Formation Radius et 802.1x !

Sommaire:

- Radius, 802.1x, c'est quoi ?
- Un protocole 802.1x particulier
- Mise en place : freeradius
- Radius sans 802.1x ?

Préparée et présentée par : Rioner :)

C’est quoi ?

- Modèle OSI : rappel

Layer OSI	Exemple protocole	Exemple “identifiant”
7 (Application)	Protocole applicatif quelconque	Propre au protocole
6 (Presentation)		
5 (Session)		
4 (Transport)	TCP/UDP	Port 69
3 (Network)	IPv4/IPv6	192.168.16.16
2 (Link)	WiFi/Ethernet	1c:ce:51:48:9c:46
1 (Physical)	...	Électricité, lumière, bit

C’est quoi Radius ?

- C’est un protocole !
- AAA : Authorization, Authentication, Accounting
  - Authentication : Tu as le droit d’être là ?
  - Authorization : Tu as le droit de faire quoi ?
  - Accounting : Quand et qui s’est connecté comment ?
- Les adhérents ne l’utilisent pas directement (il s’effectuera plutôt entre le switch et un serveur dédié)

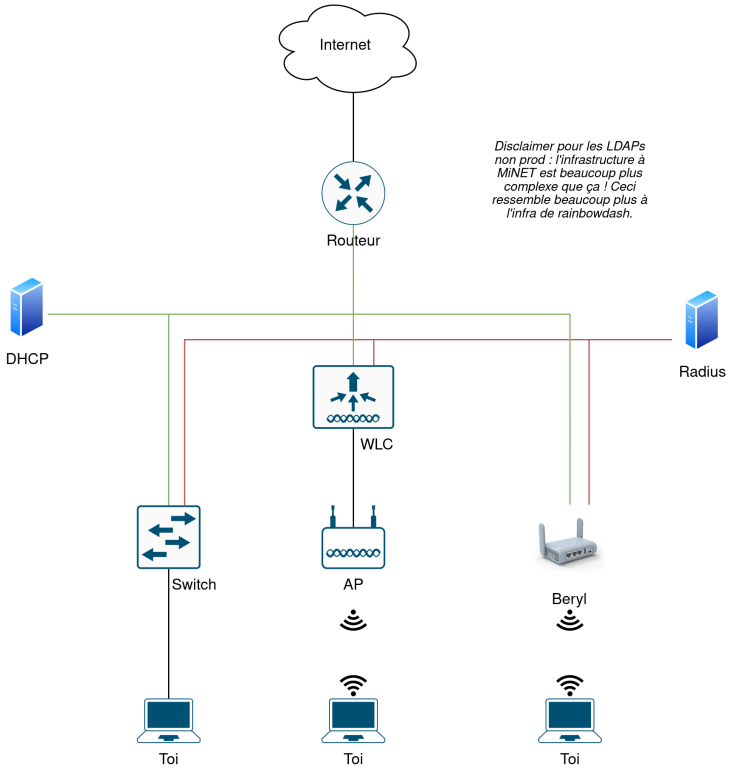
C’est quoi 802.1x ?

- C’est un standard IEEE qui définit un *ensemble* de protocoles, qui utilisent des messages EAP.
- Il vous permettent de vous authentifier en filaire et en WiFi, et vous devez le configurer sur vos ordinateurs.

