INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Automatisation du réseau

Louis Chanouha pour Capitoul

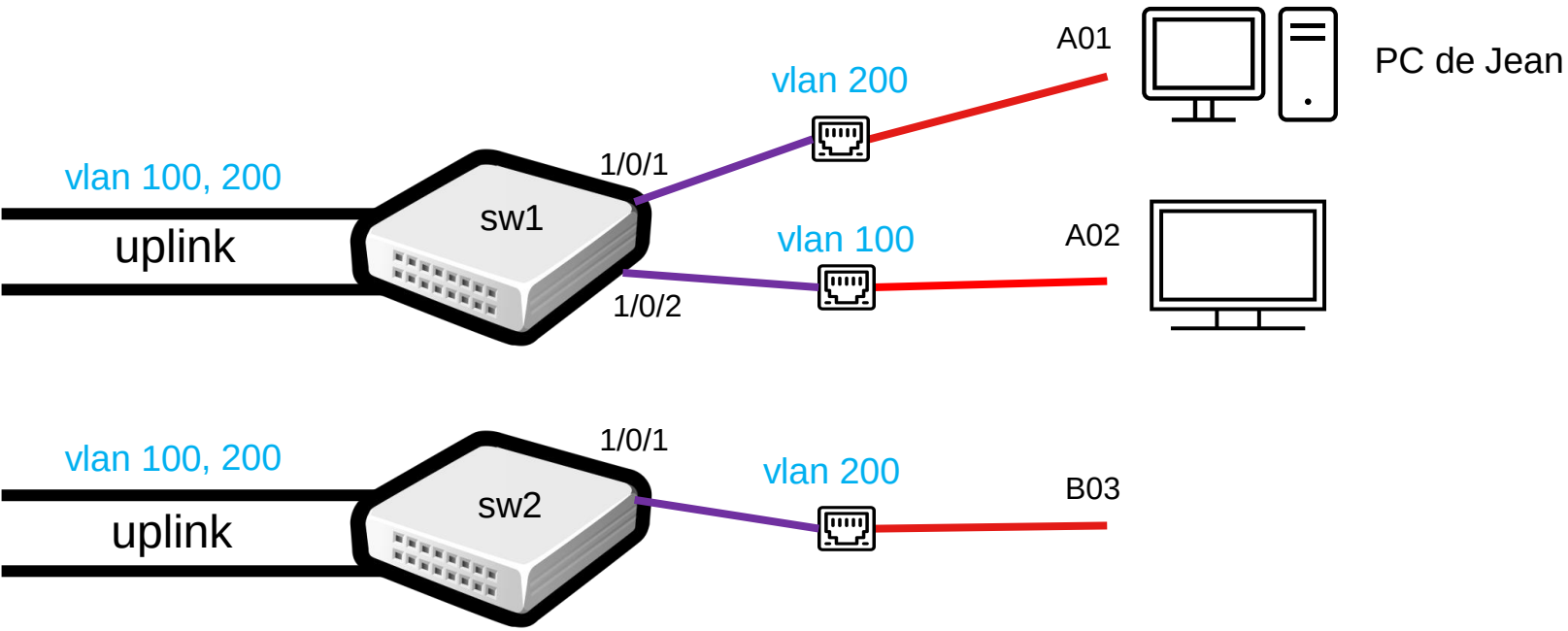
LAAS CNRS - 19/04/2023

Introduction

Projet « Améliorer la mobilité des utilisateurs à l'INSA »

2022-2023 (et +)

Exploitation d’un réseau statique (1)




```
vlan 100, 200
interface uplink
  port trunk permit vlan all
interface GI1/0/1
  description port A01
  port access vlan 200
interface GI1/0/2
  description port A02
  port access vlan 100
```

PC de Jean se déplace en B03 dans autre bâtiment

1. Identification du switch et du port
2. Brassage *B03 sur port sw2: 1/0/3*
3. Configuration N2 *ajout vlan sur uplink + chaîne*
4. Assignation du VLAN sur la prise
5. Màj documentation / Communication

Exploitation d’un réseau statique (2): Problématiques

- Usager: nomadisme
  - + Meilleure connectivité dans salles de réunion et bureaux partagés ?
  - + (plus d’)autonomie lors de déplacement / réaménagement bureaux
  - + Étudiants / invités: alternative au WiFi
  - + Éviter VPN sur Wifi

