802.1x

Protocole et retour d'expérience

Nicolas Gibelin
Nicolas.Gibelin@imag.fr

Version 1.1 (*Rev* : 65) - 20151103

Plan

Historique

Standardisation

- 1994-2003 : PPP[1]

[1] Point to Point Protocol
[2] Remove Auth Dial-In User Service
[3] Extensible Authentication Protoco

Historique

Standardisation

- 1994-2003 : PPP[1]
- 1997-2000 : RADIUS[2] (RFC2865 à RFC2869)

[1] Point to Point Protocol
[2] Remove Auth Dial-In User Service
[3] Extensible Authentication Protoco

Historique

Standardisation

- 1994-2003 : PPP[1]
- 1997-2000 : RADIUS[2] (RFC2865 à RFC2869)
- 1998 : EAP[3] (RFC2284)

[1] Point to Point Protocol
[2] Remove Auth Dial-In User Service
[3] Extensible Authentication Protoco

Historique

Standardisation

- 1994-2003 : PPP[1]
- 1997-2000 : RADIUS[2] (RFC2865 à RFC2869)
- 1998 : EAP[3] (RFC2284)
- 2001 : 802.1X-2001 - IEEE Standard for Port Based Network Access Control

[1] Point to Point Protocol
[2] Remove Auth Dial-In User Service
[3] Extensible Authentication Protoco

Historique

Standardisation

- 1994-2003 : PPP[1]
- 1997-2000 : RADIUS[2] (RFC2865 à RFC2869)
- 1998 : EAP[3] (RFC2284)
- 2001 : 802.1X-2001 - IEEE Standard for Port Based Network Access Control
- 2003 (février) : addendum 802.1aa (non rejeu, auth mutuelle, gestion de clefs)

[1] Point to Point Protocol
[2] Remove Auth Dial-In User Service
[3] Extensible Authentication Protoco

Historique

Standardisation

- 1994-2003 : PPP[1]
- 1997-2000 : RADIUS[2] (RFC2865 à RFC2869)
- 1998 : EAP[3] (RFC2284)
- 2001 : 802.1X-2001 - IEEE Standard for Port Based Network Access Control
- 2003 (février) : addendum 802.1aa (non rejeu, auth mutuelle, gestion de clefs)
- 2010 : 802.1X-2010 - IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control

[1] Point to Point Protocol
[2] Remove Auth Dial-In User Service
[3] Extensible Authentication Protoco

Contexte

Pourquoi réfléchir au 802.1x

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier
- Ajouter Nomadisme filaire

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier
- Ajouter Nomadisme filaire
- Techno de connexion ??

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier
- Ajouter Nomadisme filaire
- Techno de connexion ??
  - Sans Auth : Statique Vlan par port

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier
- Ajouter Nomadisme filaire
- Techno de connexion ??
  - Sans Auth : Statique Vlan par port
  - Avec Auth

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier
- Ajouter Nomadisme filaire
- Techno de connexion ??
  - Sans Auth : Statique Vlan par port
  - Avec Auth
    - Mac adresse

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier
- Ajouter Nomadisme filaire
- Techno de connexion ??
  - Sans Auth : Statique Vlan par port
  - Avec Auth
    - Mac adresse
    - Portail captif

Contexte

Pourquoi réfléchir au 802.1x

L'occasion fait le larron

- Actuellement : plein bâtiments, différentes gestions
- Bientôt : bâtiment Pilsi
- En profiter pour simplifier
- Ajouter Nomadisme filaire
- Techno de connexion ??
  - Sans Auth : Statique Vlan par port
  - Avec Auth
    - Mac adresse
    - Portail captif
    - 802.1x

Plan

Principe

Objectifs

- Standardiser relais authentification niveau 2
- Sécuriser l'accès au réseau
- Authentifier l'utilisateur plutôt que le matériel

Principe

Objectifs

- Standardiser relais authentification niveau 2
- Sécuriser l'accès au réseau
- Authentifier l'utilisateur plutôt que le matériel

Comment

- Requête d'authentification
- Auth **avant** connexion/conf (DHCP,PXE . . .)
  - Succès : Vlan utilisateur
  - Échec : Vlan banni - guest - portail captif . . .

Intérêt

- Sécurité réseau (filaire et sans fil)

Intérêt

- Sécurité réseau (filaire et sans fil)
- Tracabilité des incidents (intrusions, usurpation . . .)

Intérêt

- Sécurité réseau (filaire et sans fil)
- Tracabilité des incidents (intrusions, usurpation . . .)
- Mobilité utilisateur = Nomadisme

Intérêt

- Sécurité réseau (filaire et sans fil)
- Tracabilité des incidents (intrusions, usurpation . . .)
- Mobilité utilisateur = Nomadisme
- Facilité de gestion

Acteurs

- Client : supplicant en EAP

Acteurs

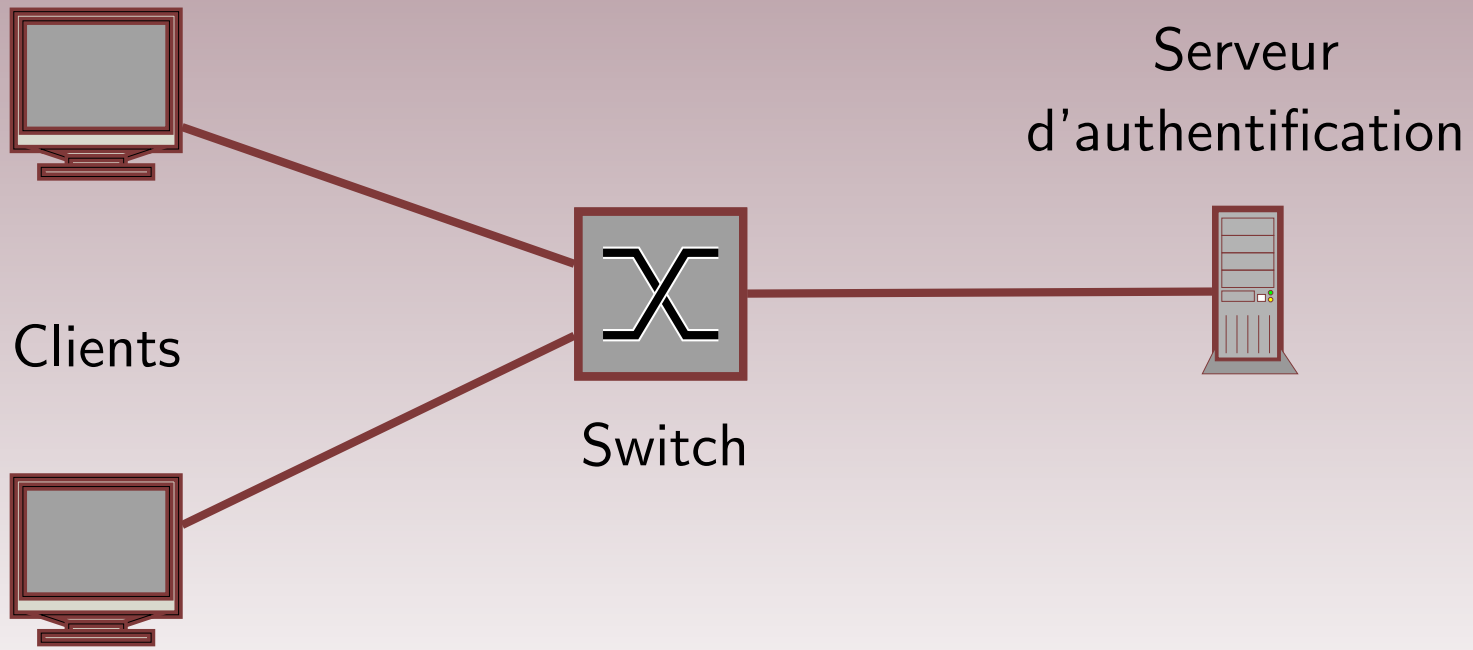
- Client : supplicant en EAP
- Équipement niveau 2 : Authenticator