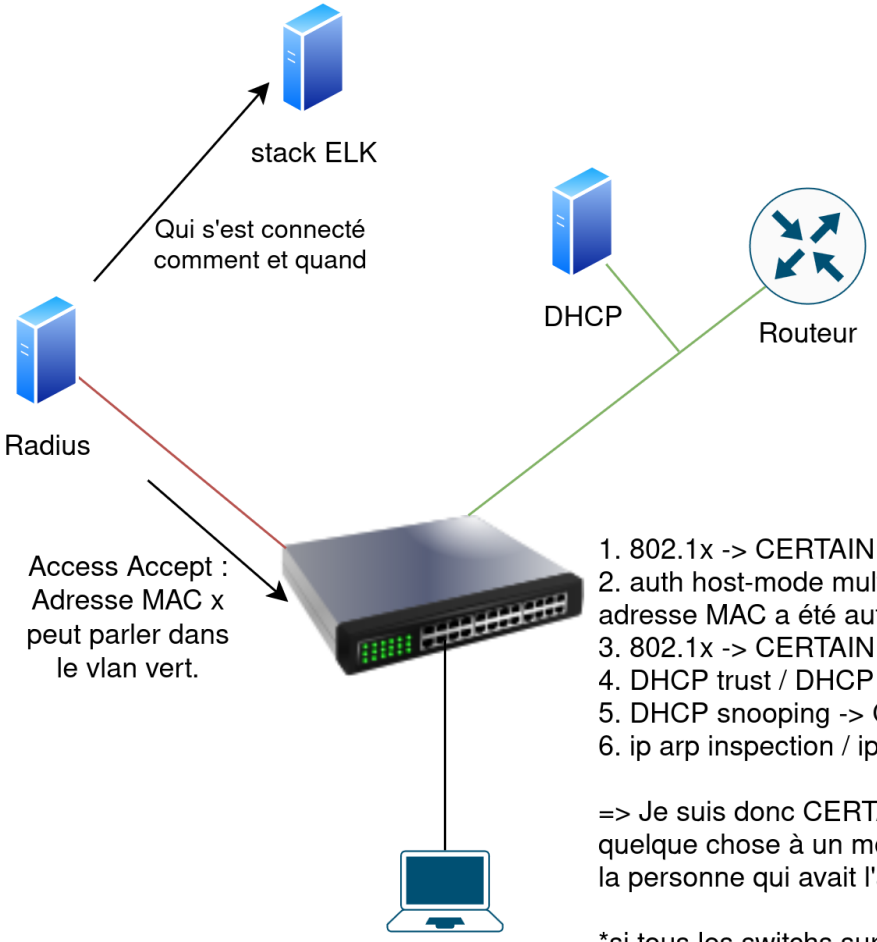
802.1x : Sécurité induite, et l’exemple du filaire

Radius et 802.1x ?

- Intervient en L2 : avant même de recevoir une IP
- Par le premier élément L2 intelligent que l'on rencontre



Sécurité induite par 802.1x et compléments



PDV switch :

1. 802.1x -> CERTAIN qu'il existe une adresse MAC autorisée de l'autre côté du port
2. auth host-mode multi-auth -> CERTAIN que si quelqu'un peut parler, son adresse MAC a été autorisée.
3. 802.1x -> CERTAIN de là où la machine peut parler (ex: VLAN vert)
4. DHCP trust / DHCP relay -> CERTAIN qu'on parle au bon DHCP*
5. DHCP snooping -> CERTAIN de la liaison MAC <-> IP
6. ip arp inspection / ip verify -> CERTAIN qu'on ne peut parler qu'avec l'IP obtenue

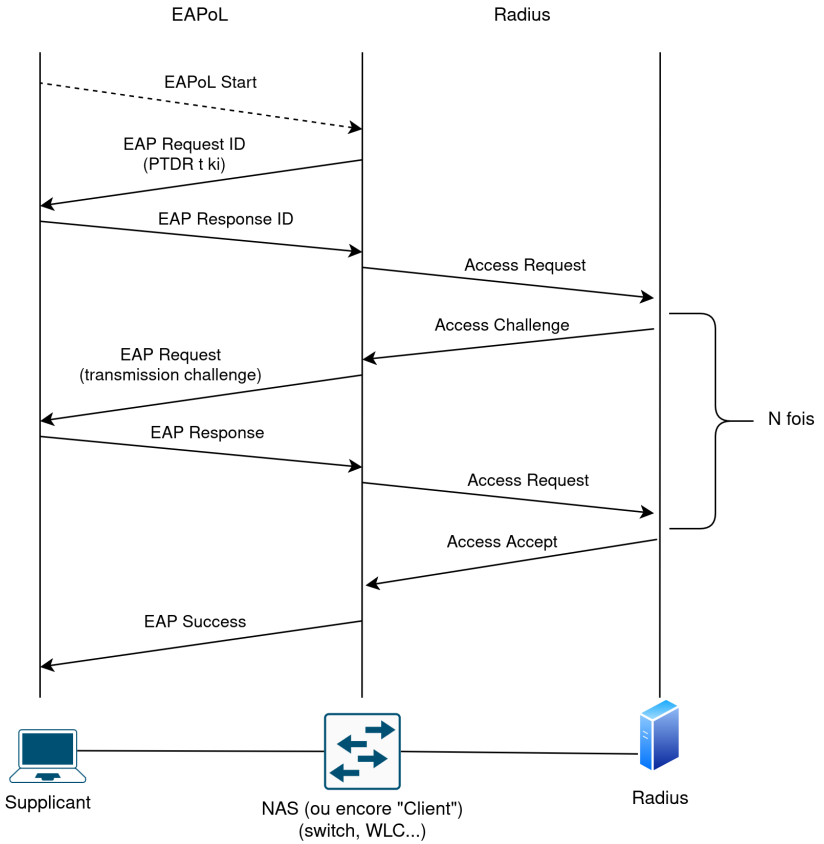
=> Je suis donc CERTAIN que si on me dit que l'IP a.b.c.d a fait quelque chose à un moment donné, alors il s'agit en fait de la personne qui avait l'adresse MAC à ce moment-là (obligation légale !!)

