Le protocole Radius

RADIUS (*Remote Authentication Dial-In User Service*)
Protocole d'authentification standard, défini par un certain nombre de RFC.

Les ***requests for comments*** (**RFC**), littéralement « demande de commentaires », sont une série numérotée de documents décrivant les aspects et spécifications techniques d'Internet, ou de différents matériels informatiques (routeurs, serveur DHCP)

Serveur AAA

Authentication, Authorization, Accounting,

En français

- authentification,
- autorisation
- compte.

Radius serveur AAA

- – Authentification : l'authentification consiste à vérifier qu'une personne/équipement est bien celle qu'elle prétend être.
- – Autorisation : l'autorisation consiste à permettre l'accès à certains services ou ressources.
- – Compte : le serveur AAA a la possibilité de collecter des informations sur l'utilisation des ressources. Ceci permet à un opérateur de facturer un utilisateur suivant sa consommation.

Radius

- Fonctionnement basé sur un système client/serveur
- Définit les accès d'utilisateurs distants à un réseau.
- Il s'agit du protocole de prédilection des fournisseurs d'accès à internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

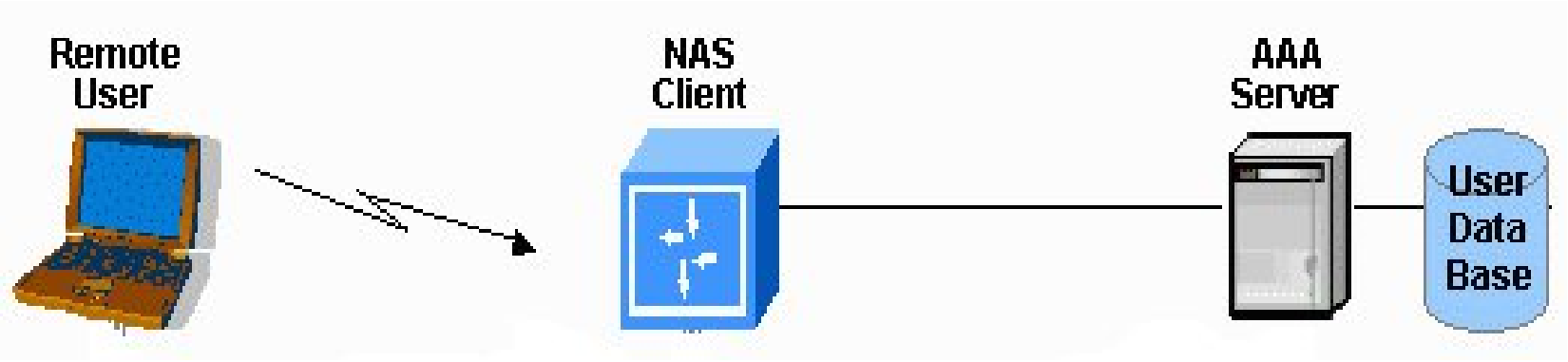
Client - serveur

- Le serveur RADIUS est relié à une base d'identification (base de données, annuaire LDAP, Active Directory etc.)
- Un client RADIUS, appelé **NAS** (*Network Access Server*), faisant office d'intermédiaire entre l'utilisateur final et le serveur.

L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé.

