Fonctionnalités avancées des VLANs

APPERT Fabien
BOUVET Adrien
CHAVERON Nicolas
-
Ingénieurs2000
IR - 3ème année
-
Février 2005

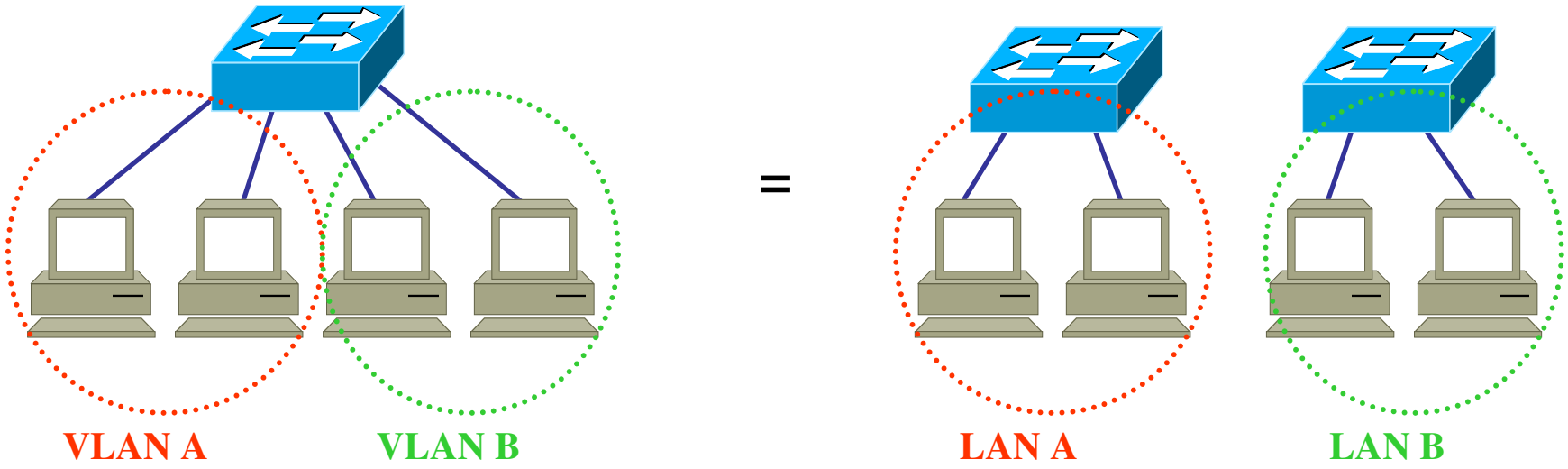
Fonctionnalités avancées des VLANs

Table des matières

VLAN - Théorie 1/2

Définition : **V**irtual **L**ocal **A**rea **N**etwork

Utilité : Plusieurs réseaux virtuels sur un même réseau physique



VLAN - Théorie 2/2

Notions essentielles :

- VLAN par défaut toujours présent
- Technologie en standard sur les switchs actuels
- Configuration au niveau de l'équipement

3 types de VLAN :

- par port ⇔ Niveau 1
- par adresse MAC ⇔ Niveau 2
- par sous-réseau / protocole ⇔ Niveau 3

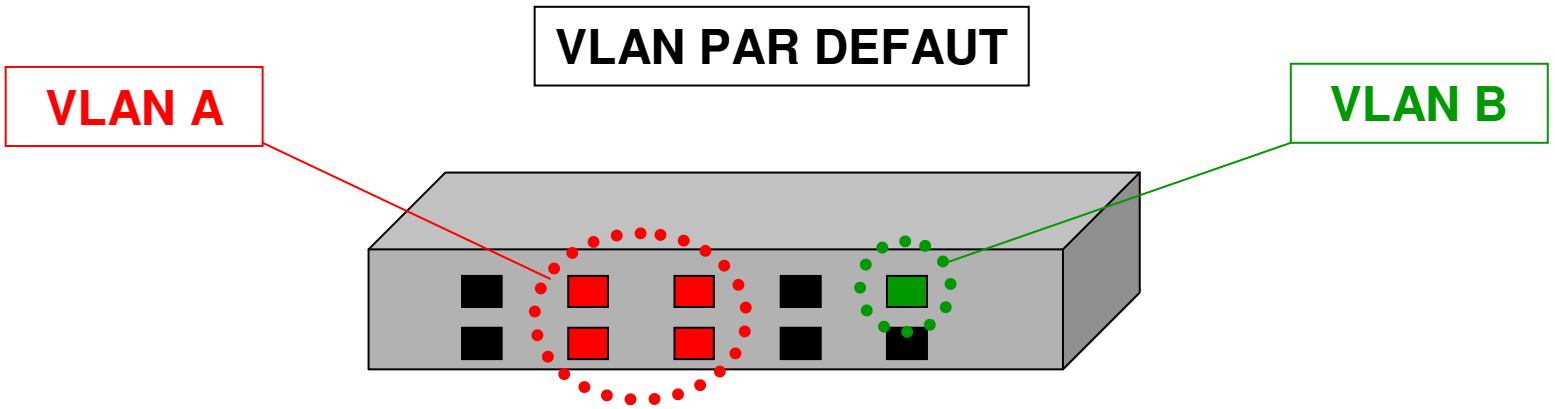
VLAN – niveau 1

VLAN de niveau 1 ⇔ VLAN par port

→ 1 port du switch dans 1 VLAN

→ configurable au niveau de l'équipement

→ 90% des VLAN sont des VLAN par port



VLAN – niveau 2

VLAN de niveau 2 ⇔ VLAN par adresse MAC

→ VLAN en fonction des adresses MAC

→ configurable au niveau de l'équipement

⊕ indépendance de la localisation de la station

⊖ difficultés de poser des règles de filtrages précises

VLAN – niveau 3

VLAN de niveau 3 ⇔ VLAN par sous-réseau ou par protocole

→ VLAN en fonction des adresses IP sources des datagrammes ou du type de protocole

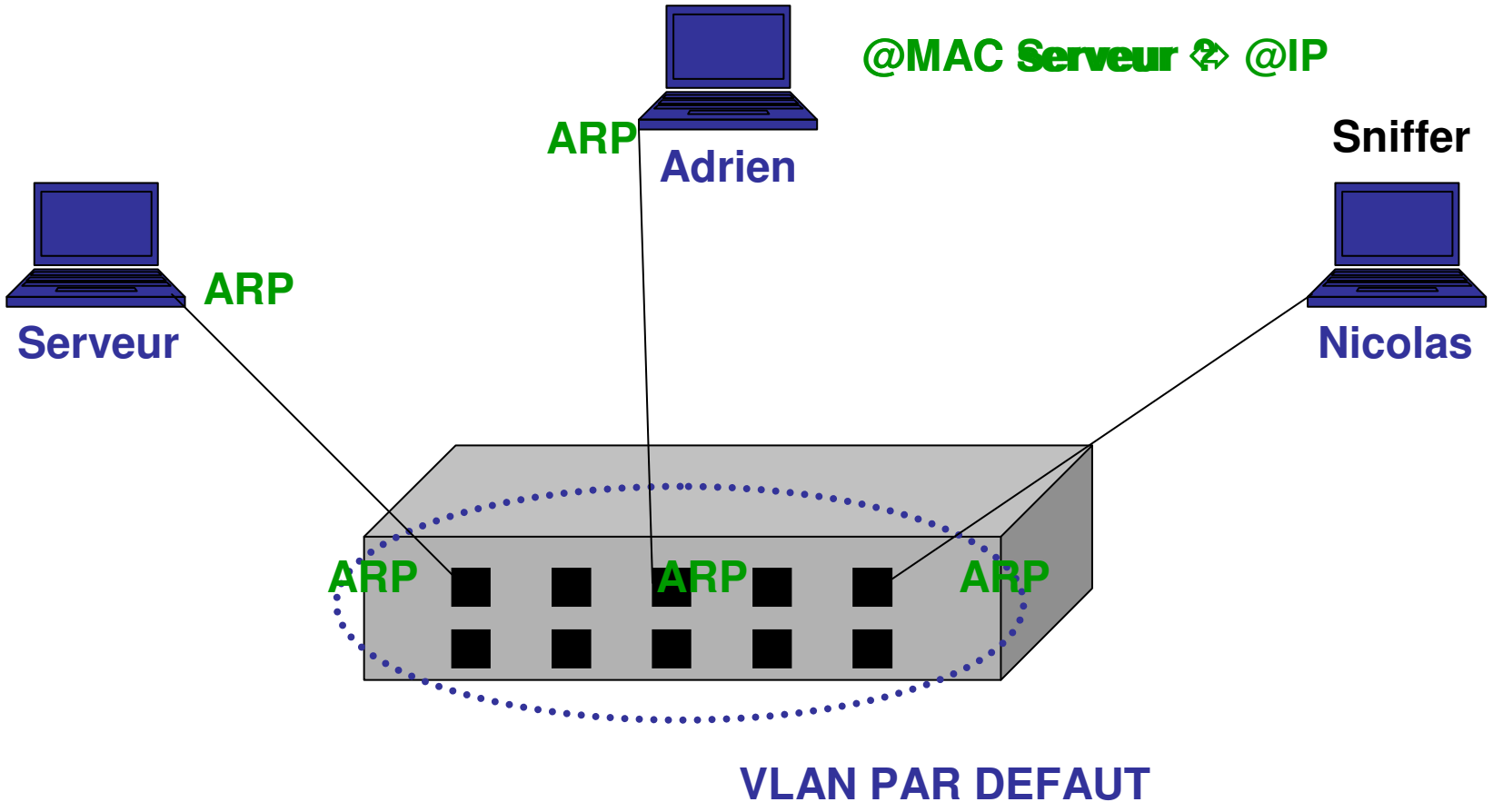
→ configurable au niveau de l'équipement

