https://www.ssi.gouv.fr/uploads/2018/08/guide_802.1x_anssi_pa_043_v1.pdf

https://www.networklife.net/2010/07/assignation-dynamique-de-vlan-avec-dot1x/

Config 802.1x avec AD DHCP NPS sur switch catalyst avec attribution de vlan (PEAP-MSCHAPv2)

Config basique switch

```
enable
conf t
vlan 2
name direction
vlan 3
name rh
vlan 4
name production
vlan 254
name public
interface vlan 1
ip address dhcp
no shutdown
exit
ip domain-name dom.alro.fr
crypto key generate rsa modulus 2048
ip ssh version 2
username admin privilege 15 secret 0 Not24get
enable secret 0 Not24get
line vty 0 15
transport input ssh
login local
exit
interface vlan 2
ip address 172.16.12.254 255.255.255.0
ip helper-address 10.196.72.1
exit
interface vlan 3
ip address 172.16.13.254 255.255.255.0
ip helper-address 10.196.72.1
exit
interface vlan 4
ip address 172.16.14.254 255.255.255.0
ip helper-address 10.196.72.1
exit
interface vlan 254
```

```
ip address 172.16.254.254 255.255.255.0
ip helper-address 10.196.72.1
exit
interface gigabitEthernet 0/1
switchport mode access
switchport access vlan 1
description To-Trusted-Network
exit
```

Installation et configuration du rôle NPS sur windows serveur

Installation

Installer le rôle “Services de stratégie et d'accès réseau” (NPS : Network Policy Server)

Créer une règle de pare-feu (wf.msc), traffic entrant : - Autoriser le traffic UDP sur les ports 1812,1813 dans tous les profils de connexions (traffic radius)

Console Serveur NPS

Ajouter un client radius - Paramètres

1. Nom convivial : c2960
2. Adresse (IP ou DNS) : 172.16.10.254
3. secret partagé : Not24get

- Avancé

1. Nom du fournisseur (facultatif) : Cisco

Ajouter une stratégie de demande de connexion (pour autoriser les demandes de connexion 802.1x venant du réseau ethernet sur ce serveur) - Nom de la stratégie : Ethernet - Type de serveur d'accès réseau : Non spécifié - Ajouter une condition

1. Type de port NAS : Ethernet

- Authentification : Authentifier les demandes sur ce serveur

Ajouter une stratégie réseau pour chaque vlan - Nom de la stratégie : vlan-direction - Type de serveur d'accès réseau : Non spécifié - Ajouter une condition

1. Groupes Windows : GP-Direction
2. Type de port NAS : Ethernet

- Autorisation d'accès : Accès accordé - Configurer les méthodes d'authentification

1. Types de protocoles EAP

1. Ajouter
    1. Microsoft: PEAP (Protected EAP)
2. Modifier “Microsoft: PEAP (Protected EAP)”
    1. Erreur de certificat, il faut soit :
        1. Génération d'un certificat en powershell :

```
    ```powershell
    New-SelfSignedCertificate -Subject "ALRO-AD1.dom.alro.fr" -TextExtension
@("2.5.29.17={text}DNS=ALRO-AD1.dom.alro.fr&DNS=ALRO-
AD1&IPAddress=10.196.72.2")
    ```
    - Installation du rôle "Services de certificats Active Directory" (AD
CS)
```

- Méthodes d'authentification moins sécurisées

1. Tout décocher

- Configurer les paramètres

1. Standard
    1. Supprimer “Framed-Protocol PPPP”
    2. Supprimer “Service-Type Framed”
    3. Ajouter “Tunnel-Type” à “N° VLAN”
    4. Ajouter “Tunnel-Pvt-Group-ID” à “Virtual LANs (VLAN)”
    5. Ajouter “Tunnel-Medium-Type” à “802 (includes all 802 media plus Ethernet canonical format)”

Préparation du client Windows

- Veiller à ce que le service “Configuration automatique de réseau câblé” (dot3svc) soit démarré et en configuration automatique (services.msc) - Activer le dot1x dans la configuration de la carte réseau (ncpa.cpl → Onglet Authentification dans les propriétés de la carte réseau)