- Service informatique
  - + Exploitation:
    - Industrialiser la gestion de ~ 90 VLANs clients, > 150 actifs sous différents OS
    - Faciliter changements N3 (création / réajustement de VLANs)
  - + Sécurité
    - Authentification du poste repose sur DHCP (donc adresse Mac)

Nouvelles notions

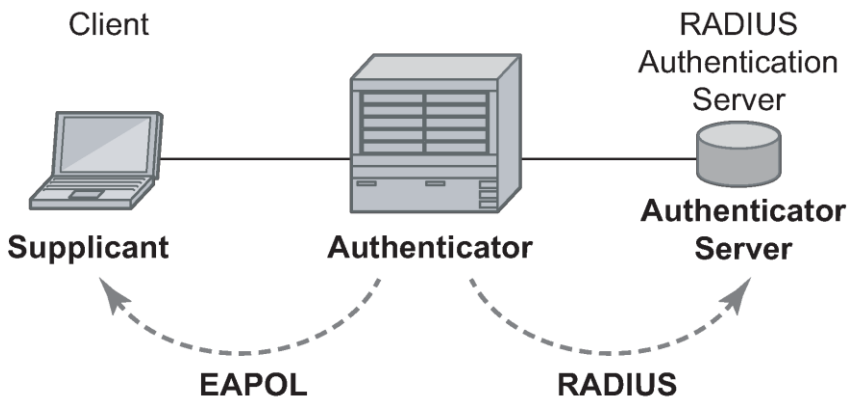
Notions (1): Port non coloré

- Prise « générique », interchangeable
  - + configuration selon le périphérique connecté
  - + l'emplacement n'importe plus
  - + comment identifier le périphérique ?
    - Par adresse MAC: imprimantes, IOT, sondes…
    - Par 802.1X (802.1x) : parc fixes et portables personnels…
  - + Configuration = VLAN

