TutoJRES 3

Wi-Fi & Eduroam:
de la théorie à la pratique

Centres de Ressources Informatiques
Université de Bourgogne – Iut Le Creusot

Wi-Fi & Eduroam: de la théorie à la pratique

Sommaire:

I. Rappels et concepts :

- Fonctionnement et normalisation,
- Topologies,
- Sécurité par défaut,
- Sécurité avancée,
- Systèmes d'authentification,
- Les réseaux privés virtuels,
- Portails captifs,
- Evolutions.

Rappels concepts : Fonctionnement et normalisation

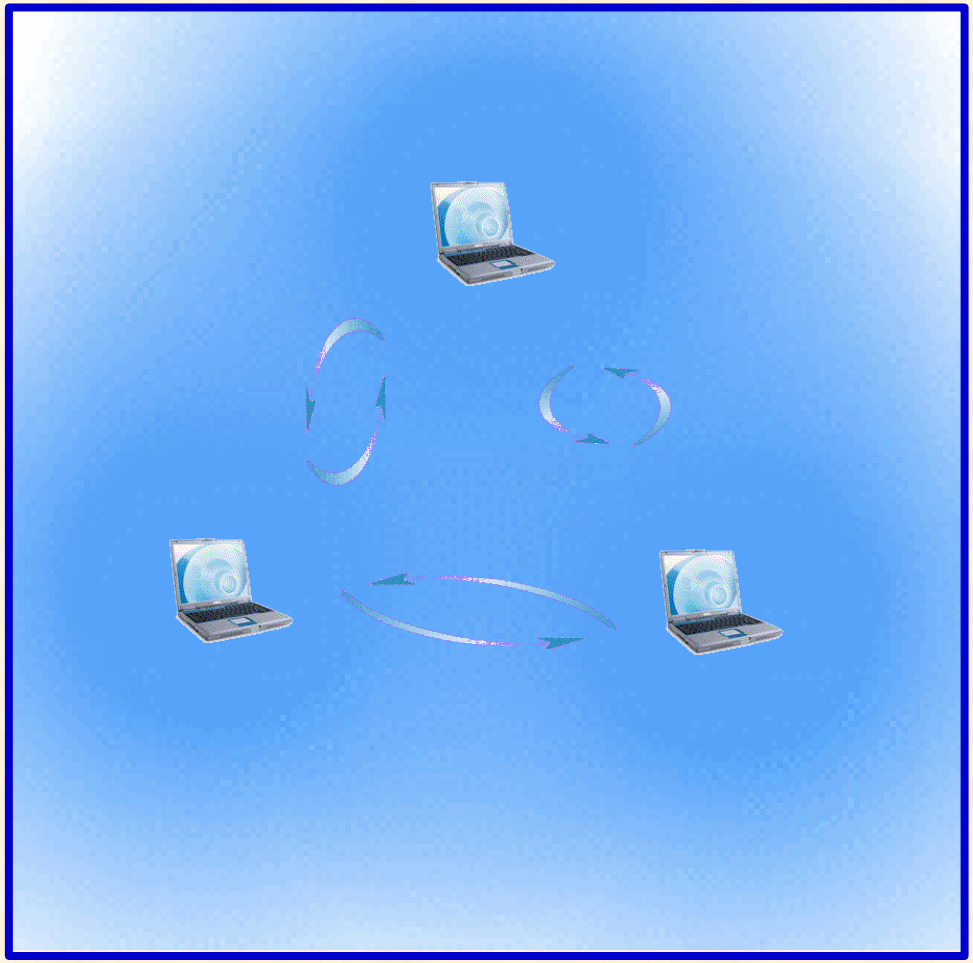
- Dénominations:
  - ✓ WPAN, Wi-Fi, WLAN, WMAN …
- Utilisation des ondes électromagnétiques (radios) pour la communication entre les équipements mobiles,
  - ✓ Bandes de fréquence: 2,4 GHz, 5 GHz
  - ✓ Utilisation de la bande ISM (Industriel Scientifique et Médical) non régulée.
- Architecture cellulaire,
  - ✓ IBSS (Independent Basic Service Set) : réseau ad-hoc
  - ✓ BSS (Basic Service Set) : cellule initiale,
  - ✓ ESS (Extended Service Set) : cellules multiples.
- Les principales normes des réseaux sans fil – normes 802.11 de l'IEEE*:

802.11 a	Débit théorique 54 Mbit/s - fréquences 5 GHz sur 8 canaux (1999) Incompatible 802.11b et g
802.11 b	Débit théorique 11 Mbit/s - fréquences 2,4 GHz sur 14 canaux (1999 13 canaux en France)
802.11g	Débit théorique 54 Mbit/s - fréquences 2,4 GHz (Juillet 2003) compatible 802.11b
802.11n	Débit théorique 300 Mbit/s - fréquences 2,4 et 5 GHz (2006) Compatible 802.11b et g
802.11i	Sécurité des WLAN – norme à volets

* IEEE : Institute of Electrical & Electronics Engineers

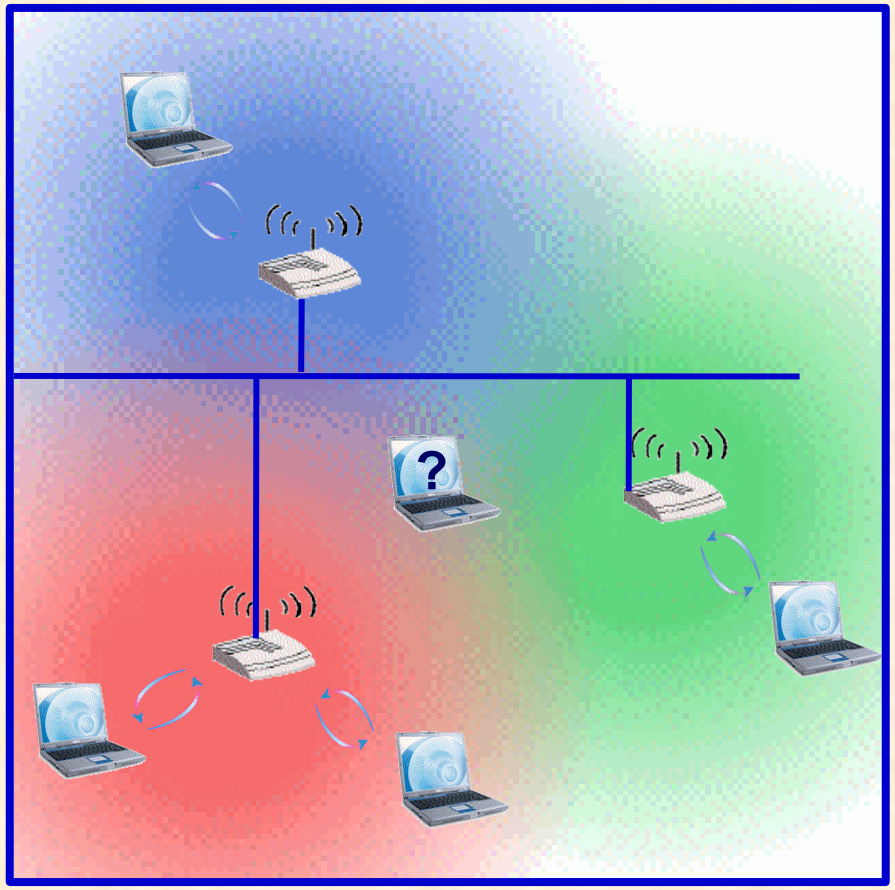
Rappels concepts : Topologies

- Mode « Ad-Hoc »:
  - ✓ Communication directe entre les équipements,
  - ✓ Sécurité limitée (WEP),
  - ✓ Adapté aux réseaux domestiques,
  - ✓ Mise en œuvre simple.



