2023

Bases sur les Réseaux

Notions indispensables

Olivier D.

Table des matières

1 Concepts de base

Typologie de réseaux informatiques

PAN : La plus petite étendue de réseau est nommée en anglais *Personal Area Network* (PAN). Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique.

LAN : De taille supérieure, le *Local Area Network* (LAN), en français Réseau Local d'Entreprise (RLE), relie entre eux des ordinateurs, des serveurs.

MAN : Le réseau métropolitain ou *Metropolitan Area Network* (MAN) est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN.

WAN : Les étendues de réseaux les plus conséquentes sont classées en *Wide Area Network* (WAN). Constitués de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux.

Historique

Au début, 2 types :

- Informatique centralisée : N terminaux + 1 mainframe : les traitements sont faits sur le mainframe.
- Informatique répartie (IBM PC, ATARI, APPLE) : les traitements sont faits sur chaque machine.

D'un point de vue logiciel, les ordinateurs reliés à un réseau sont répartis en deux catégories en fonction des actions qu'ils effectuent sur celui-ci :

- Un **client** est demandeur de services. Par exemple, cela peut être un poste de travail utilisateur demandeur de services d'applications, de fichiers, d'impression...
- Ces services sont offerts par une entité logicielle qualifiée de **serveur**.

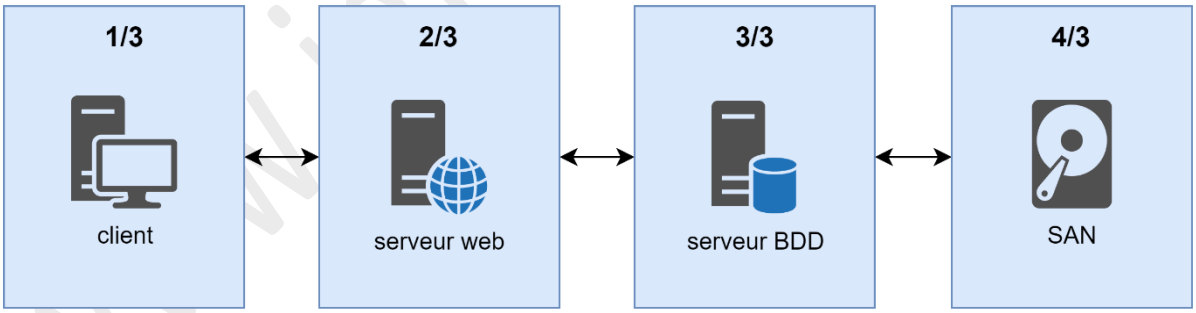
Protocole IP = Client / Serveur : il y a toujours un client potentiel et il y a toujours un serveur

Notion de tiers

Chaque tiers joue un rôle bien spécifique, remplit un service spécifique.

Exemple : un tiers pour le client communique avec le serveur web qui communique avec un serveur de base de données ou un serveur d'applications (cas de google maps).

Il peut y avoir plus de 3 tiers :

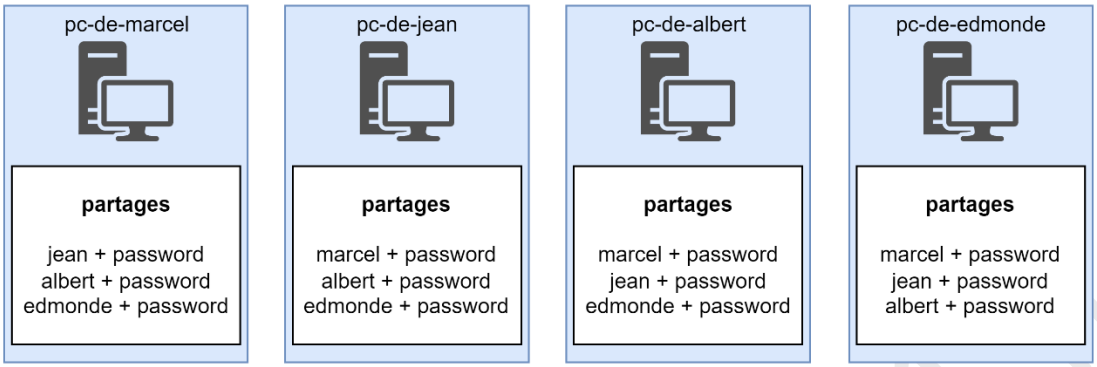


Infrastructure en tiers

P2P (peer to peer)

Infrastructure type réseau local sans domaine. Chaque ordinateur est indépendant et partage ses ressources, il doit donc contenir les informations d'identifications dans sa base locale. Cas du Peer to Peer (pair à pair).