Radius : fonctionnement

Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance

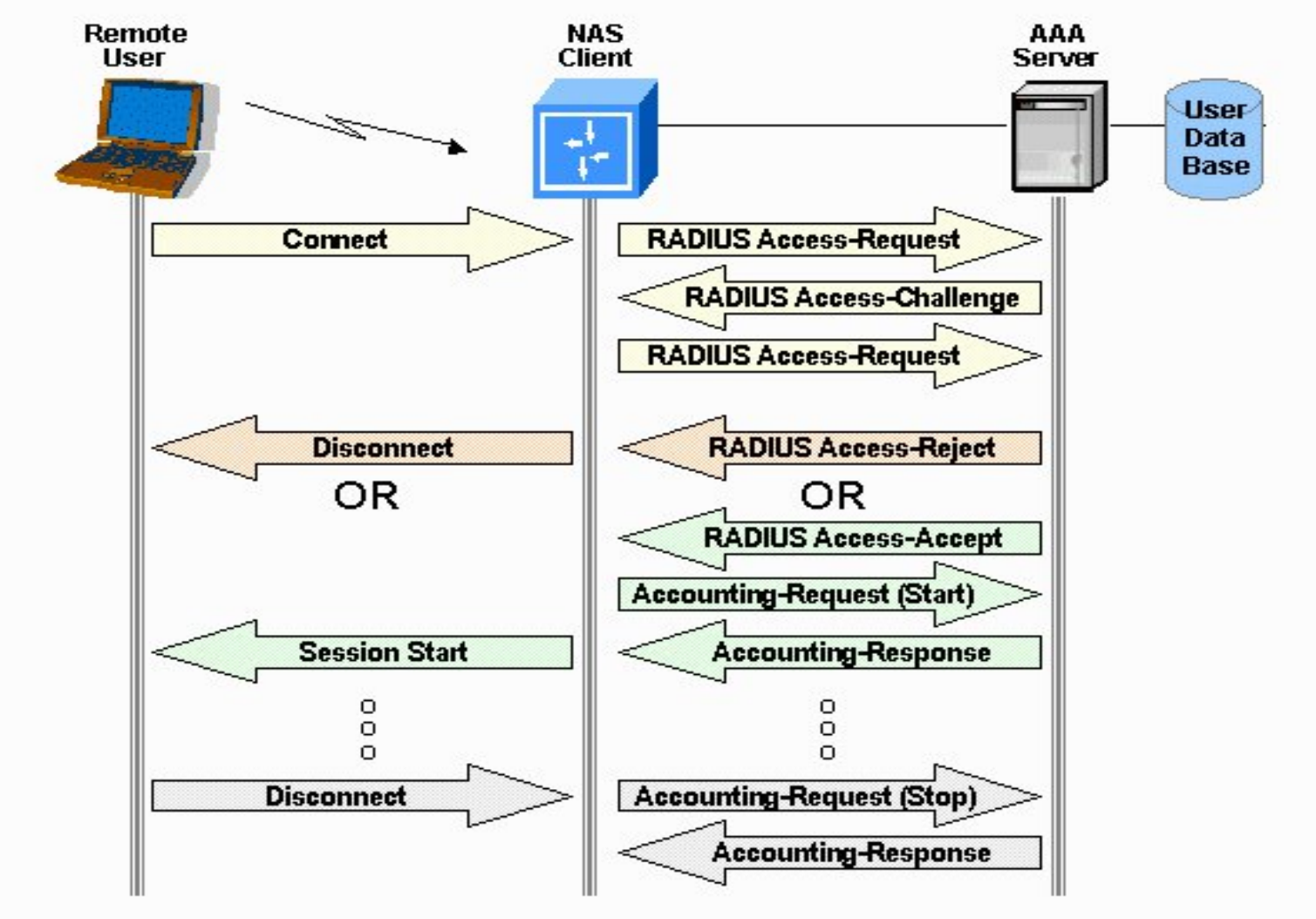


Le NAS achemine la demande au serveur RADIUS

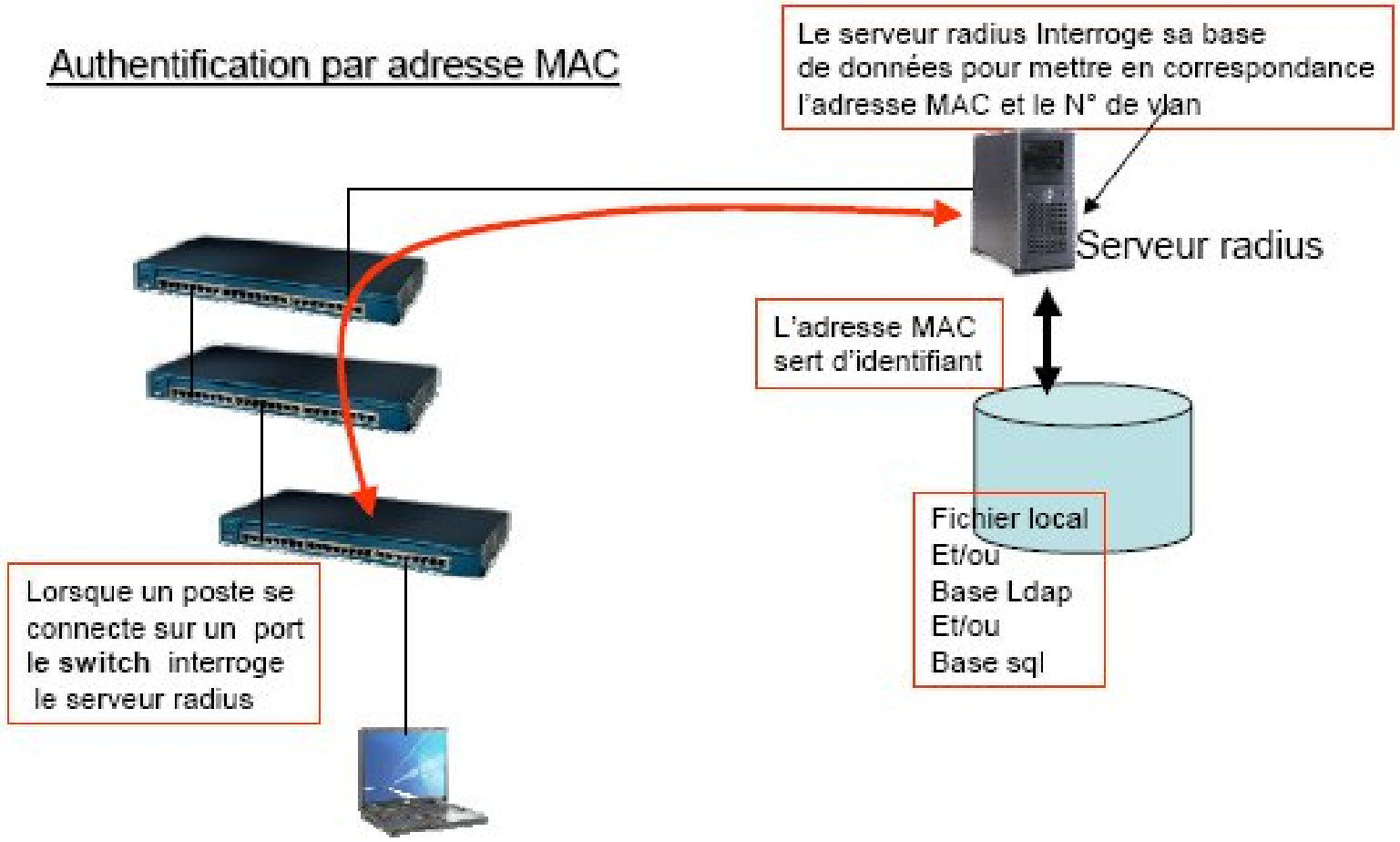
Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur.

