

Systeme et reseau Cours

INSA INSTITUT NATIONAL
DES SCIENCES
APPLIQUEES
ROUEN



4



www.wooclap.com/OZSDCU

Domain Name System

Un service vital

DNS

Application
+
Présentation
+
Session

Transport

Réseau

Liaison
de données

Physique

DNS

Objectif : Utiliser un nom à la place d'une adresse IP

- Le service **D**omain **N**ame **S**ystem assure la correspondance entre un nom d'hôte et son adresse IP
La résolution de **moodle.insa-rouen.fr** donne **193.49.10.217**
- L'opération inverse est possible
Résolution inverse de **193.49.10.217** donne **moodle-2018.insa-rouen.fr**
- Fonctionne avec des RR (Ressource Record)

Types de RR	Informations
A	moodle-2018.insa-rouen.fr → 193.49.10.217
CNAME	moodle.insa-rouen.fr → moodle-2018.insa-rouen.fr
AAAA	Pour les adresses IP V6
MX record	Pour les serveurs de messageries



Le vrai nom du serveur est moodle-2018.insa-rouen.fr
Moodle.insa-rouen.fr est un alias, un deuxième nom pour la machine.
Cela facilite les mises à jour, par exemple, il est possible de préparer un moodle-2023.insa-rouen.fr et quand le serveur est totalement configuré, il suffit de supprimer l'alias à moodle-2018 pour le donner à moodle-2023.
Ainsi les serveurs peuvent cohabiter sans changer de nom.

DNS



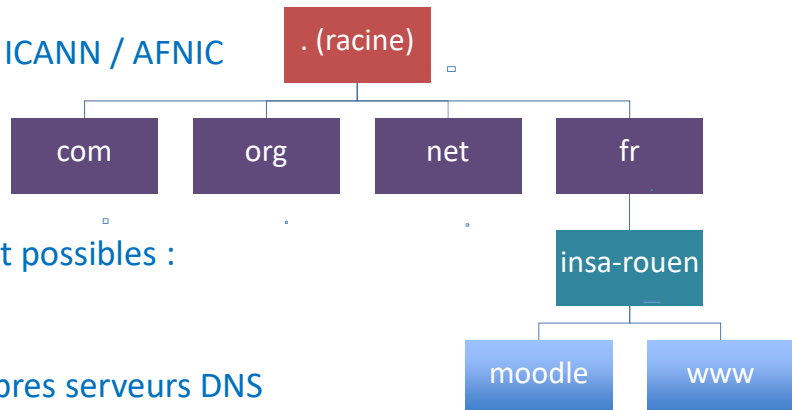
- Le service **Domain Name System** est associé à un nom de domaine, insa-rouen.fr par exemple.
Si **insa-rouen** est librement choisi, **fr** provient d'une liste de 'Top Level Domain'
- Le **serveur DNS de ce domaine** peut directement répondre aux demandes d'un FQDN (Fully Qualified Domain Name), un nom pleinement qualifié pour ce domaine → moodle.insa-rouen.fr = nom d'hôte + nom de domaine
- Il ne peut répondre aux autres demandes (moodle.u-paris.fr par exemple) sauf à faire appel à un autre serveur DNS (celui de u-paris.fr)



Le FQDN correspond au nom de l'hôte, par exemple moodle, suivi du nom complet de domaine qui l'héberge, par exemple, insa-rouen.fr : FQDN = moodle.insa-rouen.fr

DNS (Arborescence)

- Il a une organisation arborescente
- En haut se trouve la racine (www.google.com.)
- Autorité de nommage ICANN / AFNIC



- Des sous domaine sont possibles :
ad.insa-rouen.fr
litis.insa-rouen.fr
Chacun avec leurs propres serveurs DNS

L'AFNIC (Association française pour le nommage Internet en Coopération)
ICANN (Internet Corporation for Assigned Names and Numbers)

Exemple avec un utilisateur dans un autre continent, qui fait une résolution sur le nom moodle.insa-rouen.fr

La demande arrive sur un serveur DNS qui interroge le serveur racine pour connaître le serveur DNS du .fr

Il interroge le serveur du .fr pour connaître le serveur du insa-rouen

Il arrive sur le serveur de l'INSA qui est le seul qualifié pour répondre à une requête du domaine insa-rouen.fr

DNS : Enchainement de recherche

- 1 : un système de cache existe à la fois dans l'hôte et dans le serveur DNS
- 2 : Un fichier spécial nommé **hosts** peut contenir une résolution. Ancêtre du DNS toujours actif
- 3 : Le serveur DNS est interrogé
- 4 : Si le serveur DNS est indisponible et si un serveur secondaire est connu alors il est interrogé

1 : Nom disponible dans le cache ?