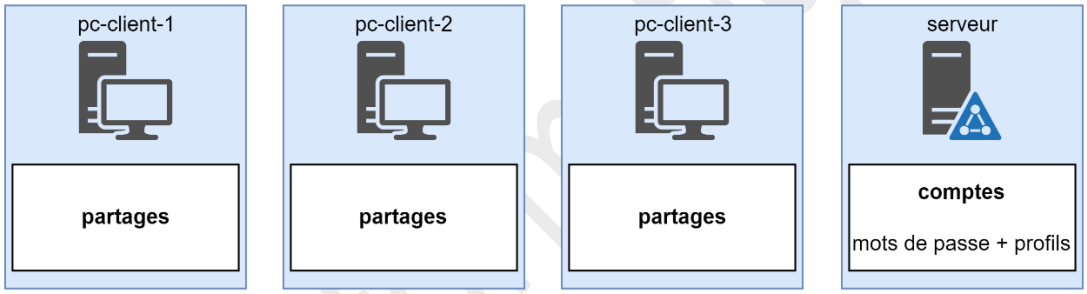
- Point négatif : gestion poste à poste (non centralisée)



Réseau centralisé

Cas d'un réseau avec domaine. C'est un serveur (qui rend un/des services) qui partage ses ressources. Les comptes sont centralisés.

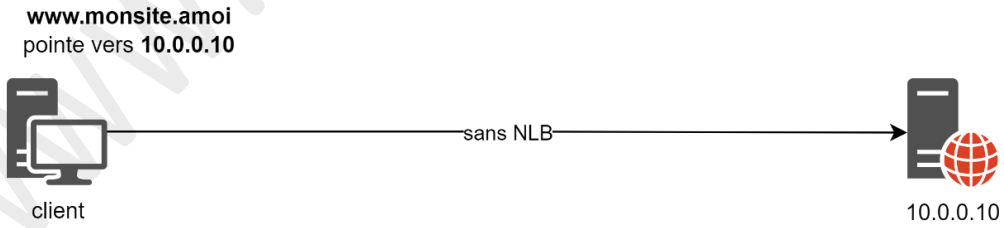
- Point négatif : multiplier la sécurité (redondance matérielle, dupliquer les infos, confidentialité sur le réseau)



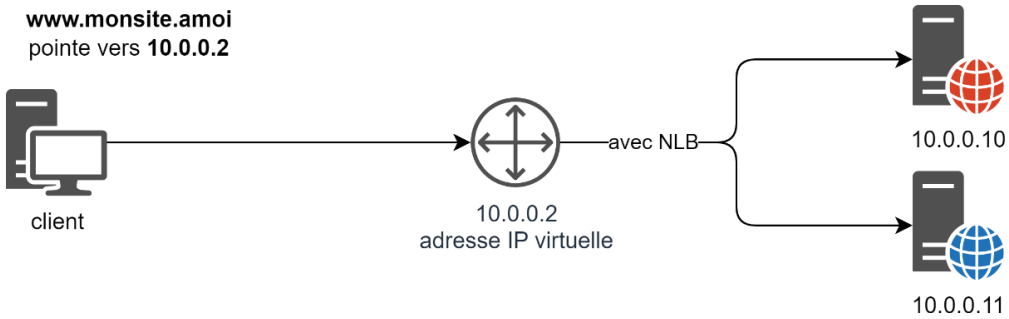
NLB

NLB : *Network Load Balancing*. Répartition de la charge réseau. Répartition des connexions.

- Les charges sont réparties (au taux qu'on veut) sur les 2 serveurs.



Si le serveur 10.0.0.10 devient indisponible, il n'y a plus d'accès web. On ajoute un deuxième site web avec du NLB



Le NLB permet de faire de la répartition de charge et de prendre en compte les indisponibilités d'un des serveurs

2 Modèle OSI

Définition et représentation

Le modèle OSI *(Open Systems Interconnection)* est une normalisation pour définir des standards de communication pour les réseaux. Fonctionne sur le principe de couches empilées. Chaque couche rajoute des données à l'information véhiculée. Chaque couche utilise des protocoles (méthodes) particuliers. Exemple : TCP, IP, Wi-FI ...

