VLAN

By Rexy

Course 5A - « network security »

FRAME

- Introduction
- Internet
- Intranet (local security)
- Intranet (security architecture)
- Controls and audits

Topic 1 (Local security)
INF 5243 - 18h

- Network reminders
  - Lab : VLAN – Tagged VLAN – static routing
  - Lab : TCP - UDP - DNS - NAT
  - Moodle : test1
- Imputability of accesses
  - Lab : captive portal
- Securing the access to media
  - Lab : network frame analysis
  - Lab : security of Ethernet (option)

MAJOR

Topic 2 (security architecture)
INF 5244 - 18h

- Firewall and DMZ
  - Lab : filtering, address translation and DMZ
  - Lab : services firewalls (proxy)
- Virtual Private Networks
  - Lab : VPN SSH/SSL/IPSEC (option)
- Intrusion detection
  - Lab : HIDS – NIDS – IPS (option)

MAJOR

Topic 3 (controls and audits)
INF 5049 - 18h

- Organization
- Ports scanning
  - Lab : nmap
- Network services knowledge
  - Lab : network services analysis
- Vulnerabilities detection
  - Lab : OpenVAS
- WIFI /Bt
  - Lab : WIFI cartography

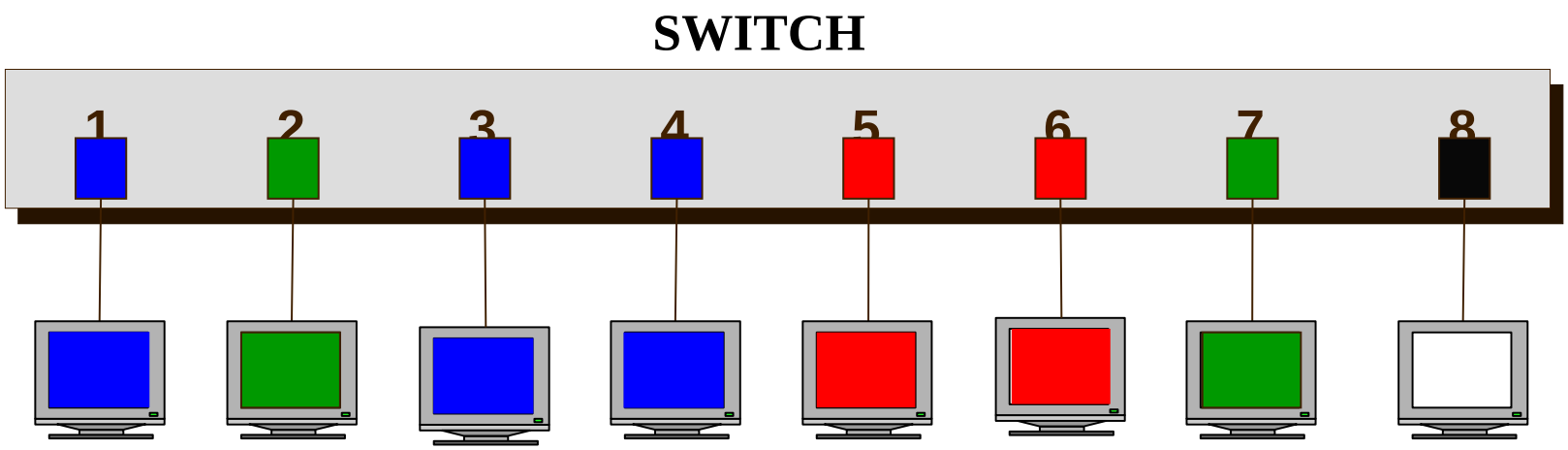
MINOR

Virtual Local Area Network

- **Goals** : create several virtual sub-networks inside a single physical network in order to :
  - optimizing the equipment (one switch / several network) ;
  - limiting the MAC broadcast « pollution » ;
  - Securing (partitioning) the networks which don’t need to communicate together.

- **3 levels** (types) :
  - by physical ports (L1) ;
  - by MAC addresses (L2) ;
  - by network address plans or by protocols (L3).

L1 - VLAN : physical ports associations

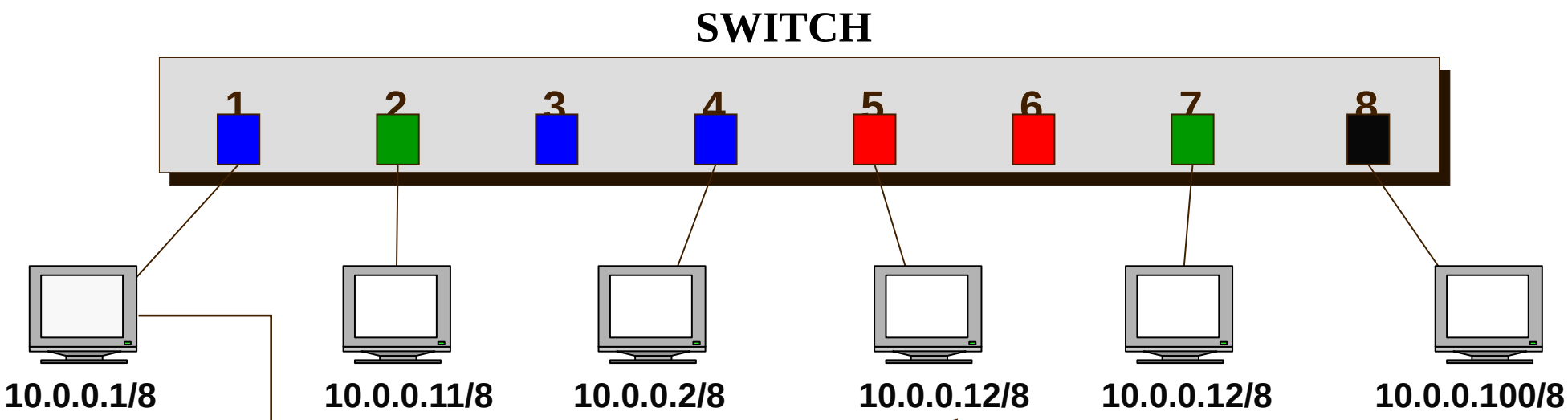


	Configuration
Port 5 et 6	**VLAN 2**
port 2 et 7	**VLAN 3**
port 1, 3 et 4	**VLAN 4**
port 8	**VLAN 1 (default VLAN)***

Disadvantage : no mobility.