1. Activer l'authentification IEEE 802.1X
2. Méthode d'authentificartion : “Microsoft : PEAP (Protected EAP)”
    1. Paramètres
    2. Méthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP version 2)
        1. Configurer : **Décocher “Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et eventuellement de domaine)” si l'ordinateur n'est pas dans le domaine corp.iia.fr (exemple ordinateur hors domaine ou ordinateur de l'IIA domaine campus53.lan)**
3. Décocher “Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté” pour tester les différents comptes
4. Paramètres supplémentaires
    1. Spécifier le mode d'authentification : Authentification utilisateur

Config 802.1x switch

```
!Enables AAA
aaa new-model

!aaa authentication dot1x {default} method1
!Creates an 802.1x authentication method list.
!To create a default list that is used when a named list is not specified in
the authentication command, use the default keyword followed by the method
that is to be used in default situations. The default method list is
automatically applied to all ports.
!For method1 , enter the group radius keywords to use the list of all RADIUS
servers for authentication.
aaa authentication dot1x default group radius

!Sets the authorization method to local. To remove the authorization method,
use the no aaa authorization network default group radius command.
aaa authorization network default group radius

!Enable 802.1x accounting using the list of all RADIUS servers.
aaa accounting dot1x default start-stop group radius

!Globally enables 802.1X port-based authentication on a switch
dot1x system-auth-control

!config radius server for aaa
radius-server host 10.196.72.1 auth-port 1812 acct-port 1813 timeout 10 key
Not24get



interface range FastEthernet0/1-22
switchport mode access
! Set the interface Port Access Entity to act only as an authenticator and
ignore messages meant for a supplicant.
dot1x pae authenticator
!Enable 802.1x authentication on the port.
authentication port-control auto
!Allow multiple hosts on an 802.1x-authorized port after a single host has
been authenticated.
!authentication host-mode multi-host
!Permettre l'authentification avec le wake-on-lan en authentificant que ce
qui vient de l'interface
authentication control-direction in
!Configure the violation mode : Removes the current session and
authenticates with the new host.
authentication violation replace
!Set the number of seconds that the switch remains in the quiet state after
a failed authentication exchange with the client. (default 60)
authentication timer inactivity 10
```

```
!Enable periodic reauthentication of the client, which is disabled by
default.
authentication periodic
! Set reauthentication attempt for the client (set to one hour by default).
authentication timer reauthenticate 1800
!Vlan guest si pas d'auth
authentication event no-response action authorize vlan 254
!Vlan guest si authentification échoue
authentication event fail action authorize vlan 254
!Vlan guest si pas de serveur radius
authentication event server dead action authorize vlan 254
spanning-tree portfast
```

Test et debug

Le client, connecté à l'un des ports Ethernet, doit fonctionner correctement : il s'authentifie (logs visble dans l'event viewer windows) et se voit attribuer une IP depuis le serveur DHCP de Windows

Debug Windows : eventvwr.msc (Observateur d'évènements) → Affichages personnalisés → Rôles de serveurs → Services de stratégie et d'accès réseau

Debug switch :

```
show dot1x all summary
show dot1x all count
show dot1x all details
show dot1x all statistics
show dot1x interface ...
show authentication...
```

Config 802.1x avec AD DHCP NPS sur borne wifi (PEAP-MSCHAPv2)

Config switch borne wifi

```
enable
conf t
vlan 5
name Wifi-BYOD
exit
interface vlan 5
description Wifi-BYOD
ip address 172.16.15.254 255.255.255.0
ip helper-address 172.16.10.1
```

```
exit
interface gigabitEthernet 0/2
switchport mode trunk
switchport trunk allowed vlan add 5,254
switchport trunk native vlan 1
description BorneWiFi
exit
```

Configuration du rôle NPS pour Borne WiFi

Lancer la console Serveur NPS

Ajouter un client radius - Paramètres

1. Nom convivial : rv110w
2. Adresse (IP ou DNS) : 172.16.10.253
3. secret partagé : Not24get

- Avancé

1. Nom du fournisseur : Cisco

Ajouter une stratégie de demande de connexion (pour autoriser les demandes de connexion 802.1x venant du réseau wifi sur ce serveur) - Nom de la stratégie : WiFi - Type de serveur d'accès réseau : Non spécifié - Ajouter une condition