Acteurs

- Client : supplicant en EAP
- Équipement niveau 2 : Authenticator
- Serveur d'authentification : RADIUS

Acteurs

- Client : supplicant en EAP
- Équipement niveau 2 : Authenticator
- Serveur d'authentification : RADIUS



Contrôle de port[4]

Innovation de 802.1x

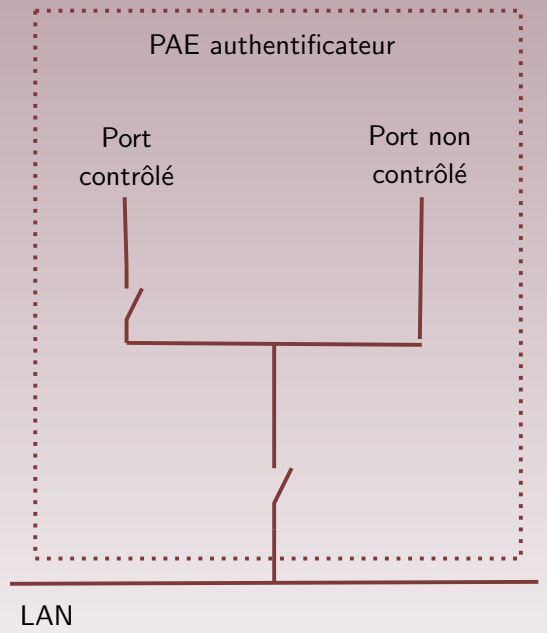
Point accès physique (rj45) ou logique (802.11) = 2 ports logiques

[4] PAE (Port Access Entity)

Contrôle de port[4]

Innovation de 802.1x

Point accès physique (rj45) ou logique (802.11) = 2 ports logiques



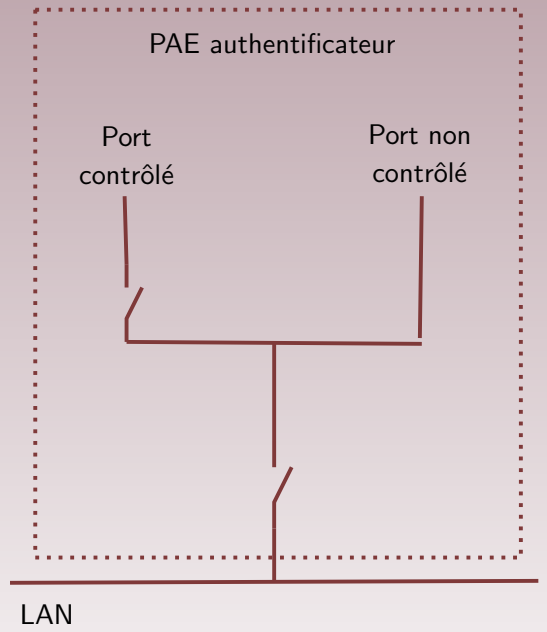
[4] PAE (Port Access Entity)

Contrôle de port[4]

Innovation de 802.1x

Point accès physique (rj45) ou logique (802.11) = 2 ports logiques

- Non controlé : échange EAP d'auth (toujours accessible)



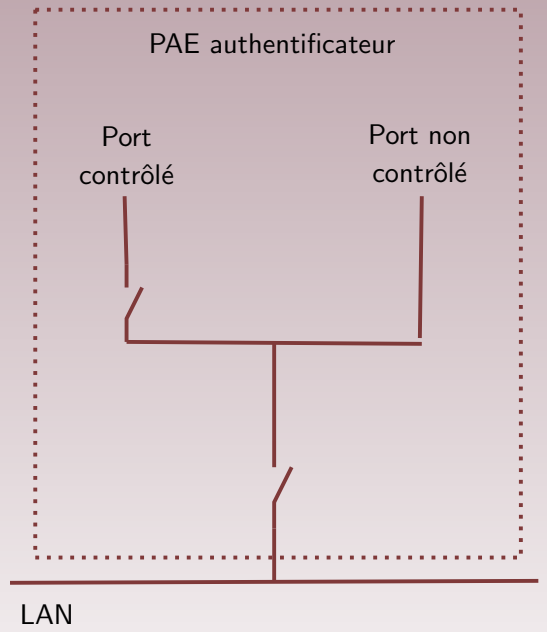
[4] PAE (Port Access Entity)

Contrôle de port[4]

Innovation de 802.1x

Point accès physique (rj45) ou logique (802.11) = 2 ports logiques

- Non controlé : échange EAP d'auth (toujours accessible)
- Controlé



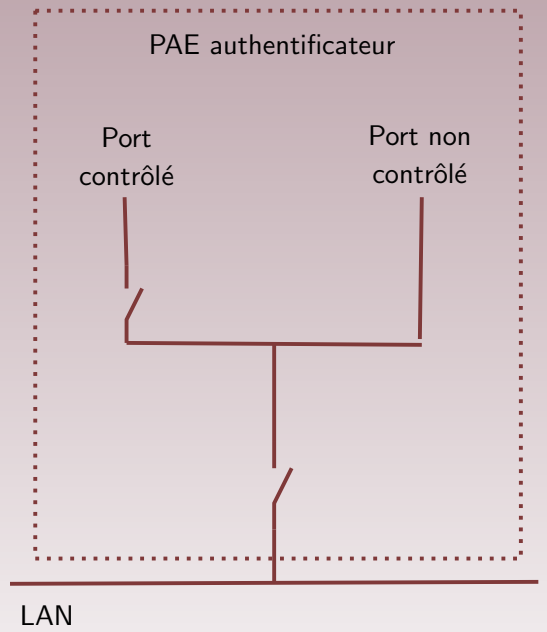
[4] PAE (Port Access Entity)

