L3 informatique TP n°4 : Configuration d'un routeur Wi-Fi

Sovanna Tan

Octobre 2009, maj novembre 2014

Plan

Le routeur Wi-Fi

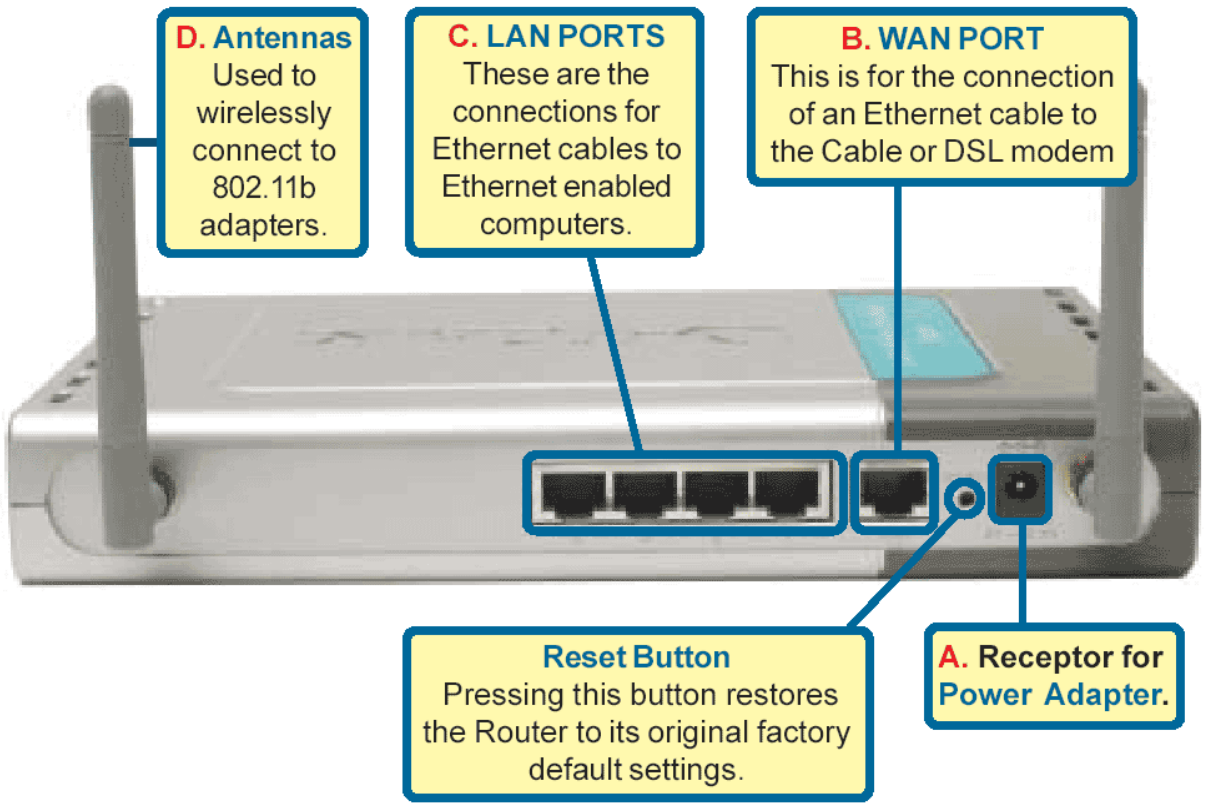

Image provenant de : `http://www.online-tech-tips.com/computer-tips/how-to-determine-your-routers-default-password/fr/`

Fonctionnalités du routeur Wi-Fi

Fonctions d'un routeur Wi-Fi

- Commutateur (switch) ethternet
- Point d'accès Wi-Fi
- Routeur effectuant de la translation d'adresse (NAT)
- Pare-feu
- Serveur DHCP

Sources

- Routeur ou point d'accès : `http://www.techwarelabs.com/articles/other/routervsap/`
- WPA, WPA2 : `http://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access`
- Wi-FI Protect Setup (WPS) : `http://kb.netgear.com/app/answers/detail/a_id/96`

Commutateur ethernet

Fonctionnement d'un commutateur

- Pour chaque port, enregistrement des nouvelles adresses MAC sources dans une table. Cette table permet au commutateur de savoir sur quel port il doit envoyer les trames qu'il reçoit.
- Si une adresse destination est inconnue, la trame est diffusée sur tous les ports sauf le port par lequel elle est arrivée.
- Si l'adresse source et l'adresse destination sont identiques, la trame n'est pas retransmise.

Les réseaux sans fil

- Utilisation la propagation des ondes radio dans l'espace.
- Il existe différents domaines de couverture.
  - WPAN (Wireless Personal Area Networks) :
    - Bluetooth
    - Liaisons infrarouges
  - WLAN (Wireless Local Area Networks) :
    - Wi-Fi
  - WMAN (Wireless Metropolitan Area Networks) :
    - WiMax
  - WWAN (Wireless Wide Area Networks) :
    - GSM (Global System for Mobile Communication)
    - GPRS (General Packet Radio Service)
    - UMTS (Universal Mobile Telecommunication System)