⊕ séparation des flux

⊖ dégradation des performances

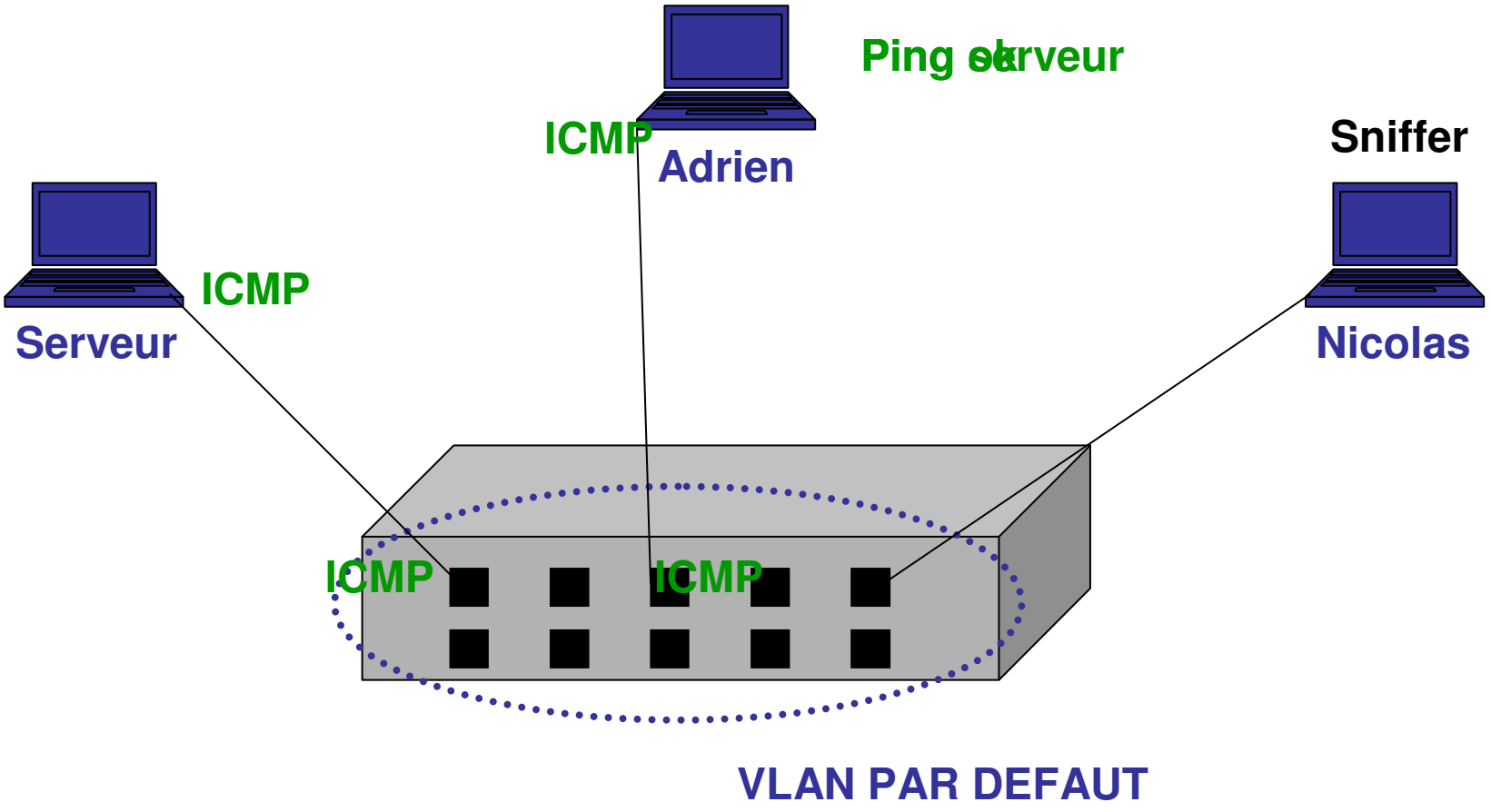
VLAN - Démonstration

Situation 1 : VLAN DEFAULT



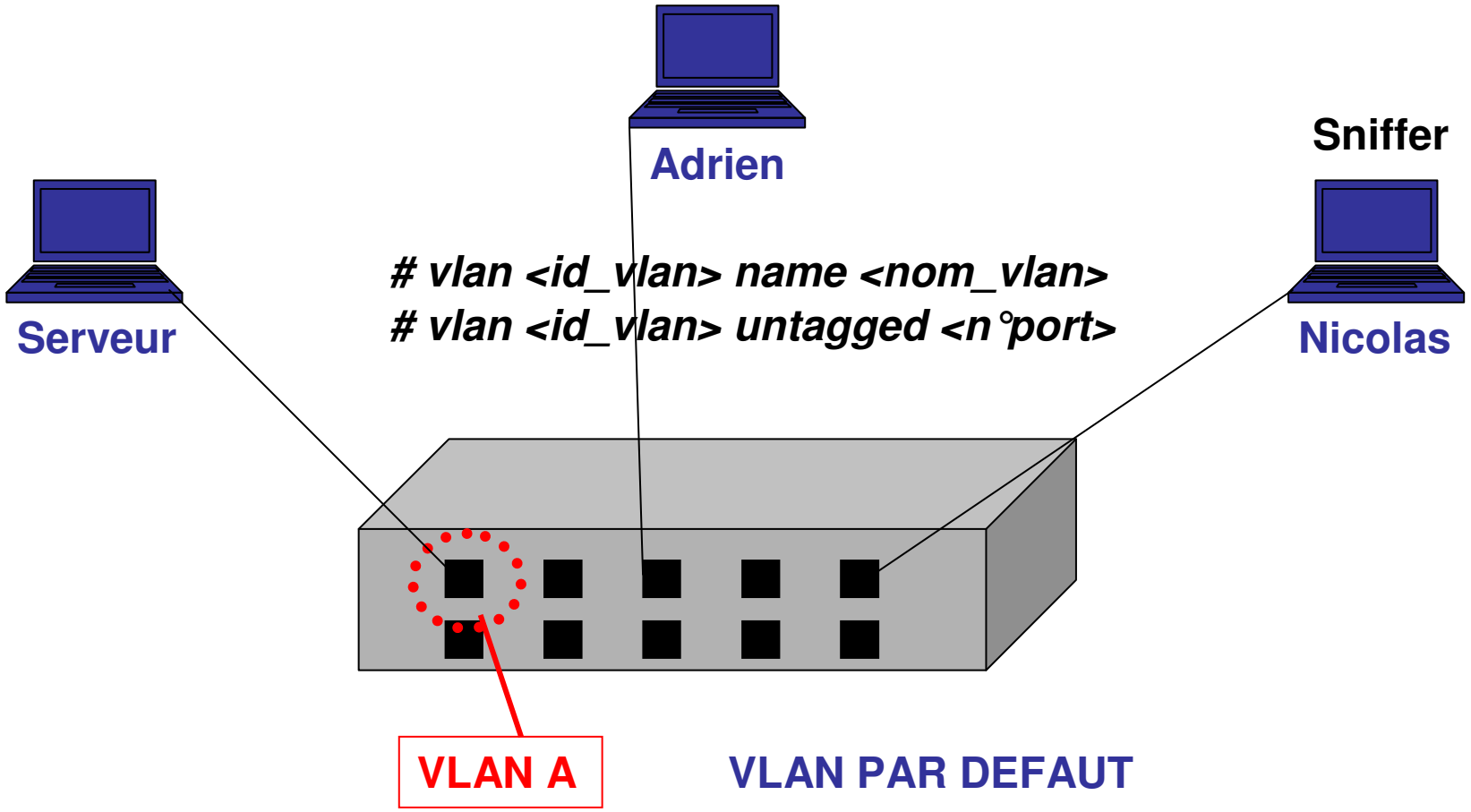
VLAN - Démonstration

Situation 1 : VLAN DEFAULT



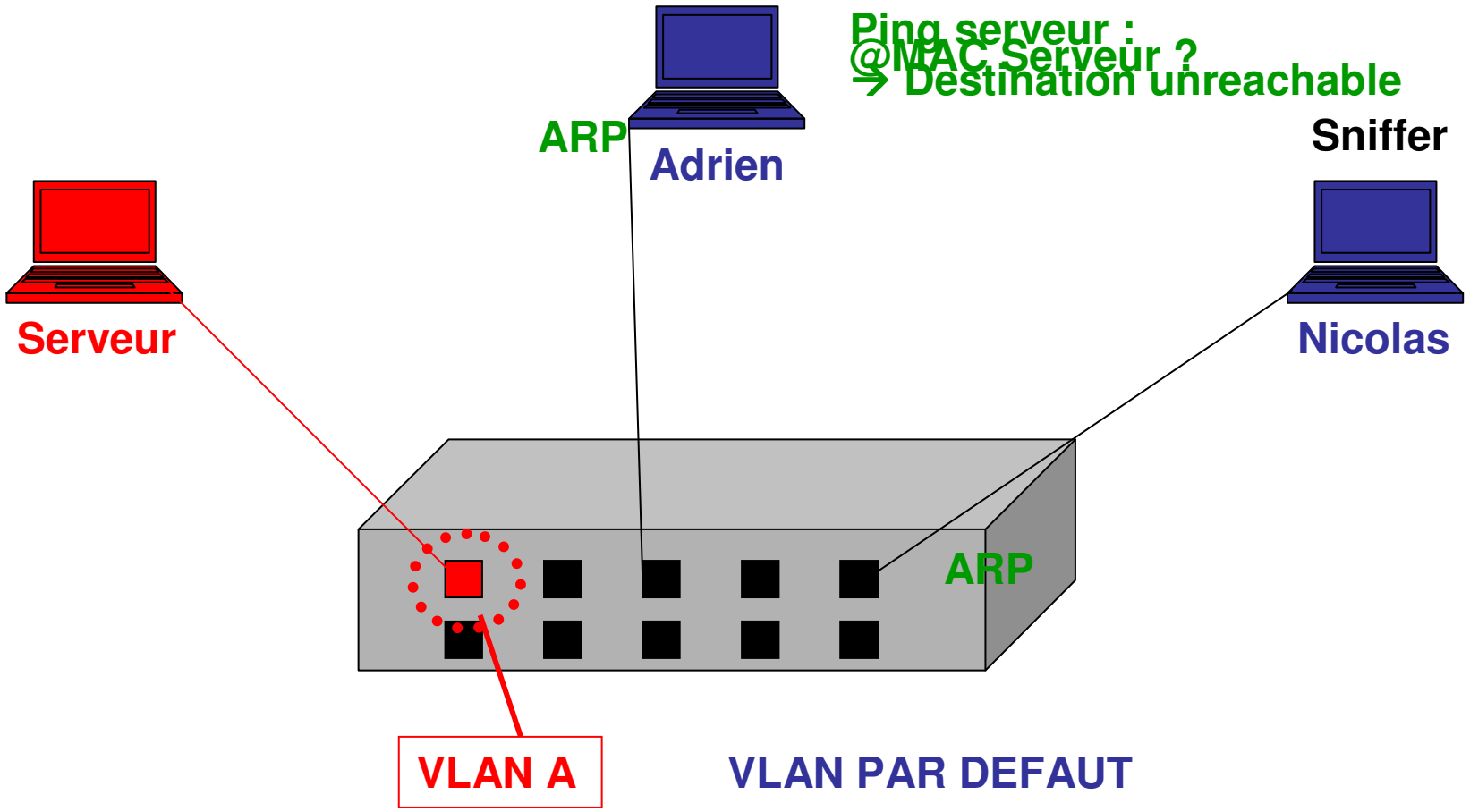
VLAN - Démonstration

Situation 2 : Serveur dans VLAN « A » , Adrien & Nicolas dans VLAN DEFAULT



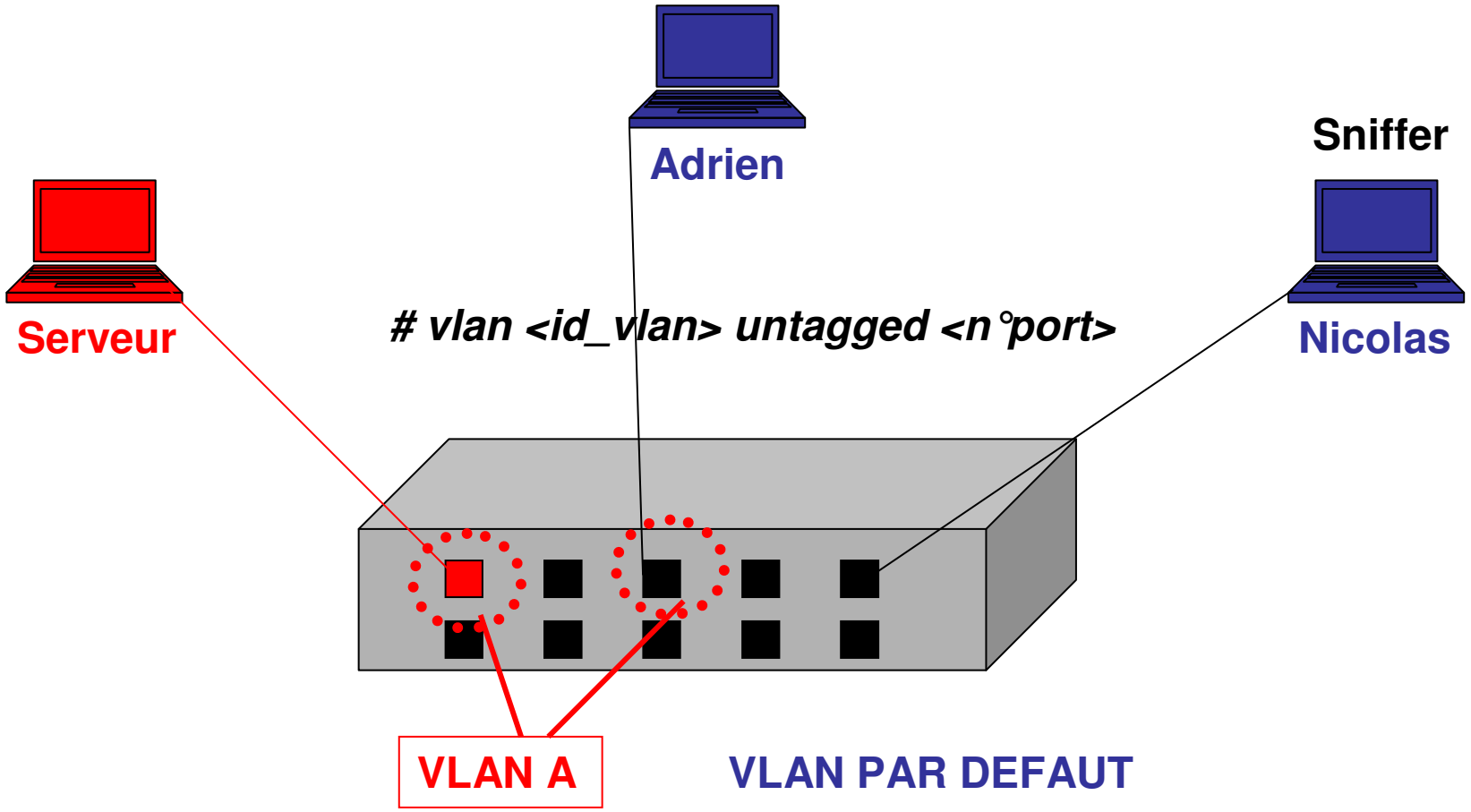
VLAN - Démonstration

Situation 2 : Serveur dans VLAN « A » , Adrien & Nicolas dans VLAN DEFAULT