*si tous les switchs sur le VLAN vert sont config correctement

802.1x : protocole**S**

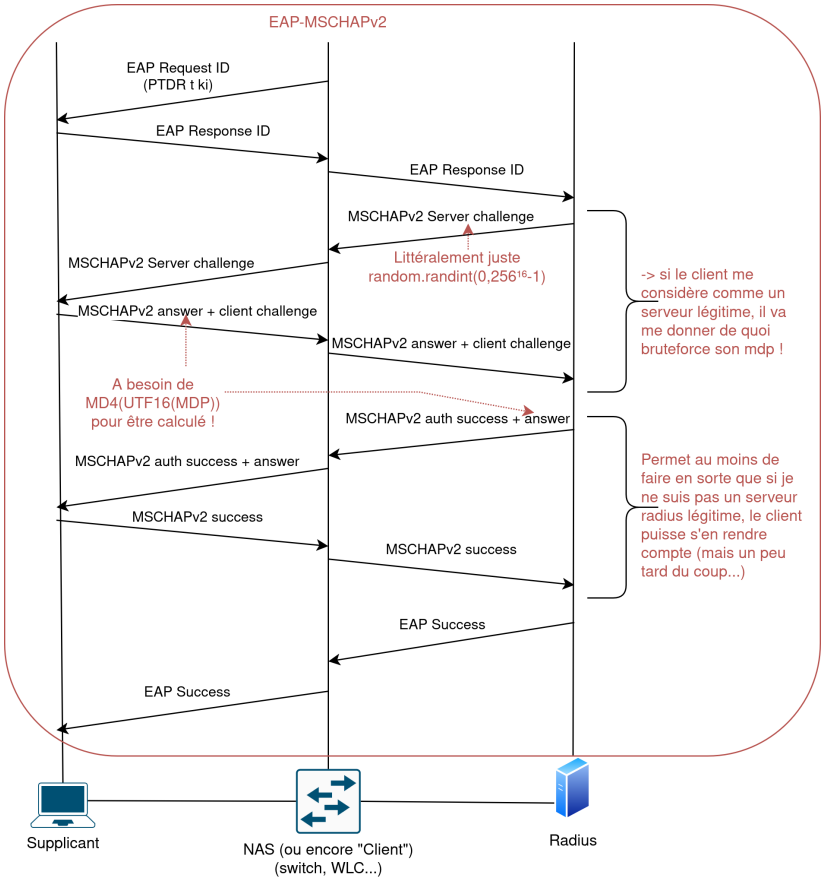
Détail des protocoles 802.1x

- Échanges EAP (EAPoL + RADIUS) : supplicant, client / NAS, AAA server



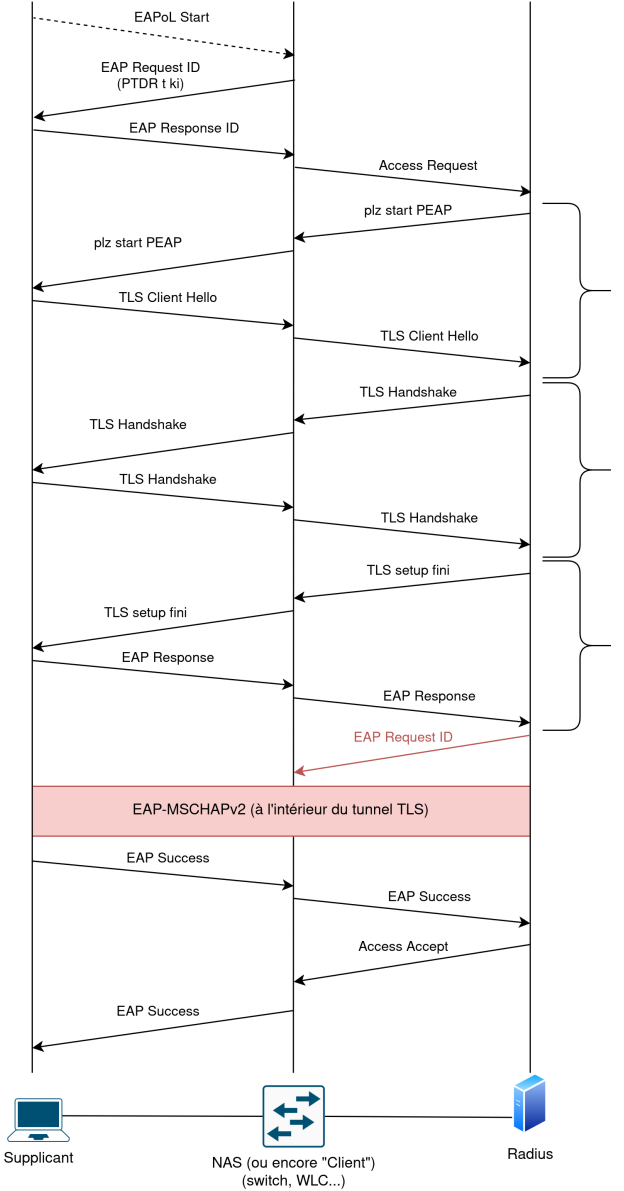
802.1x : exemple d'un protocole

- Détail d'un protocole en particulier : EAP-MS-CHAP-v2

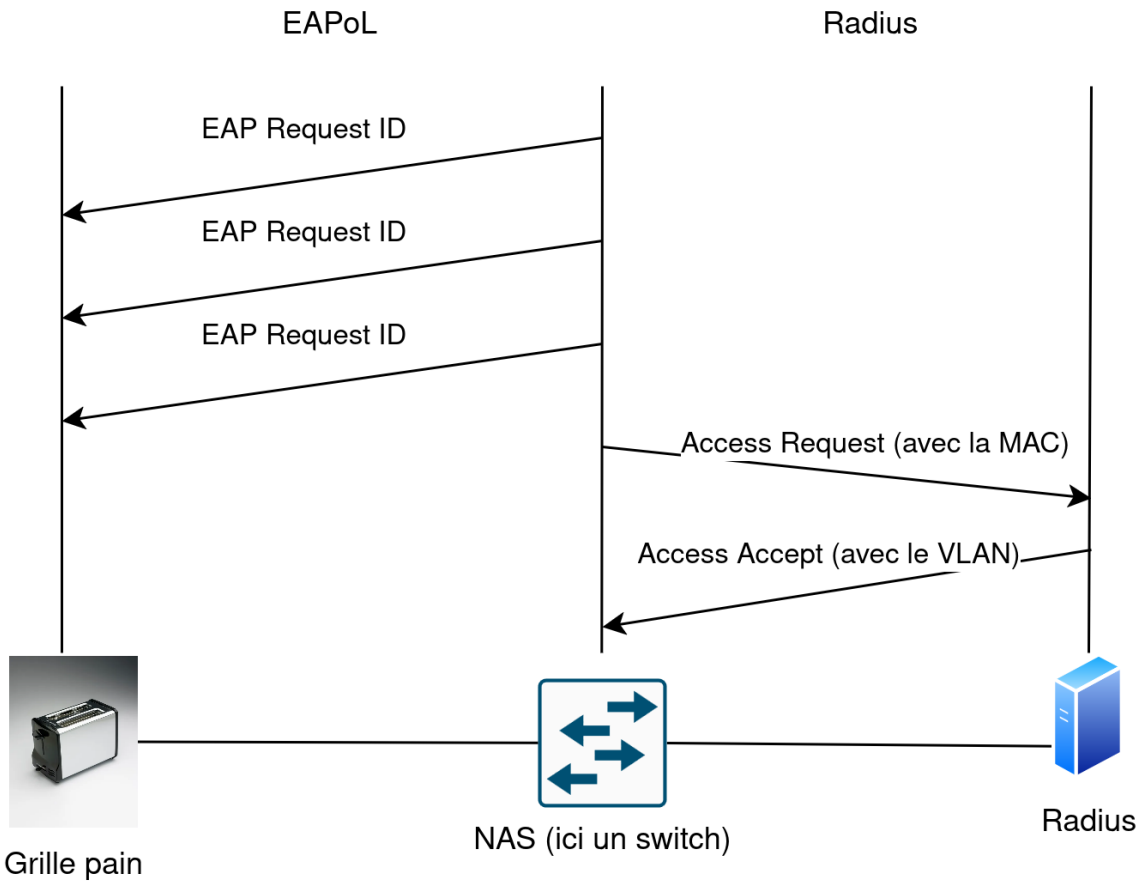


802.1x : exemple d’un protocole