Rappels concepts : Topologies

- Mode « Infrastructure »:
  - ✓ Constitué autour d'un ou plusieurs Points d'Accès (PA),
  - ✓ Le point d'accès est l'élément central de la cellule,
  - ✓ Identification d'un réseau par son SSID (Service Set IDentifier),
  - ✓ SSID identique sur plusieurs PA,
  - ✓ Renforcement de la sécurité initiale,
  - ✓ Lien entre l'accès sans fil et le réseau filaire,
  - ✓ Zone de couverture importante,
  - ✓ Mobilité entre les AP – roaming.



Rappels concepts : Sécurité par défaut

Par défaut, les techniques possibles pour assurer la sécurité sont:

- **SSID (Service Set IDentifier) - identificateur de réseau**:
  - ✓ Le point d'accès et le client doivent utiliser le même SSID lors de l'association,
  - ✓ SSID non chiffré,
  - ✓ Possibilité de supprimer la diffusion du SSID – trames de balisage

- **Cryptage WEP** (Wired Equivalent Privacy): les données qui circulent sur le wlan sont cryptées (algorithme RC4).
  - ✓ Assure l'authentification et le chiffrement (cryptage),
  - ✓ Clé secrète partagée par les stations et le(s) point(s) d'accès,
  - ✓ Clef de chiffrement statique - niveau de sécurité faible,
  - ✓ Identification possible de la clé par observation de trames vulnérables.

- **Filtrage des adresses MAC** (Ethernet): Identifier et autoriser certaines adresses à se connecter.
  - ✓ Administration lourde,
  - ✓ Niveau de sécurité faible, substitution @mac possible.

POINTS IMPORTANTS:

- Les solutions (techniques) de sécurité natives ne sont pas suffisantes.

Rappels concepts : Sécurité avancée

Pour combler les faiblesses du cryptage WEP, WPA (Wi-Fi Protected Access) développé par l'IEEE, offre une sécurité nettement supérieure:

La nouvelle norme de sécurité IEEE 802.11i : **Norme à 2 volets**

- VOLET 1: Solution de transition compatible avec le matériel existant (WPA):
  - ✓ WPA Perso
    - WPA Pre-Shared Key
  - ✓ WPA Entreprise
    - 802.1x + EAP

⇒ **Rotation de clés - TKIP (Temporel Key Integrity Protocol) + algorithme de cryptage RC4**

- VOLET 2: Solution définitive incompatible avec le matériel existant:
  - ✓ WPA2 Perso
    - WPA Pre-Shared Key
  - ✓ WPA2 Entreprise
    - 802.1x + EAP

⇒ **Nouveau cryptage AES (Advanced Encryption Standard) en remplacement de RC4**

- ✓ Incompatibilité avec certains équipements 802.11 actuels.

Rappels concepts : Systèmes d'authentification

WPA Entreprise: authentification indispensable des utilisateurs

La norme IEEE 802.1x: Transport des méthodes d'authentification entre le client et le serveur RADIUS.

EAP (Extensible Authentification Protocol): Protocole de transport des méthodes d'authentification:

- Authentifications par noms d'utilisateurs / mots de passe:
  - ✓ LEAP: méthode propriétaire Cisco,
  - ✓ EAP-MD5 : le client s'authentifie par mot de passe - non adapté aux réseaux sans fil.
- Authentifications basées sur des certificats:
  - ✓ PEAP (Protected EAP): authentification par login / mot de passe - Certificat côté serveur,
  - ✓ EAP-TLS (Transport Layer Security): Certificats X.509 côté client & côté serveur,
  - ✓ EAP-TTLS (Tunneled TLS): Login / mot de passe – certificat côté serveur.
- Authentifications par cartes à puces sécurisées: EAP-SIM
- Biométrie.

Ces solutions requièrent un serveur d'authentification RADIUS.

JRES 2005 – Projet ARREDU - C. CLAVELEIRA – V. CARPIER http://2005.jres.org/slides/7.pdf

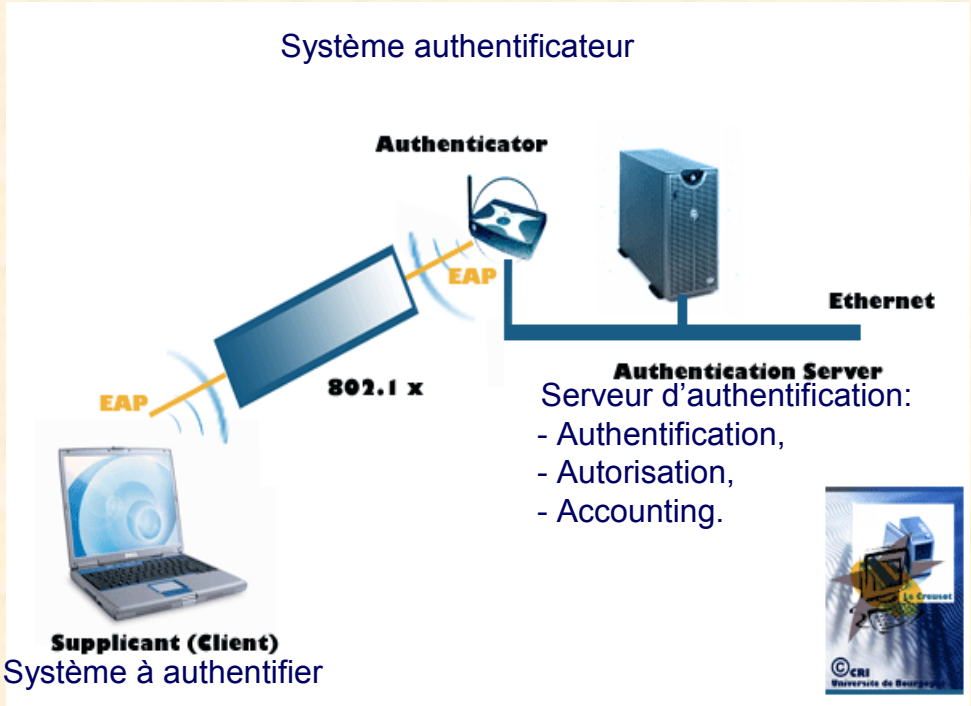
Rappels concepts : Systèmes d'authentification