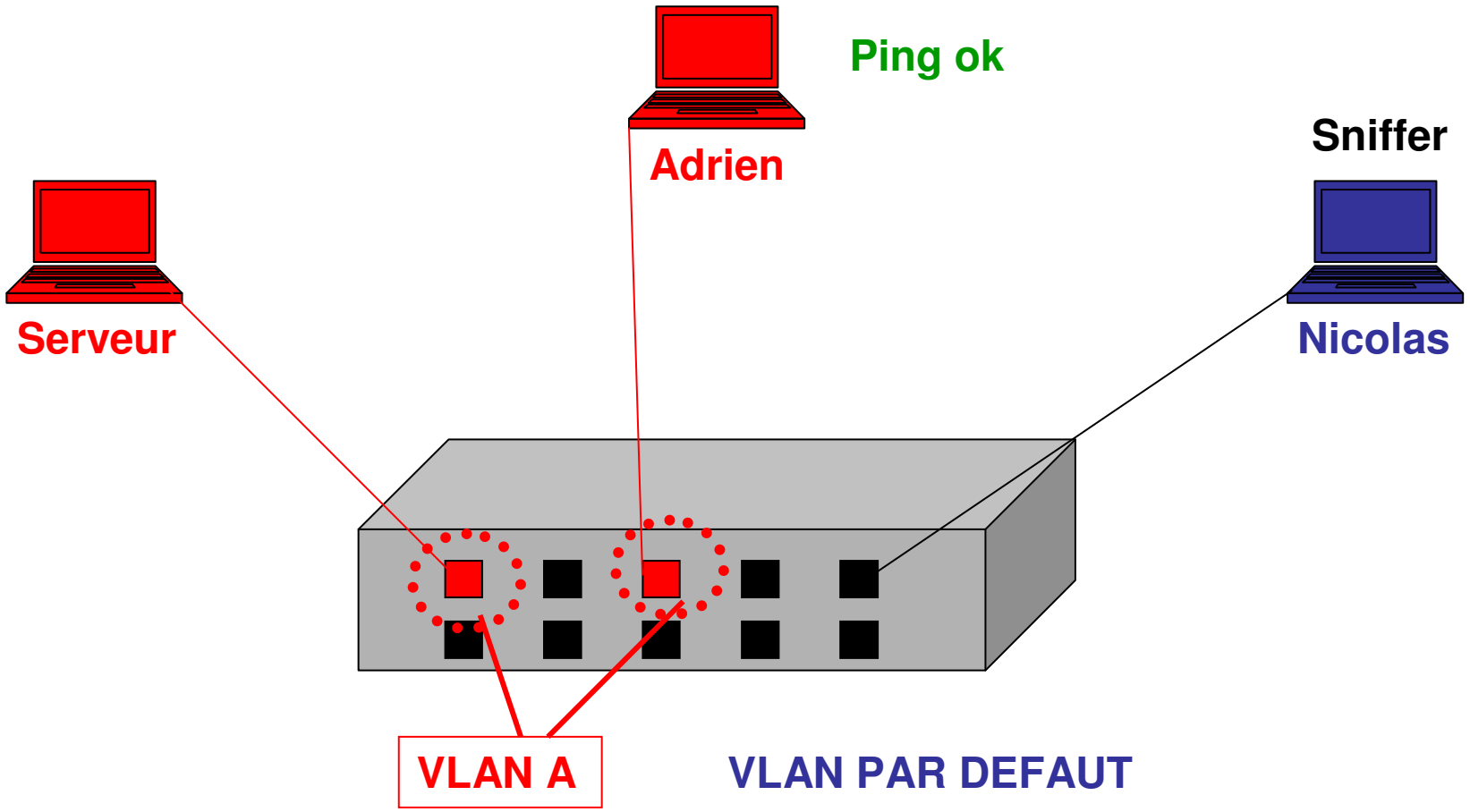
VLAN - Démonstration

Situation 3 : Serveur & Adrien dans VLAN « A » , Nicolas dans VLAN DEFAULT



VLAN - Démonstration

Situation 3 : Serveur & Adrien dans VLAN « A » , Nicolas dans VLAN DEFAULT



VLAN - Avantages

Performances :

- Permet à des utilisateurs éloignés géographiquement de partager des données
- Limite la diffusion des broadcasts

Sécurité :

- Séparation des flux entre différents groupes d'utilisateurs

Finances :