* By default (without configuration), all ports of a switch are in this VLAN

L1 - VLAN : the network is “nearly” physically partitioned



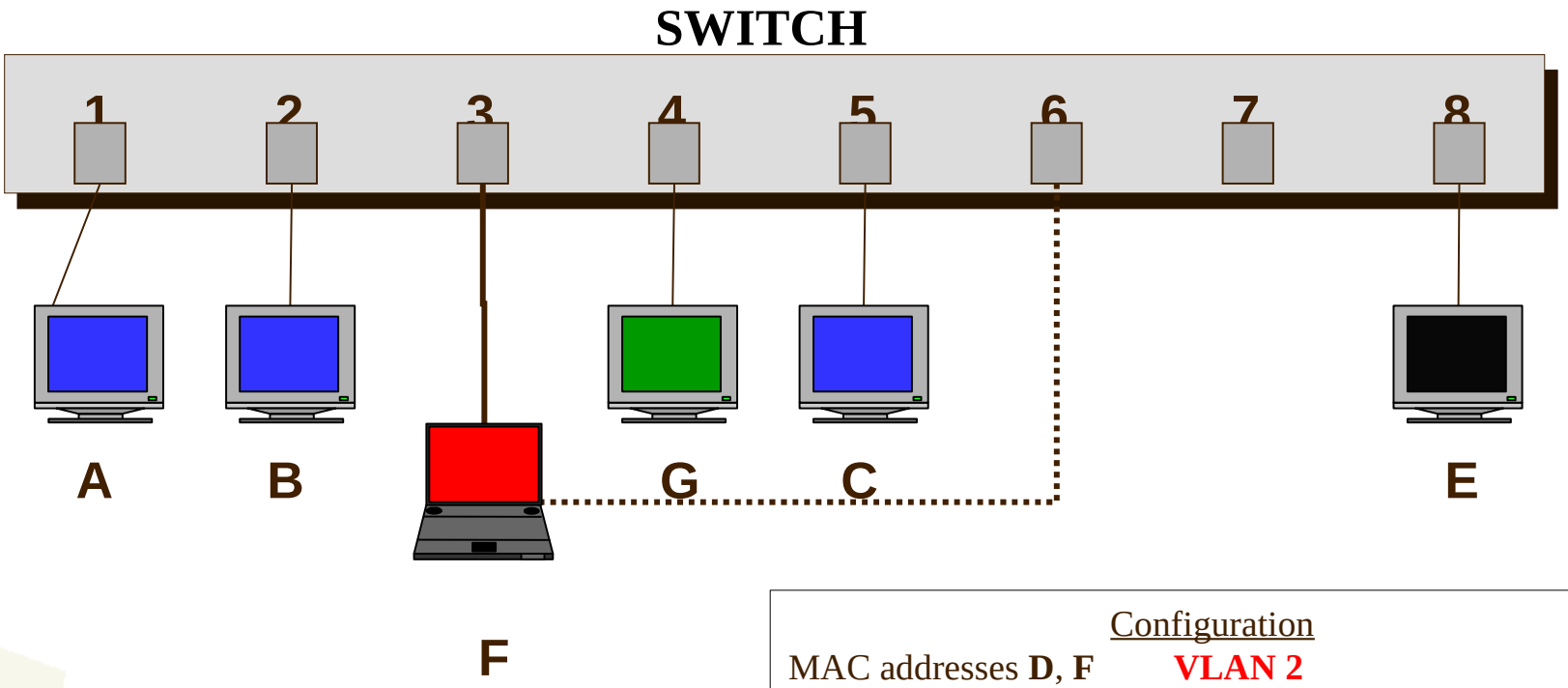
Ping 10.0.0.11 : impossible. The equipment isn’t in the same VLAN.

Same IP addresses !!! : it’s possible if the equipment are not in the same VLAN.

	Configuration
Port 5 et 6	**VLAN 2**
port 2 et 7	**VLAN 3**
port 1, 3 et 4	**VLAN 4**
port 8	**VLAN 1 (default VLAN)**

A broadcast frame sent by this equipment is propagated on the port 1, 3 and 4

L2 - VLAN : MAC addresses association

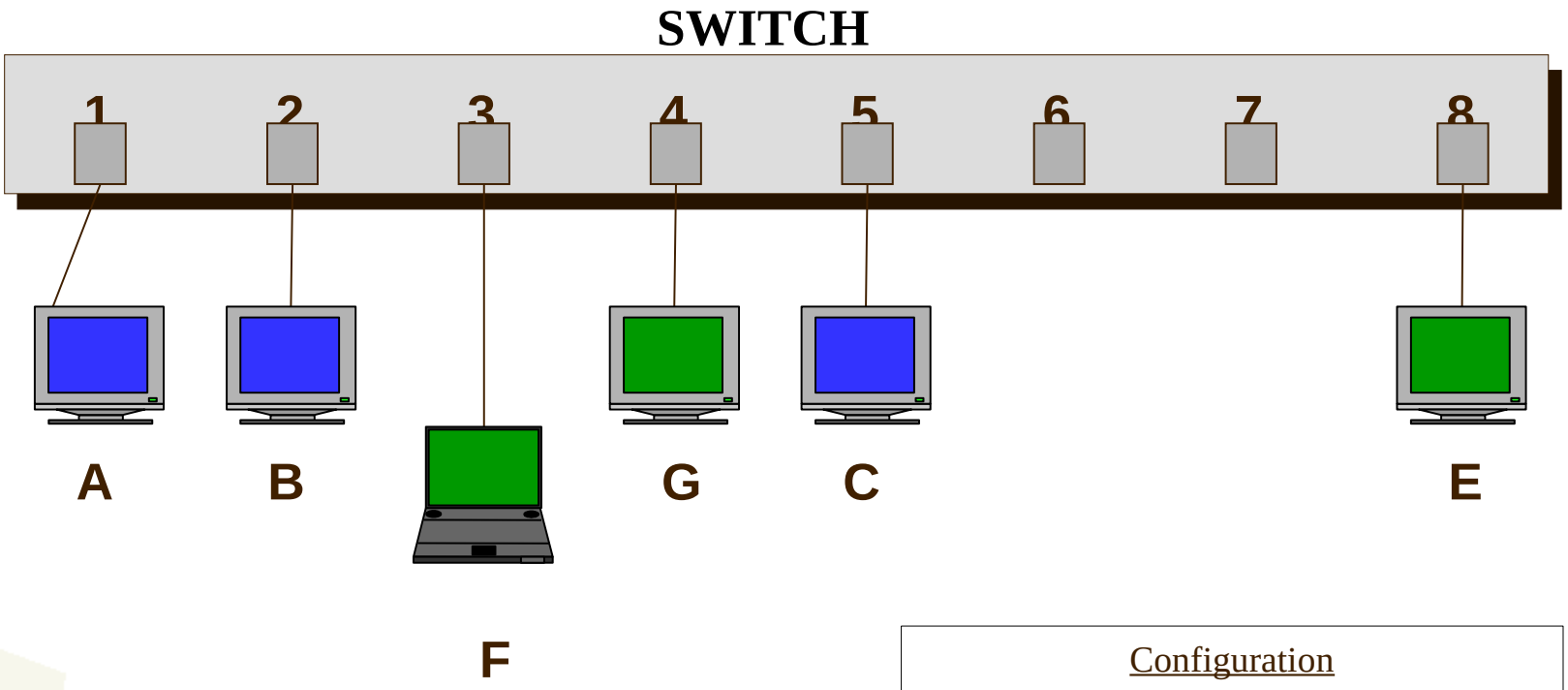


Configuration	
MAC addresses **D**, **F**	**VLAN 2**
MAC address **G**	**VLAN 3**
MAC addresses **A**, **B**, **C**	**VLAN 4**
MAC address **E**	**VLAN 1 (default VLAN)**

Advantage: mobility of equipment is possible

Disadvantage: the rules must be input in the switch (administration load)

L3 - VLAN : network protocols association

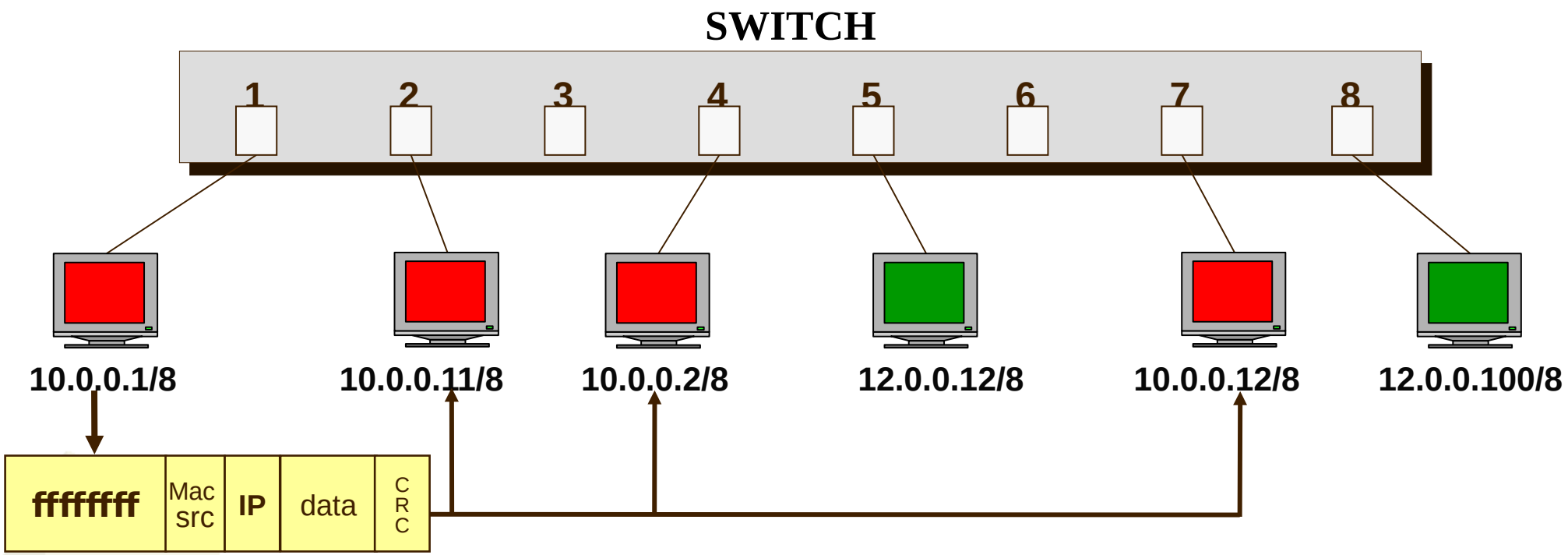


Configuration
VLAN 1 : protocol **IP**
VLAN 2 : protocol **AppleTalk**

Advantage:
- mobility of equipments is possible
- flows separation

Disadvantage
- The switches must know L3 protocols !!!
- poor switching performance
- the rules must be input in the switch (administration load)