- Soit le scénario actuel convient, soit une autre méthodes d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
  - **ACCEPT** : l'identification a réussi ;
  - **REJECT** : l'identification a échoué ;
  - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « *challenge* ») ;
  - **CHANGE PASSWORD** : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.
- Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

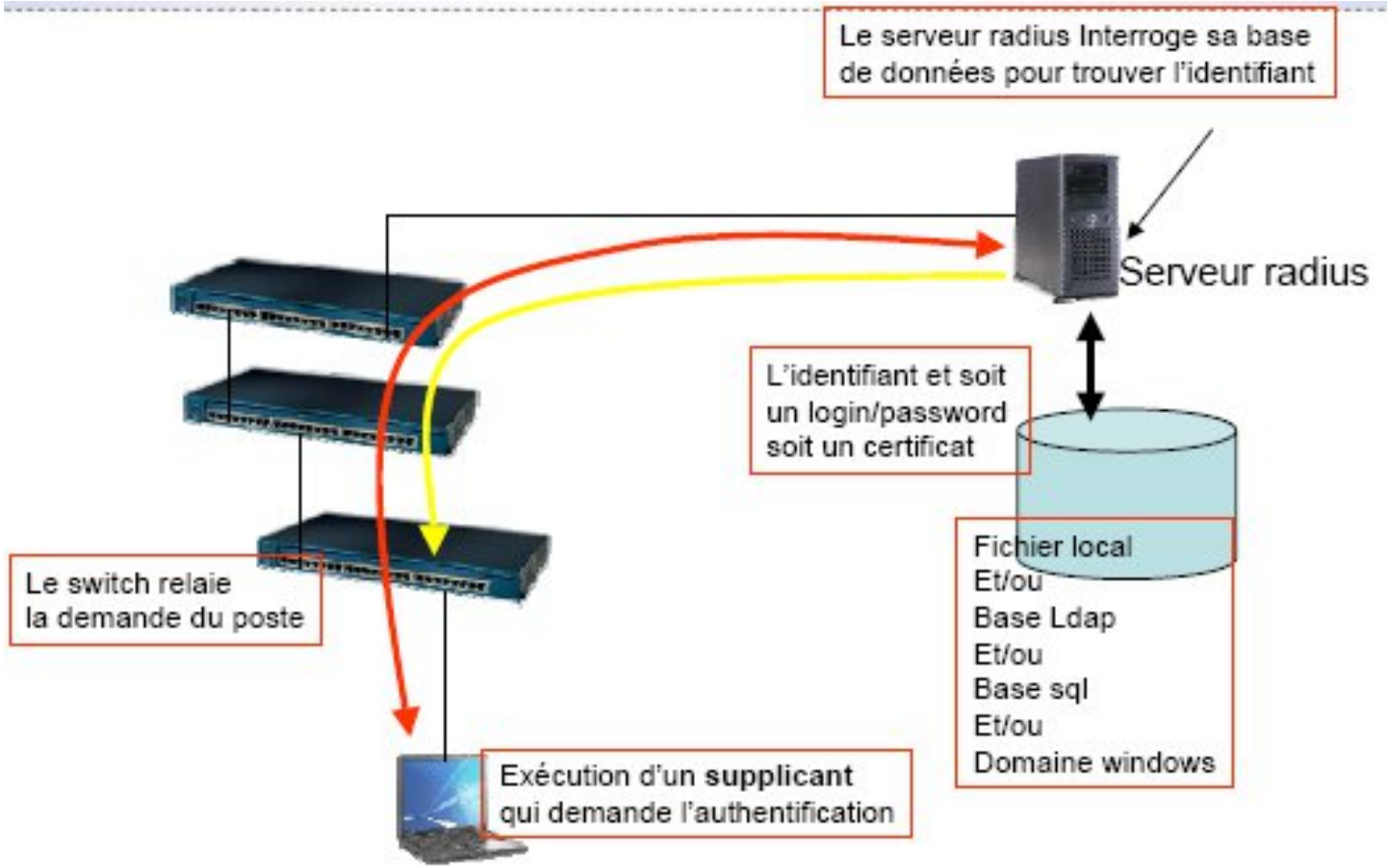
Les échanges clients-serveurs



Utilisation de Radius



Radius et 802.1x



802.1X Contrôle d’accès aux switchs et bornes wifi

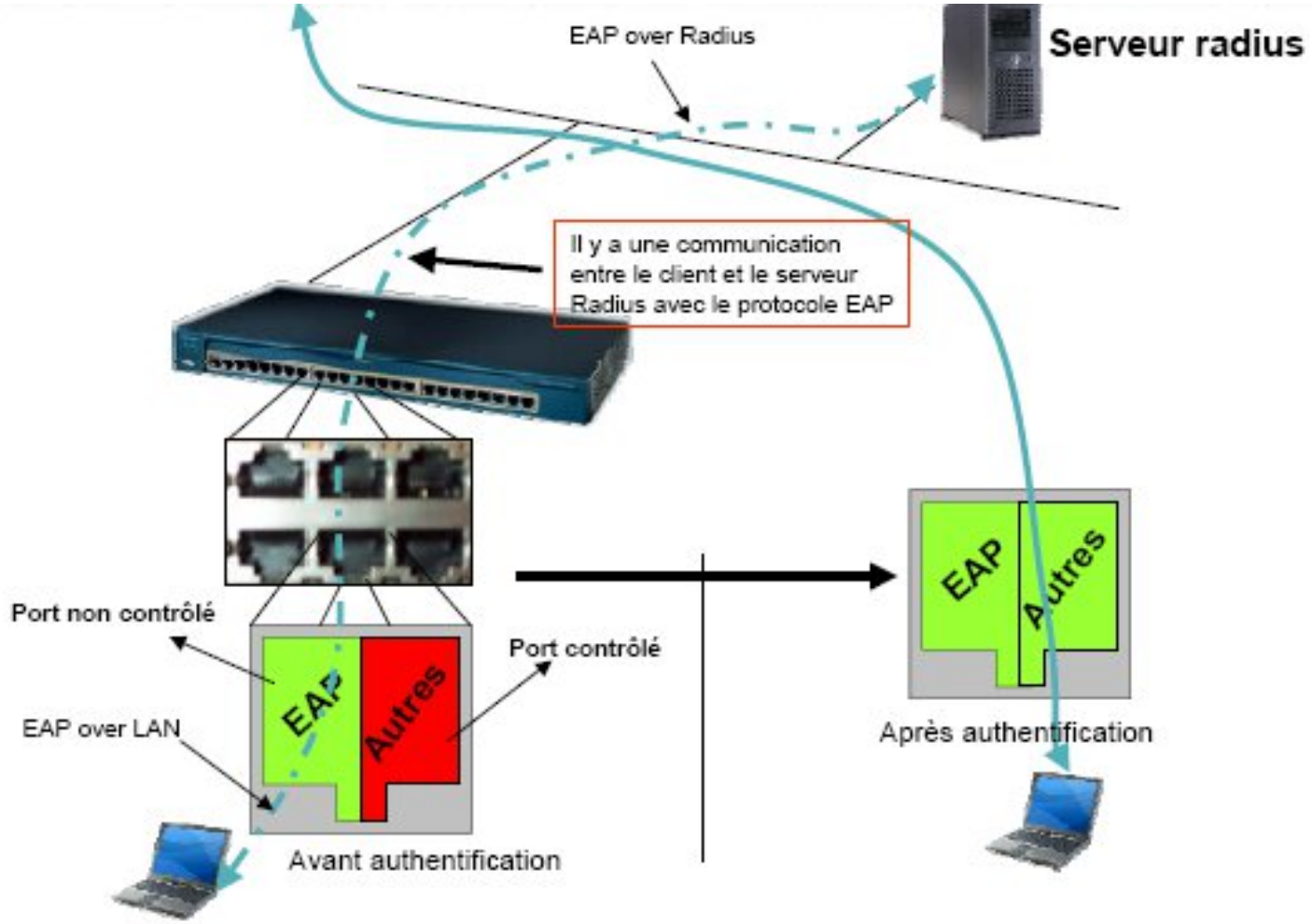
- **802.1X** Il permet de contrôler l'accès aux équipements d'infrastructures réseau (et par ce biais, de relayer les informations liées aux dispositifs d'identification).
- En s'appuyant sur le protocole EAP pour le transport des informations d'identification en mode client/serveur, et sur un serveur d'authentification (tel que RADIUS, TACACS, CAS, etc.) le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.

- Si un équipement réseau actif, tel qu'un commutateur réseau ou une borne Wi-Fi est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (PAE : Port Access Entity).

Le standard 802.1 X utilise un serveur Radius

- La mise en œuvre d'un contrôle d'accès par port 802.1X nécessite l'activation du standard IEEE 802.1X sur :
- les commutateurs réseau ou les points d'accès sans fil (clients d'identification) ;
- chaque point terminal appelé « supplicant » en EAP ordinateur hôte (et éventuellement chaque imprimante, PDA, équipement VOIP, etc.) ;
- le serveur d'identification est chargé de valider l'identité de l'utilisateur du port ; la norme 802.1X ne présente qu'un seul exemple de protocole : RADIUS, seule mise en œuvre actuelle.

Contrôle des connections



Les protocoles utilisés

802.1x met en œuvre le protocole EAP pour les communications du client vers le serveur d'authentification.

EAP (Extensible Authentication Protocol) est un protocole de transport de protocole d'authentification.

L'intérêt de l'architecture de EAP est de pouvoir utiliser divers mécanismes d'authentification sans que l'équipement réseau (NAS) aient besoin de les connaître. Dans ce cas il agit comme un tunnel transparent vers un serveur qui lui implémente les mécanismes souhaités.

Par exemple: Mot de passe, certificats, carte à puce ….