- 1 seul équipement pour plusieurs réseaux

802.1Q - Problématique 1/2

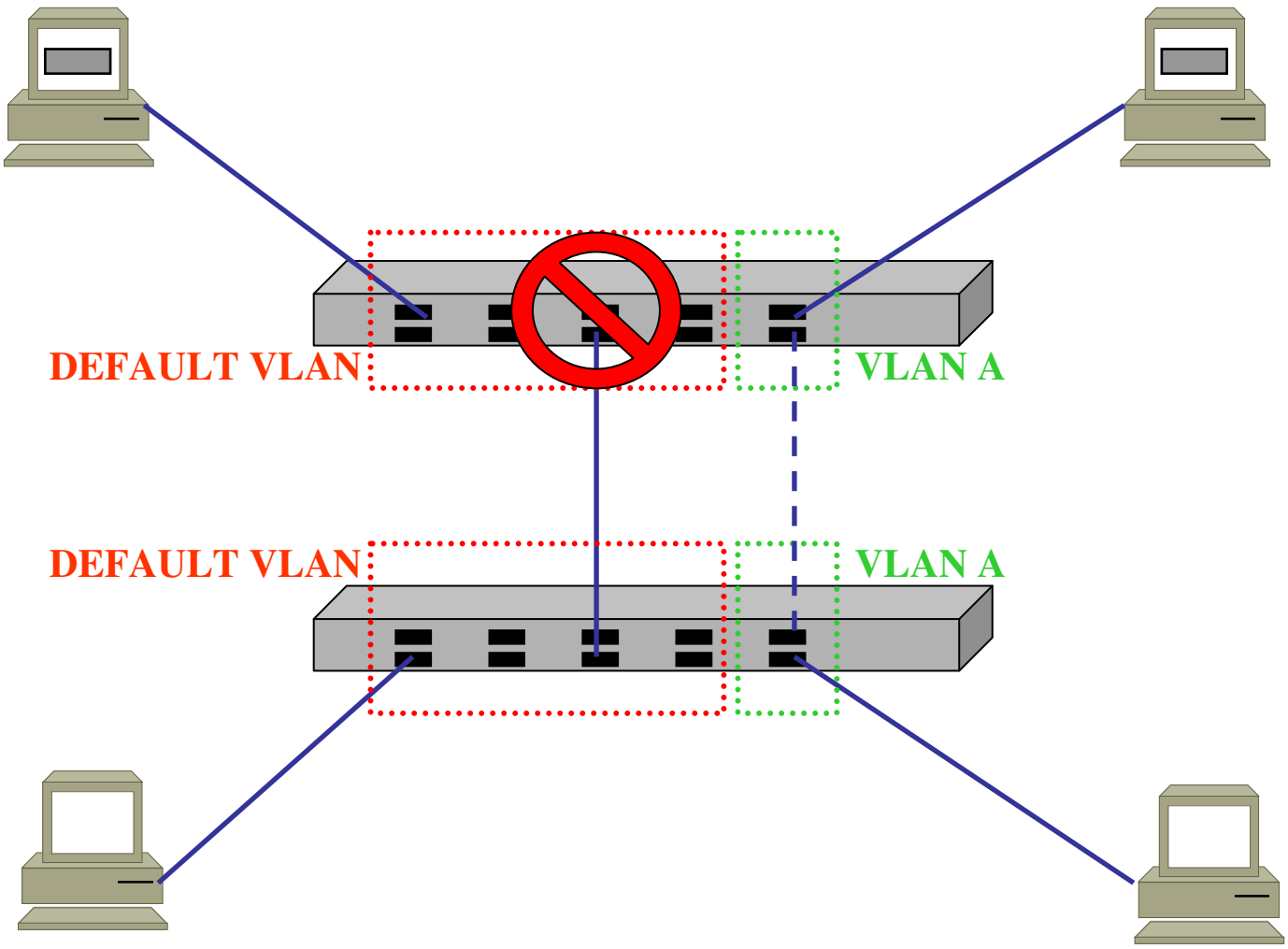
✓ Notion de vlan au niveau du commutateur

✓ Mais jusqu'à présent, aucune notion de vlan au niveau Ethernet ni à des niveaux supérieurs

➢ Donc comment propager l'appartenance à un VLAN d'un commutateur vers un autre ?

<u>Problématique :</u> lorsqu'une trame circule d'un commutateur à un autre, comment identifier son appartenance à un vlan ?

802.1Q - Problématique 2/2



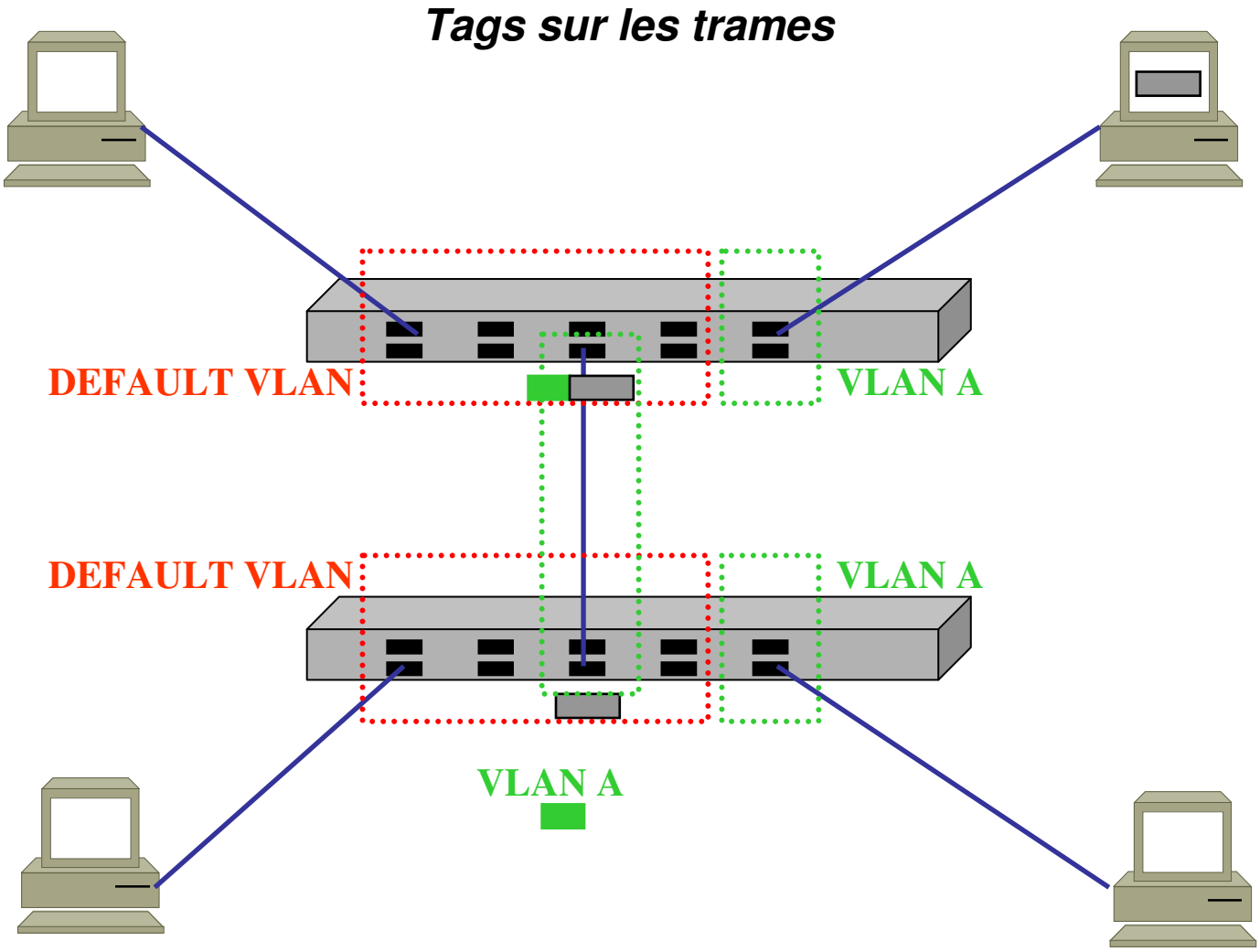
802.1Q - Théorie 1/2

Objectif : Transport de plusieurs VLANs sur un lien unique, par exemple :