L3 - VLAN : network IP addresses partitioning



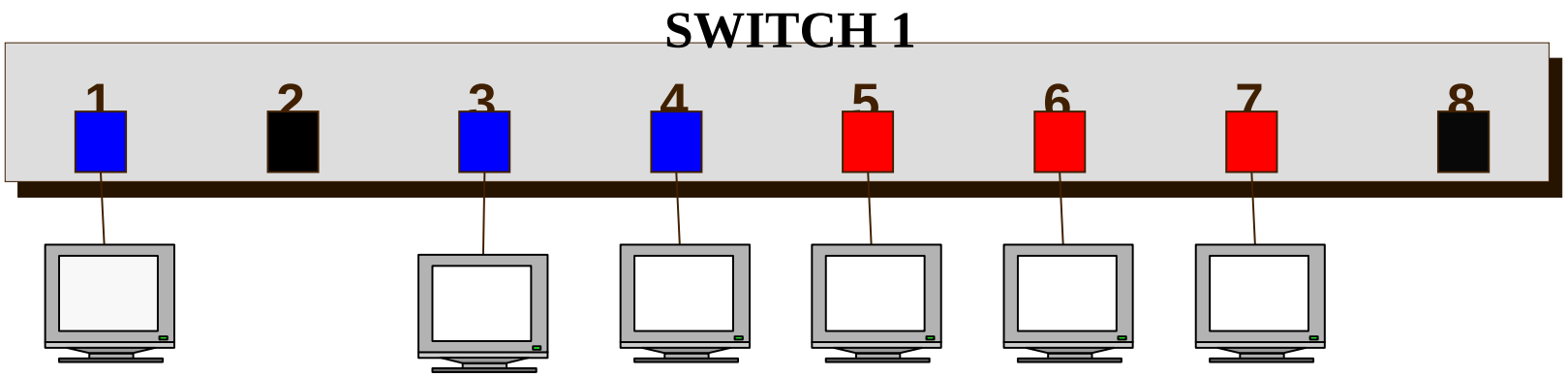
Configuration

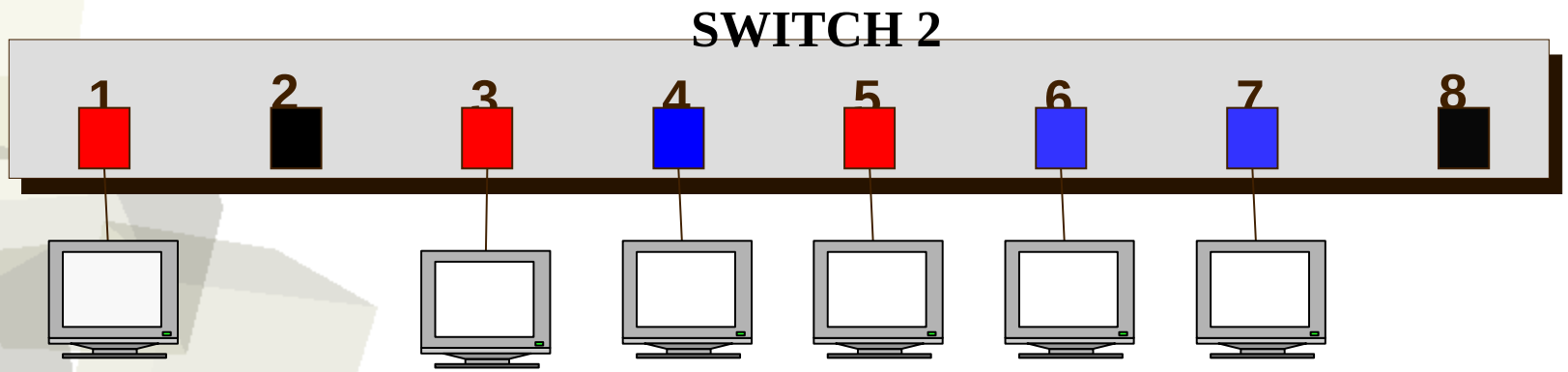
10.0.0.0/8	VLAN 2
12.0.0.0/8	VLAN 3

Advantage :
- no administration
- mobility of equipments is possible

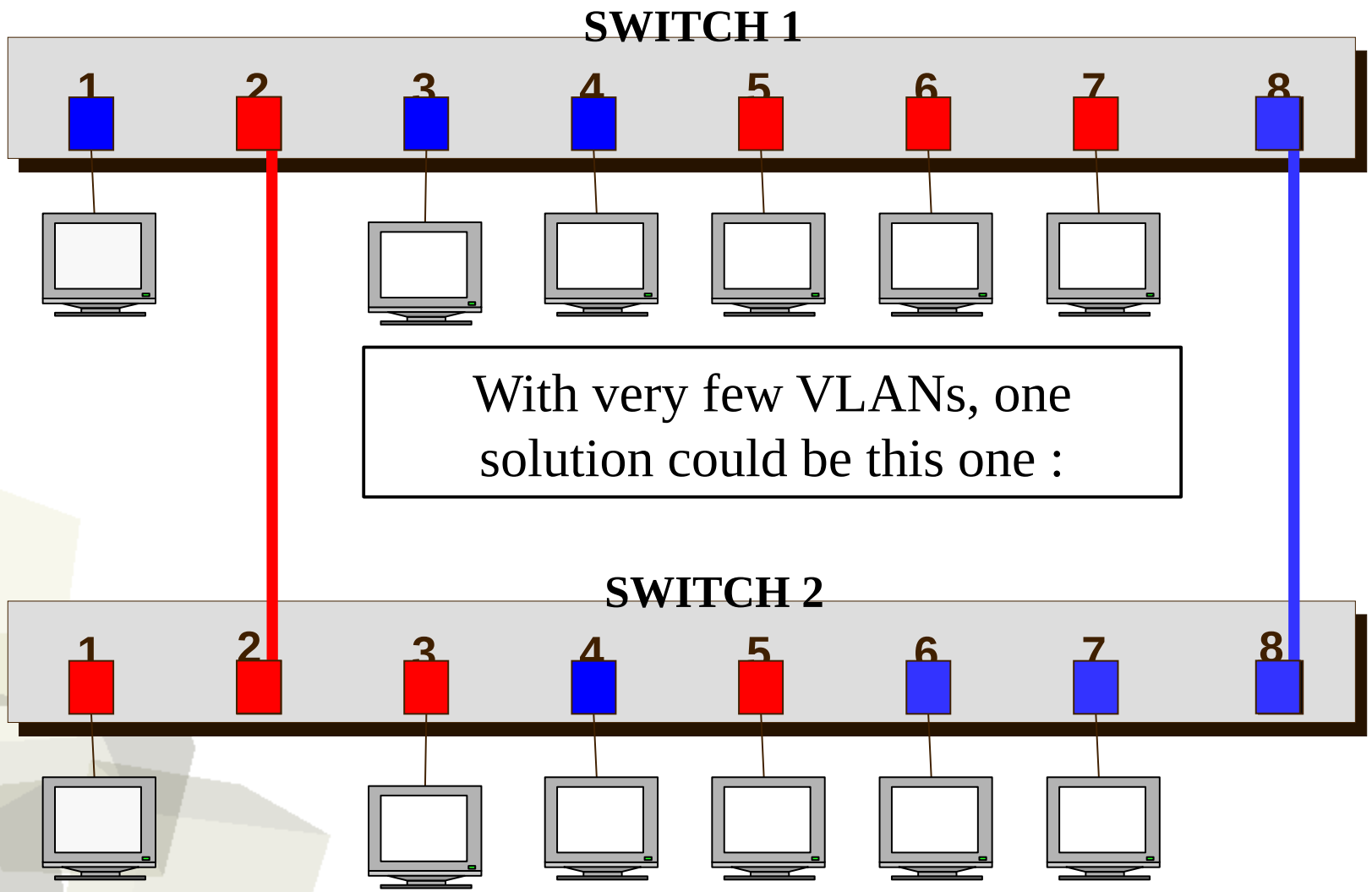
Disadvantage :
- the partitioning is logical only (no security)
- a broadcast frame is received by all equipments

Problem : How extend the VLAN on several switches ?