7 - Application	Couches hautes	DHCP, DNS, HTTP, SMTP, Telnet ...
6 - Présentation		Unicode, Mime, Ascii ...
5 - Session		Appletalk, H323, socks, TLS ...
4 - Transport	Couches moyennes	TCP / UDP / SPX
3 - Réseau		IP / IPX
2 - Liaison	Couches basses	FDDI, WiFi, Ethernet
1 - Physique		Paire torsadée, bluetooth, 10 base2 ...

Nommer l'information transmise :

- Au niveau de la couche 4 on parle de datagrammes.
- Au niveau de la couche 3 on parle de paquets.
- Au niveau de la couche 2 on parle de frames

Au niveau de la **couche 4** :

UDP :

- Mode non connecté (plus rapide mais avec des risques de pertes) : streaming
- La VoIP fonctionne en UDP : envoie tout en vrac sans se soucier de la bonne réception des paquets

TCP :

- Mode connecté (plus lent mais plus sûr) : transfert de fichiers
- Etape 1 : SYNC ; étape 2 : SYNC ACK ; étape 3 : ACK, etc. : accusé réception à chaque datagramme

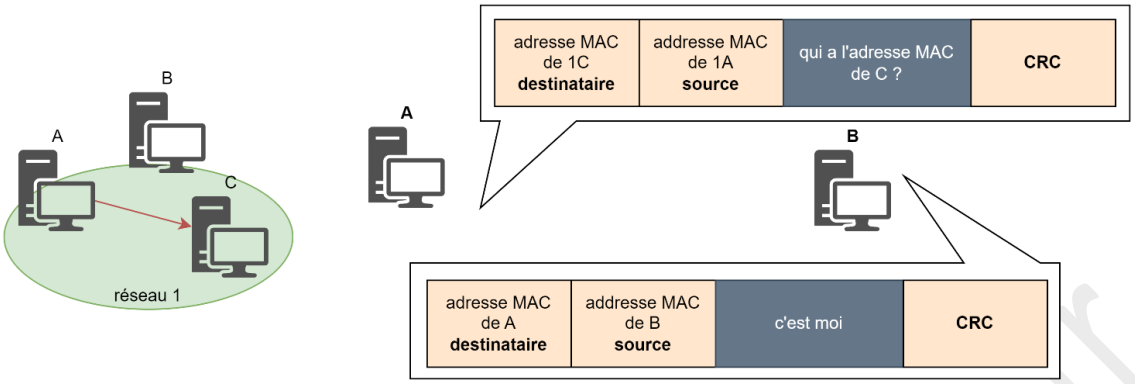
Les trames réseau

- Couche 3 (réseau) : **adressage logique** (adresses IP)
- Couche 2 (liaison) : **adressage physique** (adresses MAC)

Une trame réseau, au niveau de la couche liaison ressemble donc à ceci

Exemple COUCHE 2 : requête ARP :

L'hôte (A) veut joindre l'hôte (B) mais ne connait pas son adresse MAC. Il envoit donc une requête ARP et reçoit une réponse :



Requête ARP et réponse (couche 2)

Exemple COUCHE 3 : IP et le routeur :

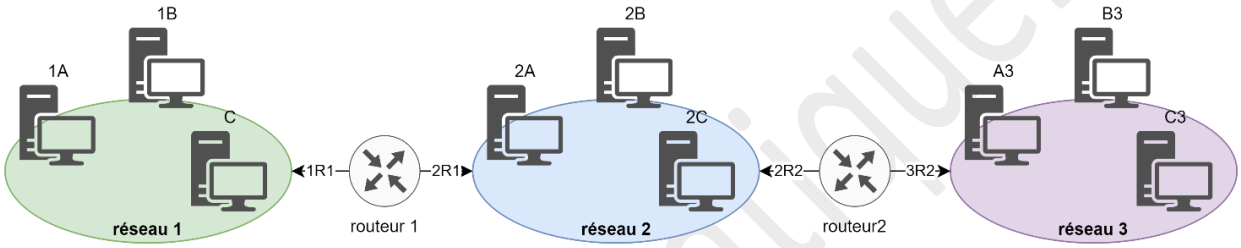
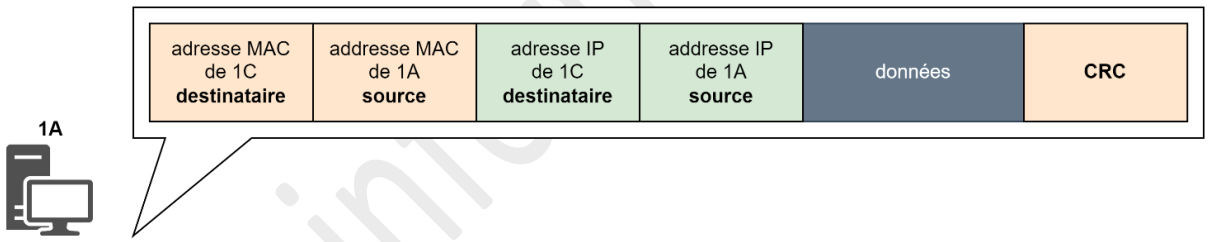