- Commutateurs / Commutateurs
- Commutateurs / Serveurs

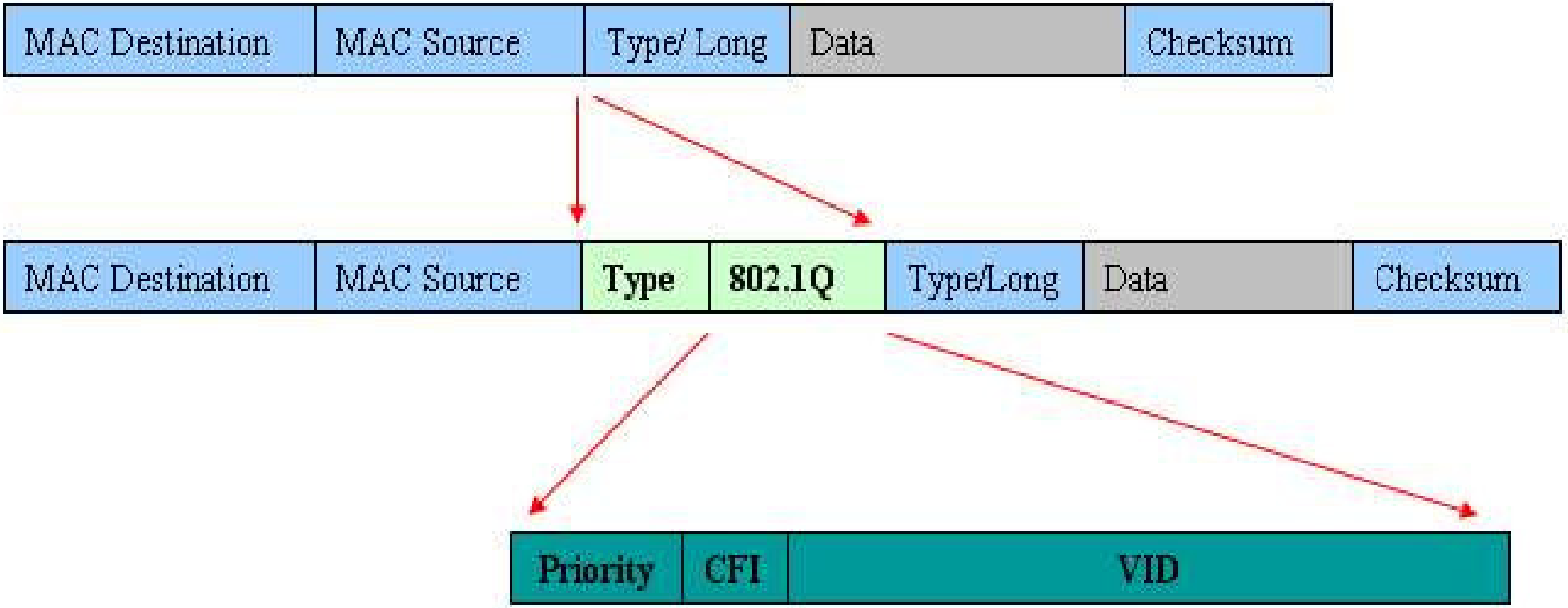
- Cela implique donc :
  - nécessité de définir les mêmes VLANs sur chaque commutateurs (même VLAN Id)
  - les trames doivent être taggées lors du transfert

802.1Q - Théorie 2/3



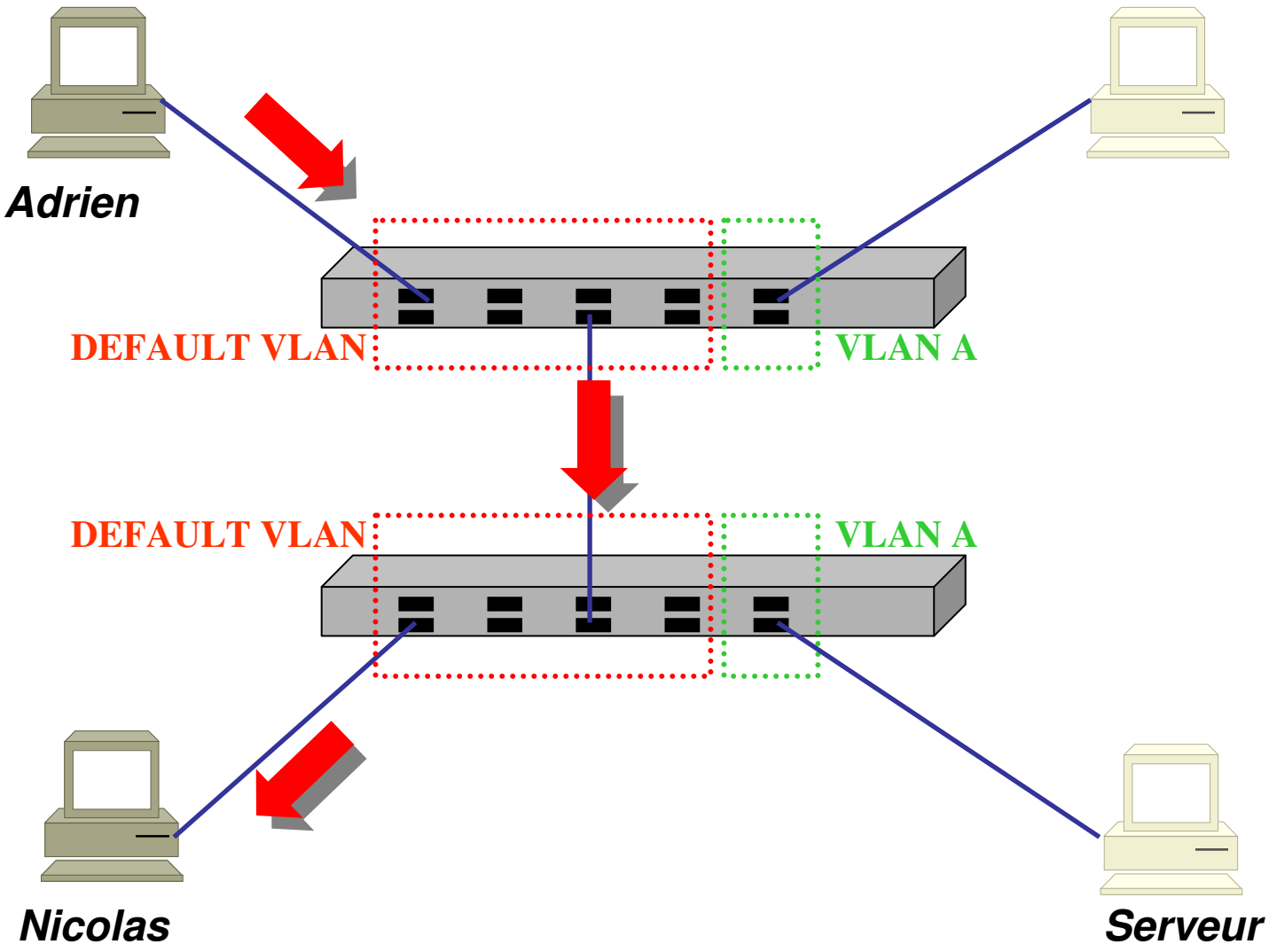
802.1Q - Théorie 3/3

- Extension du format Ethernet, ajout de 4 octets

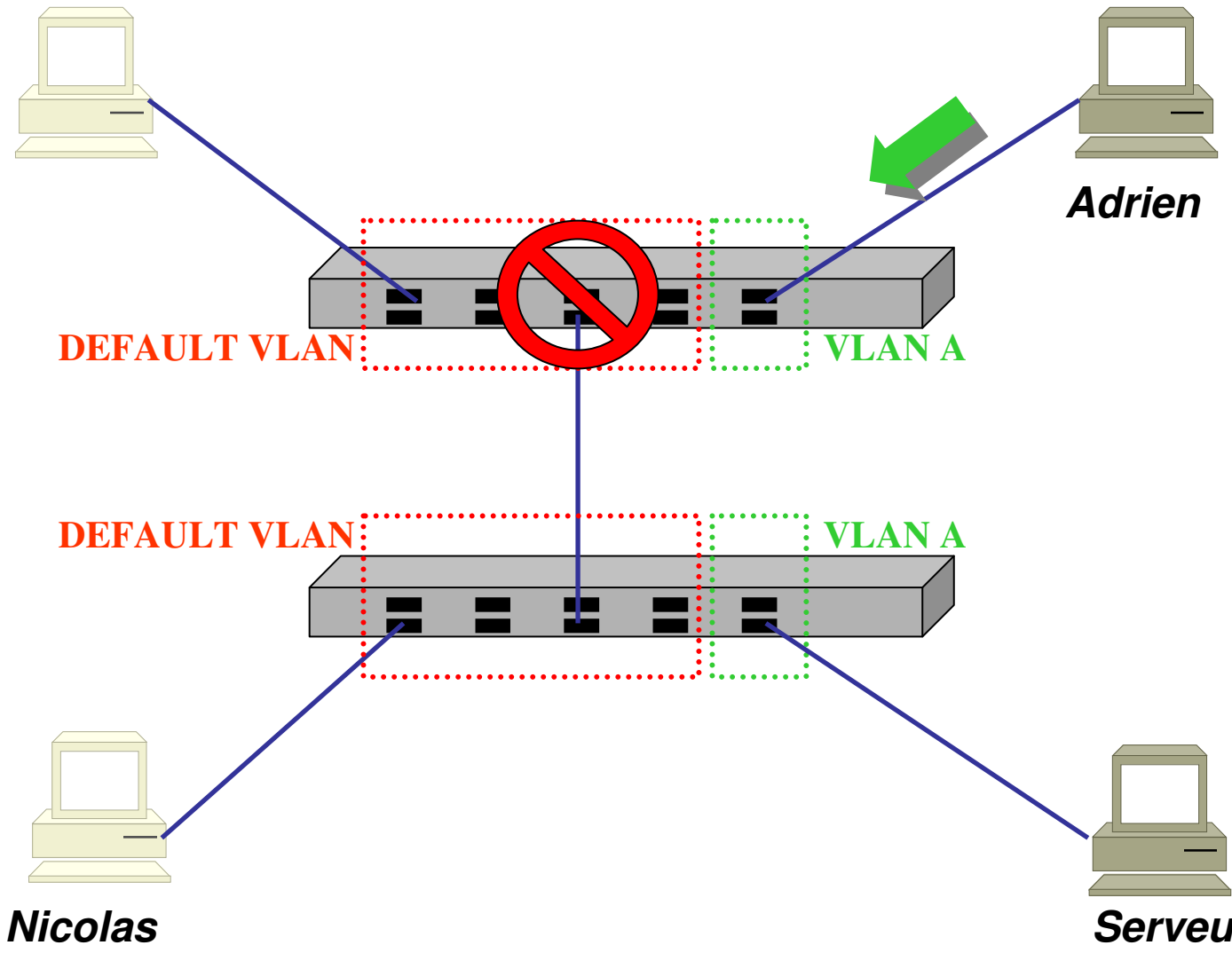


- Type : « 0x8100 » pour le protocole 802.1Q
- 802.1Q :
  - Priority (3 bits)
  - CFI (1 bit)
  - VID (12 bits)