2 : Nom connu localement ?



3 : Requête sur DNS Principal



4 : Requête DNS Secondaire

Les systèmes linux n'ont pas de cache par défaut.

Sous Windows, vider le cache ou le consulter se fait avec la commande ipconfig (Ex ipconfig /displaydns et ipconfig /flushdns)

DNS : affichage de configuration DNS 'client'

- Exemple Linux (cat /etc/resolv.conf)

```
# cat /etc/resolv.conf
domain insa-rouen.fr
search insa-rouen.fr
nameserver 193.49.10.1
```

- **domain** : le domaine local (celui du serveur DNS)
- **search** : le ou les domaines de recherche par défaut
- **nameserver**: l'adresse IP du serveur DNS

- Exemple Windows (ipconfig /all)

```
C:\ipconfig /all

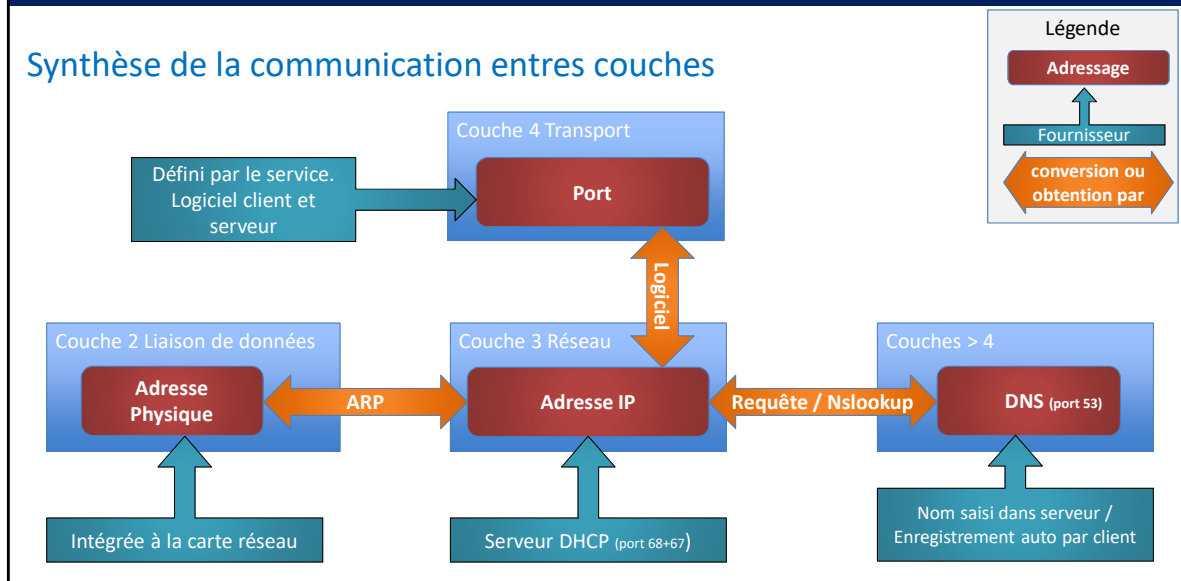
Liste de recherche du suffixe DNS.: mshome.net

Suffixe DNS propre à la connexion. : mshome.net
Adresse IPv4. . . . . : 172.18.70.57
Masque de sous-réseau. . . . . : 255.255.255.240
Passerelle par défaut. . . . . : 172.18.70.49
Serveurs DNS. . . . . : 172.18.70.49
```

- **Liste de recherche** : le domaine local (celui du serveur DNS)
- **Suffixe DNS** : le ou les domaines de recherche par défaut
- **Serveurs DNS** : IP du serveur DNS