Protocole EAP - PEAP

Principales méthodes d'authentification EAP:

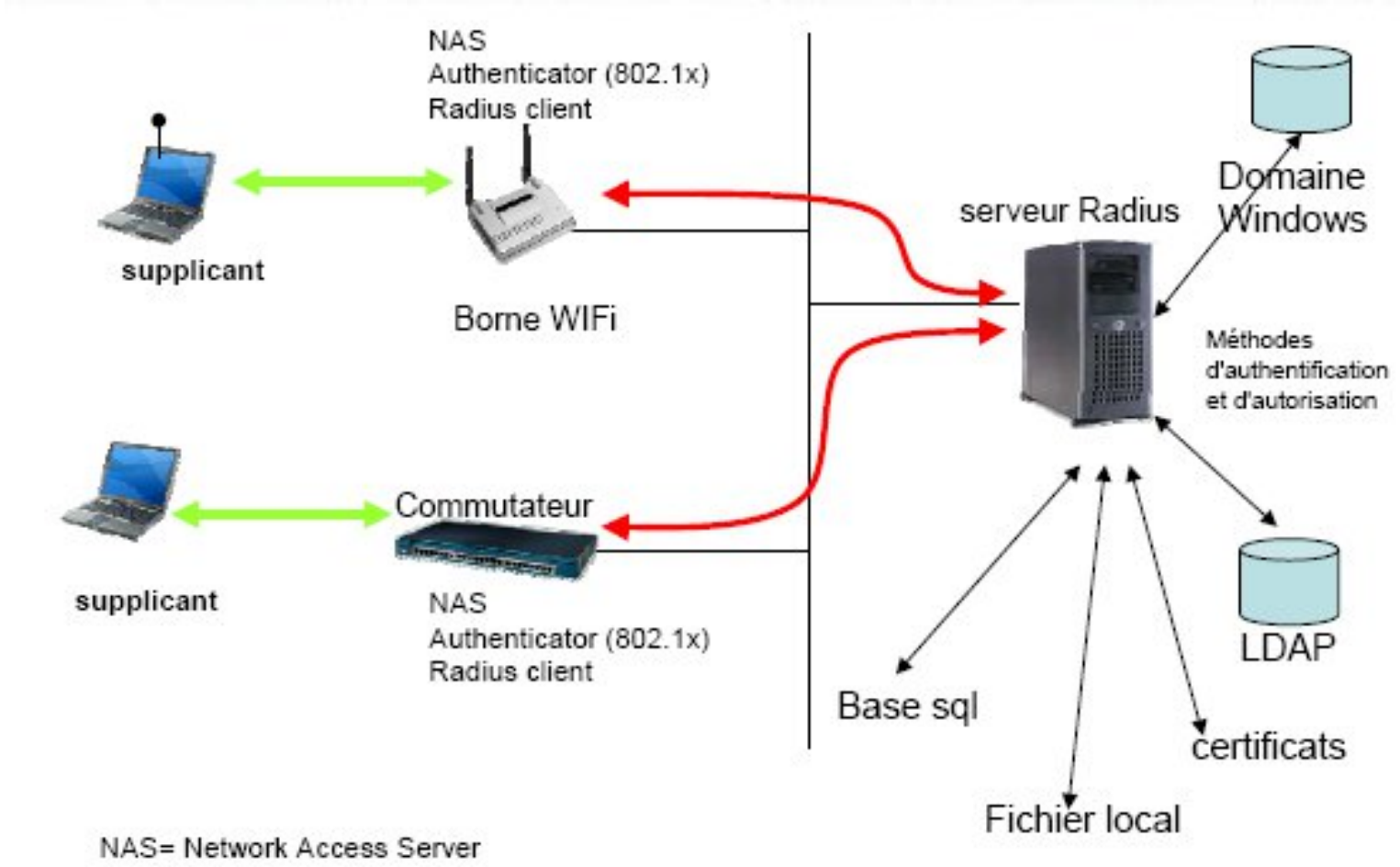
- **EAP/TLS**

  Authentification mutuelle entre le serveur et le client par certificat.

- **EAP/PEAP ou EAP/TTLS**

  Le client est authentifié par un login/mot de passe.
  Le serveur peut être authentifié par son certificat.

Les solutions



Utilisation de Radius

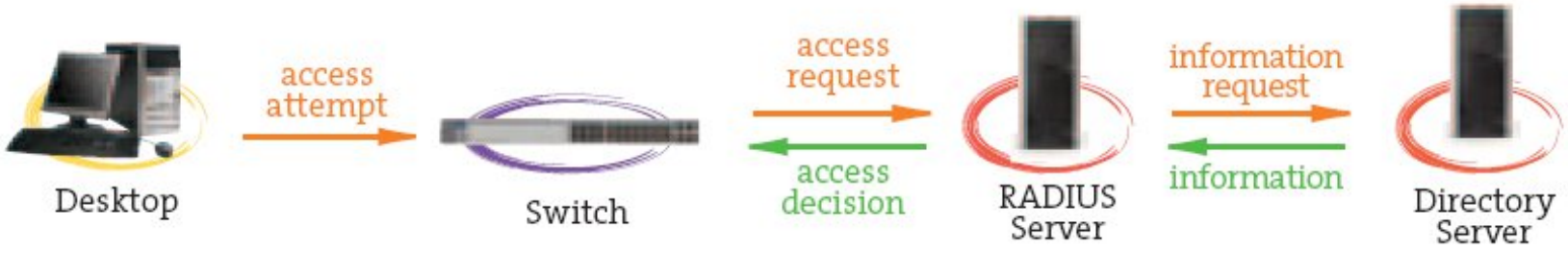
Network access control is based on four elements:

The Client
(network user).