802.1 x – Radius: Processus d'authentification

1) **Négociation entre le supplicant et le serveur d'authentification via le système authentificateur qui se comporte comme un proxy (trame 802.1X),**

2) **Si l'authentification réussit, le système authentificateur donne accès au supplicant,**

3) **Le serveur d'authentification gère l'authentification en dialoguant avec le système à authentifier.**



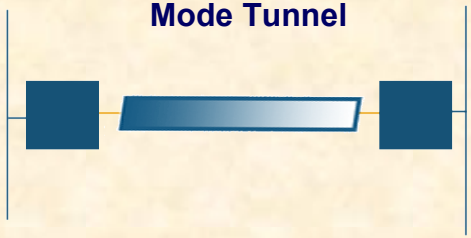
Rappels concepts : Les réseaux privés virtuels

VPN: Réseaux Privés Virtuels

- VPN est totalement indépendant des WLAN,
- L'infrastructure VPN complète efficacement la sécurité des WLAN.
- Services apportés par les VPN:
  - ✓ Authentification et autorisation d'accès:
    - Authentification des deux extrémités,
  - ✓ Chiffrage (confidentialité) et protection (intégrité) des données véhiculées.
  - ✓ Principaux protocoles utilisés:
    - PPTP (Point to Point Tunneling Protocol),
    - L2TP (Layer 2 Tunneling Protocol),
    - IPSEC (IP Security).
- Bande passante diminuée de 30 % en moyenne,
- Problème avec les PDA.