Repérage et protocoles dans la famille TCP/IP

Synthèse de la communication entre couches



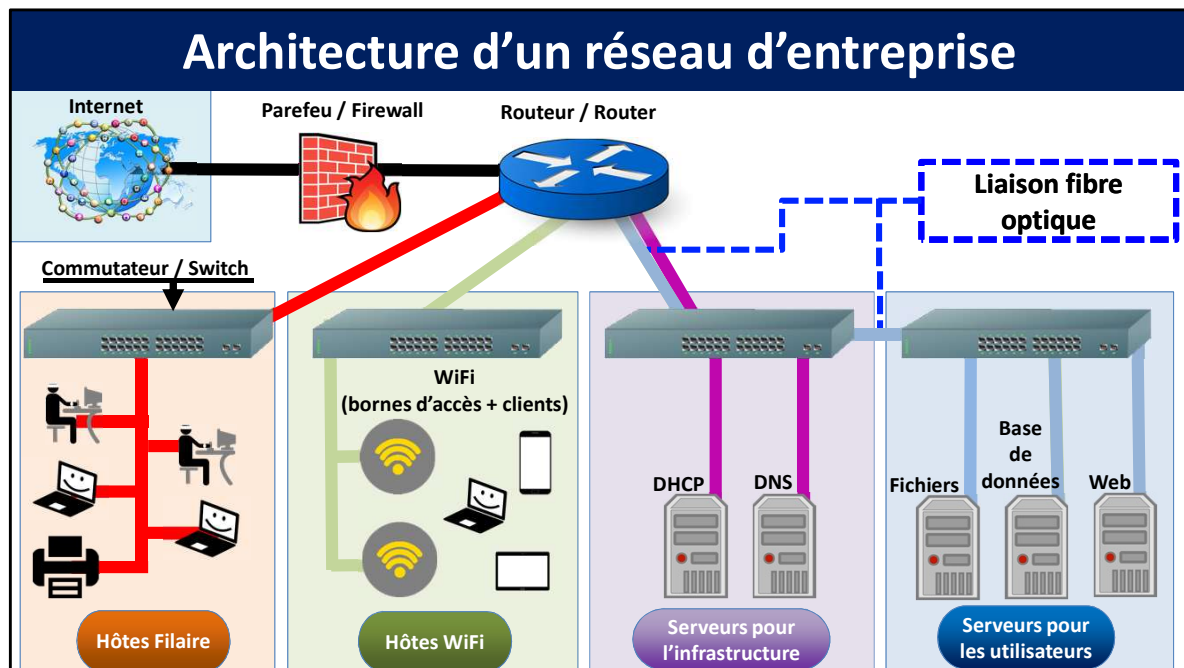
Couche 2 : Communication entre hôte du même réseau local

Couche 3 : Communication locale ou distante car capacité à sortir du réseau local

Couche 4 : Communication entre services réseaux (client-serveur)

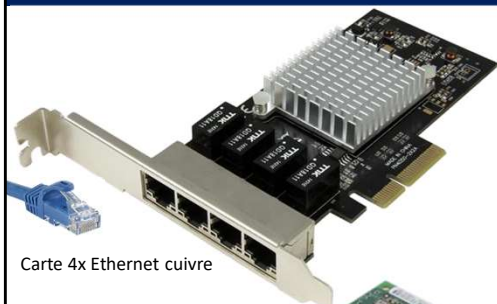
Eléments de réseau Architecture

- Gestion d'un réseau
- Notions de sécurité

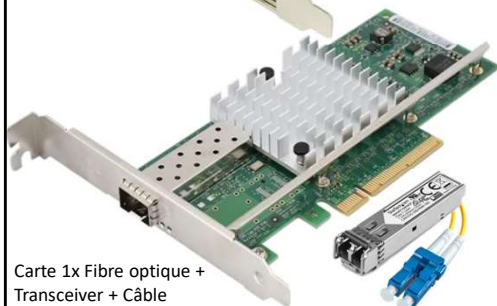


Ce schéma illustre un exemple d'architecture de réseau d'entreprise.

Elements du réseau : Les cartes réseaux



Carte 4x Ethernet cuivre



Carte 1x Fibre optique +
Transceiver + Câble

- Niveau 1 & 2
- Gère le medium Physique (cuivre, fibre ou ondes)
- Sécurité : possibilité d'usurper une adresse physique



Carte WiFi pour portable

Elements du réseau : Le concentrateur ou HUB



La photo montre un hub mais il est impossible de différencier HUB et SWITCH à l'œil. Il faut vérifier la modèle.

- Niveau 1
- Un concentrateur est un système de connexion centralisé où se connectent tous les câbles d'un réseau.
- Le concentrateur répète un signal reçu sur l'ensemble de ses ports
- Sécurité : Tous les utilisateurs peuvent suivre les conversations des hôtes connectés au concentrateur.
A REMPLACER PAR UN COMMUTATEUR AU PLUS VITE
- Gestion indispensable : qui est physiquement connecté ?