- Détail d’un protocole en particulier : PEAPv0/EAP-MS-CHAP-v2
- Règle le problème majeur de EAP-MS-CHAP-v2 : le supplicant sait désormais que le serveur est légitime *avant* de lui donner de quoi bruteforce le mot de passe ! (mais il faut alors que le client n’accepte pas n’importe quel certificat…)
- Et aussi le fait qu’EAP envoie les messages en clair, ce qui fait que n’importe qui d’autre se mettant entre supplicant et NAS ou entre NAS et radius aurait aussi pu bruteforce le mot de passe… Maintenant on a le chiffrement TLS qui protège le moment critique.
- Note : il existe d’autres protocoles utilisables que PEAPv0/EAP-MS-CHAP-v2 pour faire de l’authentification 802.1x en utilisant Radius



Connecter un grille-pain en filaire : Radius sans 802.1x, l'exemple du MAB

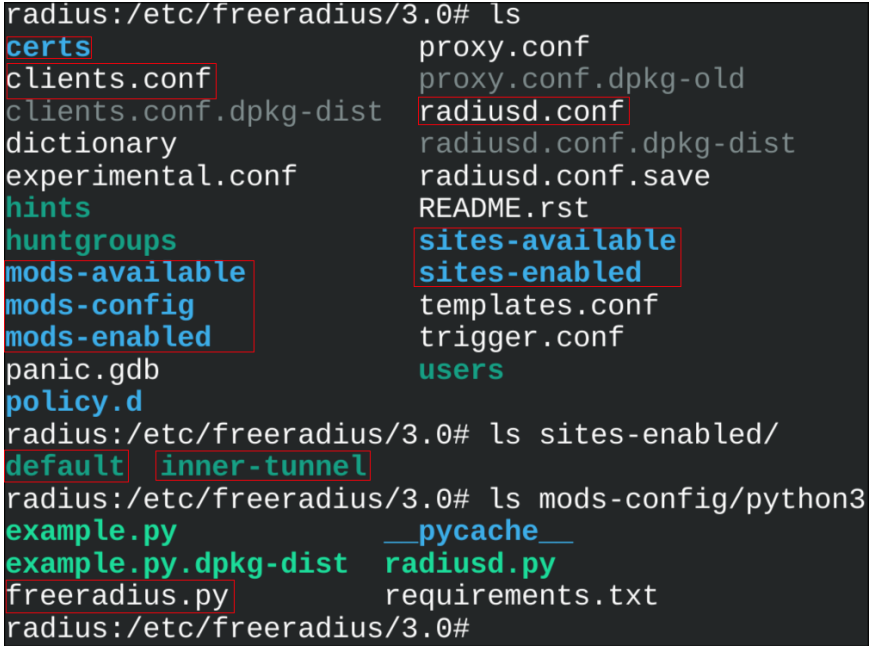


Et donc : 802.1x vs Radius ?