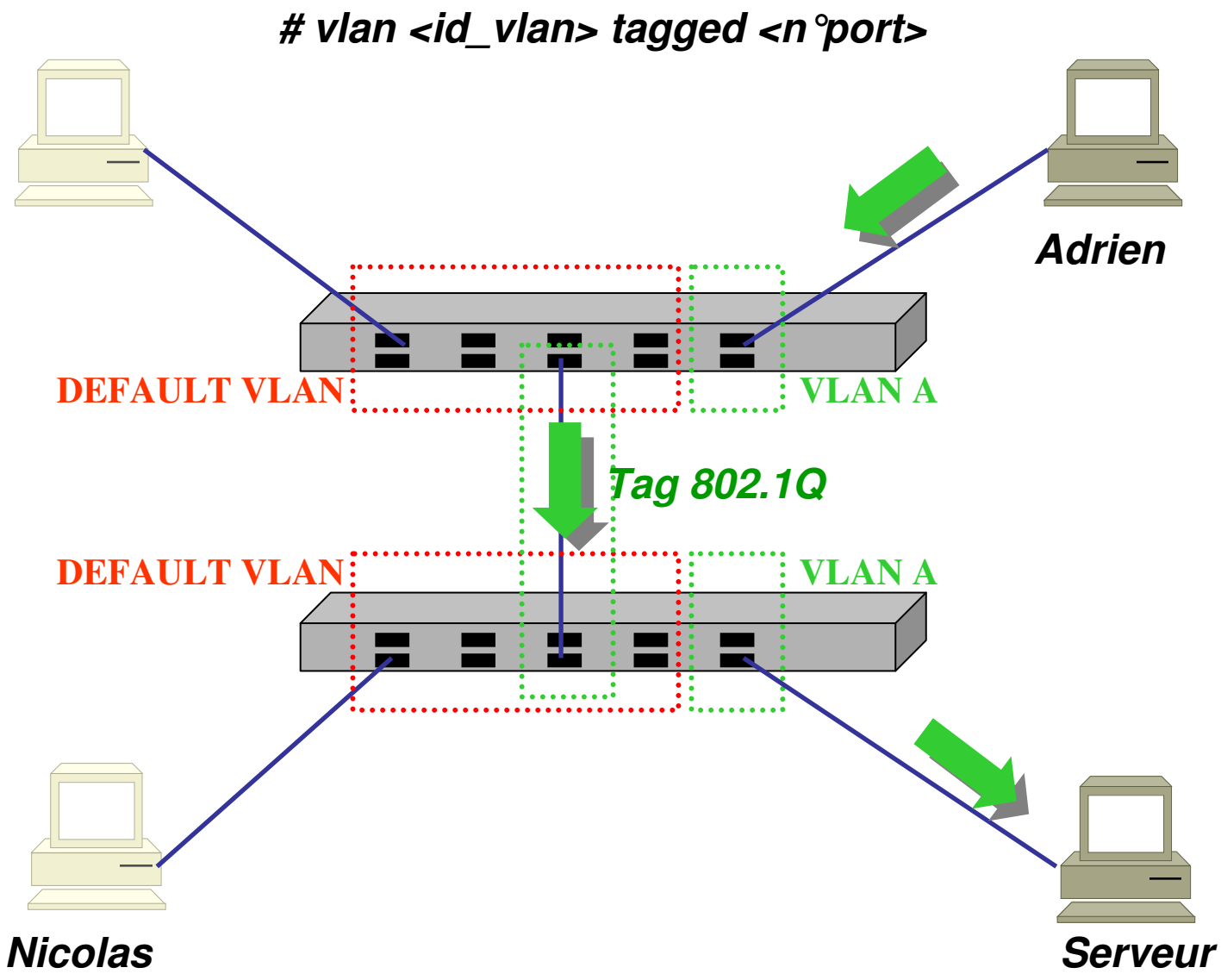
802.1Q – Démonstration 1



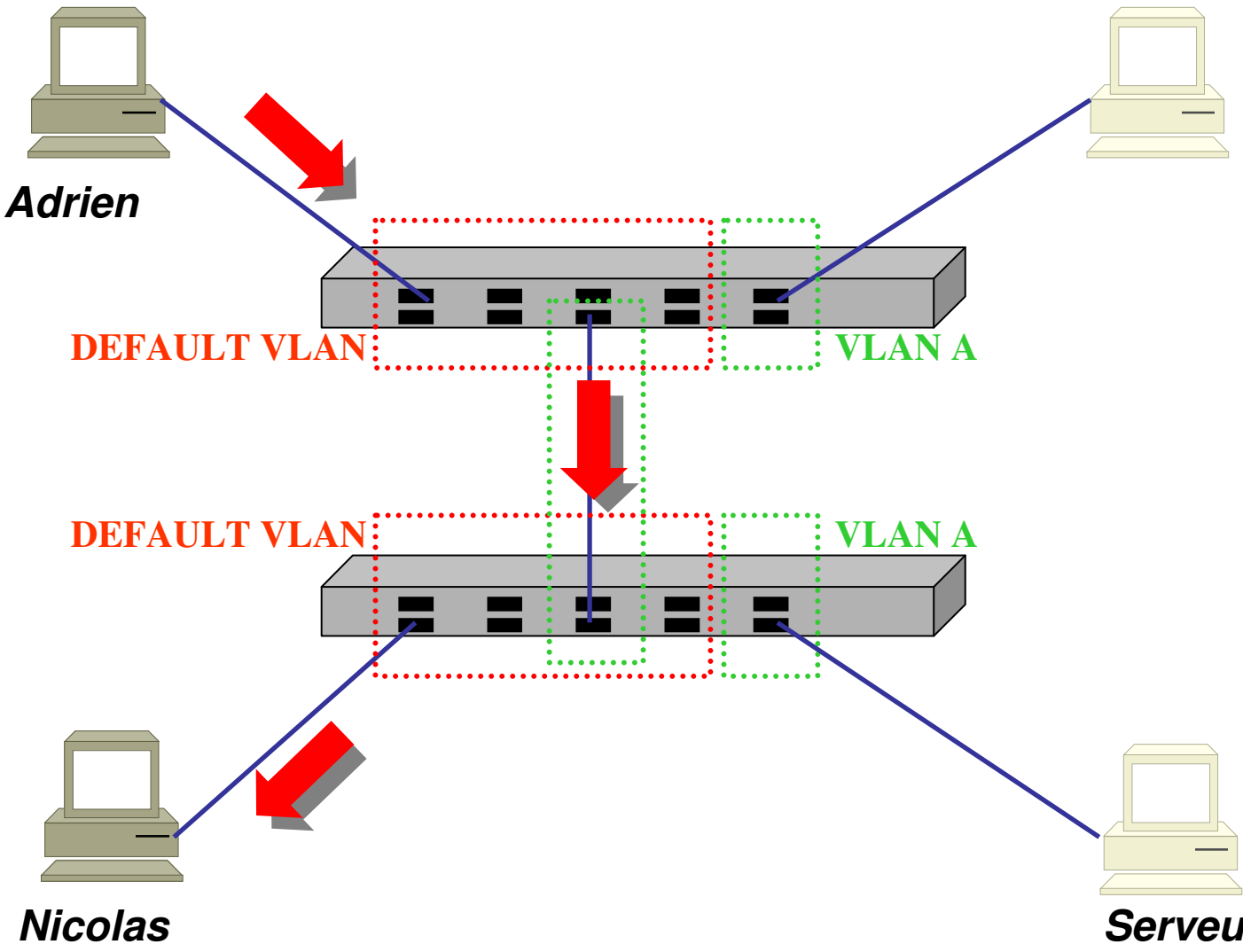
802.1Q – Démonstration 2



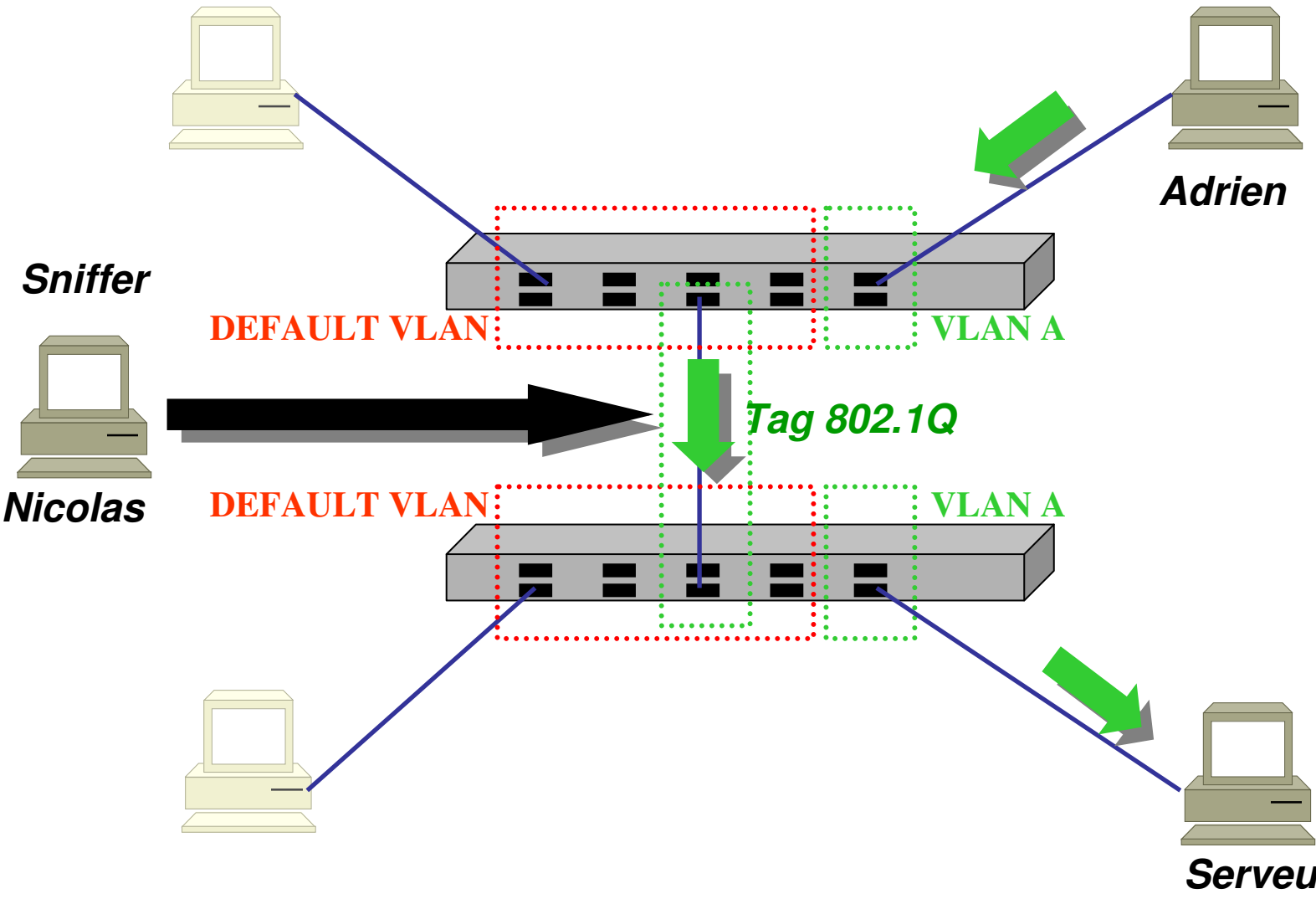
802.1Q – Démonstration 3



802.1Q - Démonstration 4



802.1Q – Démonstration Snif Snif



802.1s - Introduction

Architecture réseau des entreprises importantes :