Note : Les concentrateurs ont disparus des infrastructures réseaux

Elements du réseau : Le commutateur ou SWITCH



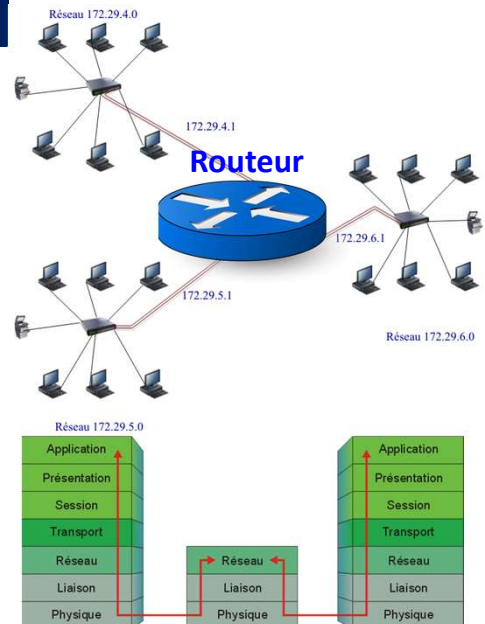
Armoire avec des switchs câblés



- Niveau 2
- Système de connexion centralisé avec des fonctions avancées
- Chaque hôte ne reçoit que les communications qui lui sont destinées
- Système administrable pour séparer différents réseaux et filtrer les ordinateurs.
- Sécurité : Risque d'attaque pour passer en mode concentrateur, changement de réseau 'vlan hopping'

Elements du réseau : Routeurs

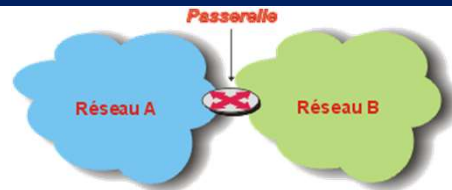
- Niveau 3
- Il fait le lien entre plusieurs réseaux IP.
- Il aiguille les paquets IP qui circulent entre réseaux.
- Il dispose d'une carte réseau dans chaque réseau avec une adresse IP et un masque spécifique.
- Les routeurs opèrent sur des réseaux physiques Ethernet totalement disjoints.
- Les routeurs s'appuient sur une table de routage, cette table peut être construite à la main ou bien automatiquement au moyen de protocoles plus évolués (RIP, BGP).



Elements du réseau : Passerelle et Pont

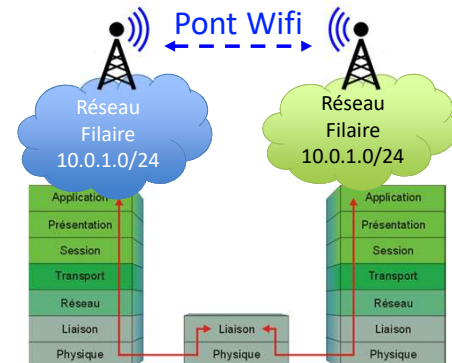
- **Passerelle :**

Les passerelles permettent d'interconnecter plusieurs réseaux de manière à permettre le passage de l'information d'un réseau à l'autre. (Réseau avec des technologie différentes)



- **Le pont (bridge) :**

Permet de relier deux réseaux physiquement séparés mais qui utilise le même réseau IP. Avec deux cartes réseaux, le pont assure le transfert des trames (niveau 2) d'un réseau physique à un autre en utilisant les adresses MAC pour optimiser le trafic.



La passerelle est très proche du routeur mais, une passerelle ne route pas les paquets, alors qu'un routeur peut contenir une passerelle

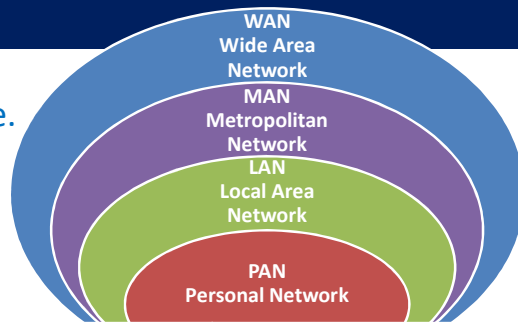
Réseau sans fil : Le WiFi


- Norme IEEE 802.11 (Wifi est un nom commercial)
Utilisation des ondes électromagnétiques (2,4 GHz, 5 GHz, 6 GHz et 60 GHz)
La norme définit les couches basses du modèle OSI :