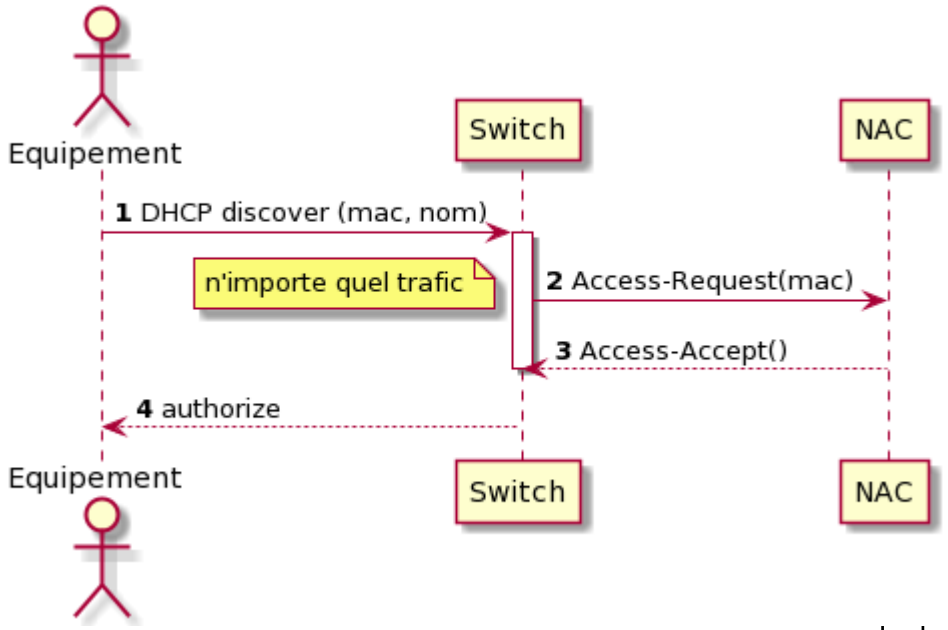
Notions (2): Le NAC

- Network Access Control
  - Le switch authentifie le client auprès du NAC

IEEE 802.1X



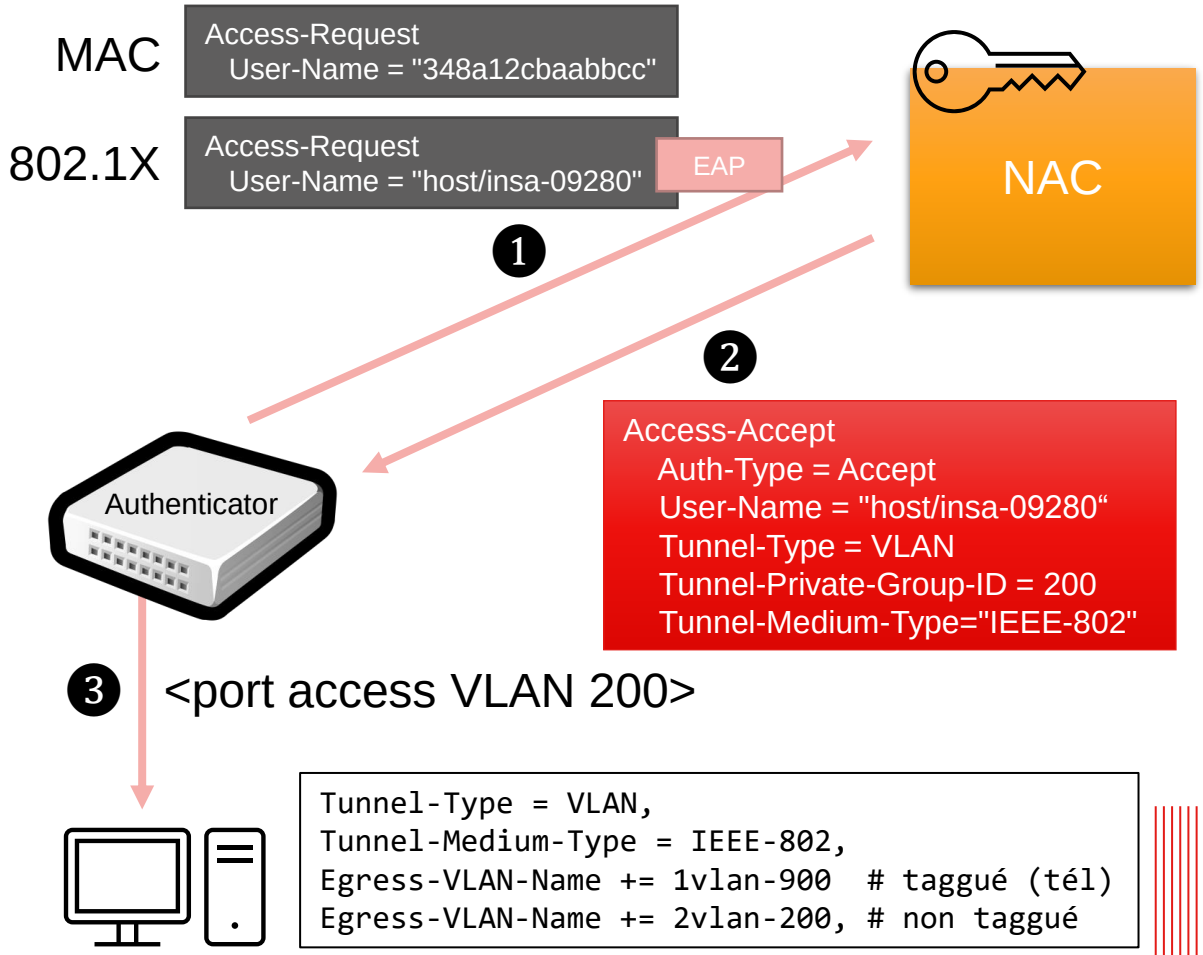
Mac



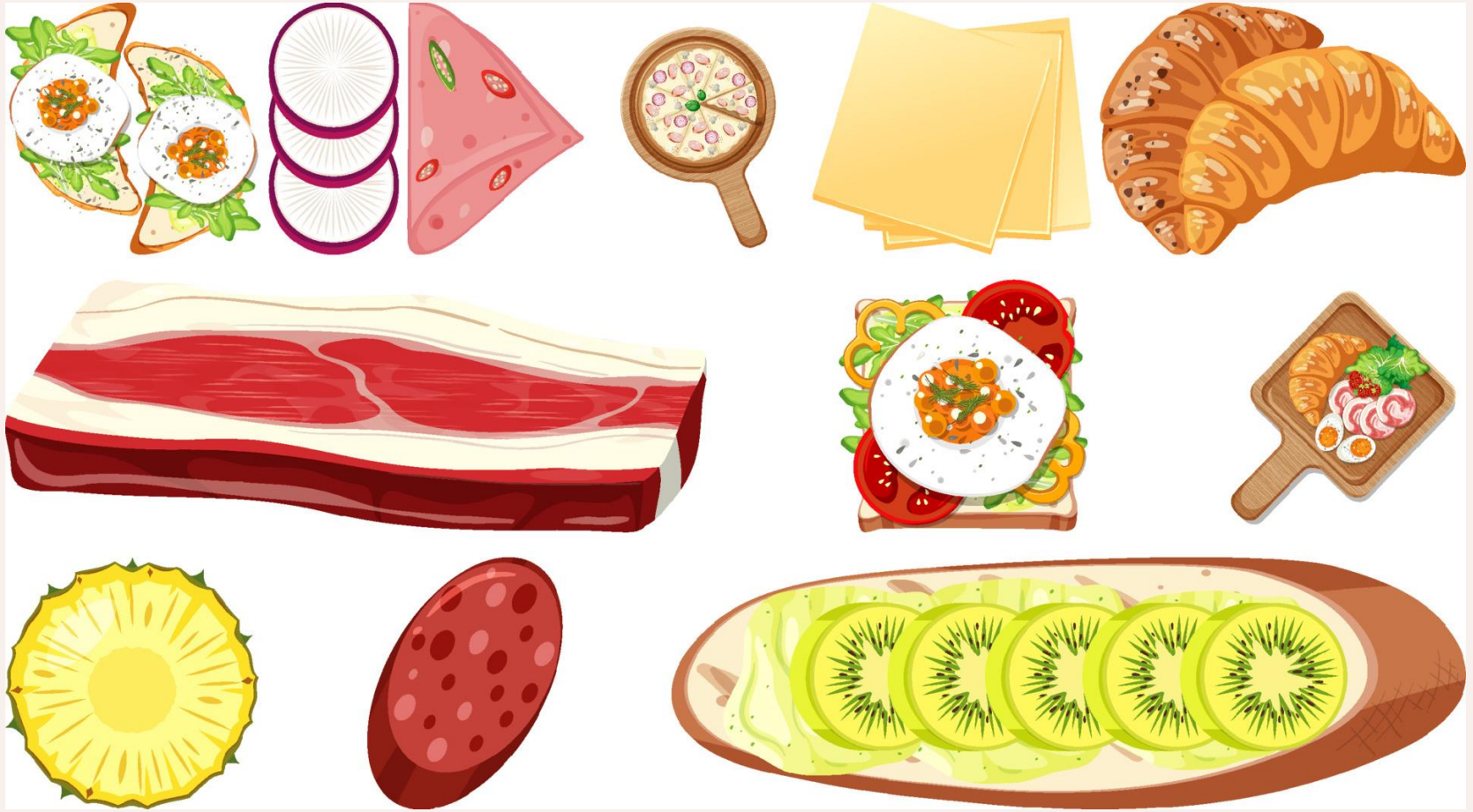
Notions (3): La RFC 2868 (Juin 2000)

- Définit les attributs
  - + Tunnel-Type = VLAN
  - + Attribut Tunnel-Private-Group-ID
    - Access VLAN
  - + Renvoyés par le NAC à l'authenticator

- RFC 4675 (2006)
  - + Egress-VLANID / Egress-VLAN-Name
  - + 802.1Q (trunk)



1. Authenticator transfère demande au NAC
2. Le NAC renvoie des informations sur le réseau
3. Le switch configure la prise