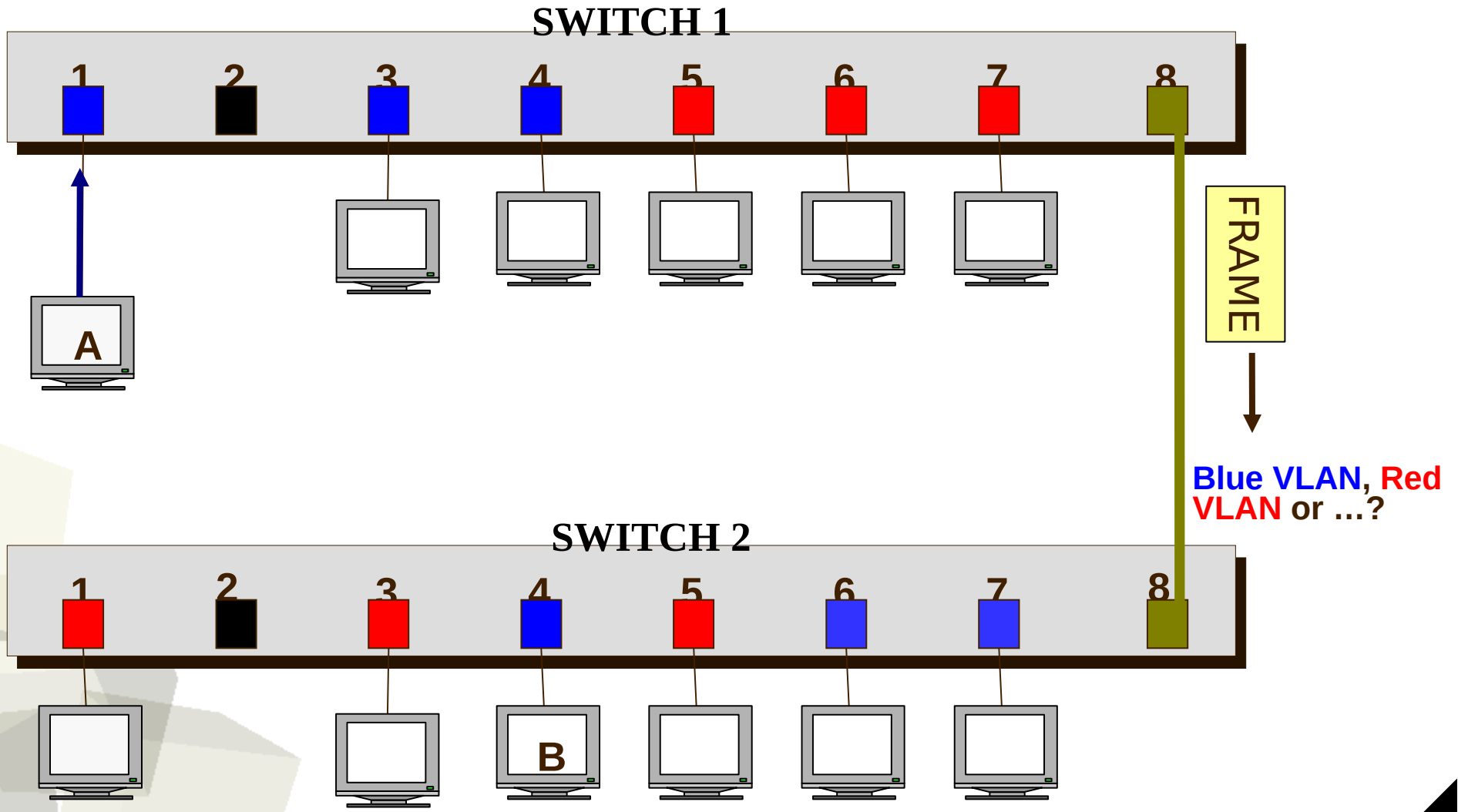


Problem : How extend the VLAN on several switches ?



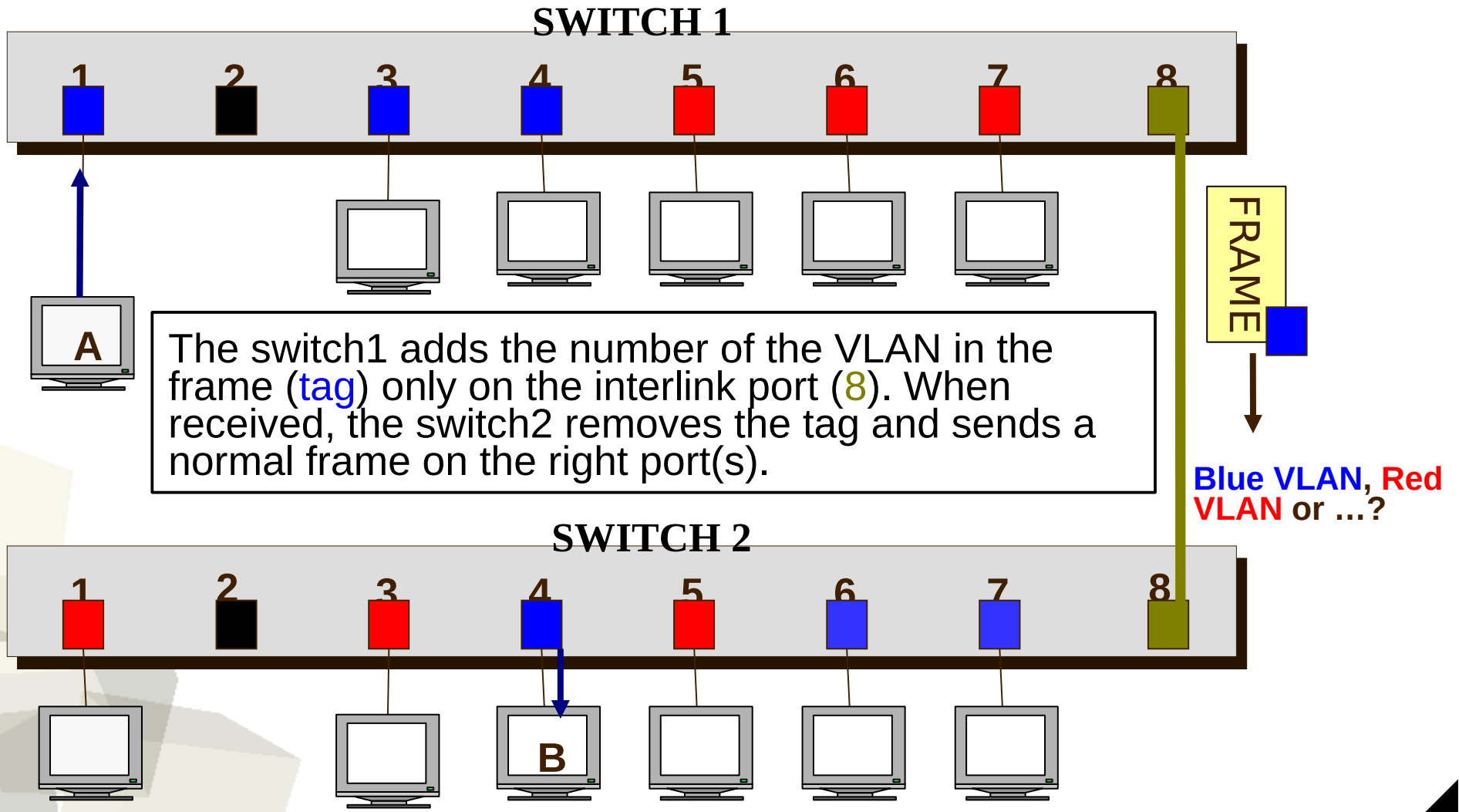
Solution : one link for all VLANS

How does the next switch know the VLAN of a frame (in order to send it to the right port(s)) ?