Normes	Noms	Débits théoriques Mbps/s	Fréquences	Informations diverses	Dates
802.11a	Wi-Fi	54	5 GHz	Portée de 35 m	1999
802.11b	Wi-Fi	11	2,4 GHz	Le plus répandu au début, 13 canaux en France, 11 aux USA, 14 au Japon	1999
802.11g		54	2,4 GHz	Compatible 802.11b	2003
802.11n	WWiSE ou TGn Sync	450	2,4 GHz et 5 GHz	Utilise 4 flux MIMO (Multiple Input Multiple Output) Portée de 70 m	2009
802.11ac	WiFi 5	1300 (2013) 2500 (2015)	5 GHz	8 flux MiMo	2013
802.11s	Réseau Mesh	10 à 20	Utilise les autres normes	Mobilité sur réseau ad-hoc	2012
802.11ad	WiGig	6800	60 GHz	Portée de 10 m	2016
802.11ax	Wifi 6/6e	5/10 Gb/s	2,4 GHz 5 GHz et 6 GHz	Portée de 500 m	2018/2021

Réseau sans fil

Suivant la couverture, le vocabulaire change.



	PAN	LAN	MAN	WAN
Standard	Famille 802.15 Ex : Bluetooth	802.11a,11b,11g 802.11n,11ac,11ax	802.11 MMDS, LMDS 802.16 WiMax	GSM à 5G
Vitesse	1 à 100 Mbps	2 à 2500 Mbps	22 à 46 Mbps	GSM : 9 kbit/s 4G LTE : 150 Mbits/s (40 Mbits) 5G : 1 Tbit/s (100 Mbits/s mini)
Couverture	Faible	Moyenne	Moyenne à étendue	Etendue
Applications	Point à point Équipement à équipement	Réseau d'entreprises 	Fixe, accès au dernier kilomètre	GSM

PAN : Personal Area Network ou Réseau domestique

Réseau de proximité

LAN : Local Area Network ou Réseau Locaux

Le réseau local d'entreprise dans un même bâtiment ou même locaux

MAN : Metropolitan Area Network ou Réseaux Métropolitains

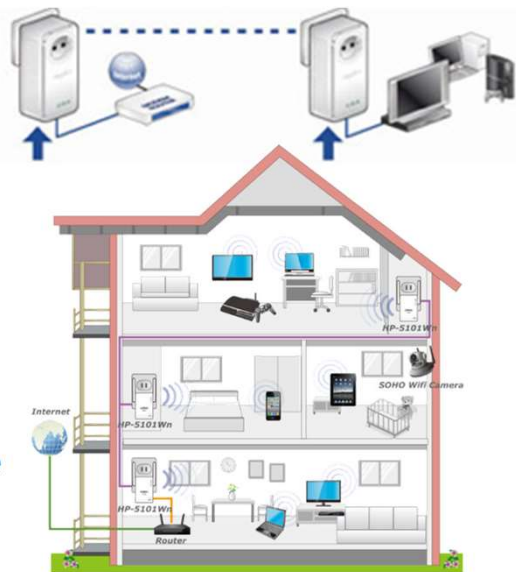
Typiquement le réseau d'agences dans une même ville

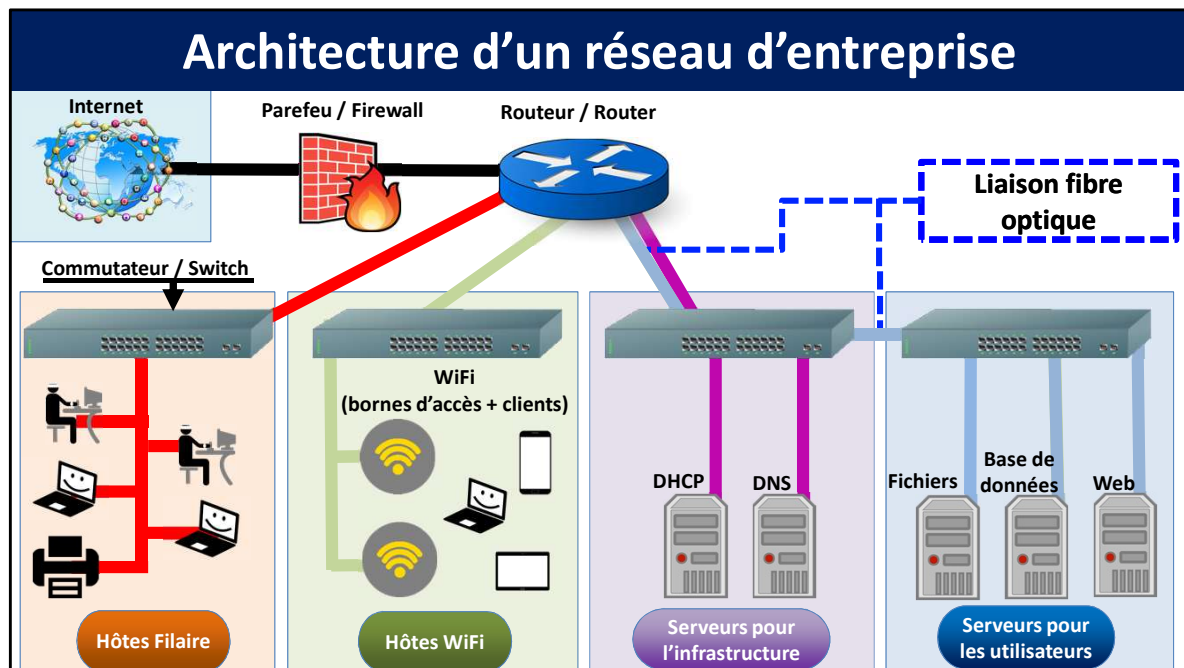
WAN : Wide Area Network ou Réseaux Etendus