Contrôle de port[4]

Innovation de 802.1x

Point accès physique (rj45) ou logique (802.11) = 2 ports logiques

- Non controlé : échange EAP d'auth (toujours accessible)
- Controlé
  - Autorisé : interrupteur fermé



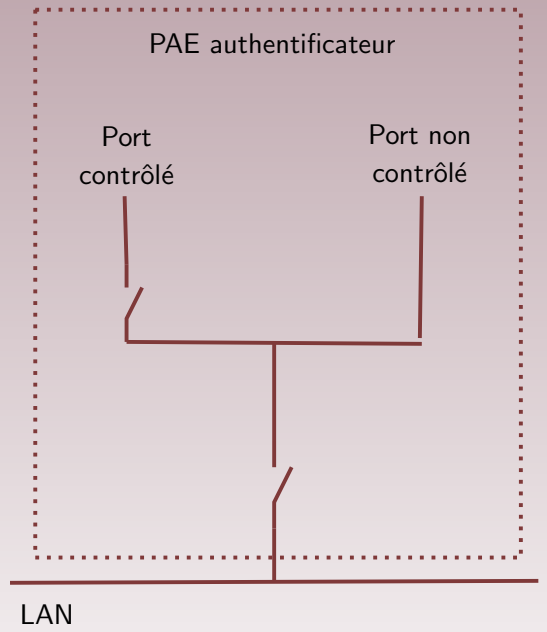
[4] PAE (Port Access Entity)

Contrôle de port[4]

Innovation de 802.1x

Point accès physique (rj45) ou logique (802.11) = 2 ports logiques

- Non controlé : échange EAP d'auth (toujours accessible)
- Controlé
  - Autorisé : interrupteur fermé
  - Non autorisé : interrupteur ouvert



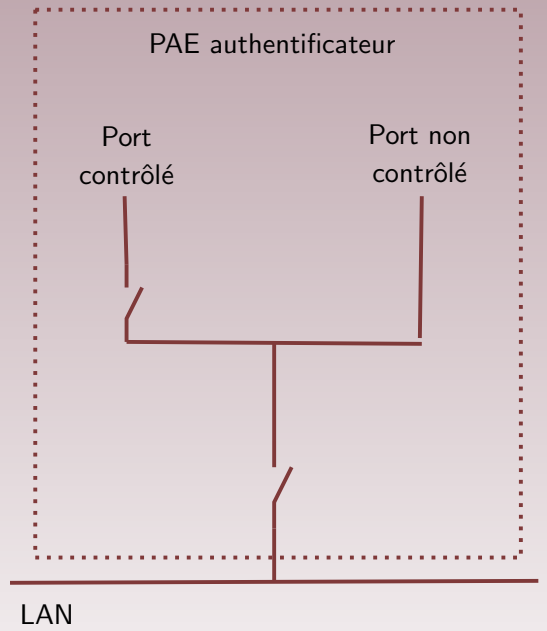
[4] PAE (Port Access Entity)

Contrôle de port[4]

Innovation de 802.1x

Point accès physique (rj45) ou logique (802.11) = 2 ports logiques

- Non controlé : échange EAP d'auth (toujours accessible)
- Controlé
  - Autorisé : interrupteur fermé
  - Non autorisé : interrupteur ouvert
  - Variable *AuthControlledPortControl*
    - ForceUnauthorised
    - ForceAuthorised
    - Auto

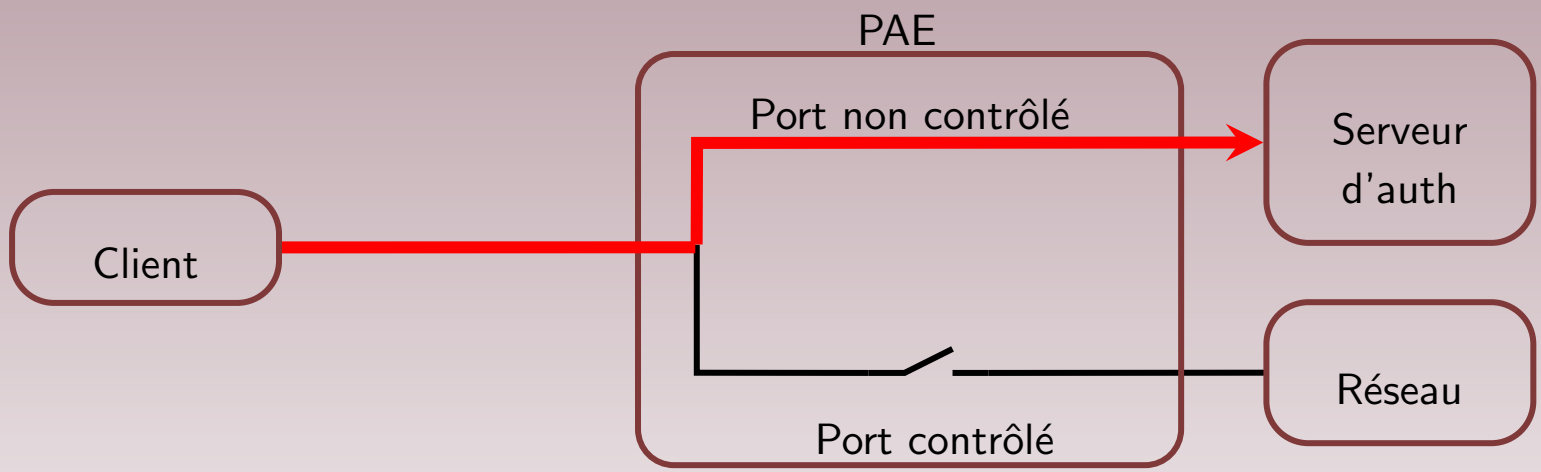


[4] PAE (Port Access Entity)