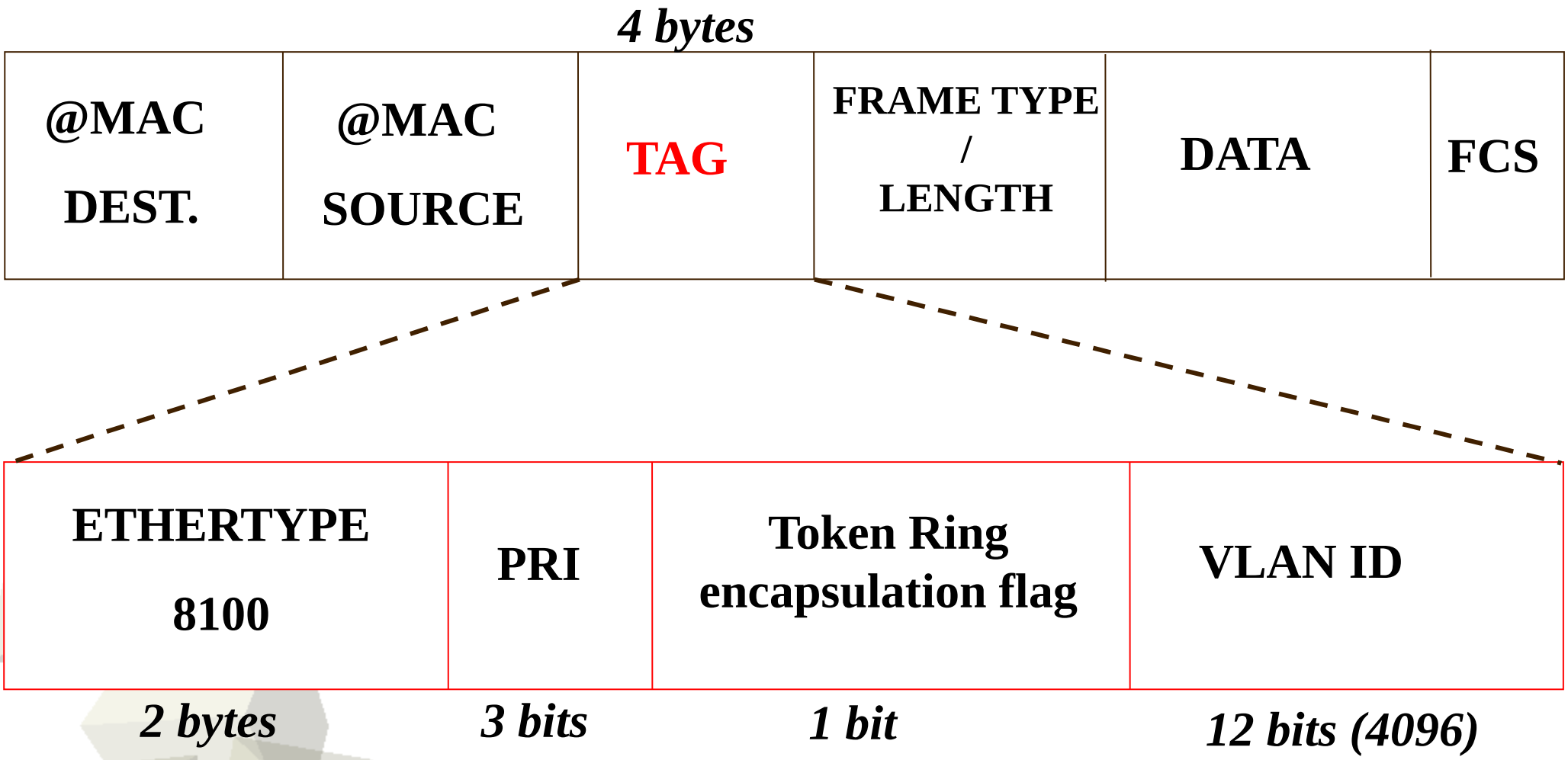


Solution : one link for all VLANS

How does the next switch know the VLAN of a frame (in order to send it to the right port(s)) ?

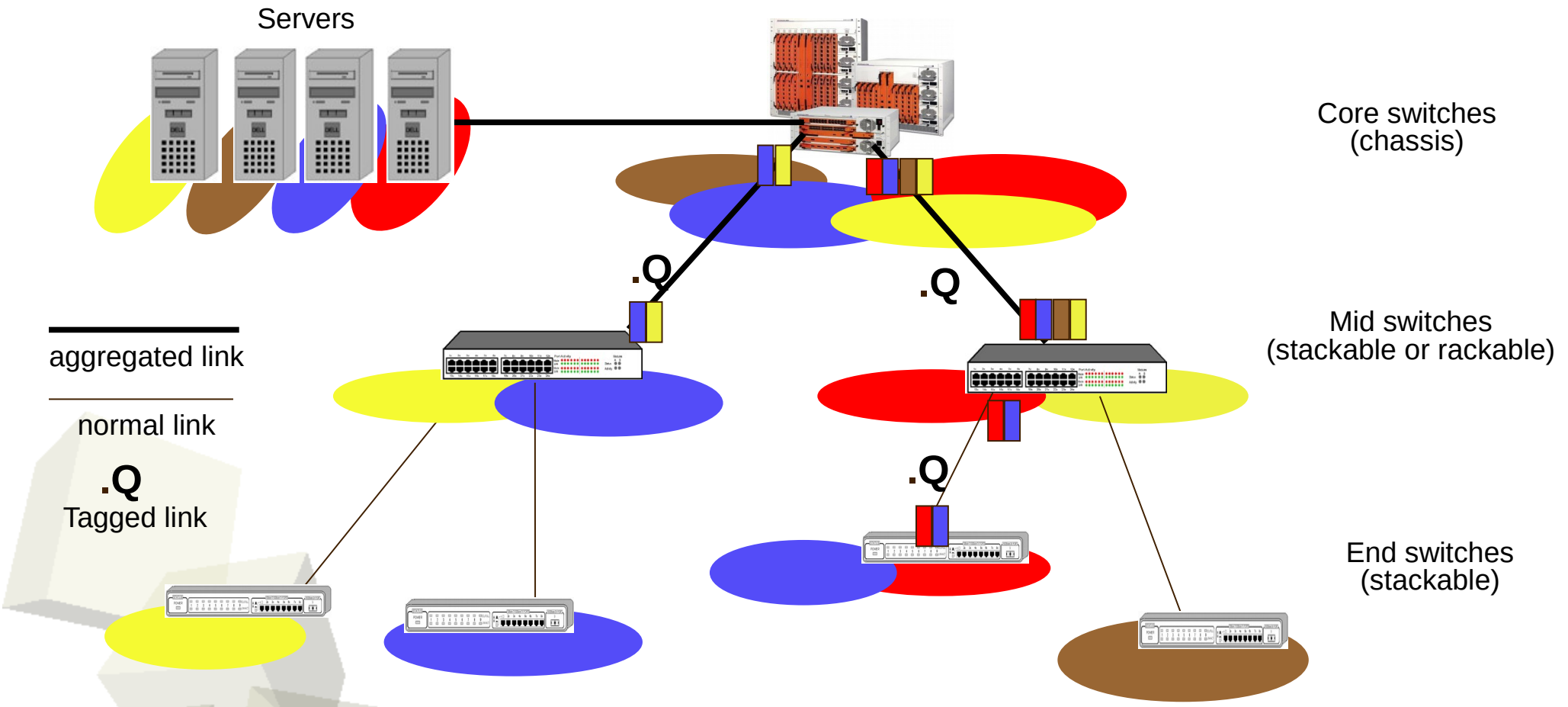


Solution : The Ethernet frame tagging (**802.1Q**)