Typiquement les réseaux nationaux ou continentaux

CPL: Courant Porteur en Ligne

- Permet de construire un réseau informatique sur le réseau électrique.
- **Avantages :**
souple, simple et facile à mettre en œuvre
- **Inconvénients :**
Mise en œuvre et bon fonctionnement dépendant de l'architecture du réseau électrique, le manque de standardisation pose un problème d'interopérabilité entre équipements





On peut comparer cette architecture avec celle de notre établissement

- Les différents switches et répartiteurs dans chaque bâtiment (locaux techniques)
- Les switches dans les salles informatiques, postes de travail connectés
- Les imprimantes, scanners, ...
- les différents serveurs (Web, données, Bases de données, ...)

Les hôtes du réseau sont interconnectés par les switches.

Ils peuvent être dans le même réseau ou dans des réseaux séparés par des VLAN.

Le routeur est en charge de faire communiquer les VLAN entre eux et du changement d'adresse IP privé vers publique lors de la sortie vers Internet.

Le pare-feu contrôle les flux, principalement en autorisant que certains ports en entrée.

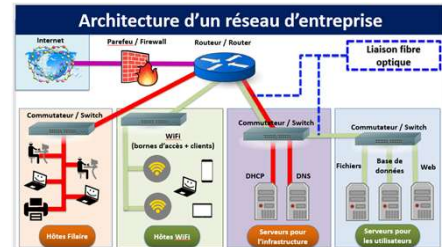
Architecture

- Utiliser des réseaux IP différents en fonction des besoins

- ⊗ Obligation d'utiliser un routeur
- ☺ Réduction des broadcast
- ☺ Gestion de la sécurité simplifiée

- Utilisation de commutateurs (switch) performants

- ⊗ Coût élevé
- ☺ Utilisation de VLAN (plusieurs réseau niveau 2 dans 1 switch)
- ☺ Gestion de la sécurité simplifiée
 - Interdiction des DHCP sauvage
 - Blocage de ports automatiques (trop d'erreurs, de requêtes)



- Câblage RJ45 cuivre vers les hôtes

- Efficace et coûts faibles, distance limité (100m) 1 Gb/s



- Câblage fibre optique entre switches ou vers les serveurs

- Débit élevé (40 Gb/s) longue distance possible >km



Pour l'école il y a :

Un réseau pour les PC à destination des étudiants

Un réseau par département (ou presque, il y a des départements mélangés)

Un réseau pour les PC d'analyse

Un réseau pour l'administration

Un réseau pour le wifi

Etc.

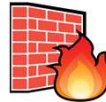
Sécurité

- Les services DHCP et DNS étant vitaux pour la sécurité il faut les surveiller
- Ne pas voir sur le réseau un autre serveur DHCP ou DNS faire des annonces



- Wifi :

Limiter la portée, restreindre les accès (firewall)
Authentifier si possible (Radius)



- Filaire

Limiter les prises actives
Limiter les accès physiques au réseau (commutateur)
Chasser les 'petits' commutateurs