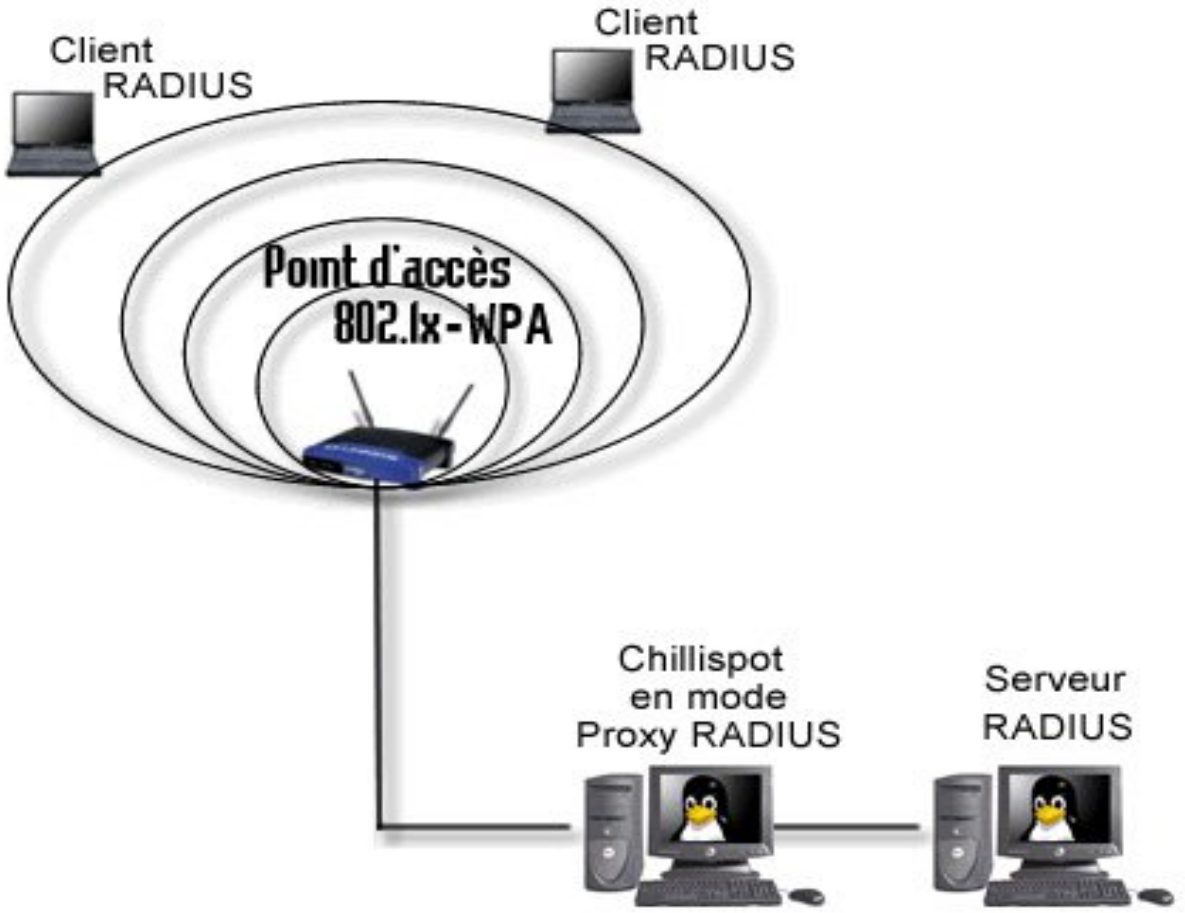
The Policy Enforcement Point (PEP)
has two roles:
access request generator
and access decision enforcer.

The Policy Decision Point (PDP)
translates network policies into instructions that policy enforcement points can understand. This entails generation of device-specific configuration information, such as whether to enable/disable forwarding on a port or specifying the VLAN VID for a port.

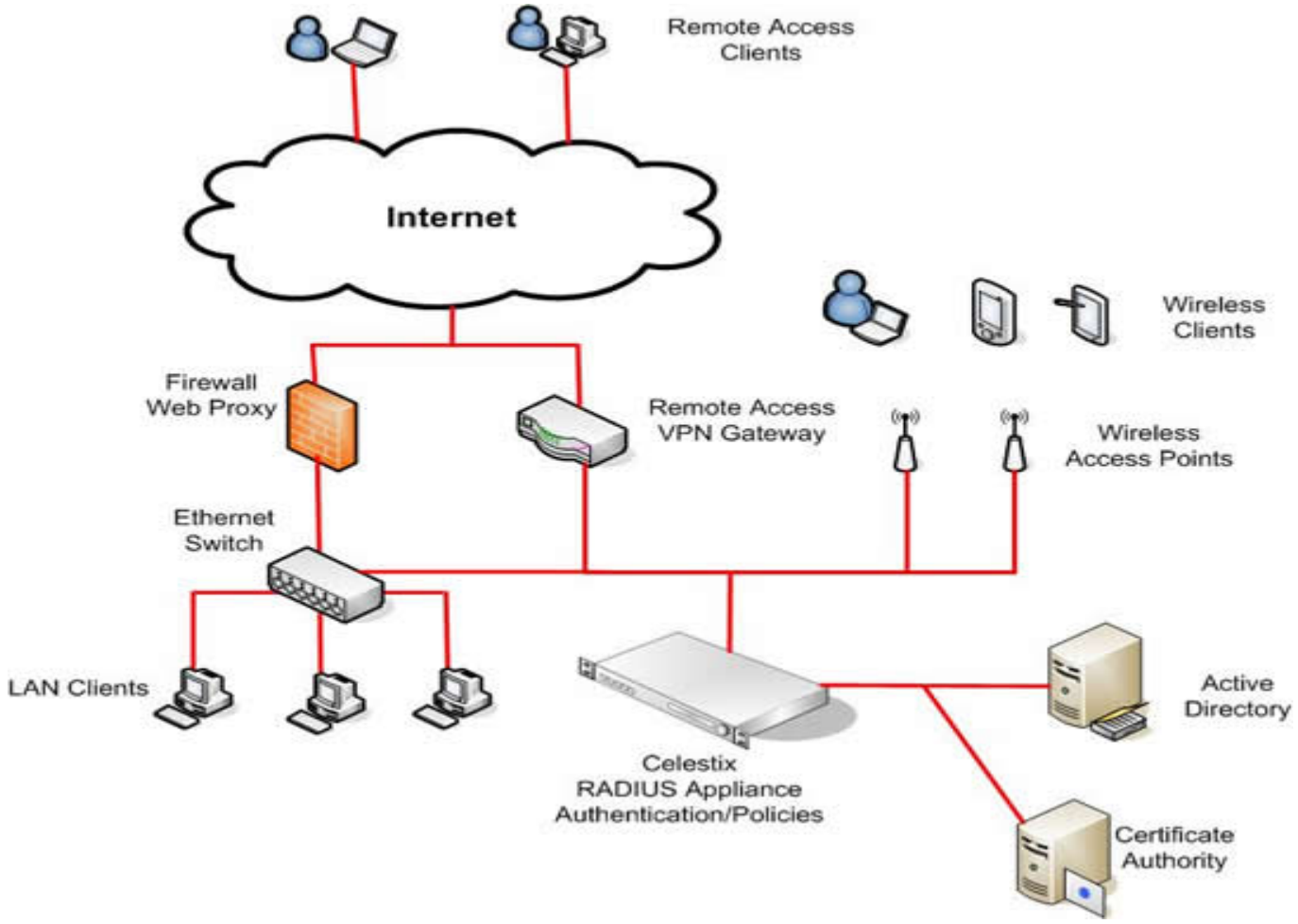
The Policy Repository
has the primary role of storing the network policy rules. Network policies relate to information about users, such as their current MAC address, IP address, or location at a particular time of day.