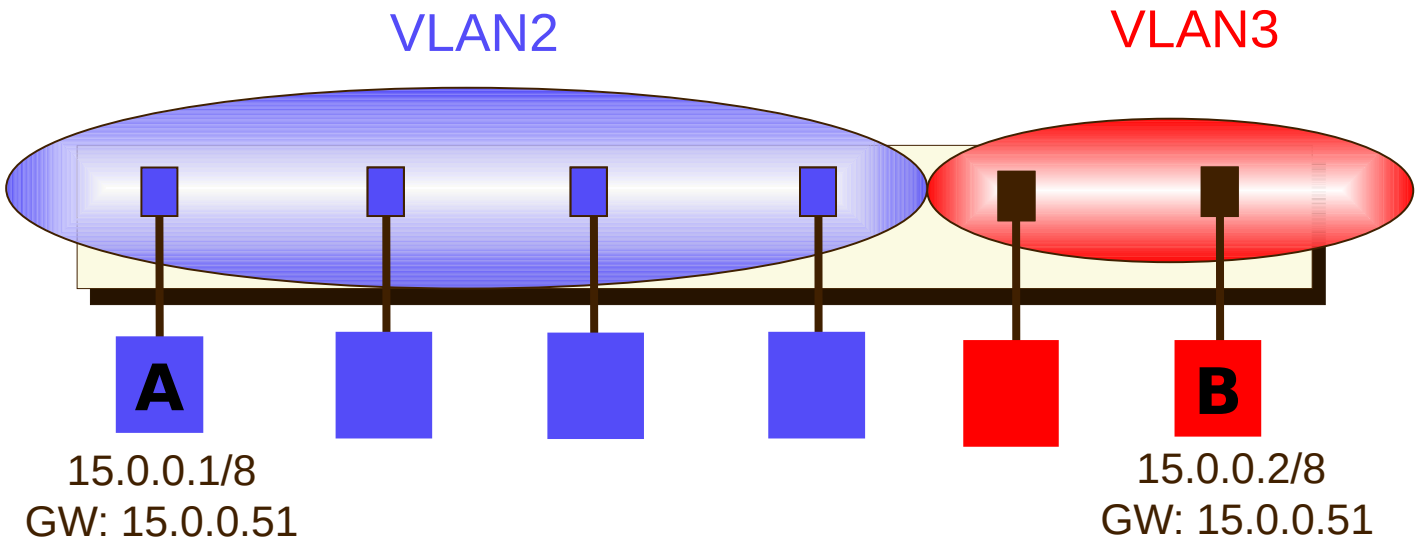


What do you think about the commutation mode (fast-forward / store&forward) ?

Solution : The Ethernet frame tagging (**802.1Q**)



Problem : How can equipments of VLAN1 communicate with equipments of VLAN2 ?

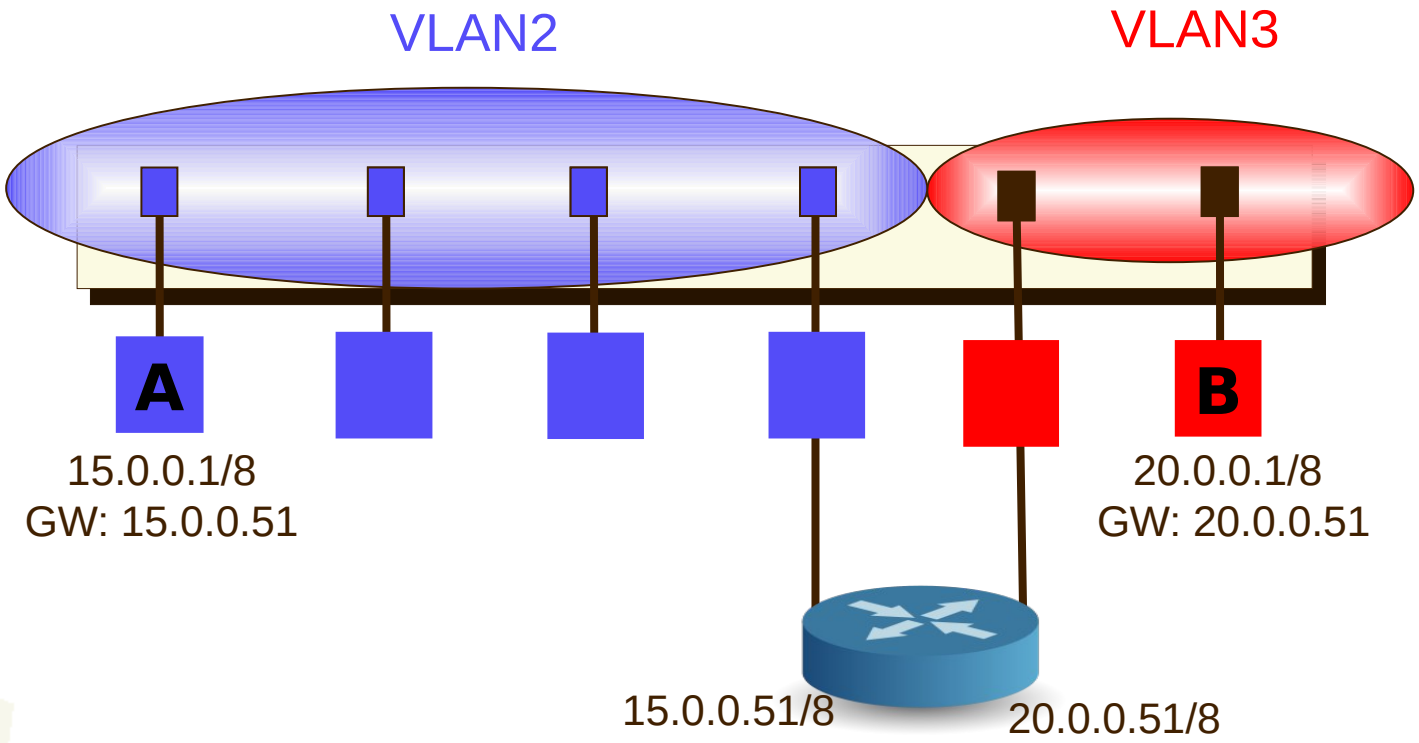


Ping A to B ?