1. Type de port NAS : Sans fil - IEEE 802.11

- Authentification : Authentifier les demandes sur ce serveur

Ajouter une stratégie réseau pour le SSID BOYD - Nom de la stratégie : Wifi-BYOD - Type de serveur d'accès réseau : Non spécifié - Ajouter une condition

1. Groupes Windows : Utilisateurs du domaine
2. Type de port NAS : Sans fil - IEEE 802.11

- Autorisation d'accès : Accès accordé - Configurer les méthodes d'authentification

1. Types de protocoles EAP
    1. Ajouter
        1. Microsoft: PEAP (Protected EAP)
    2. Modifier “Microsoft: PEAP (Protected EAP)”
        1. Si erreur de certificat, il faut soit :
            1. Génération d'un certificat en powershell : `$cert = New-SelfSignedCertificate -certstorelocation cert:\localmachine\my -dnsname ad1.corp.iia.fr`
            2. Installation du rôle “Services de certificats Active Directory” (AD CS)
2. Méthodes d'authentification moins sécurisées
    1. Tout décocher

- Configurer les paramètres

1. Standard
    1. Supprimer “Framed-Protocol PPPP”
    2. Supprimer “Service-Type Framed”

Configuration Borne WiFi

Ré-initialiser l'AP (Boutton reset 10sec) et se connecter à son interface web (@192.168.1.1 et cisco/cisco) - Désactiver le wizard - Changer l'adresse IP du LAN sur le vlan1 pour 172.16.10.253/24 et désactiver le serveur DHCP : “Networking → LAN → LAN Configuration” - Ajouter le vlan 5 : “Networking → LAN → VLAN membership”, ajouter une ligne avec le vlan 5 byod tag sur tout les ports - Configurer le SSID BYOD “Wireless → Basic Settings → Sélectionner le premier SSID”

1. “Edit” : Donner le nom du SSID, attribuer le vlan 5
2. “Edit Security Mode”
    1. Security Mode : WPA2-Entreprise
    2. Radius server : 172.16.10.1
    3. Radius port : 1812
    4. Shared key : Not24get

Test et debug

Le client (PC ou smartphone) peux se connecter au SSID, une alerte sur le certificat autosigné apparaitra si il n'a pas été importé avant, ensuite on peux rentrer le login / mot de passe AD et test l'accès (on doit avoir une adresse DHCP vlan 5)

Debug Windows : eventvwr.msc (Observateur d'évènements) → Affichages personnalisés → Rôles de serveurs → Services de stratégie et d'accès réseau

Config 802.1x avec AD DHCP NPS AD-CS avec borne wifi avec distribution de certificats (EAP-TLS)

Config switch borne wifi

```
enable
conf t
vlan 6
exit
interface vlan 6
description CORP
ip address 172.16.16.254 255.255.255.0
ip helper-address 172.16.10.1
```

```
exit
interface gigabitEthernet 0/2
switchport trunk allowed vlan add 5,6,254
exit
```

Configuration Borne WiFi

- Ajouter le vlan 6 : “Networking → LAN → VLAN membership”, ajouter une ligne avec le vlan 6 corp tag sur tout les ports
- Configurer le SSID CORP “Wireless → Basic Settings → Sélectionner le deuxième SSID”
  - “Edit” : Donner le nom du SSID, attribuer le vlan 6
  - “Edit Security Mode”
    - Security Mode : WPA2-Entreprise
    - Radius server : 172.16.10.1
    - Radius port : 1812
    - Shared key : Not24get

Configuration du rôle NPS pour Borne WiFi avec AD DC

Installer le rôle “Services de certificats Active Directory” (AD CS) - Services de rôles

1. Autorité de certification
2. Inscription de l'autorité de certification via le Web (Ajouter toutes les fonctionnalités précochés : IIS, etc...) → Servira pour demander des certificats via navigateur

…. config CA, config NPS, config GPO, etc ….

https://networklessons.com/uncategorized/peap-and-eap-tls-on-server-2008-and-cisco-wlc/
https://frankfu.click/microsoft/windows-server/nps-wireless-authentication-with-computer-certificate-eap-tls/