Mode Transport

Mode Tunnel



Rappels concepts : Portails captifs

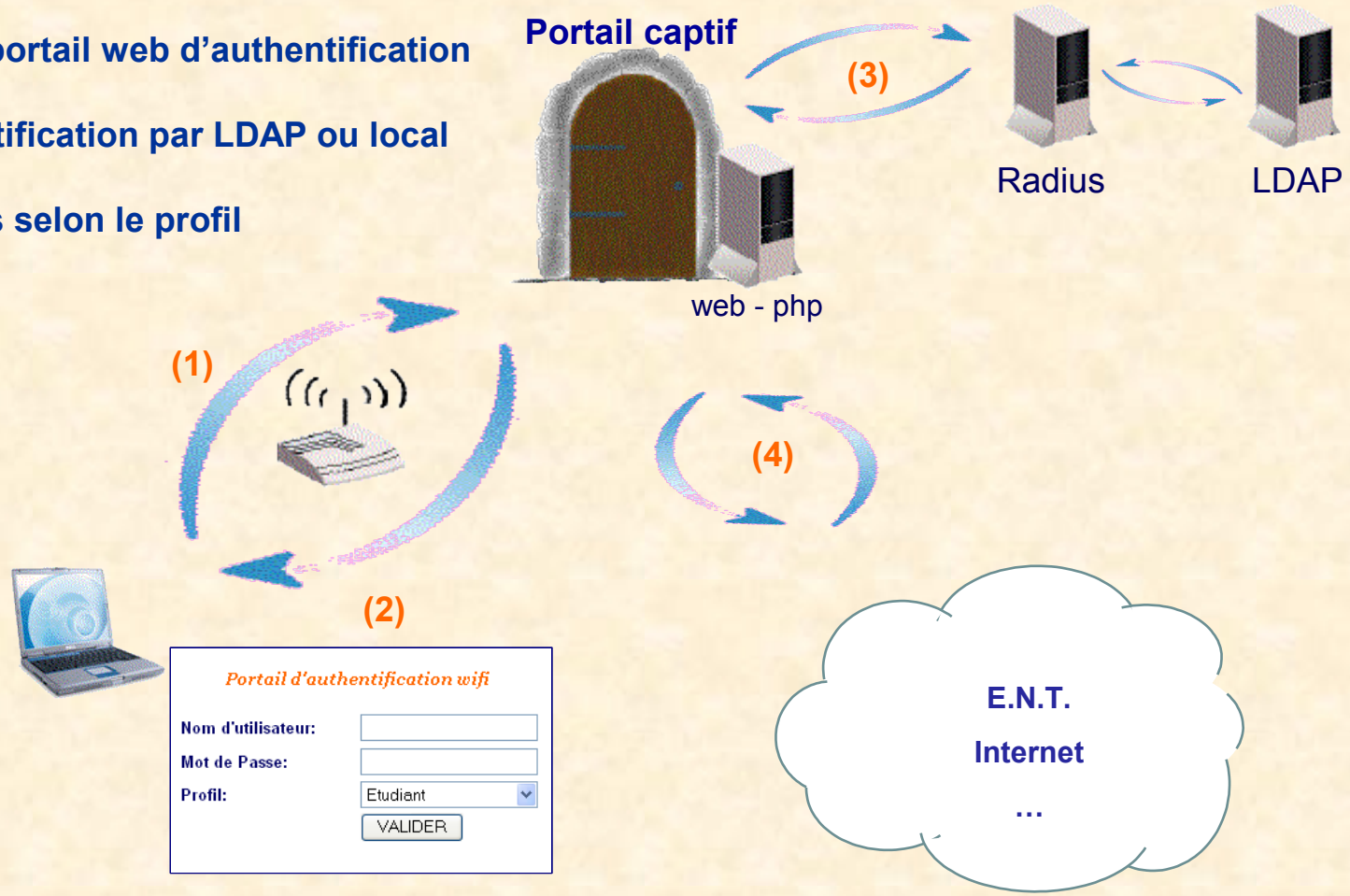
(1) Obtention d'une @IP par DHCP

(2) Redirection vers le portail web d'authentification

(3) Processus d'authentification par LDAP ou local

(4) Autorisation d'accès selon le profil

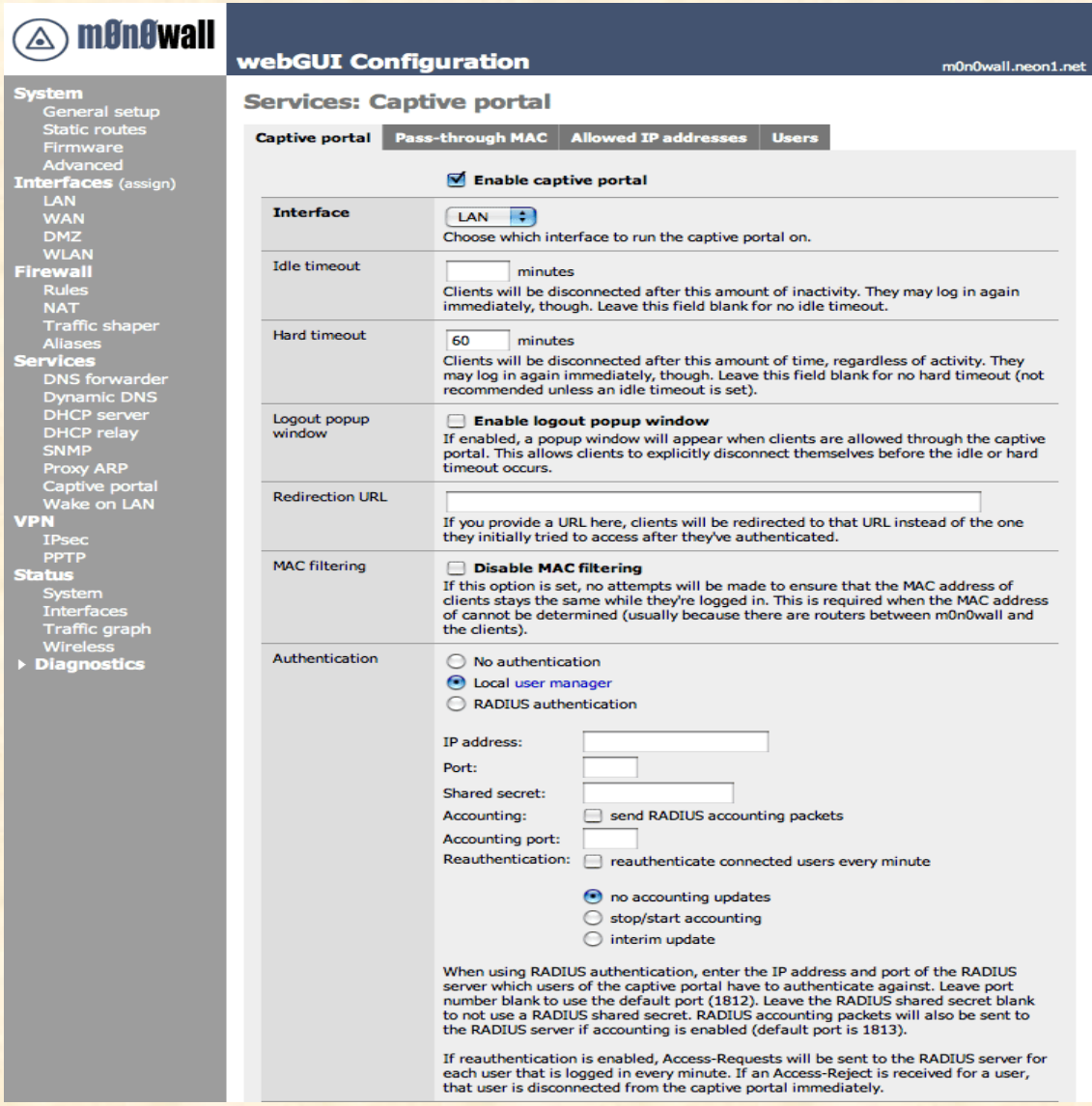
Déconnexion après utilisation ou time-out



Implémentations libres (ex: M0n0wall, Talweg, Chillispot …) ou commerciales !

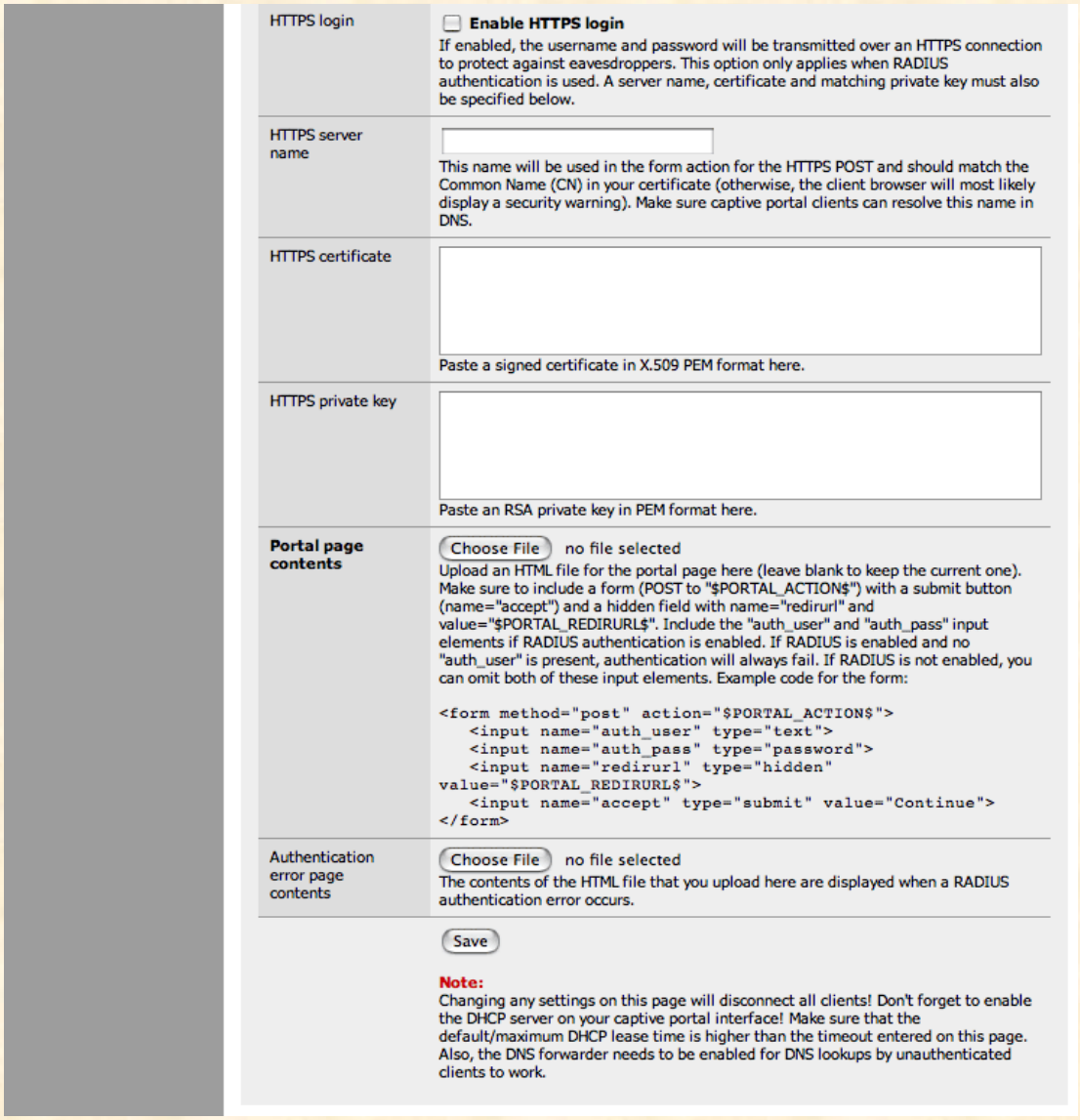
Rappels concepts : Portails captifs - m0n0wall

- M0n0wall est une solution libre basée sur un noyau freebsd
- Il est disponible sous la forme d'un cdrom bootable ou d'une image d'un fs
- Il comprend :
  - ✓ Un Firewall,
  - ✓ Un serveur web PHP,
  - ✓ Toute la config dans un fichier XML stocké sur un support amovible,
- Exemple de configuration du portail de m0n0wall :



Rappels concepts : Portails captifs - m0n0wall

- La configuration du portail captif de m0n0wall permet de définir :
  - ✓ La présence d'un pop-up de logout,
  - ✓ Une URL de redirection,
  - ✓ Un filtrage par @mac,
  - ✓ Le type d'authentification (local ou radius),
  - ✓ Authentification sécurisée https,
  - ✓ Les personalisations de pages html (auth, succés et erreur),
  - ✓ ...