- Journaux

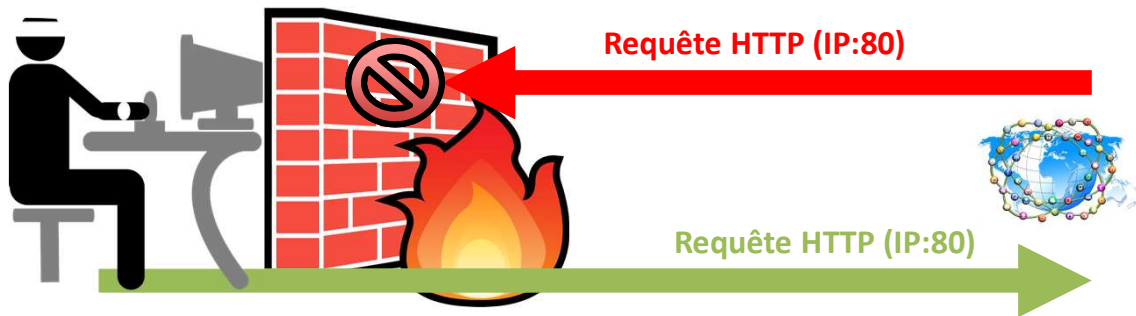
Garder une trace des activités



Pare-feu / Firewall

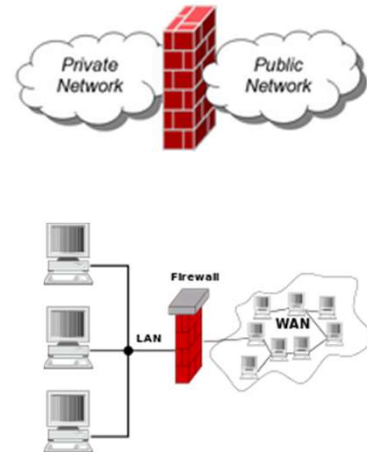
PareFeu ou Firewall

- Logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau.
- Sur un Pc :
 - * Laisse généralement sortir les flux sortants
 - * Bloque les flux entrants



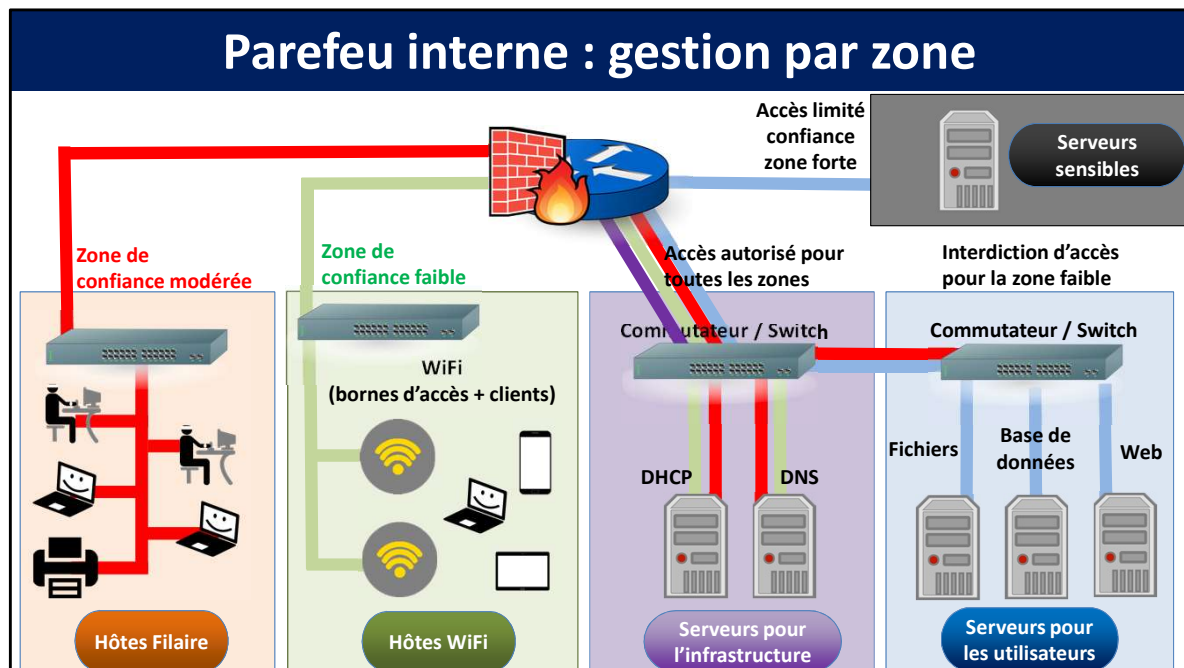
Pare-feu ou Firewall

- Il surveille et contrôle les applications et les flux de données (paquets).
- Contrôle le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.
- Peut s'utiliser aussi entre les réseaux privés interne
- Utilise des règles contenant des IP sources et destinations et des ports sources et destinations.



Les firewall sont aussi présents sur vos PC pour contrôler les connexions entrantes. Par défaut, toute connexion sortante est autorisée et le pare-feu laissera entrer la réponse.