Le Wi-Fi

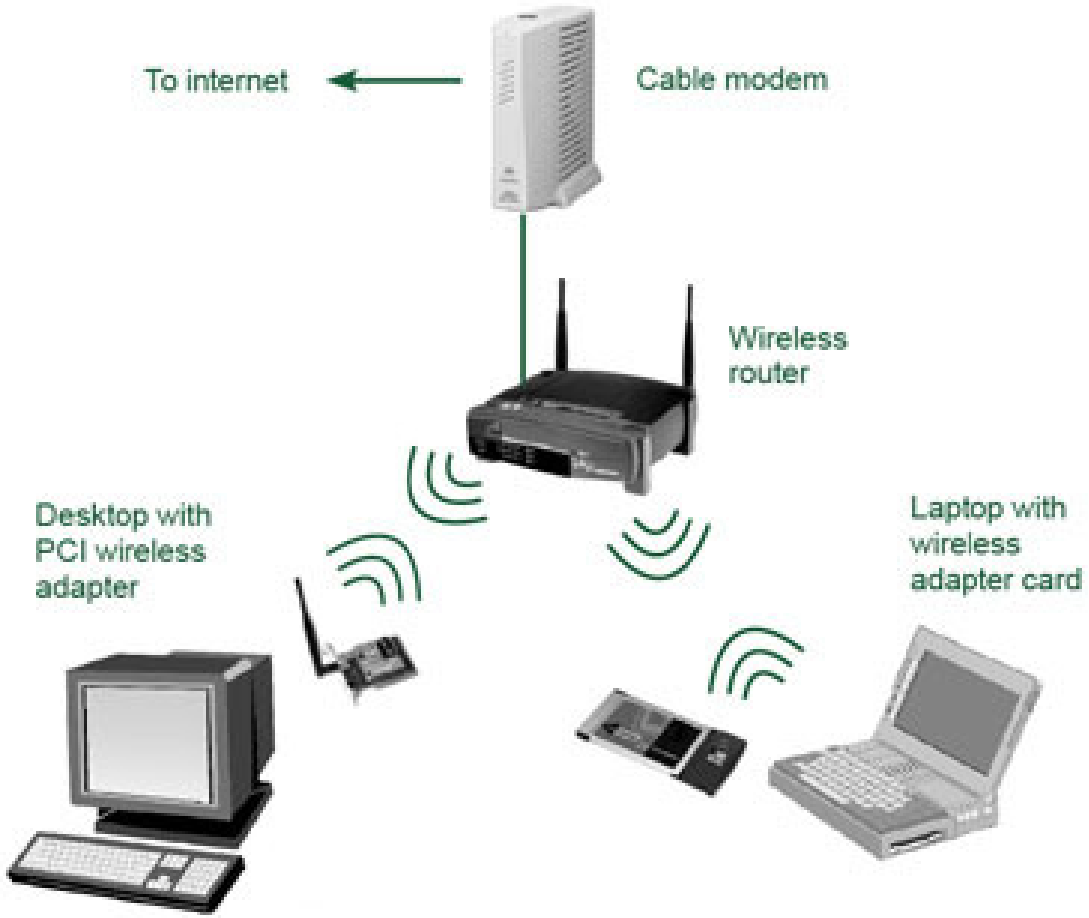

Image provenant de :

`http://www.mcintyreconstructionservicesllc.com/wireless_lan.html`

Terminologie

Service Set IDentifier (SSID)

Nom d'un réseau local wi-fi. Tous les équipements qui veulent dialoguer entre eux doivent utiliser le même SSID et le même canal (fréquence).

Mode ad-hoc

Dans le mode ad-hoc, les équipements dialoguent directement entre eux. Chaque ordinateur transmet les trames à tous les autres.

Mode infrastructure

Le communications sont centralisées par un point d'accès. Chaque équipement dialogue avec le point d'accès qui diffuse les trames. Les points d'accès peuvent être connectés entre eux pour augmenter la portée du réseau.

Wi-Fi sécurisé

Techniques de sécurisation

- Filtrage d'adresse MAC
- Chiffrement Wire Equivalent Privacy (WEP) : Il faut éviter de l'utiliser car il se craque en quelques minutes.
- Chiffrement Wi-fi Protectected Access (WPA), WPA2
- Chiffrement Wi-Fi Protected Setup (WPS)

WPA, WPA2 Personal

Dans les versions PSK, les équipements partagent une clé.

WPA Personal ou PSK (Pre-Shared Key)

Ce protocole utilise les briques suivantes :

- Chiffrement par flot Rivest Cipher 4 (RC4) ;
- Temporal Key Integrity Protocol (TKIP) pour l'échange de clés de façon dynamique ;

WPA Personal ou PSK (Pre-Shared Key) 2

Cette version utilise l'algorithme de chiffrement Advanced Encryption Standard (AES).

- Le protocole WAP avec TKIP est craqué.
- Le protocole WPA2 n'est pas encore craqué.
- Le mode PSK est vulnérable aux attaques par dictionnaire.

WPA, WPA2 Enterprise

Extensible Authentication Protocol (EAP)

Norme définie dans le RFC 3748 pour l'authentification utilisant un serveur d'authentification.

- Les version Enterprise utilisent des mécanismes EAP.

Mécanismes EAP utilisables dans WPA et WPA2 Enterprise

- EAP-TLS (Transport Layer Security)
- EAP-TTLS/MSCHAPv2 (Tunneled Transport Layer Security)
- PEAPv0/EAP-MSCHAPv2 (Protecte EAP v0/(Microsoft Challenge Handshake Authentication Protocol v2)
- PEAPv1/EAP-GTC (Generic Token Card)
- EAP-SIM (Subscriber Identity Module) pour les téléphones portables

WPS

Wi-Fi Protected Setup

Standard simple pour sécuriser un réseau Wi-Fi. Le SSID et la protection WPA sont configurés automatiquement à l'aide d'un code PIN (Personnal Identification Number) ou d'un bouton dédié.

- La génération aléatoire des clés déjoue l'attaque par dictionnaire.
- Dans le fonctionnememnt avec code PIN, le protocole d'échange de clés est trop simple et a été craqué en 2011.