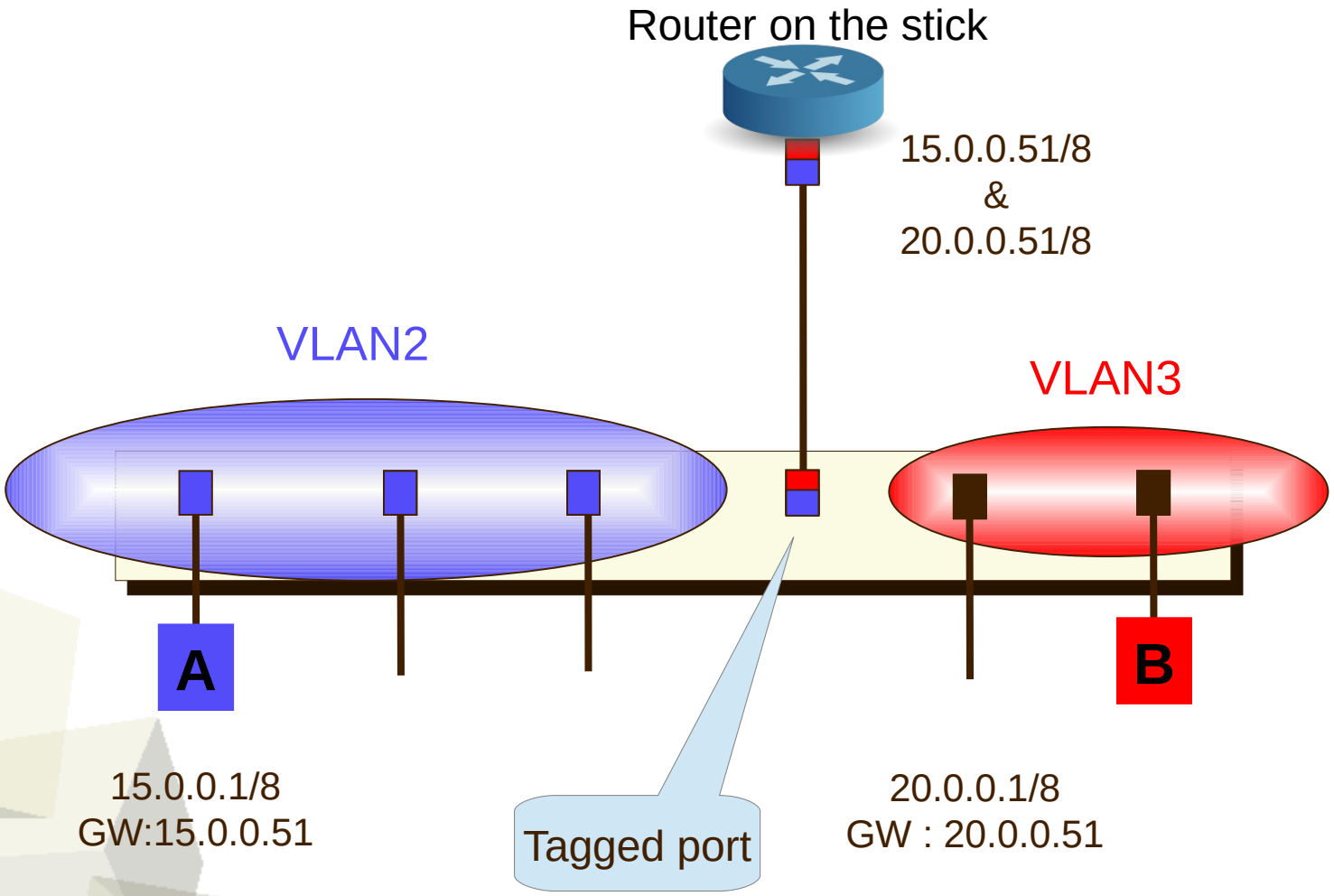
Even if A and B ∈ 15.0.0.0/8, they can't communicates together. Because :

- they don't use their gateway (same IP network / subnet mask) :
- the SWITCH doesn't forward their Ethernet frames (different VLAN).

Solution 1 : On small LAN, use a router and change the IP address plan.



Solution 2 : Use a 802.1Q compatible router and change the IP address plan.



Virtual Local Area Network

GAINS

- Improve the performance (less broadcast frames on each VLAN)
- Improve the security by partitioning the working groups.
- Use of switches is optimized (less but bigger is cheaper)

LIMITS

- Equipment connected on different VLAN can’t communicate together
- Number of VLAN is « limited » to 4094 (4*00 and 4*FF are reserved)
- Must use other equipments in order to communicates between VLAN.

VLAN

By Rexy

Course 5A - « network security »

FRAME

- Introduction
- Internet
- Intranet (local security)
- Intranet (security architecture)
- Controls and audits

Topic 1 (Local security)
INF 5243 - 18h

- Network reminders
  - Lab : VLAN – Tagged VLAN – static routing
  - Lab : TCP - UDP - DNS - NAT
  - Moodle : test1
- Imputability of accesses
  - Lab : captive portal
- Securing the access to media
  - Lab : network frame analysis
  - Lab : security of Ethernet (option)

MAJOR

Topic 2 (security architecture)
INF 5244 - 18h

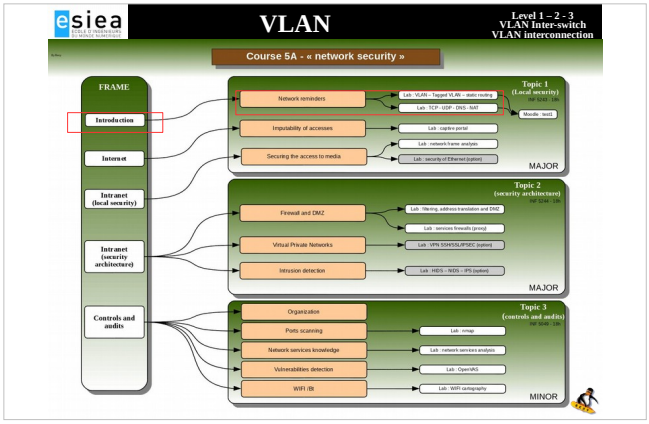
- Firewall and DMZ
  - Lab : filtering, address translation and DMZ
  - Lab : services firewalls (proxy)
- Virtual Private Networks
  - Lab : VPN SSH/SSL/IPSEC (option)
- Intrusion detection
  - Lab : HIDS – NIDS – IPS (option)

MAJOR

Topic 3 (controls and audits)
INF 5049 - 18h

- Organization
- Ports scanning
  - Lab : nmap
- Network services knowledge
  - Lab : network services analysis
- Vulnerabilities detection
  - Lab : OpenVAS
- WIFI /Bt
  - Lab : WIFI cartography

MINOR


esiea
VLAN
Level 1 – 2 - 3
VLAN Inter-switch
VLAN interconnection
Course 5A - « network security »
FRAME
Introduction
Internet
Intranet (local security)
Intranet (security architecture)
Controls and audits
Network reminders
Impulsability of accesses
Securing the access to media
Lab : VLAN – Tagged VLAN – static routing
Lab : TCP - UDP - DNS - NAT
Moodle : test1
Lab : captive portal
Lab : network frame analyses
Lab : security of Ethernet (option)
Topic 1
(Local security)
MAJOR
Firewall and DMZ
Virtual Private Networks
Intrusion detection
Lab : filtering, address translation and DMZ
Lab : services firewalls (proxy)
Lab : VPN SSH/SSL/IPSEC (option)
Lab : HIDS – NIDS – IPS (option)
Topic 2
(security architecture)
MAJOR
Organization
Ports scanning
Network services knowledge
Vulnerabilities detection
WIFI /Bt
Lab : nmap
Lab : network services analysis
Lab : OpenVAS
Lab : WIFI cartography
Topic 3
(controls and audits)
MINOR

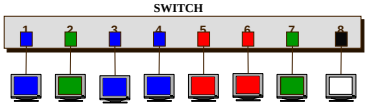
Virtual Local Area Network

- **Goals** : create several virtual sub-networks inside a single physical network in order to :
  - optimizing the equipment (one switch / several network) ;
  - limiting the MAC broadcast « pollution » ;
  - Securing (partitioning) the networks which don't need to communicate together.
- **3 levels** (types) :
  - by physical ports (L1) ;
  - by MAC addresses (L2) ;
  - by network address plans or by protocols (L3).

4

L1 - VLAN : physical ports associations

SWITCH



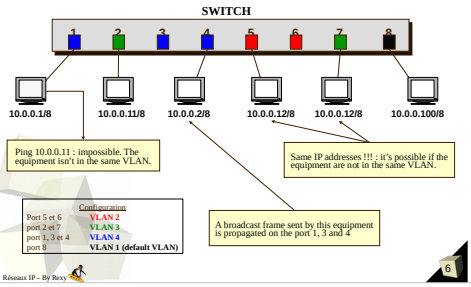
Configuration	
Port 5 et 6	**VLAN 2**
port 2 et 7	**VLAN 3**
port 1, 3 et 4	**VLAN 4**
port 8	**VLAN 1 (default VLAN)***

Disadvantage : no mobility.