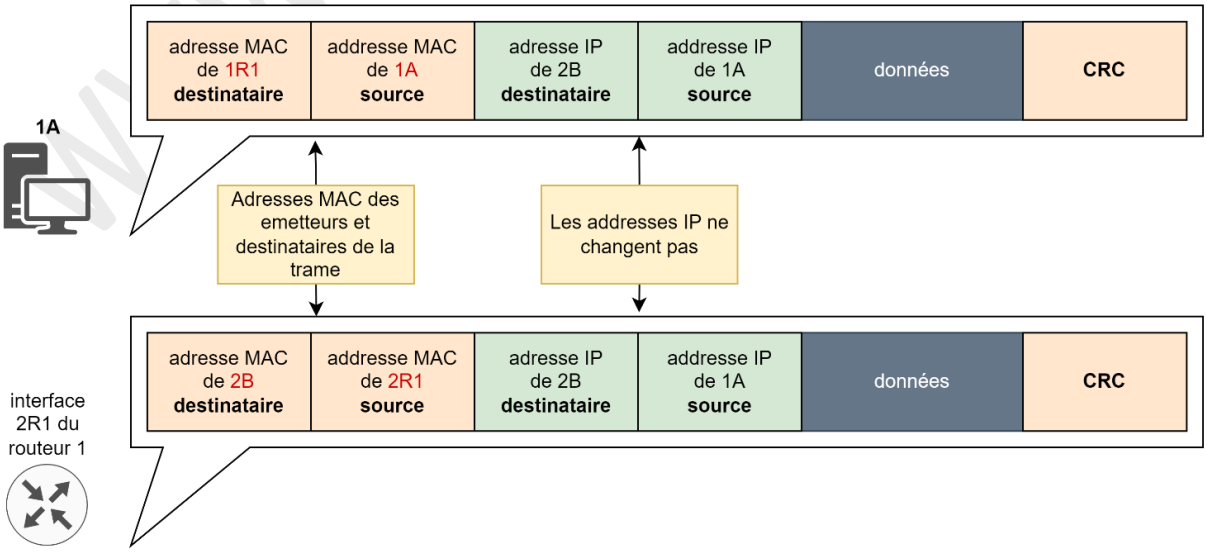
Schéma avec trois réseaux

Cas 1 : de l'ordinateur (1A) vers l'ordinateur (1C) :