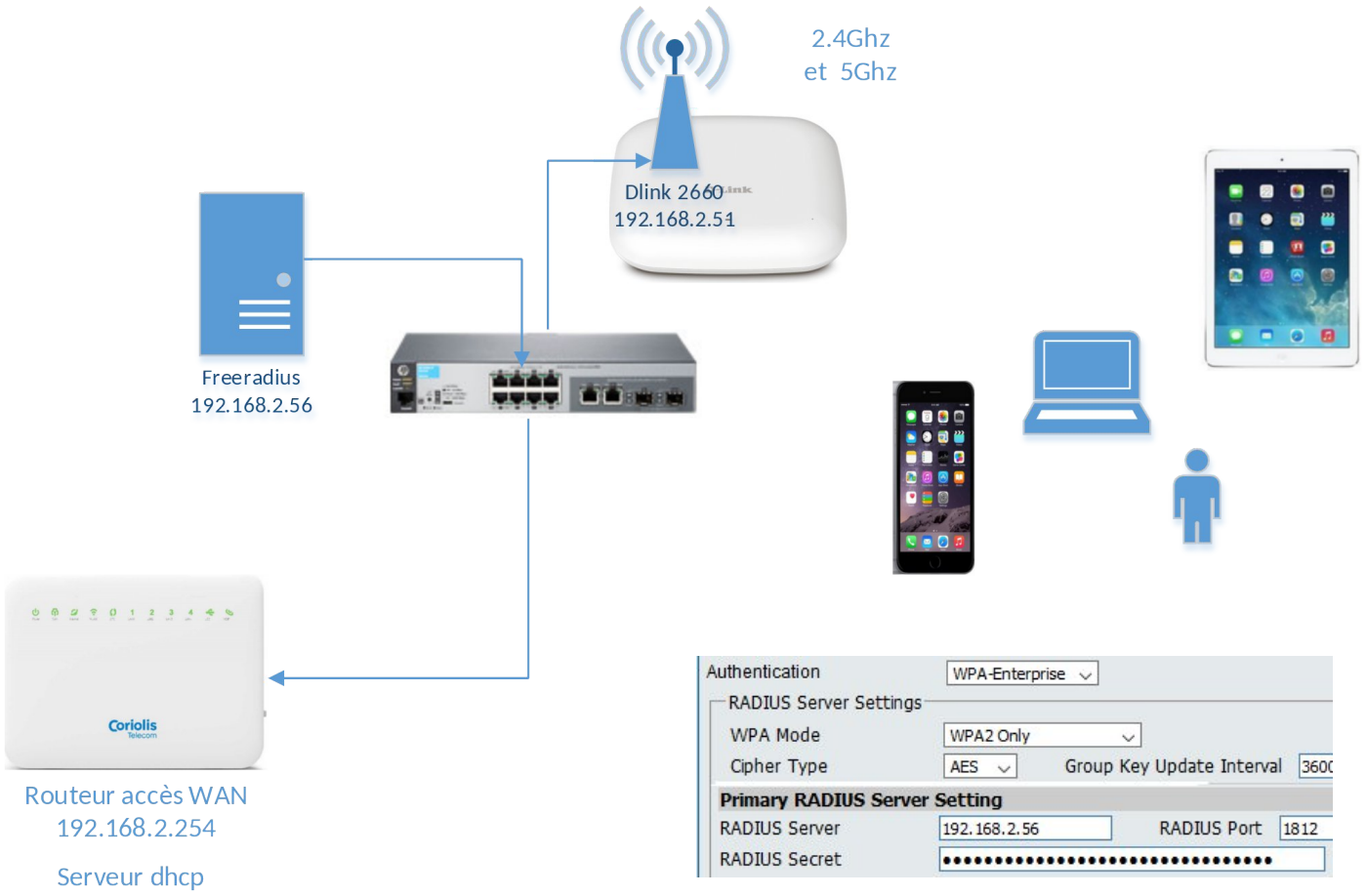
Architecture -Radius



Radius

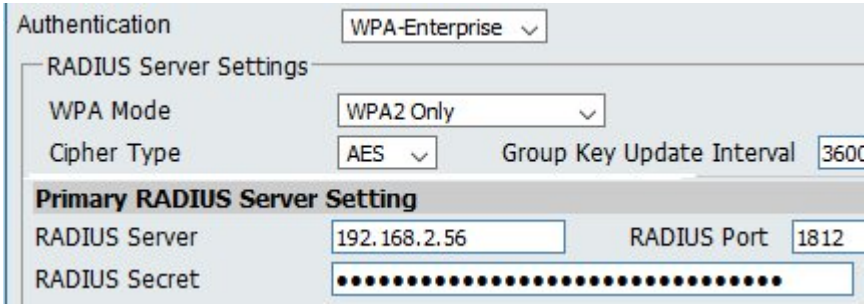

Remote Access
Clients
Internet
Wireless
Clients
Firewall
Web Proxy
Remote Access
VPN Gateway
Wireless
Access Points
Ethernet
Switch
LAN Clients
Active
Directory
Celestix
RADIUS Appliance
Authentication/Policies
Certificate
Authority

Freeradius3 - Dlink 2660



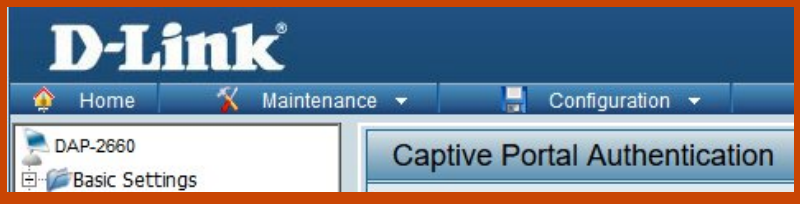