Détail

Port non contrôlé

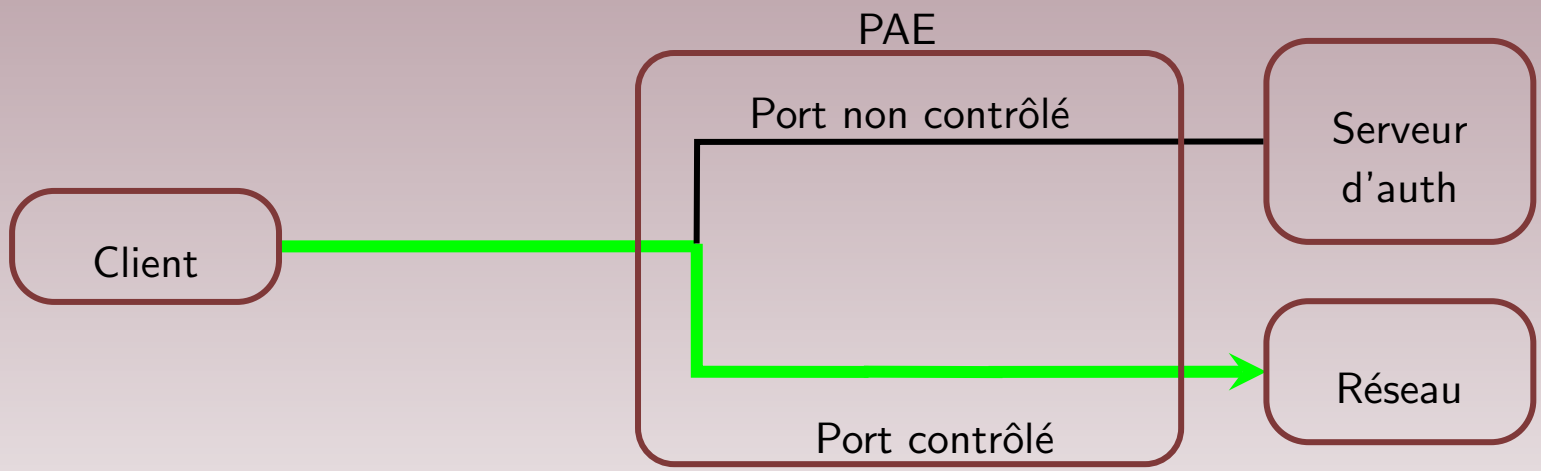
- Début de connexion : port en état non contrôlé.
- Seuls les paquets 802.1X autorisés.



Détail

Port contrôlé

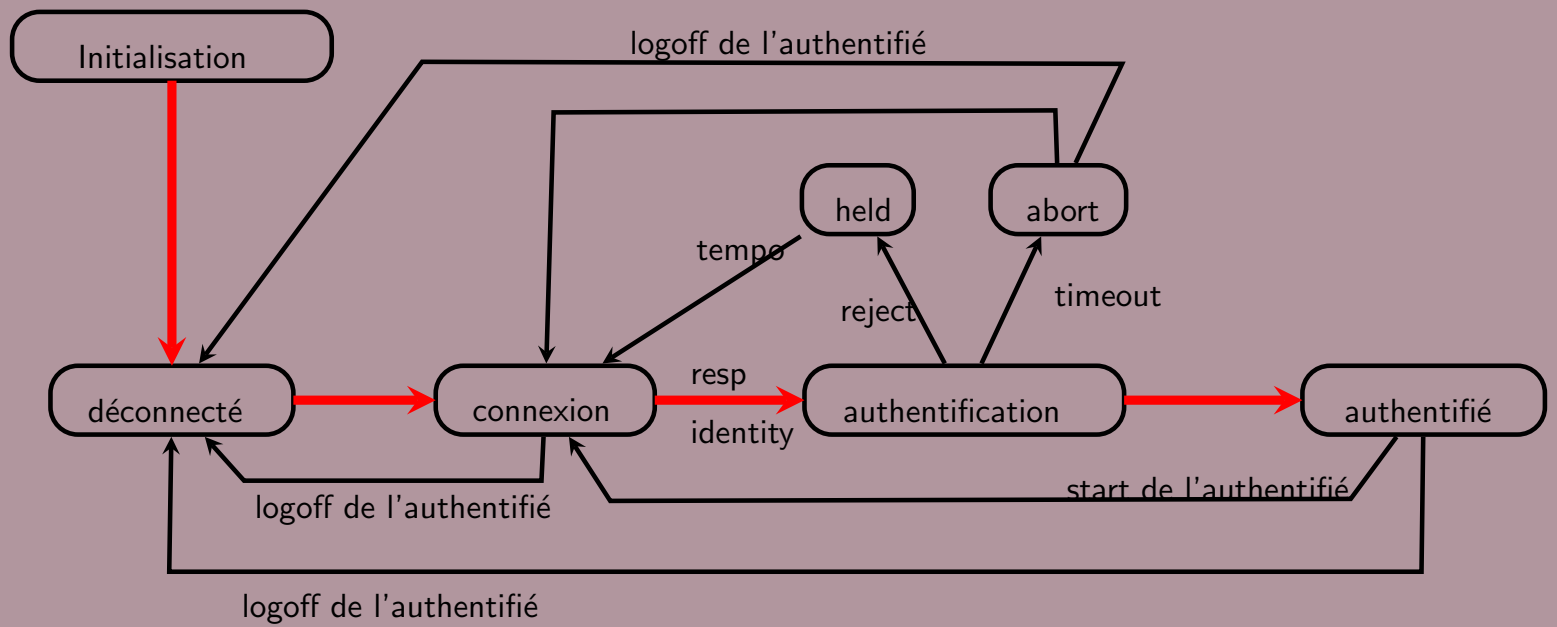
- Auth ok : port en état contrôlé.
- Tous les flux acceptés