- Radius est un protocole AAA, utilisable entre un NAS et un serveur Radius
- 802.1x est le protocole qui permet de s’authentifier en réseau qui utilise des trames EAP.
- Il est possible d’utiliser le 802.1x sans utiliser RADIUS (exemple: avec Diameter)
- Il est possible d’utiliser RADIUS sans utiliser 802.1x (exemple: MAB)

Radius en 802.1x : mise en place, l’exemple de freeradius

Quelques fichiers importants de config



- `radiusd.conf` → la config globale du service

- `sites-enabled/` → différents “tunnels” (principal "`default`", intra-PEAP "`inner-tunnel`"...) en service (leurs fichiers de configuration)

- `mods-available/` → extensions disponibles (pour enable : `ln -s mods-available/abc mods-enabled/abc`)

- `mods-config/python3/` → Là où config le script utilisé par l’extension python3

- `clients.conf` → là où donner la liste des NAS valides

- `certs` → dossier où il faudra mettre tous types de certificats (dont ceux utilisés pour PEAP)

Configuration (haut-niveau) à MiNET

- `sites-enabled/default` : Si pas de message EAP, alors freeradius.py pour MAB (*authorize*), sinon PEAP-MSCHAPv2 pour l'authorization, puis freeradius.py (*authenticate*)
- `freeradius.py - authorize(p)` : Si mini-routeur alors OK voice vlan 31, sinon on regarde à qui appartient l'adresse MAC parmi les adresses MAC autorisées en MAB, puis si la personne a une cotisation valide, on trouve puis on lui donne son VLAN
- `freeradius.py` - `authenticate(p)` : est-ce que l'user a une cotisation valide ? Est-ce que l'adresse MAC présentée lui appartient bien ? Si on est en filaire, on trouve puis on lui donne son VLAN, sinon on dit juste oui sans information supplémentaire*
- Ces 3 instances font appel à la base de données dès qu'ils en ont besoin (pour *MD4(UTF16(password))*, informations sur la durée de cotisation, le vlan à donner...)

*le WLC ignore les attributs de VLAN par défaut, car il connaît déjà l'information autrement

Cisco IOS : Une commande à connaître

- `sh auth [session] int Gix/y [details]`
- `sh auth [session] mac aaaa.bbbb.cccc [details]`

```
switch-U3#sh authentication sessions int Gi2/0/3 details
           Interface:  GigabitEthernet2/0/3
         MAC Address:  0000.3600.0117
        IPv6 Address:  Unknown
        IPv4 Address:  172.30.0.117
          User-Name:  000036000117
             Status:  Authorized
             Domain:  VOICE
      Oper host mode:  multi-auth
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
Periodic Acct timeout:  N/A
    Common Session ID:
     Acct Session ID:  Unknown
              Handle:
      Current Policy:  POLICY_Gi2/0/3

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
          Vlan Group:  Vlan: 31

Method status list:
      Method           State

      dot1x            Stopped
      mab              Authc Success
```

L'adresse MAC de l'appareil

L'addresse IP obtenue par DHCP snooping (après réussite de l'authentification)