La cuisine INSA

trouver sa configuration réseau

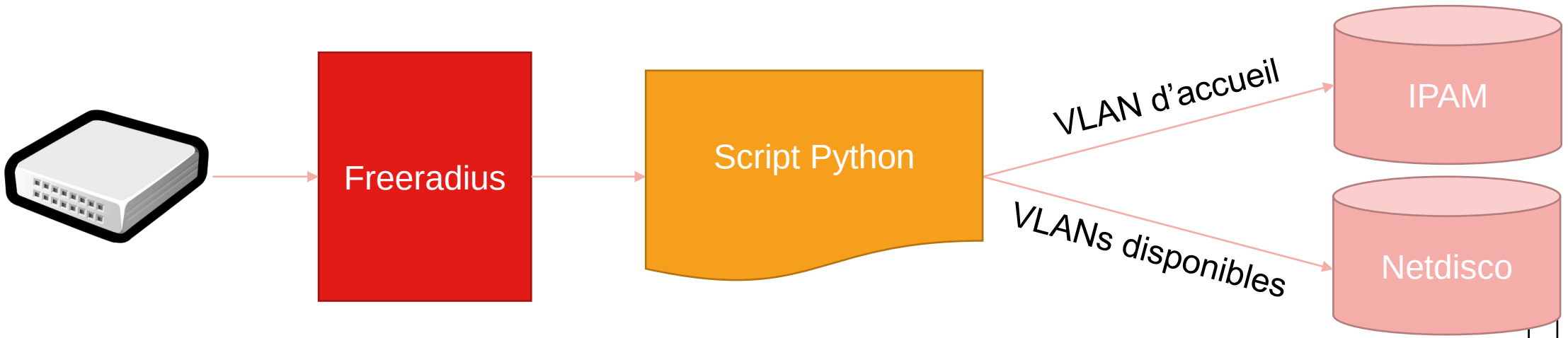
(not) a poor’s man solution

La cuisine INSA (1): le référentiel

- Quel configuration réseau ?
  - + Depuis un référentiel: l'IPAM => IP actuelle !

La cuisine INSA (2): des règles métier

- Programmer des règles
  - + Toujours fournir une connectivité
    - Bascule sur réseau intermédiaire si VLAN pas disponible sur le SW => comment ?
    - Bascule sur réseau invité (portail captif) si échec d'identification
  - + 802.1x requis, mais Mac suffisant pour:
    - IoT, Imprimantes, enseignement…
    - Switchs du service informatique (atelier): netboot / déploiement WSUS par ex
  - + ToIP, IoT: VLAN / préfixes MAC raspberry PI, postes SIP



La cuisine INSA (3): sous le capot

- 802.1X: authentification par certificat x509
  - Déploiement d'un certificat auto-renouvelé tous les 4 mois via PKI ADCS (Microsoft)
  - Protocole EAP-TLS, authentification machine (nom DNS dans entrée AD)

- Architecture Radius
  - Freeradius

```
update { control: += `getVLANAssignedToMachine --auth-hostname '%{TLS-Client-Cert-Common-Name}' --switch-name '%{NAS-Identifier}' }
```

  - Script Python

```
availableVLANs = findActiveVLANOnNetDisco(args.switch_name)
user_vlans     = lookupVLANOnIPAM(args.auth_hostname, args.switch_name)

# Attribution du VLAN
vlan = next(v for v in user_vlans if v in availableVLANs)

if user_vlans and not vlan: # reseau intermédiaire (user_vlan pas sur le SW)
   vlan = 3230

print ("Auth-Type = Accept" )
print ("Tunnel-Private-Group-ID = %s" % vlan)
```

~300 lignes de code

La cuisine INSA (4): configuration de switches

- Switchs
  - HP ProCurve

```
aaa authentication port-access eap-radius
aaa port-access gvrp-vlans


aaa port-access authenticator active
aaa port-access authenticator 1-16 client-limit 8
aaa port-access authenticator 1-16

aaa port-access mac-based 1-16
aaa port-access mac-based 1-16 addr-limit 10
aaa port-access mac-based 1-16 unauth-vid 3200

aaa port-access 1-16 controlled-direction in
```