HTTPS login	☐ **Enable HTTPS login** If enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. This option only applies when RADIUS authentication is used. A server name, certificate and matching private key must also be specified below.
HTTPS server name	This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS.
HTTPS certificate	Paste a signed certificate in X.509 PEM format here.
HTTPS private key	Paste an RSA private key in PEM format here.

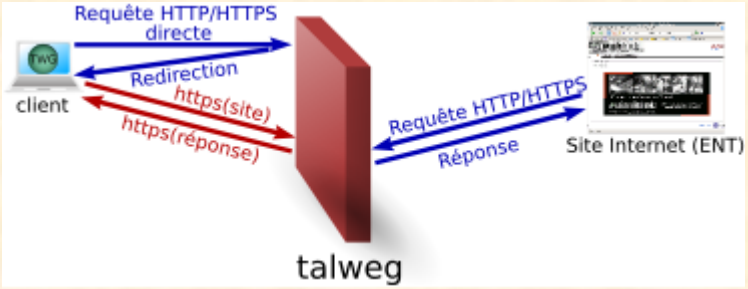
Portal page contents	Choose File no file selected
	Upload an HTML file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "$PORTAL_ACTION$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="$PORTAL_REDIRURL$". Include the "auth_user" and "auth_pass" input elements if RADIUS authentication is enabled. If RADIUS is enabled and no "auth_user" is present, authentication will always fail. If RADIUS is not enabled, you can omit both of these input elements. Example code for the form:
	`<form method="post" action="$PORTAL_ACTION$">`
	`<input name="auth_user" type="text">`
	`<input name="auth_pass" type="password">`
	`<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">`
	`<input name="accept" type="submit" value="Continue">`
	`</form>`

Authentication error page contents	Choose File no file selected The contents of the HTML file that you upload here are displayed when a RADIUS authentication error occurs.
	Save **Note:** Changing any settings on this page will disconnect all clients! Don't forget to enable the DHCP server on your captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the timeout entered on this page. Also, the DNS forwarder needs to be enabled for DNS lookups by unauthenticated clients to work.

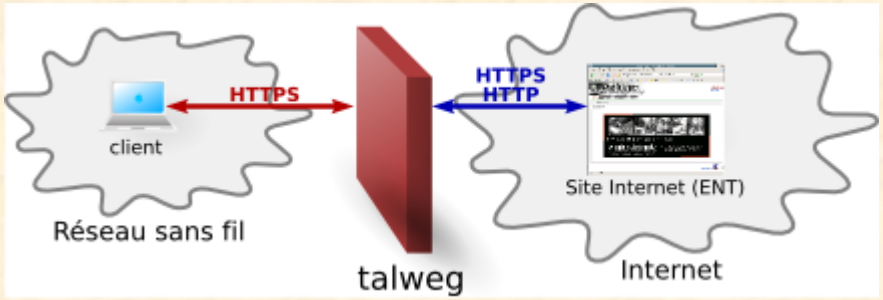
Rappels concepts : Portails captifs - Talweg