Illustrations et définition issues de Wikipédia



Pour gérer les accès aux ressources (serveurs par exemple) il est commun de faire des zones de confiance.

Suivant le réseau sources, le pare-feu peut autoriser ou non les flux vers un réseau ou un hôte.

Ici, la zone de confiance faible accède uniquement aux serveurs nécessaires a son bon fonctionnement (DHCP, DNS)

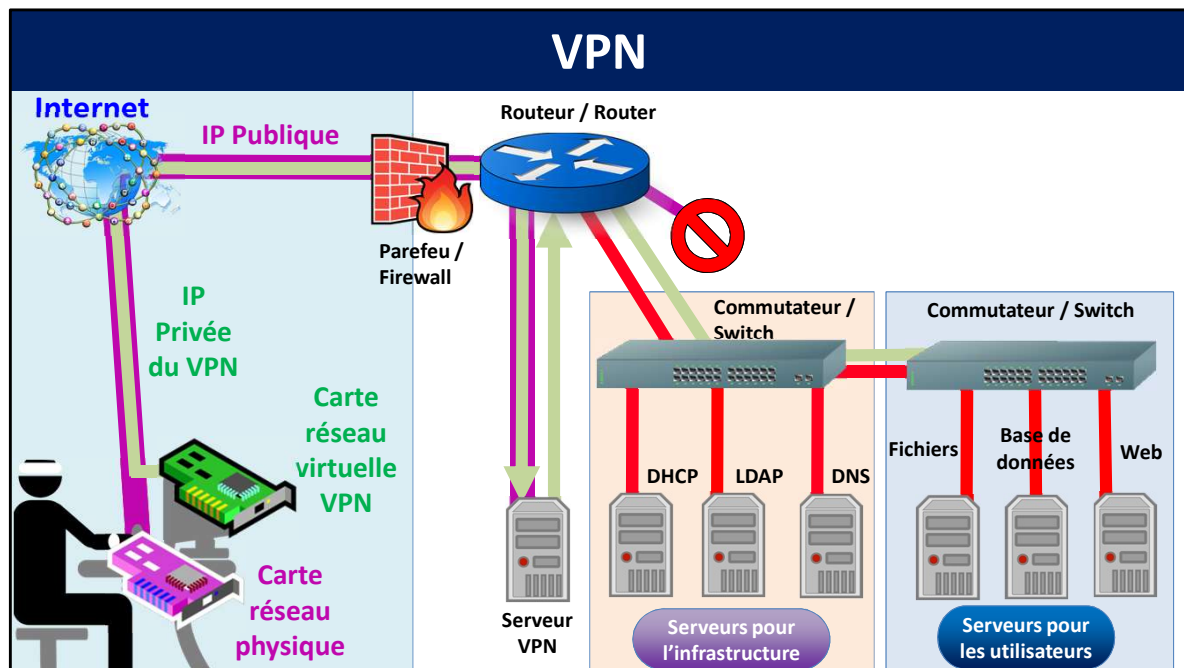
La zone de confiance modérée peut accéder aux autre ressources (serveurs de fichiers ...)

Pour l'accès a des serveurs sensibles (gestion informatique par exemple) il faut faire partie d'une zone de confiance forte (réseau particulier, réseau VPN)



VPN

Virtual Private Network



Le VPN permet de simuler une connexion interne au réseau à partir d'une connexion externe, de l'Internet en général.

Votre PC installe un logiciel VPN

Il est alors créé une carte réseau virtuelle.

Une fois établie la connexion au serveur VPN, en utilisant des adresses IP publiques en source et destination, votre PC reçoit une adresse IP privée supplémentaire.

Cette adresse est autorisée à dialoguer avec les serveurs de l'établissement, quand les adresses publiques de l'Internet ne le sont pas.

Le dialogue encapsulé dans votre communication 'normale' est chiffré pour plus de confidentialité.

La table de routage du PC client est modifiée, des serveurs DNS ajoutés

Il faut être identifié pour avoir accès au serveur VPN

Le serveur LDAP est un annuaire des utilisateurs utilisés pour l'authentification.

VPN

- A partir du client, il y a création d'un tunnel de communication avec le serveur VPN
- Le client dispose d'une adresse IP privée appartenant au réseau local où se trouve le serveur VPN.
Accès aux fichiers, aux ressources de la bibliothèque.
- Peut, en option, re-router le trafic Web
L'utilisateur 'semble' venir du serveur VPN
- Généralement, les communications dans le tunnel VPN sont chiffrées. Evite les risques dans le cas de l'utilisation d'un réseau non fiable.