Borne wifi Dlink

Borne wifi supplicant (NAS) du serveur freeradius

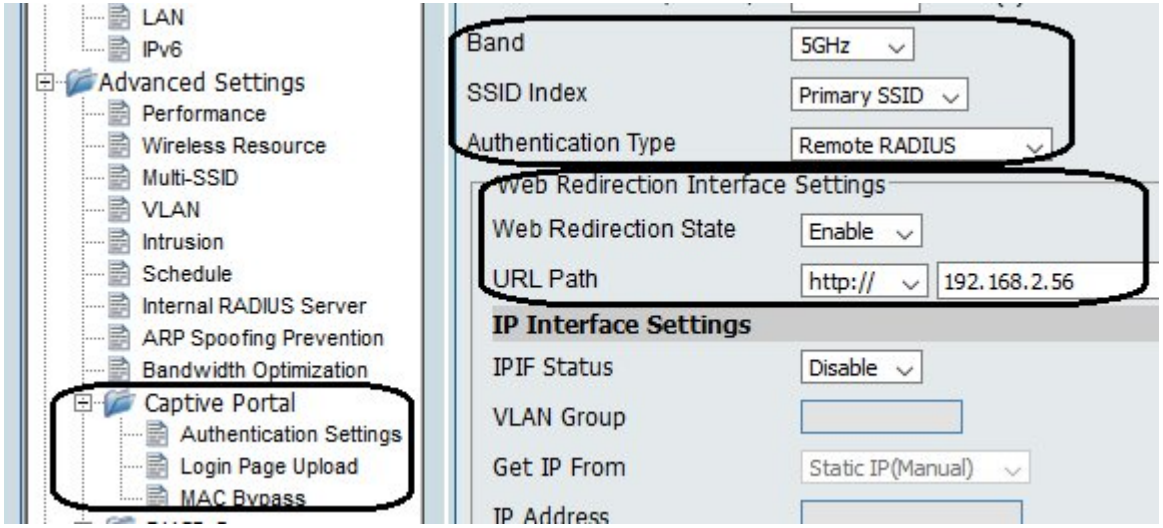


Mode WPA2 (wpa2 Entreprise)
Protocole AES

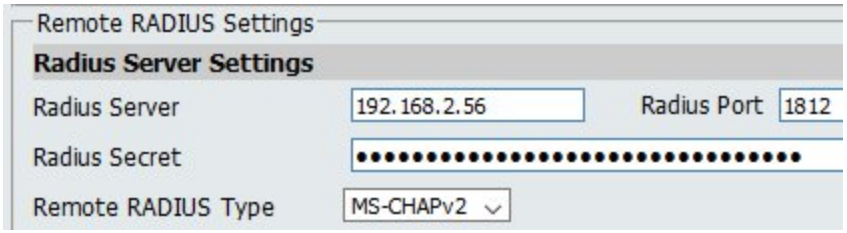
AP portail captif



Portail captif activé
Redirection vers page d'accueil



Authentification sur
serveur Free radius 3
Protocole MS-Chapv2



Serveur NPS (Microsoft) en tant que serveur RADIUS pour un large éventail de clients d'accès