Solution dévelopée par l'Université de Metz,

- **Permet une authentification via CAS, Radius et LDAP,**

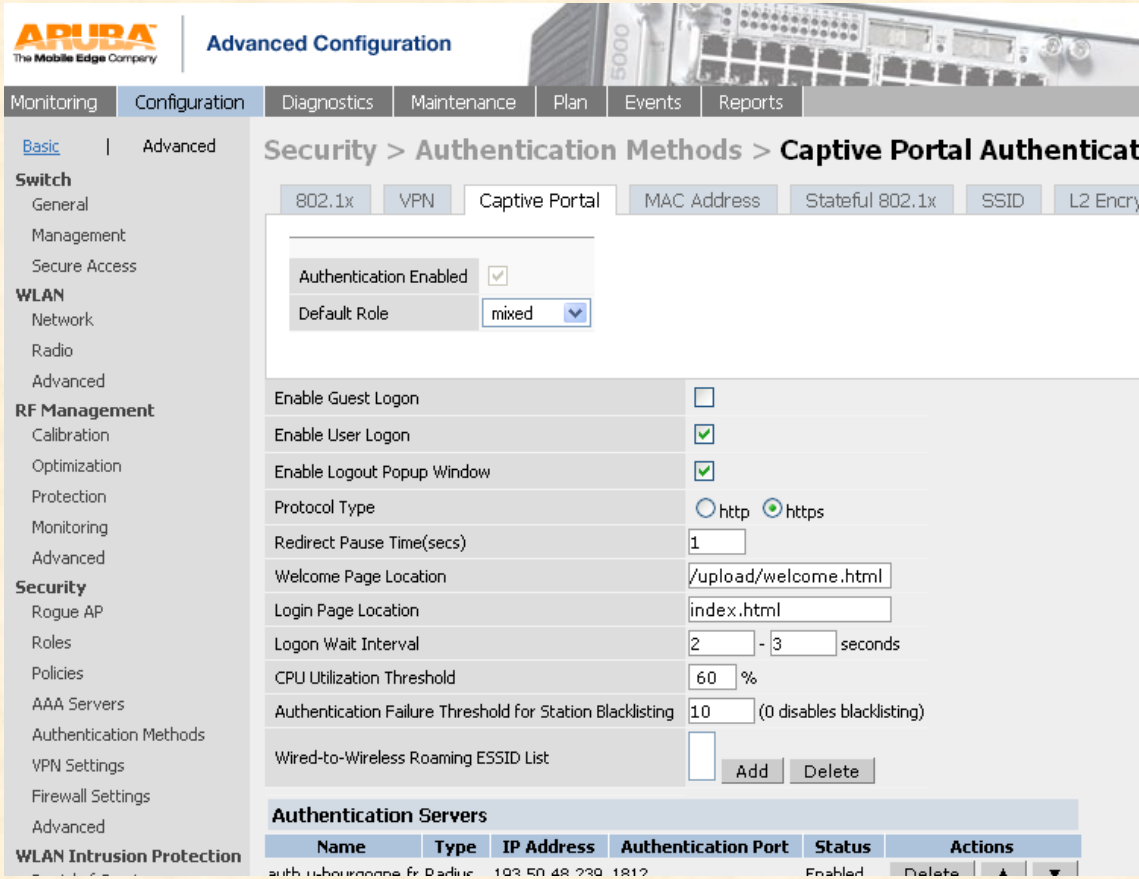


- **Disponible sous forme de sources ou de LiveCD (tests uniquement),**



Rappels concepts : Portails captifs - Aruba

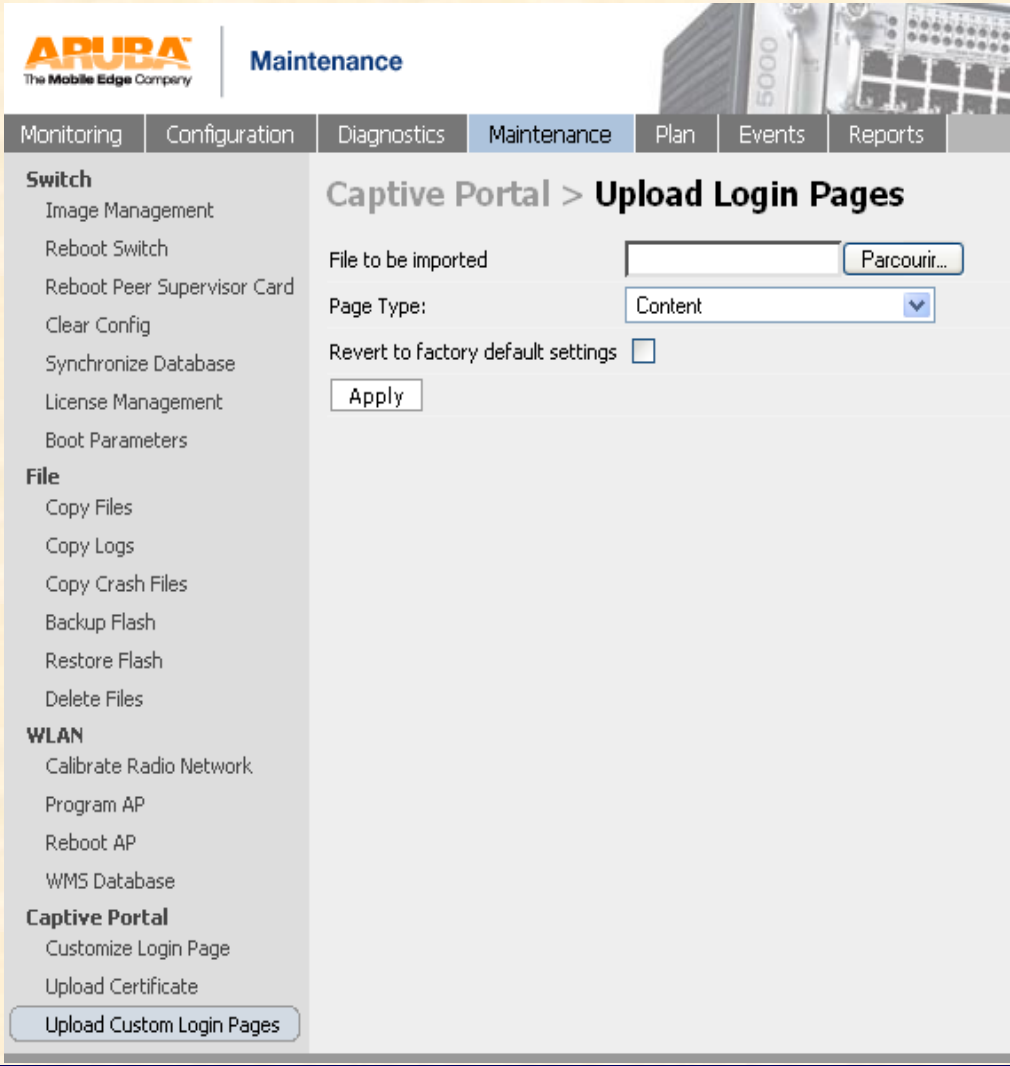
- Solution commerciale,
- Basée sur un linux « fermé »,
- « Contrôleur à tout faire » car:
  - ✓ Concentrateur VPN:
    - Pptp,
    - ipsec/l2tp.
  - ✓ Portail captif,
  - ✓ Fonctionnalités 802.1x,
  - ✓ Logs et stats graphiques,
  - ✓ Firewall assez complet,
  - ✓ ...
- Mais .... coûteux !!!



Rappels concepts : Portails captifs - Aruba

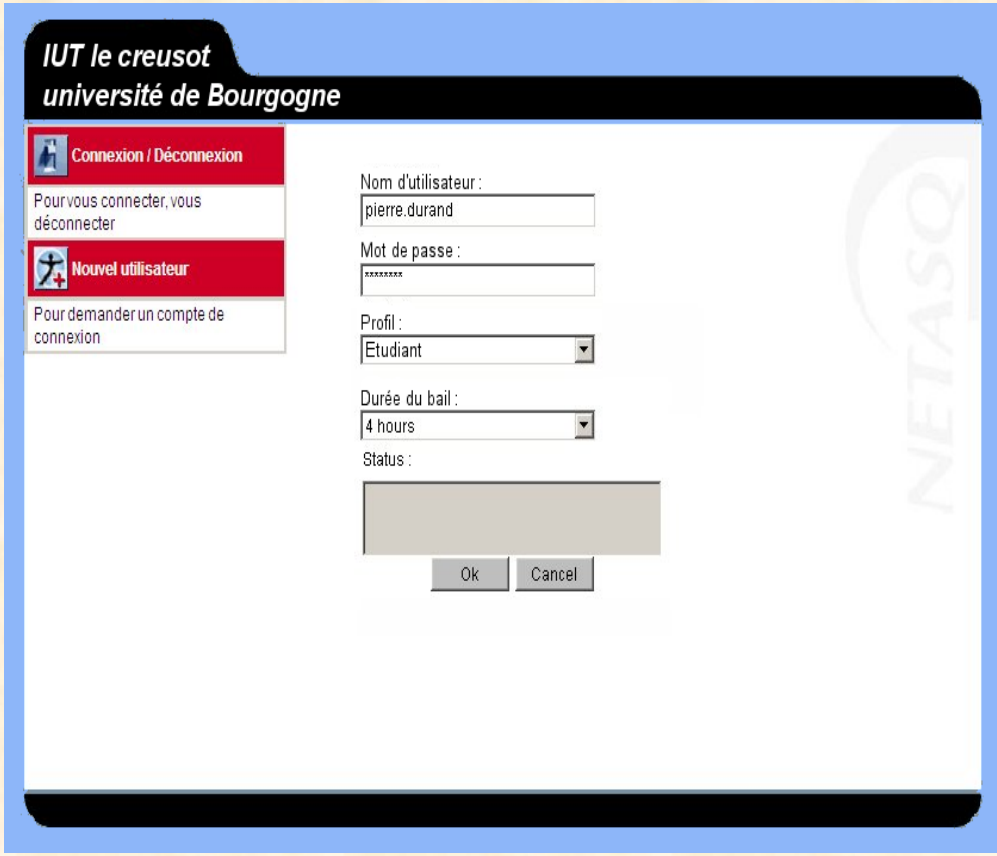
Le portail captif est presque entièrement paramètrable:

- Pages html personalisables,
- Certificat x509 téléchargable,
- Modes http/https,
- Méthodes d'authentification variées:
  - ✓ Serveur LDAP,
  - ✓ Radius,
  - ✓ Base interne.
- Redirection possible, après authentification, sur une page html donnée.