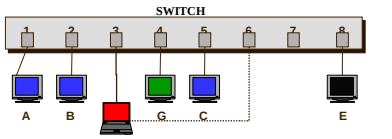
* By default (without configuration), all ports of a switch are in this VLAN

5

L1 - VLAN : the network is “nearly” physically partitioned



L2 - VLAN : MAC addresses association



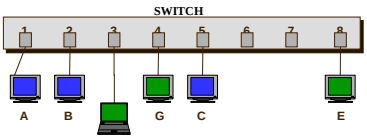
Configuration	
MAC addresses **D**, **F**	**VLAN 2**
MAC address **G**	**VLAN 3**
MAC addresses **A**, **B**, **C**	**VLAN 4**
MAC address **E**	**VLAN 1 (default VLAN)**

Advantage: mobility of equipment is possible

Disadvantage: the rules must be input in the switch (administration load)

7

L3 - VLAN : network protocols association



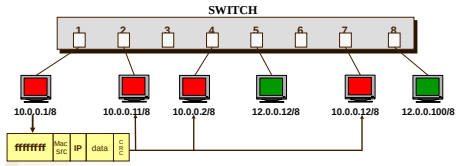
Configuration
VLAN 1 : protocol **IP**
VLAN 2 : protocol **AppleTalk**

Advantage:
- mobility of equipments is possible
- flows separation

Disadvantage
- The switches must know L3 protocols !!!
- poor switching performance
- the rules must be input in the switch (administration load)

8

L3 - VLAN : network IP addresses partitioning

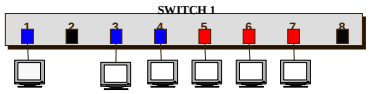


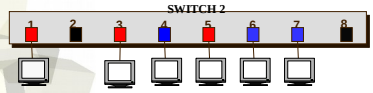
Configuration
10.0.0.0/8 VLAN 2
12.0.0.0/8 VLAN 3

Advantage :
- no administration
- mobility of equipments is possible

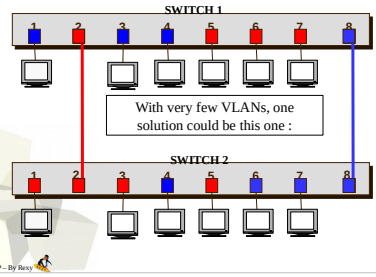
Disadvantage :
- the partitioning is logical only (no security)
- a broadcast frame is received by all equipments

Problem : How extend the VLAN on several switches ?



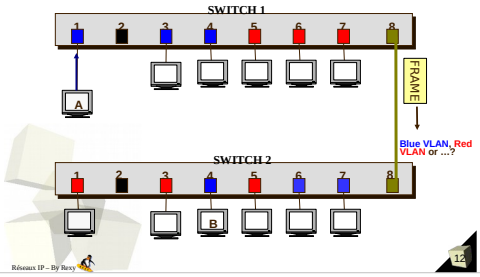


Problem : How extend the VLAN on several switches ?



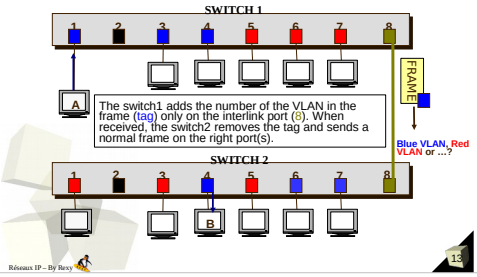
Solution : one link for all VLANS

How does the next switch know the VLAN of a frame (in order to send it to the right port(s)) ?

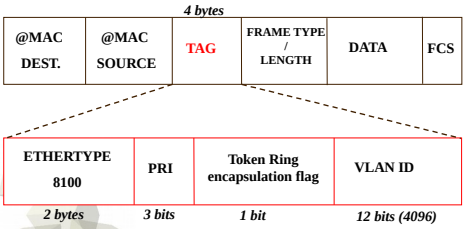


Solution : one link for all VLANS

How does the next switch know the VLAN of a frame (in order to send it to the right port(s)) ?



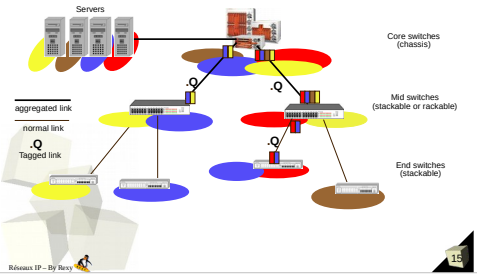
Solution : The Ethernet frame tagging (**802.1Q**)



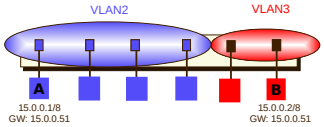
What do you think about the commutation mode (fast-forward / store&forward) ?

14

Solution : The Ethernet frame tagging (**802.1Q**)



Problem : How can equipments of VLAN1 communicate with equipments of VLAN2 ?



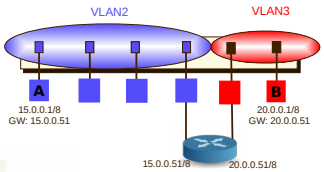
15.0.0.1/8
GW: 15.0.0.51

15.0.0.2/8
GW: 15.0.0.51

Ping A to B ?

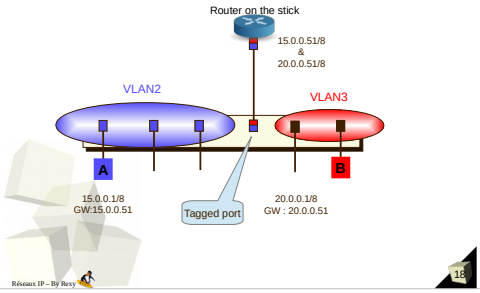
Even if A and B ∈ 15.0.0.0/8, they can't communicates together. Because :
- they don't use their gateway (same IP network / subnet mask) :
- the SWITCH doesn't forward their Ethernet frames (different VLAN).

Solution 1 : On small LAN, use a router and change the IP address plan.



17

Solution 2 : Use a 802.1Q compatible router and change the IP address plan.



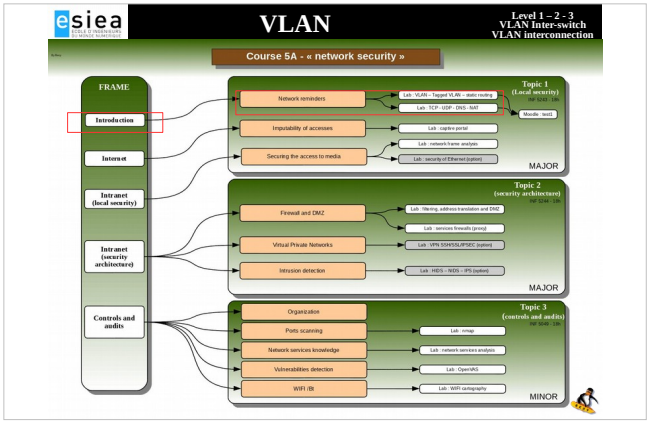
Virtual Local Area Network

GAINS

- Improve the performance (less broadcast frames on each VLAN)
- Improve the security by partitioning the working groups.
- Use of switches is optimized (less but bigger is cheaper)

LIMITS

- Equipment connected on different VLAN can't communicate together
- Number of VLAN is « limited » to 4094 (4*00 and 4*FF are reserved)
- Must use other equipments in order to communicates between VLAN.


esiea
VLAN
Level 1 – 2 - 3
VLAN Inter-switch
VLAN interconnection
Course 5A - « network security »
FRAME
Introduction
Internet
Intranet (local security)
Intranet (security architecture)
Controls and audits
Network reminders
Impulsability of accesses
Securing the access to media
Lab : VLAN – Tagged VLAN – static routing
Lab : TCP - UDP - DNS - NAT
Moodle : test1
Lab : captive portal
Lab : network frame analyses
Lab : security of Ethernet (option)
Topic 1
(Local security)
MAJOR
Firewall and DMZ
Virtual Private Networks
Intrusion detection
Lab : filtering, address translation and DMZ
Lab : services firewalls (proxy)
Lab : VPN SSH/SSL/IPSEC (option)
Lab : HIDS – NIDS – IPS (option)
Topic 2
(security architecture)
MAJOR
Organization
Ports scanning
Network services knowledge
Vulnerabilities detection
WIFI /Bt
Lab : nmap
Lab : network services analysis
Lab : OpenVAS
Lab : WIFI cartography
Topic 3
(controls and audits)
MINOR