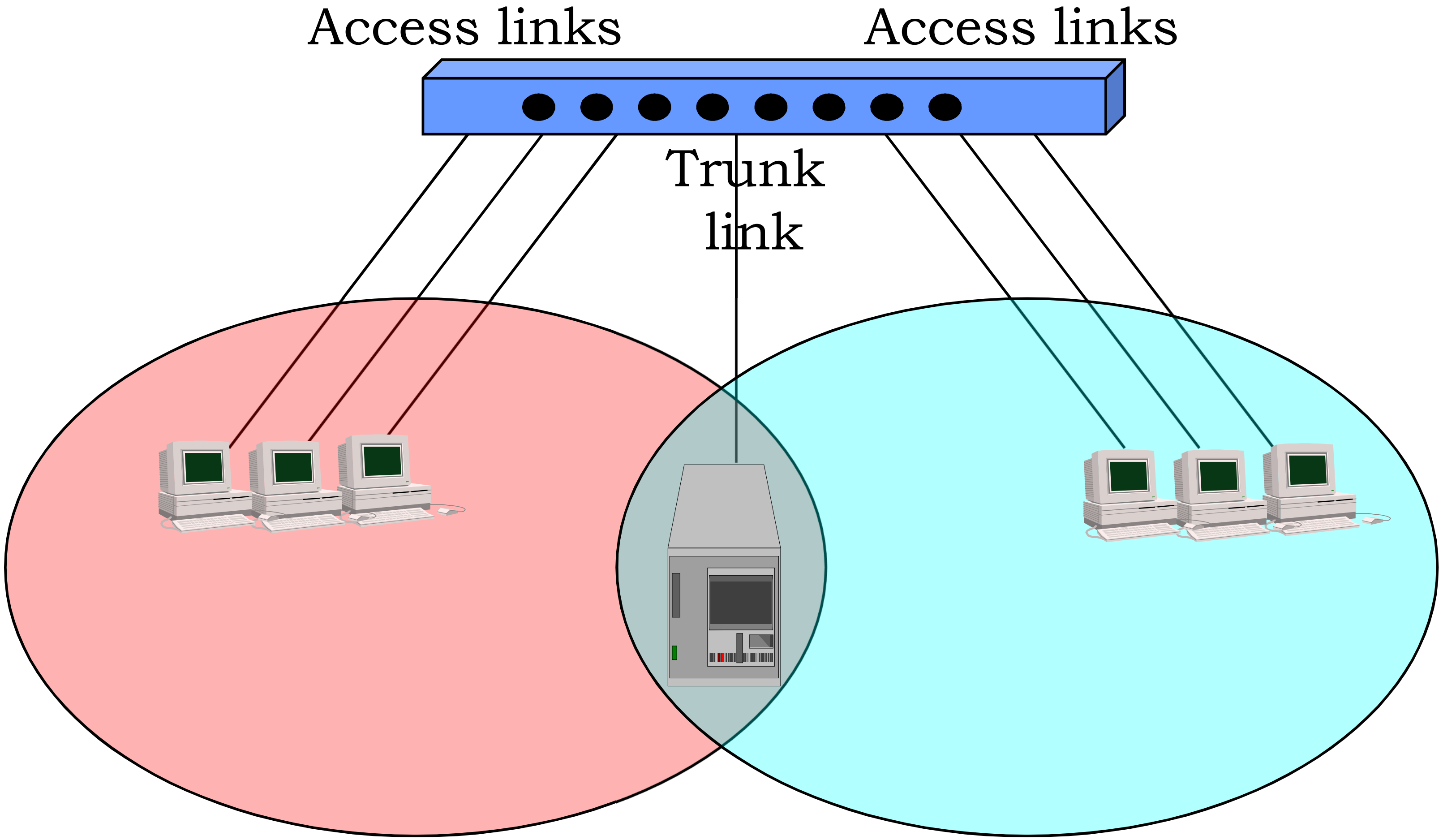
User Priority (802.1p)

0	BE	Best Effort (default)
1	BK	Background
2	---	Unspecified
3	EE	Excellent Effort
4	CL	Controlled Load
5	VI	Video < 100ms latency/jitter
6	VO	Voice < 10 ms latecny/jitter
7	NC	Network Control

Managed via separated output queues

- typically with priority queueing
- but more complex scheduling mechanisms can be used

May a station belong to more than 1 VLAN?



Yes! (typical case: servers)