Rappels concepts : Portails captifs – Netasq F1000

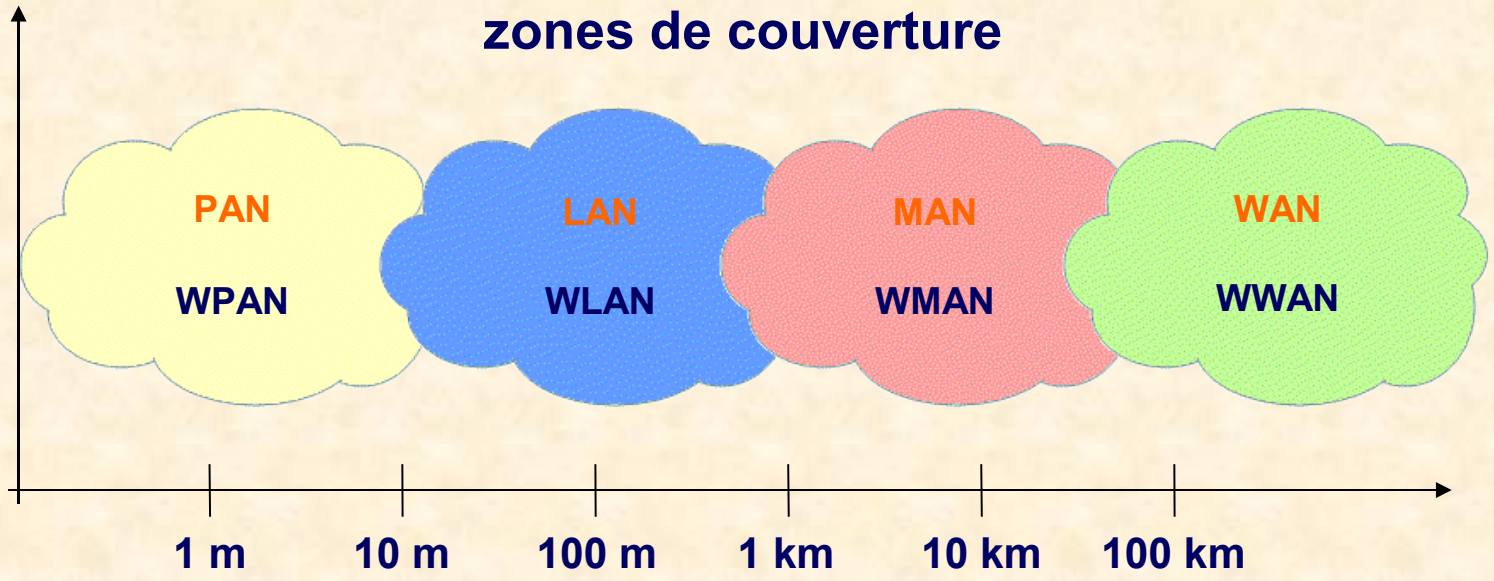
- **Portail captif intégré au Firewall:**
  - ✓ **Pages html personalisables,**
  - ✓ **Certificat x509 téléchargable,**
  - ✓ **Protocole SRP (cryptage de l'authentification),**
  - ✓ **Méthodes d'authentification variées:**
    - **Base interne,**
    - **Radius,**
    - **Serveur LDAP.**
  - ✓ **Service DHCP:**
    - **Association @IP/@mac,**
  - ✓ **Bail maximum 4 heures.**



- **Solution commerciale…**

Rappels concepts : Evolutions

Organisation des réseaux sans fil par zones de couverture:



WPAN: Wireless Personal Area Network

WMAN: Wireless Metropolitan Area Network

WLAN: Wireless Local Area Network

WWAN: Wireless Wide Area Network

Rappels concepts : Evolutions – W.P.A.N.

- **WUSB (Wireless Universal Serial Bus) IEEE 802.15.3:**
  - ✓ Performances équivalentes à USB 2,
  - ✓ Nombre maximale de périphériques: 127,
  - ✓ Couverture maximale 10 mètres,
    - Débits théoriques :
      - 480 Mbit/s à 3 mètres,
      - 110 Mbit/s à 10 mètres.
  - ✓ Bande de fréquences: de 3,1 à 10,6 GHz,
  - ✓ Sécurisation IEEE 802.11i – Cryptage AES 128 bits,
  - ✓ Consommation d'énergie réduite,
  - ✓ Disponibilité premier semestre 2007.
- **Usages de WUSB:**
  - ✓ Connexions informatiques,
  - ✓ Distribution audio/vidéo.

Rappels concepts : Evolutions – W.P.A.N.

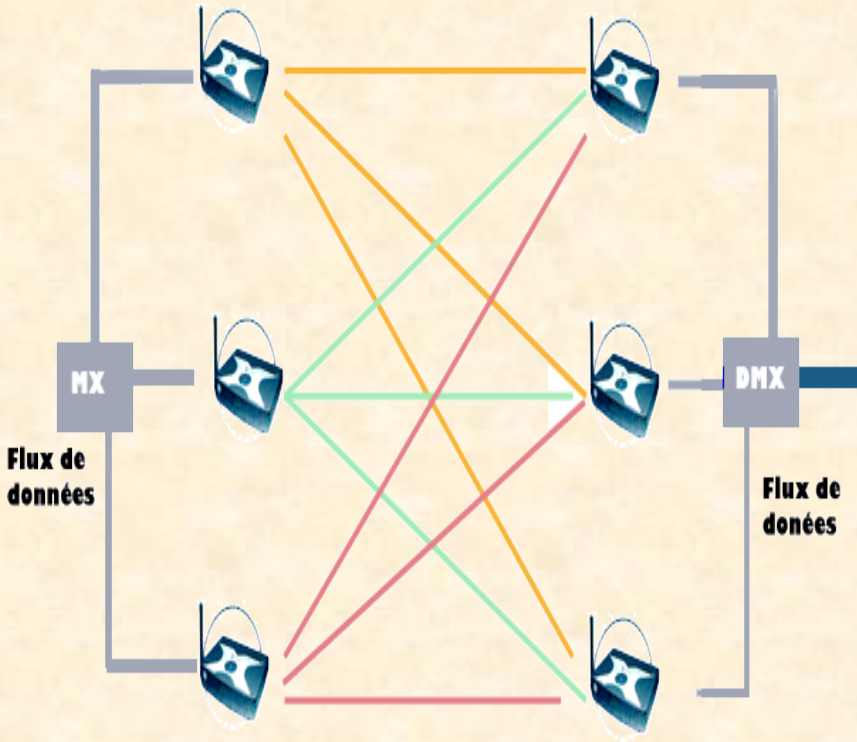
- **Zigbee: (IEEE 802.15.4):**
  - ✓ **Consommation électrique la plus faible possible,**
  - ✓ **Couverture maximale 100 mètres,**
  - ✓ **Débits théoriques: 20 Kbit/s et 250 Kbit/s,**
  - ✓ **Utilisation de 3 bandes de fréquences:**
    - **2,4 GHz et 868 MHz en Europe et 915 MHz aux Etats-Unis,**
  - ✓ **Prix de revient faible,**
  - ✓ **Disponibilité - 2006.**
- **Usages de Zigbee:**