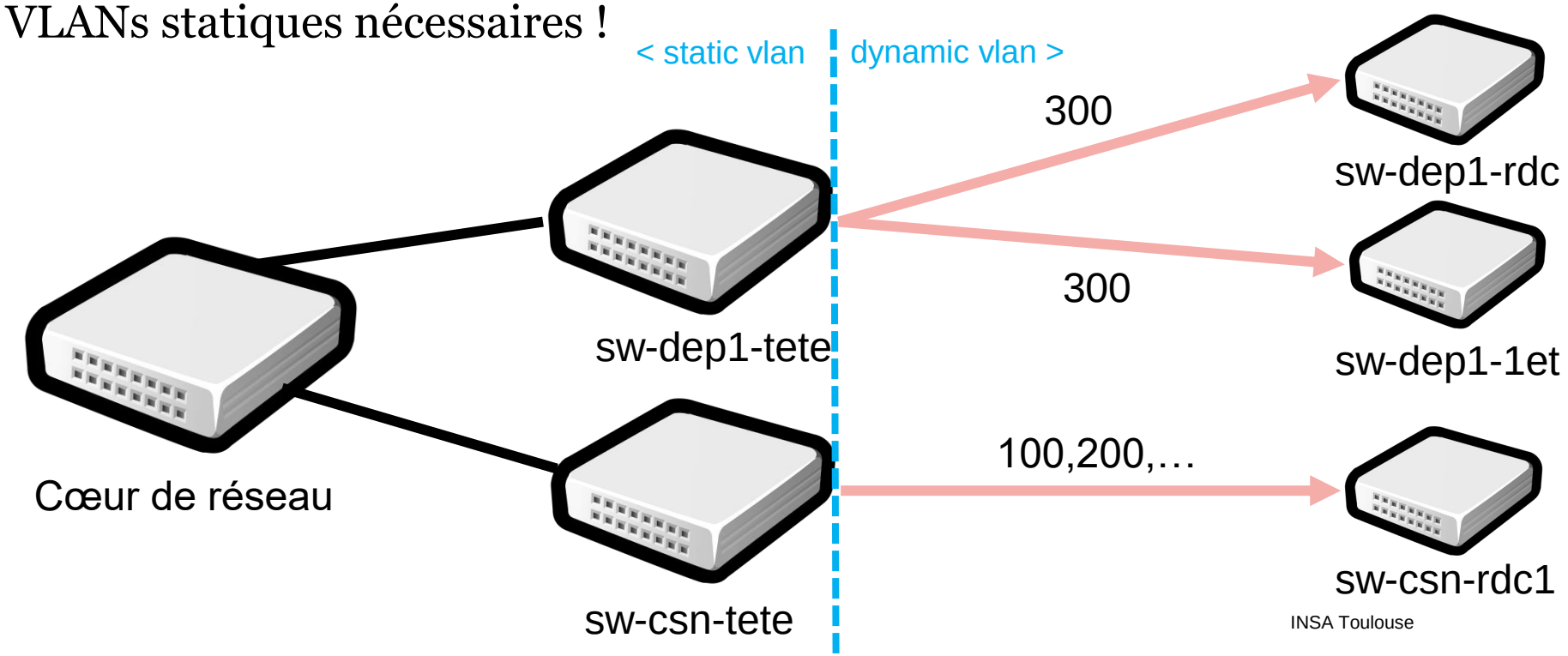
  - HP Comware

```
dot1x authentication-method eap
mac-authentication user-name-format
mac-address with-hyphen lowercase
mac-authentication authentication-method chap
port-security enable
port-security authentication open global

interface GigabitEthernet1/0/16

port access vlan 3001
dot1x guest-vlan 3001
dot1x auth-fail vlan 3001
dot1x critical vlan 3001
mac-authentication timer auth-delay 4
mac-authentication guest-vlan 3001
mac-authentication critical vlan 3001
mac-authentication parallel-with-dot1x
port-security port-mode userlogin-secure-or-mac-ext
```

Autres vecteurs d’amélioration

Faciliter le déploiement de réseaux

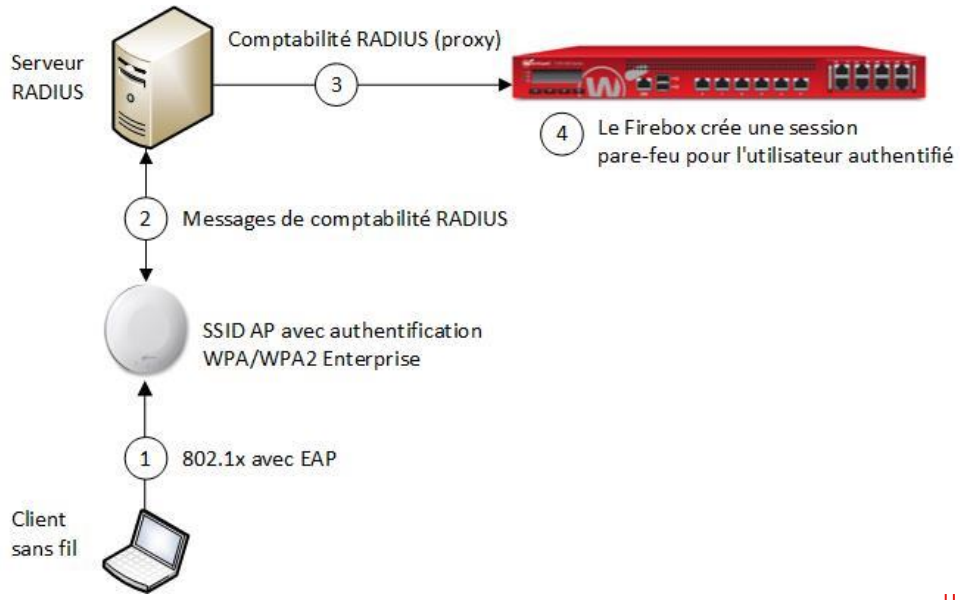
- Porter automatiquement les VLAN
  - Protocole MVRP (Multiple VLAN Registration Protocol)
  - Portage depuis les têtes de département à l'INSA (réseau en étoile)
    - Cœur de réseau ne supporte pas
  - 2 VLANs statiques nécessaires !