- nombreux vlans
- 802.1Q
- redondance de niveau 2 : STP
- liens souvent surdimensionnés

=> avantages des vlans et du STP : 802.1s

802.1s - Théorie

- 802.1s = MSTP = PVST
- Une instance STP par vlan au lieu d'une par boite
- Complexe à mettre en place (au niveau conception)
- Technologie récente, pas encore supportée par tous les matériels

802.1s – Objectifs / Limitations

Objectifs :

- Meilleure utilisation des liens
- Temps de convergence de 3 secondes
- Redondance de niveau 2 accrue

Limitations :

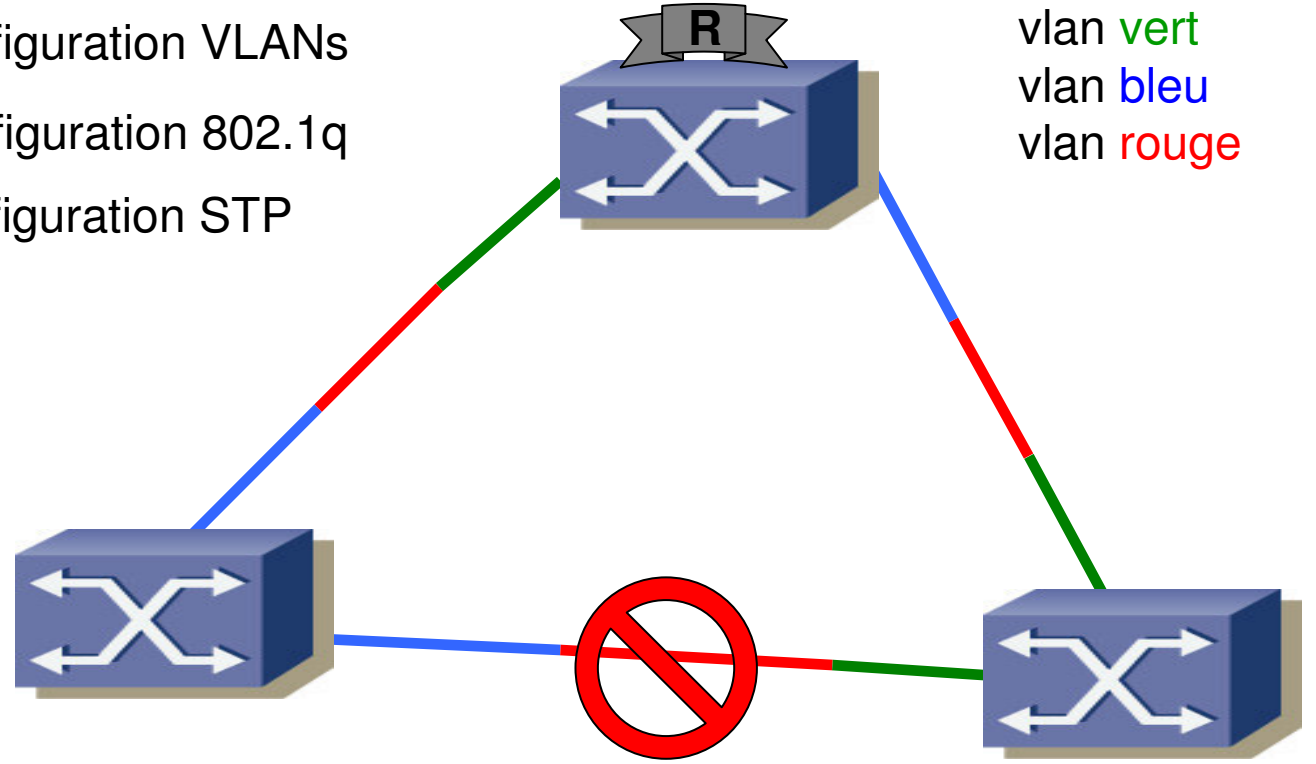
- Matériels limités en nombre d'instances
- Peu de softs snmp savent gérer 802.1s

802.1s – Exemple sans MSTP (1/2)

1/ Configuration VLANs

2/ Configuration 802.1q

3/ Configuration STP



vlan vert
vlan bleu
vlan rouge

vlan vert
vlan bleu
vlan rouge

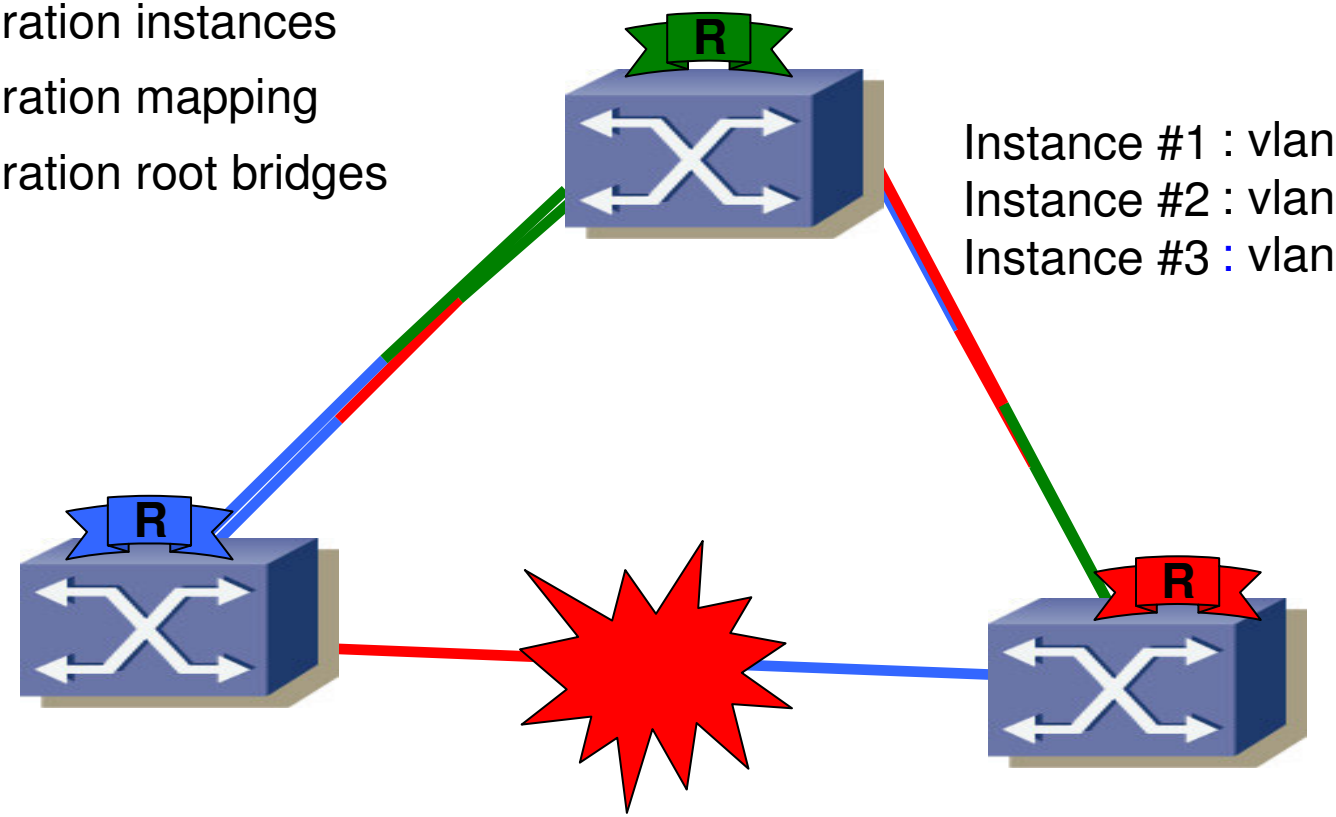
vlan vert
vlan bleu
vlan rouge

802.1s – Exemple avec MSTP (2/2)