Authenticateur

- Initialisation : activation du proto, de la prise, du matériel

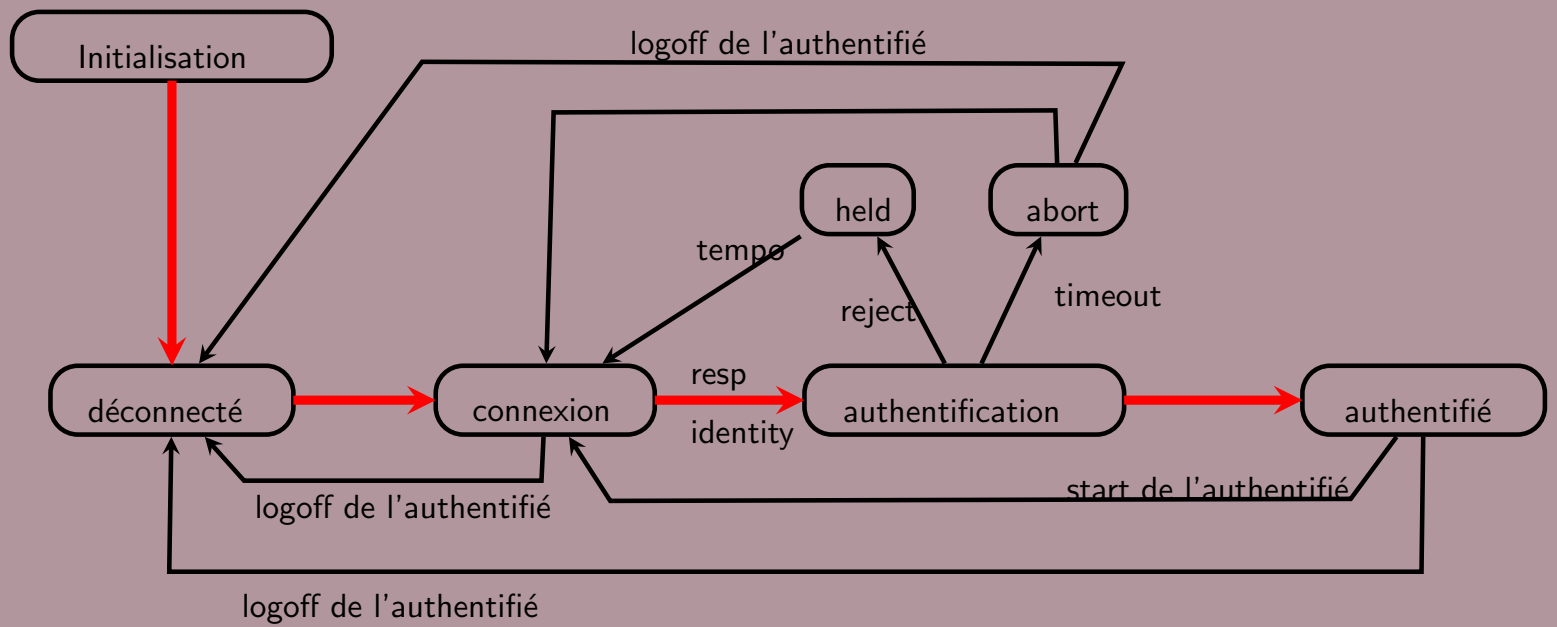
Automate



Authenticateur

- Déconnecté : port physique actif, port controlé ouvert
- Connexion : envoi EAP-Identify au client, puis attend réponse

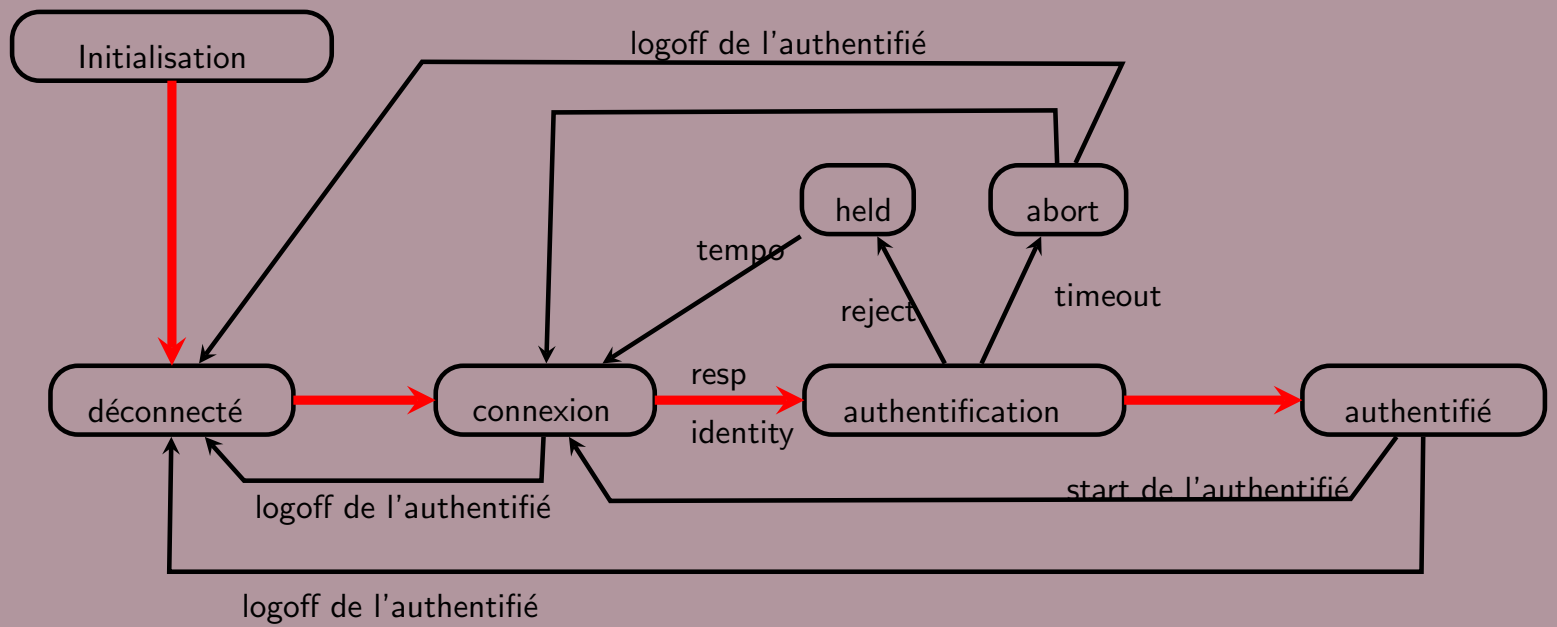
Automate



Authenticateur

- Authentification : relais vers serveur d'auth
- Authentifié : port controlé fermé (accés ok)