Identification de l'utilisateur en mobilité

- Radius-Accounting
  - Tracer les connexions des utilisateurs lors d'une authentification 802.1X

```
Accounting-Request
  Acct-Status-Type = Start
  NAS-IP-Address = 192.168.45.78
  User-Name = jdoe@insa-toulouse.fr
  Framed-IP-Address = 10.32.99.99
  Aruba-Essid-Name = "eduroam"
  Aruba-Location-Id = "CSN-AP01"
```



  - Traité par l'équipement de sécurité (FW)
    - FortiGate RSSO
  - Distinguer le client pour politique de sécurité
    - X509 (postes gérés)
    - PAP (mot de passe): téléphones, PCs persos (BYOD)

Bilan

Bilan (1): Mobilité

Profil	
Administratif	• peut connecter son PC **indifféremment sur toutes les prises à l'INSA** • peut utiliser **indifféremment le filaire et le Wifi:** les accès sont identiques
Service informatique	• peut tester **les accès réseaux d'une machine utilisateur en conditions réelles sur toutes les prises du service,** • peut se connecter sur toutes les prises, mais **sera sur un réseau limité hors de son bâtiment**
Service patrimoine	• peut **brancher une sonde de température sur un actif à l'INSA** après avoir donné son @Mac au service informatique,
Étudiant, autre BYOD	• est redirigé **vers un portail captif.**

- Le confort est amélioré
  - + plus besoin d'une connexion VPN dans les locaux INSA
  - + EAP-TLS: connexion automatique et transparent sur nouveau PC

Bilan (2): sous le capot

- Déploiement de switches génériques
- Sécurité: connaissance à terme de tous nos clients sur notre réseau
  - + Directement sur le FW ! Y compris Wifi
- Problématiques
  - + Complexification du serveur Radius
    - Inter-dépendances système - réseau
    - Gestion d'incident système prises de secours
    - Prise en main par les équipes
  - + Diversité des switchs (Aruba, H3C, vieux Comware)
  - + Accounting: Wifi OK (Aruba 505/515), filaire NOK (`Framed-IP-Address manquant`)
- Déploiement
  - + Fait au service numérique
  - + En cours dans les départements au fur et à mesure des remplacements des switchs

Perspectives

- Quels actifs acheter ? On a fait avec l'existant
- Convergence des accès filaire, wifi (eduroam et portail captif), VPN
  - Passer d'une politique réseau à une politique utilisateur
  - Factorisation des réseaux et règles
  - Projet à mener avec le renouvellement du firewall (Fortinet RSSO / FSSO par ex.)
- Sécurité
  - filtrage N2 / fixage de l'IP client (RFC 4849)
  - Authentification SSH sur les switchs
  - Compromission d'un poste: isolation réseau
- Bonus: questions ouvertes ?
  - Tunneliser les réseaux métier (pratiques FAI)
    - Déploiement dans environnements non maitrisés
    - Centralisation des flux
  - Débat 🌳 : peut-on aller au-delà de la durée de ~~vie~~ garantie d'équipements interchangeables ?

```
Nas-filter-Rule += "permit in 1 from any to any"
Nas-filter-Rule += "deny in ip from any to 10.45.1.0/24"
Nas-filter-Rule += "permit in ip from any to any«
```

```
Tunnel-Type             = L2TP
Tunnel-Medium-Type      = IP
Tunnel-Assignment-ID    = "vlan300"
Tunnel-Server-Endpoint  = "193.65.245.200"
Tunnel-Client-Auth-ID   = "insa-09280"
Tunnel-Password         = "insainsainsa"
```