  Transmettre des commandes à des objets communicants:
  - ✓ **Domotique, capteurs,**
  - ✓ **Applications médicales,**
  - ✓ **Détecteurs de fumée et d'intrusion,**
  - ✓ **Badges actifs.**

Rappels concepts : Evolutions – W.L.A.N.

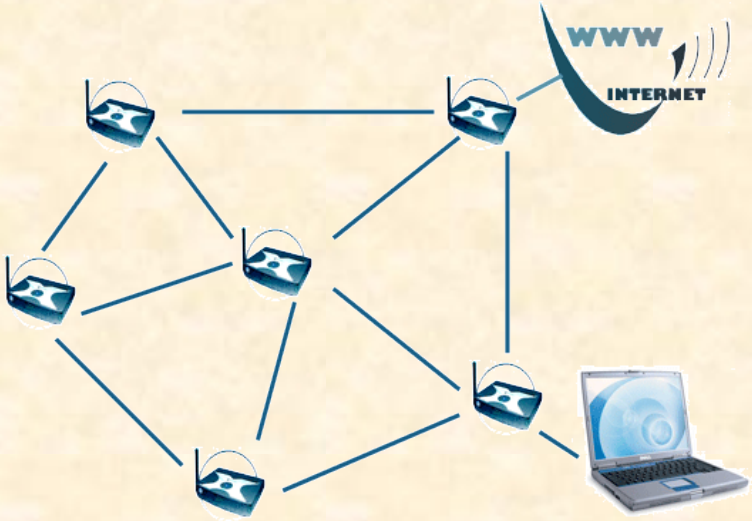
WI-FI: IEEE 802.11 n

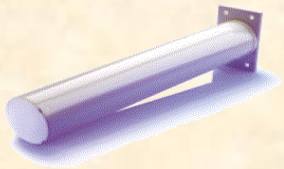
- Disponible dès janvier 2007 pour ordinateurs portables,
  - ✓ Norme 802.11n draft 1.1.
- Débit maximale théorique de 540 Mbit/s,
- Utilisation des technologies:
  - ✓ MIMO (Multiple Input Multiple Output),
    - Envoi de plusieurs signaux à des fréquences proches,
- Utilisation de 2 bandes de fréquences:
  - ✓ 2,4 GHz et 5 GHz.
- Compatible avec 802.11b et 802.11g (à vérifier),
- Sécurité accrue - norme 802.11i – WPA2,
- Zone de couverture plus importante (à vérifier),
- Norme finalisée en 2008,



Rappels concepts : Evolutions – W.L.A.N.

- **Mesh: (802.11s)**
- **Connexions entre points d'accès,**
- **Réseau maillé,**
- **Permet d'étendre facilement un réseau,**
- **Cellule 802.11g pour les connexions utilisateurs,**
- **Cellule 802.11a pour les connexions entre les points d'accès:**
  - ✓ **Utilisation d'antennes directionnelles.**





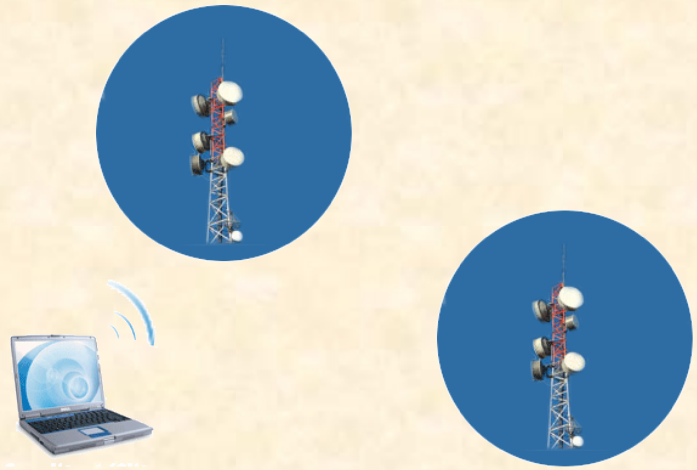
Rappels concepts : Evolutions – W.M.A.N.

Standards IEEE 802.16 – WiMAX:

- **WiMAX (802.16d):**
  - ✓ **Révision intégrant les standards:**
    - **802.16, 802.16a, 802.16b, 802.16c.**
  - ✓ **Usage fixe – réseaux métropolitains:**
    - **Réseaux de transport et de collecte.**
  - ✓ **Modulation OFDM (Orthogonal Frequency Division Multiplexing):**
    - **Transport du signal sur de multiples fréquences porteuses.**
  - ✓ **Pas de vue directe entre les équipements connectés pour les bandes de fréquences de 2 à 11GHz.**
  - ✓ **Bande de fréquences:**
    - **10 à 66 GHz,**
    - **2 à 11GHz.**
  - ✓ **Débit théorique: 70 Mbit/s sur 50 km.**
  - ✓ **Débit pratique: 12 Mbit/s sur 20 km.**
  - ✓ **Licence d'exploitation obligatoire (ARCEP),**
  - ✓ **Région Bourgogne - déploiement de 103 stations de base.**

Rappels concepts : Evolutions – W.M.A.N.

Standards IEEE 802.16 – WiMAX:



- **WiMAX mobile (802.16e):**
  - ✓ Connexion des clients mobiles aux réseaux métropolitains,
  - ✓ Utilisation pour les Réseaux de desserte,
  - ✓ Modulation OFDM,
  - ✓ Bande de Fréquences: 2-6 GHz
  - ✓ Débit: 30 Mbit/s sur 3,5 Km
  - ✓ Disponibilité sur les ordinateurs portables en janvier 2007,
  - ✓ Adapté aux services mobiles haut débit.

- **WiMAX (802.16f):**
  - ✓ Equivalent à 802.11s (réseaux mesh Wi-Fi).

Rappels concepts : Evolutions – Handover

Pour l'ensemble des réseaux sans fil:

- **Handover (IEEE 802.21):**
  - ✓ **Passer de façon transparente d'une cellule ou d'un réseau à l'autre sans interruption de service.**