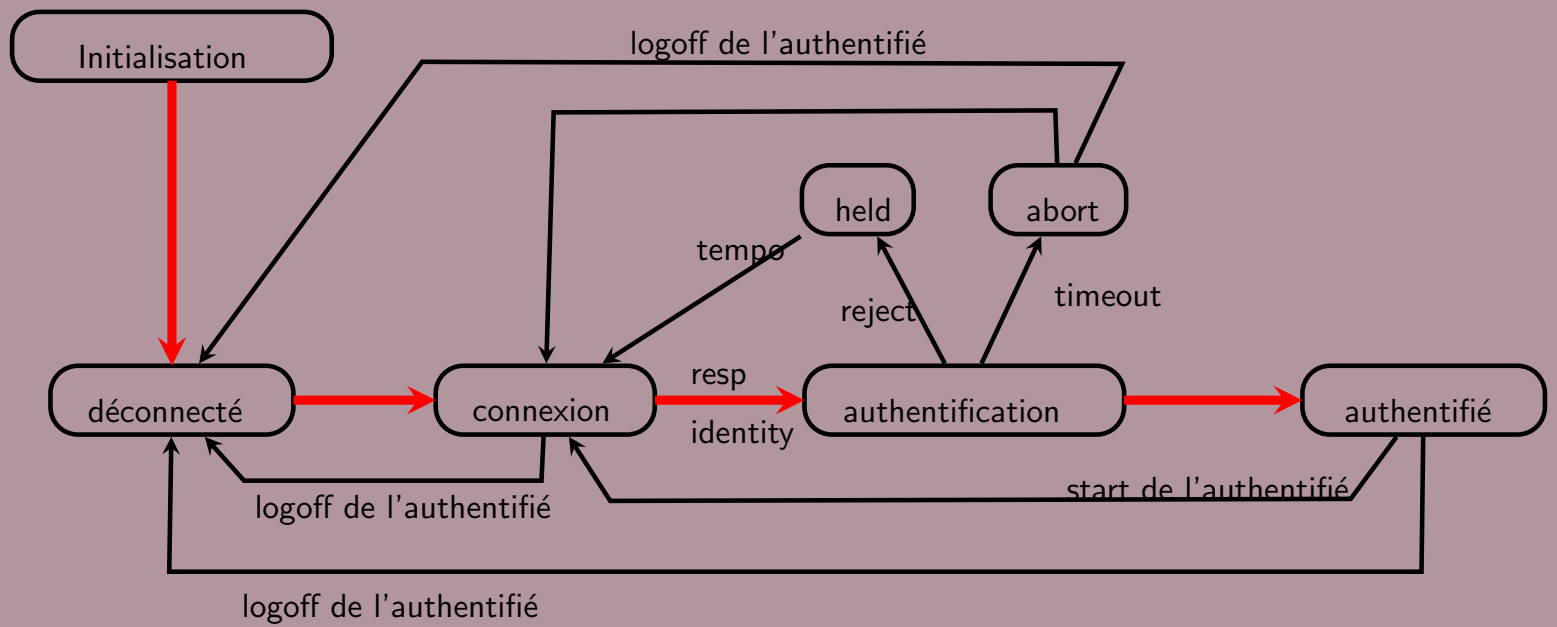
Automate



Authenticateur

- Held : tempo (parade brute force), tout ignoré
- Abort : auth interrompue (logoff, re-auth, start . . .)

Automate



Types d'EAP

EAP-TLS (Transport Layer Security)

Authentification par certificat du client et du serveur

Types d'EAP

EAP-TLS (Transport Layer Security)

Authentification par certificat du client et du serveur

EAP-TTLS (Tunneled Transport Layer Security)

Authentification par certificat et mot de passe grâce à la génération d'un tunnel sécurisé

Types d'EAP

EAP-TLS (Transport Layer Security)

Authentification par certificat du client et du serveur

EAP-TTLS (Tunneled Transport Layer Security)

Authentification par certificat et mot de passe grâce à la génération d'un tunnel sécurisé

EAP-MD5

Authentification avec mot de passe

Types d'EAP

EAP-TLS (Transport Layer Security)

Authentification par certificat du client et du serveur

EAP-TTLS (Tunneled Transport Layer Security)

Authentification par certificat et mot de passe grâce à la génération d'un tunnel sécurisé

EAP-MD5

Authentification avec mot de passe

PEAP (Protected EAP)

Authentification avec mot de passe via une encapsulation sécurisée

Types d'EAP

EAP-TLS (Transport Layer Security)

Authentification par certificat du client et du serveur

EAP-TTLS (Tunneled Transport Layer Security)

Authentification par certificat et mot de passe grâce à la génération d'un tunnel sécurisé

EAP-MD5

Authentification avec mot de passe

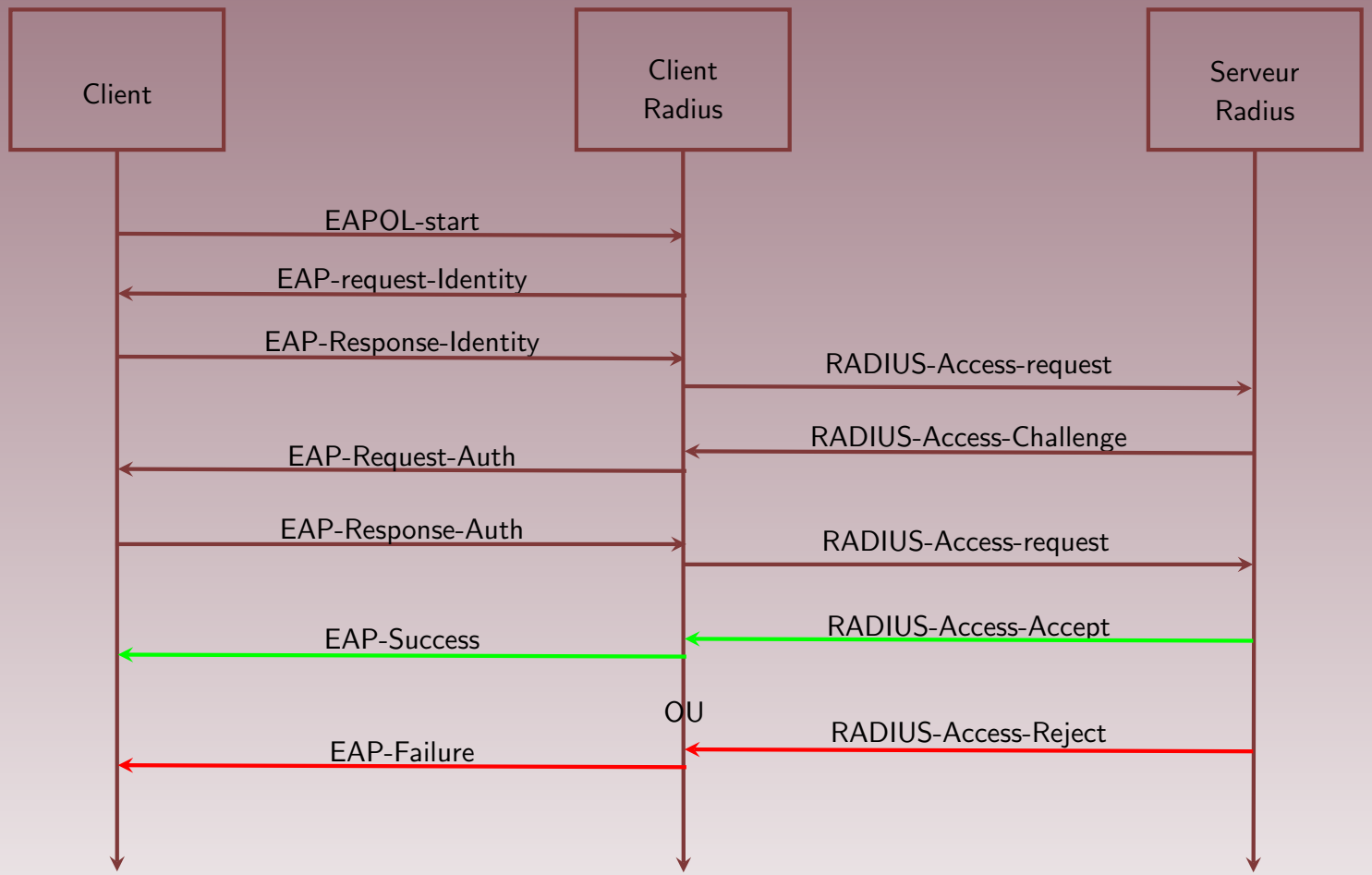
PEAP (Protected EAP)