Où on en est de l'authentification

La machine a le droit de parler dans le vlan VOICE et non pas DATA

Extrait de la configuration du port

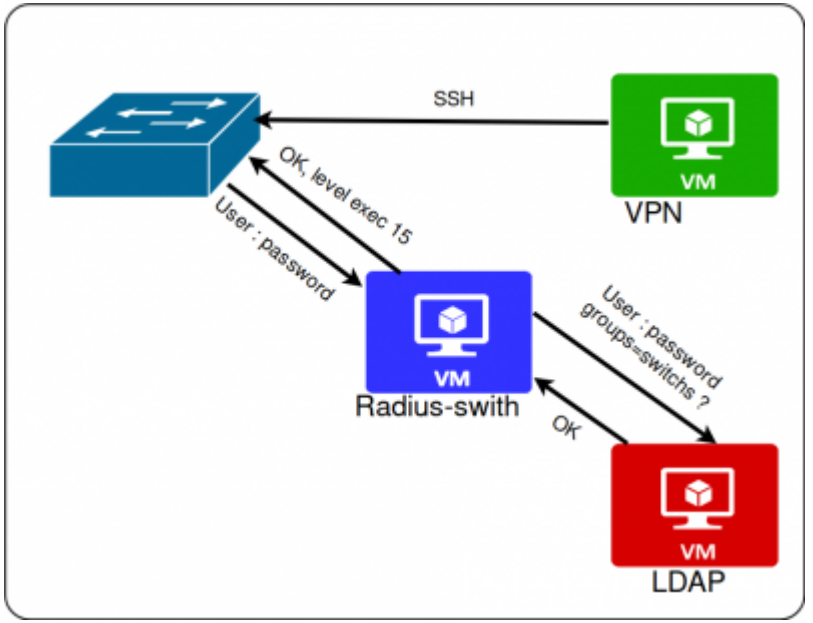
Radius a dit que lorsque cette machine parle, son traffic doit aller dans le vlan 31

Le switch a essayé de faire du 802.1x sans réponse...

...donc il est passé au MAB, et ça a réussi (AuthentiCation success)

Radius : autres usages que 802.1x

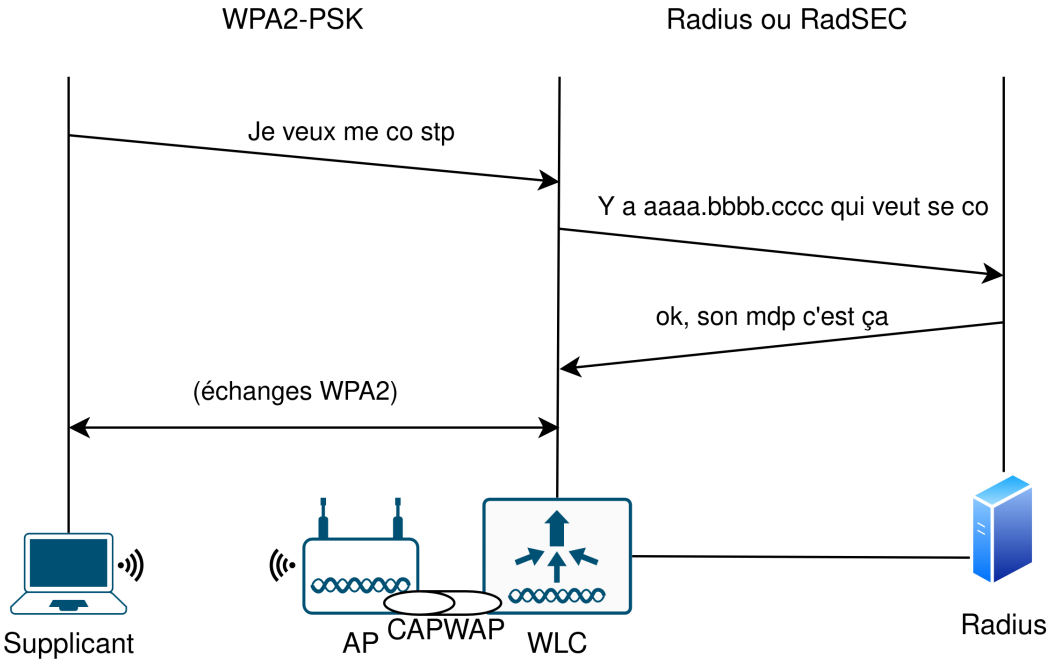
Utilisation de radius pour se ssh aux switchs



(image volée du wiki)

Ouverture : WPA2-iPSK

- Se connecter de manière sécurisée… avec Radius… mais sans 802.1x ??



*Bientôt à MiNET ? *wink**

Blooket time !