1/ Configuration instances

2/ Configuration mapping

3/ Configuration root bridges



Instance #1 : vlan vert
Instance #2 : vlan bleu
Instance #3 : vlan rouge

Instance #1 : vlan vert
Instance #2 : vlan bleu
Instance #3 : vlan rouge

Instance #1 : vlan vert
Instance #2 : vlan bleu
Instance #3 : vlan rouge

802.1x - Introduction

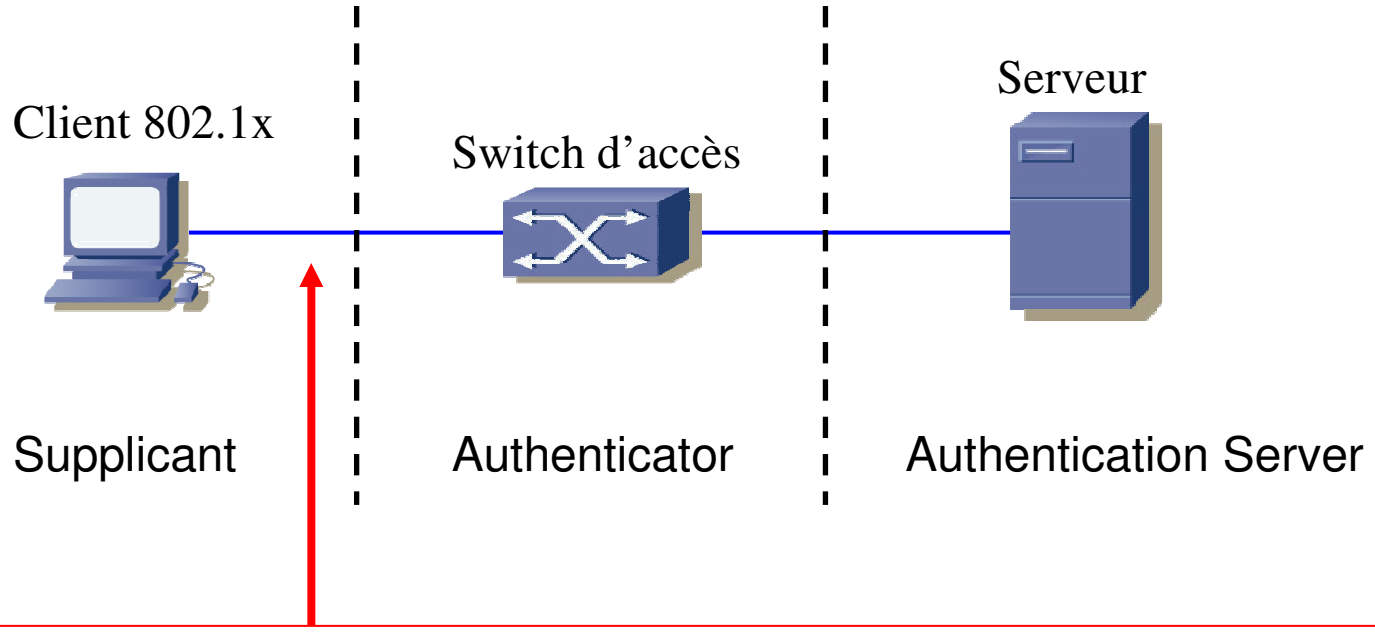
• Permet l'élaboration de mécanismes d'authentification et d'autorisation pour l'accès au réseau

• Se développe grâce au WiFi

• Norme développée à l'origine pour les VLANs

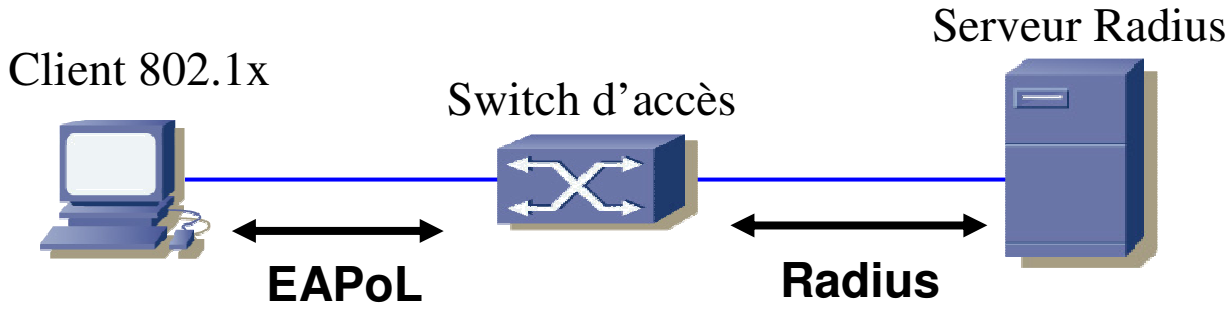
=> Attribution d'un VLAN en fonction de l'identification

802.1x - Architecture



- Avant authentification : seul trafic nécessaire à l'authentification est permis
- Après authentification : tout trafic

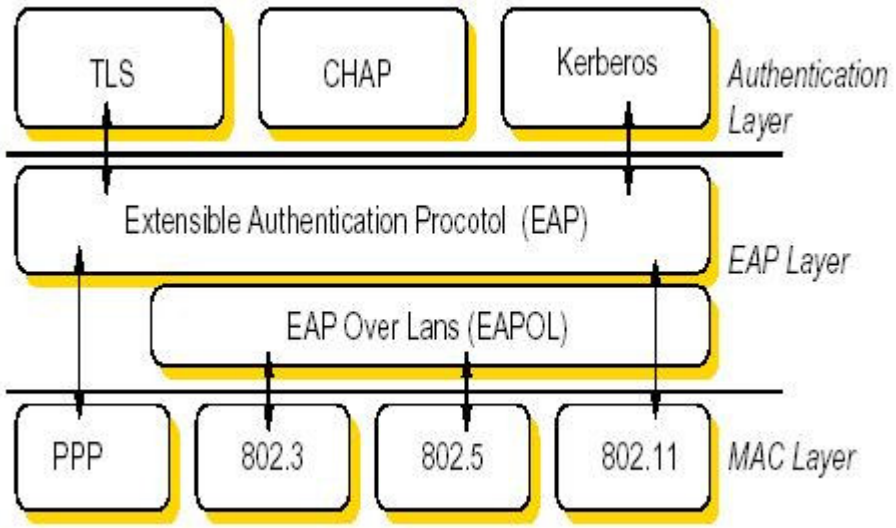
802.1x - Protocoles



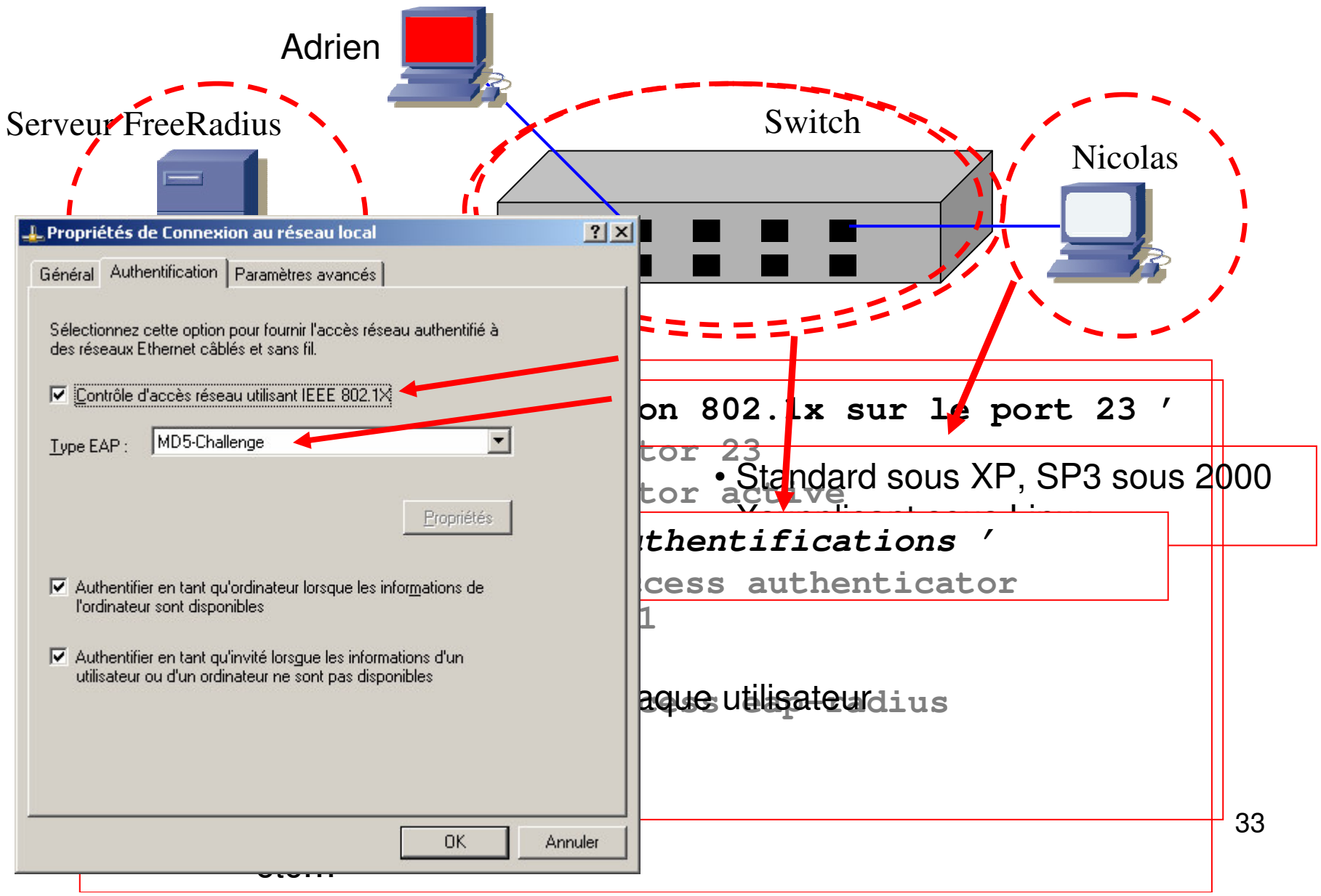
- EAP au dessus du réseau local : EAPOL (EAP over LAN)
- EAP peut encapsuler plusieurs types de protocoles d'authentification :
  - MD5
  - TLS
  - TTLS

- Le commutateur joue le rôle

- Le protocole Radius encaps
- Le serveur Radius pourra s
soit sur un annuaire LDAP



802.1x – Démonstration




DEBIAN
RIP
PLOO 2005