Authentification avec mot de passe via une encapsulation sécurisée

LEAP (protocole Cisco)

Authentification avec mot de passe via une encapsulation sécurisée

Session 802.1X/EAP



Divers

MAC authentication bypass

Pour le matériel sans supplicant (imprimantes . . .)

Voix

Switchs et routeurs supportent configuration de VoiceVlan sur interfaces 802.1x

Faiblesses

802.1x

- Vieux matériels faibles : spoofing, hub
- Des contremesures existent maintenant

Faiblesses

802.1x

- Vieux matériels faibles : spoofing, hub
- Des contremesures existent maintenant

Radius

- Secret partagé (taille courte = brute force, dico)
- Secret fragile (interception Access Request/Response)
- Hash faible du UserPassword (MD5)
- Rejeu des réponses du serveur possible

Plan

Environnement

Tests en environnement de production

Environnement

Tests en environnement de production

Humain

- Georges Schwing
- Moi
- Bonnes volontées locales

Environnement

Tests en environnement de production

Humain

- Georges Schwing
- Moi
- Bonnes volontées locales

Matériel

- 2 Catalyst 6800 en Virtual Switching System (VSS)
- Carte Firewall
- Switchs cisco
- Clients de test

Environnement

Tests en environnement de production

Humain

- Georges Schwing
- Moi
- Bonnes volontées locales

Matériel

- 2 Catalyst 6800 en Virtual Switching System (VSS)
- Carte Firewall
- Switchs cisco
- Clients de test

Logiciel

- Plateforme VMWare
- VMs pour les serveurs
- Supplicant : Windows, Linux, Mac

Choix de déploiement

Réseau guest : Vlan666

- Adresses privées en 198.168.x.x
- Pas d'accès en entrée
- En sortie : ports 80 et 443
- Pas de communications vers/de les autres Vlans

Choix de déploiement

Réseau guest : Vlan666

- Adresses privées en 198.168.x.x
- Pas d'accès en entrée
- En sortie : ports 80 et 443
- Pas de communications vers/de les autres Vlans

Choix EAP (Idem Eduroam) = Nomadisme

- Securité : WPA et WPA2 Entreprise
- Authentication : Tunneled TLS
- Inner authentication : PAP
- User + Password

Mise en place : supplicant

À l'utilisateur

- Linux : NetworkManager, WPA supplicant ...
- Windows > XP : expérience Eduroam
- Mac : en standard (si OS récent)

Mise en place : authenticateur

Switch Cisco

```
(config)#aaa new-model
(config)#aaa authentication dot1x default group radius
(config)#aaa authorization network default group radius
(config)#radius-server host 192.168.x.x
(config)#radius-server key passw0rd

(config)#interface range FastEthernet 0/6 - 12
(config-if-range)#switchport mode access
(config-if-range)#dot1x port-control auto
(config-if-range)#dot1x guest-vlan 40
(config-if-range)#exit
(config)#dot1x system-auth-control
```

Mise en place : authenticateur

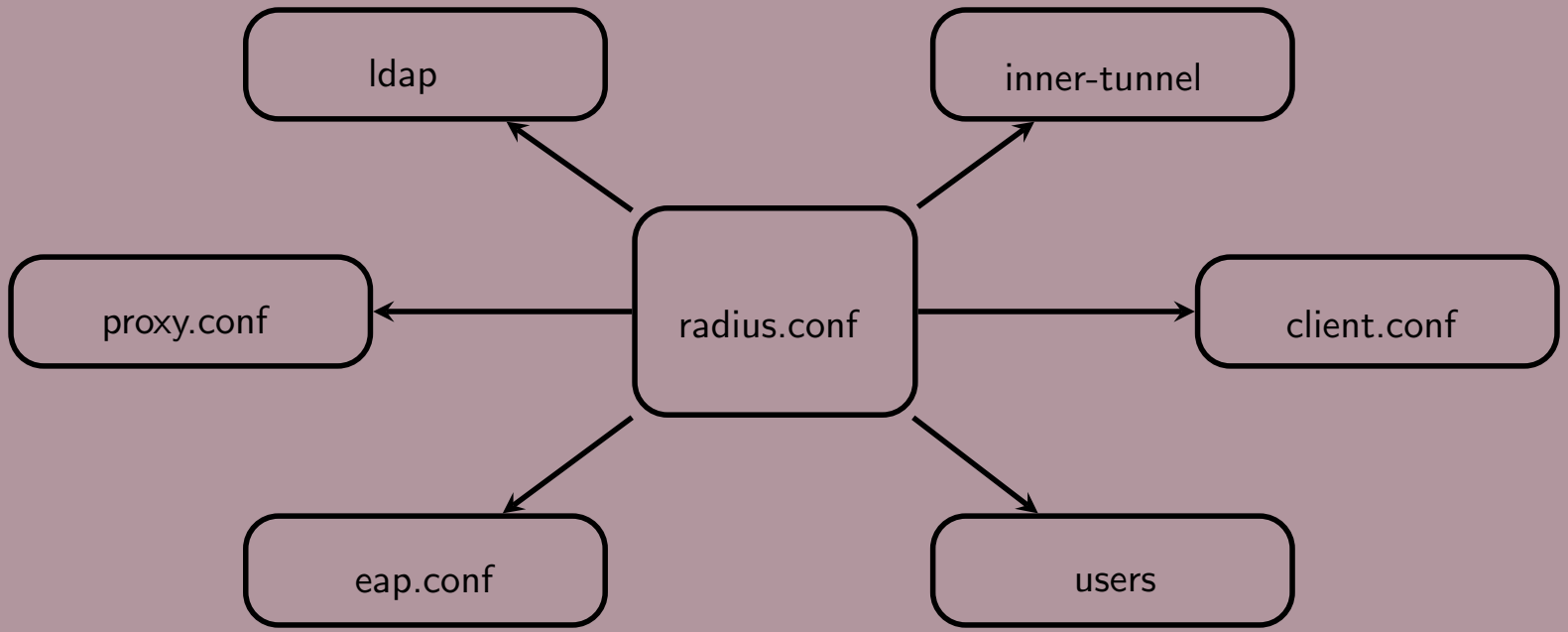
Attention à l'IOS

```
Cisco IOS Release 12.2(33)SXI or later releases:
 Router(config)# interface fastethernet 5/1
 Router(config-if)# authentication port-control auto
 Router(config-if)# authentication event fail retry 3 \
                    action authorize vlan 2
 Router(config-if)# dot1x pae authenticator

Releases earlier than Release 12.2(33)SXI:
 Router(config)# interface fastethernet 5/1
 Router(config-if)# dot1x port-control auto
 Router(config-if)# dot1x auth-fail vlan 2
 Router(config-if)# dot1x auth-fail max-attempts 3
```

Mise en place : serveur d'authentification

FreeRadius



Exemple FreeRadius

Radius en TTLS (eap.conf)

```
eap {
default_eap_type = ttls
timer_expire     = 60
ignore_unknown_eap_types = no
  gtc { auth_type = PAP }
tls {
certdir = ${confdir}/certs
cadir = ${confdir}/certs
    private_key_file = ${raddbdir}/certs/xxx.key
    certificate_file = ${raddbdir}/certs/xxx.pem
    CA_file = ${raddbdir}/certs/ca-terena.pem
    dh_file = ${raddbdir}/certs/dh
    random_file = ${raddbdir}/certs/random
cipher_list = "DEFAULT"
make_cert_command = "${certdir}/bootstrap"
cache {
      enable = no
      lifetime = 24 # hours
      max_entries = 255
    }
  }
ttls {
default_eap_type = gtc
copy_request_to_tunnel = yes
use_tunneled_reply = yes
  }
}
```

Services et coeur de réseau

Services

- DHCP pour le guest

Services et coeur de réseau

Services

- DHCP pour le guest
- DHCP pour les Vlans

Services et coeur de réseau

Services

- DHCP pour le guest
- DHCP pour les Vlans
- Base utilisateur avec VlanId (ex. ldap) couplé au radius

Services et coeur de réseau

Services

- DHCP pour le guest
- DHCP pour les Vlans
- Base utilisateur avec VlanId (ex. ldap) couplé au radius

Coeur de réseau

- Relay Dhcp

Services et coeur de réseau

Services

- DHCP pour le guest
- DHCP pour les Vlans
- Base utilisateur avec VlanId (ex. ldap) couplé au radius

Coeur de réseau

- Relay Dhcp
- PAT, NAT

Services et coeur de réseau

Services

- DHCP pour le guest
- DHCP pour les Vlans
- Base utilisateur avec VlanId (ex. ldap) couplé au radius

Coeur de réseau

- Relay Dhcp
- PAT, NAT
- Filtrage

Difficultés

- Doc Cisco pas toujours à jour

Difficultés

- Doc Cisco pas toujours à jour
- Doc pas toujours très claire

Difficultés

- Doc Cisco pas toujours à jour
- Doc pas toujours très claire
- Évolution du firmware (commandes deprecated)

Difficultés

- Doc Cisco pas toujours à jour
- Doc pas toujours très claire
- Évolution du firmware (commandes deprecated)
- Configuration *historique* du matériel

Difficultés

- Doc Cisco pas toujours à jour
- Doc pas toujours très claire
- Évolution du firmware (commandes deprecated)
- Configuration *historique* du matériel
- S.I + ldap adaptés à mettre en place

Conclusion

Mise en place

- Configuration matérielle plutôt simple (avec suptilités)

Conclusion

Mise en place

- Configuration matérielle plutôt simple (avec suptilités)
- Portail captif invité = ajoute complexité

Conclusion

Mise en place

- Configuration matérielle plutôt simple (avec suptilités)
- Portail captif invité = ajoute complexité
- Gros travail sur le S.I.

Conclusion

Mise en place

- Configuration matérielle plutôt simple (avec suptilités)
- Portail captif invité = ajoute complexité
- Gros travail sur le S.I.

À l'usage

- Administration matérielle simplifiée

Conclusion

Mise en place

- Configuration matérielle plutôt simple (avec suptilités)
- Portail captif invité = ajoute complexité
- Gros travail sur le S.I.

À l'usage

- Administration matérielle simplifiée
- Sécurisé

Conclusion

Mise en place

- Configuration matérielle plutôt simple (avec suptilités)
- Portail captif invité = ajoute complexité
- Gros travail sur le S.I.

À l'usage

- Administration matérielle simplifiée
- Sécurisé
- Nomadisme

Conclusion

Mise en place

- Configuration matérielle plutôt simple (avec suptilités)
- Portail captif invité = ajoute complexité
- Gros travail sur le S.I.

À l'usage

- Administration matérielle simplifiée
- Sécurisé
- **Nomadisme**
- Simple (comme Eduroam) pour les utilisateurs

Plan

Références I

[1] Blunk, L., and Vollbrecht, J.
PPP Extensible Authentication Protocol (EAP).
RFC 2284 (Proposed Standard), Mar. 1998.
Obsoleted by RFC 3748, updated by RFC 2484.

[2] Committee, C. L. S.
802.1x-2001 - ieee standard for port based network access control, 2001.
Superseded by: 802.1X-2010.

[3] Group, W. H. L. L. P. W.
802.1x-2010 - ieee standard for local and metropolitan area networks–port-based network access control, 2010.

[4] Rigney, C.
RADIUS Accounting.
RFC 2866 (Informational), June 2000.
Updated by RFCs 2867, 5080, 5997.

[5] Rigney, C., Willats, W., and Calhoun, P.
RADIUS Extensions.
RFC 2869 (Informational), June 2000.
Updated by RFCs 3579, 5080.

[6] Rigney, C., Willens, S., Rubens, A., and Simpson, W.
Remote Authentication Dial In User Service (RADIUS).
RFC 2865 (Draft Standard), June 2000.
Updated by RFCs 2868, 3575, 5080, 6929.

[7] Simpson, W.
The Point-to-Point Protocol (PPP).
RFC 1661 (INTERNET STANDARD), July 1994.
Updated by RFC 2153.

Références II

[8] Zorn, G., Aboba, B., and Mitton, D.
RADIUS Accounting Modifications for Tunnel Protocol Support.
RFC 2867 (Informational), June 2000.

[9] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and Goyret, I.
RADIUS Attributes for Tunnel Protocol Support.
RFC 2868 (Informational), June 2000.
Updated by RFC 3575.

Plan

Questions ?

?