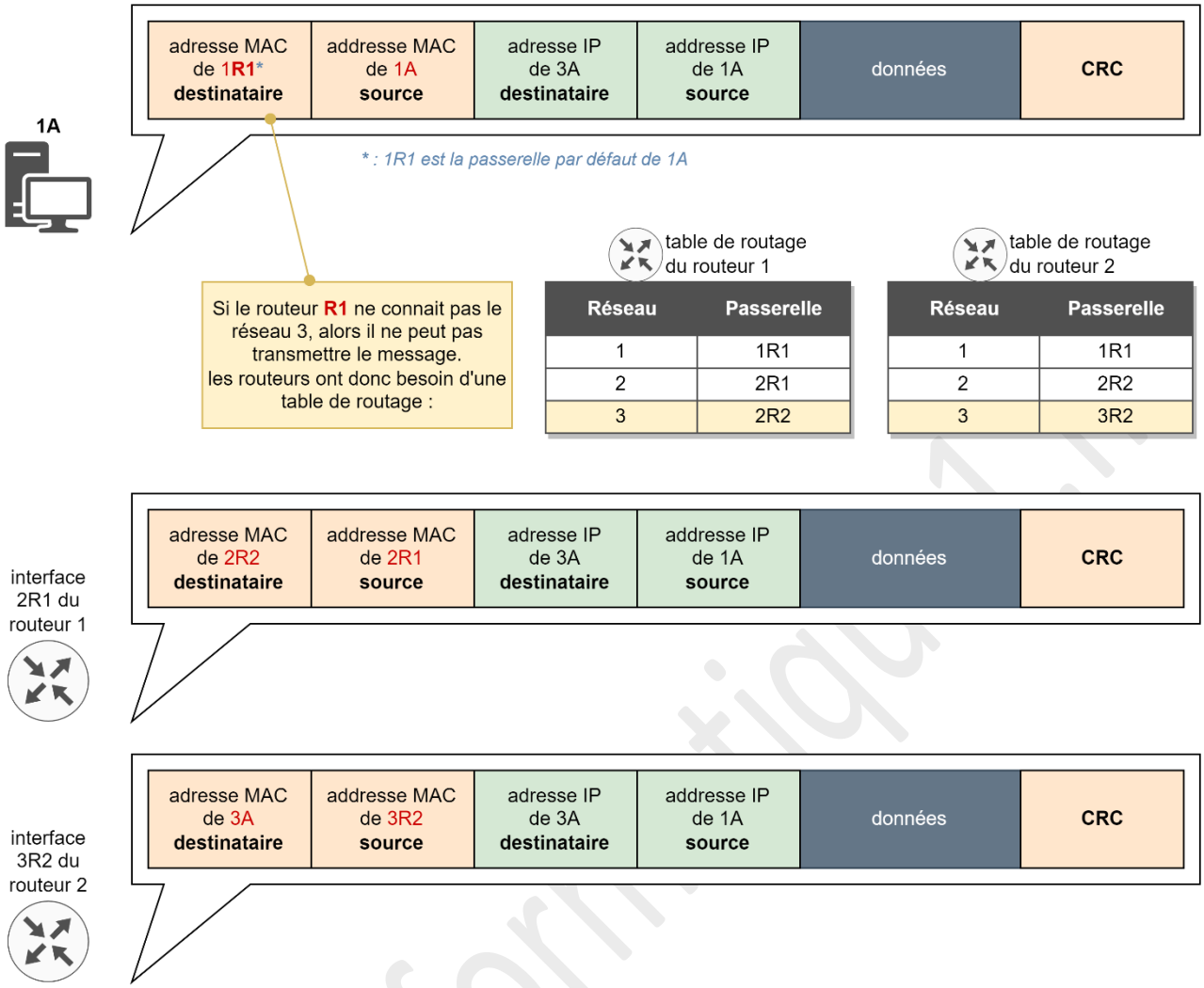
Au sein d'un même réseau, les machines communiquent directement

Cas 2 : de l'ordinateur (1A) vers l'ordinateur (2B) :



La machine du réseau 1 ne peut pas joindre seule la machine du réseau 2, elle passe donc par son routeur qui comprend qu'il doit envoyer au réseau.

Cas 3 : de l'ordinateur (1A) vers l'ordinateur (3A) :



Pour joindre d'autres réseaux, il y a besoin d'une passerelle par défaut et d'une table de routage

- L'adresse MAC change lors du transit (en fonction de l'expéditeur et du destinataire direct)
- L'adresse IP ne change jamais lors du transit

Routage statique : renseigner manuellement dans le routeur des entrées dans la table de routage

Routage dynamique : renseigne automatiquement en questionnant les routeurs. Efface automatiquement les liaisons rompues

- Quand plusieurs ont les mêmes tables : convergence des tables
- Protocoles de routage véhiculant des trames IP : RIP / EIGRP (CISCO seulement) / OSPF / IS-IS / BGP
- Au niveau de la couche 3 et typique IP : les ports (DNS port 53 ; WEB : 80) correspondent à un adressage interne dans la machine
- Mode connecté (TCP) : mode « fiable » (fichiers ...) :
  1. SYNC (synchronisation) puis
  2. ACK SYNC (accusé réception de synchronisation) puis
  3. ACK (accusé réception des paquets)
- Mode non connecté (UDP) : mode « non fiable » (streaming, VoIP ...)

3 Transmission des données, couche physique

La couche physique est dédiée aux éléments de la couche 1

A propos des adresses MAC

Une adresse MAC est codée sur 6 octets exprimés en hexadécimal (couche 2 - liaison).

- Exemple : A1 – B5 – 0C – FF – 05 – 8E

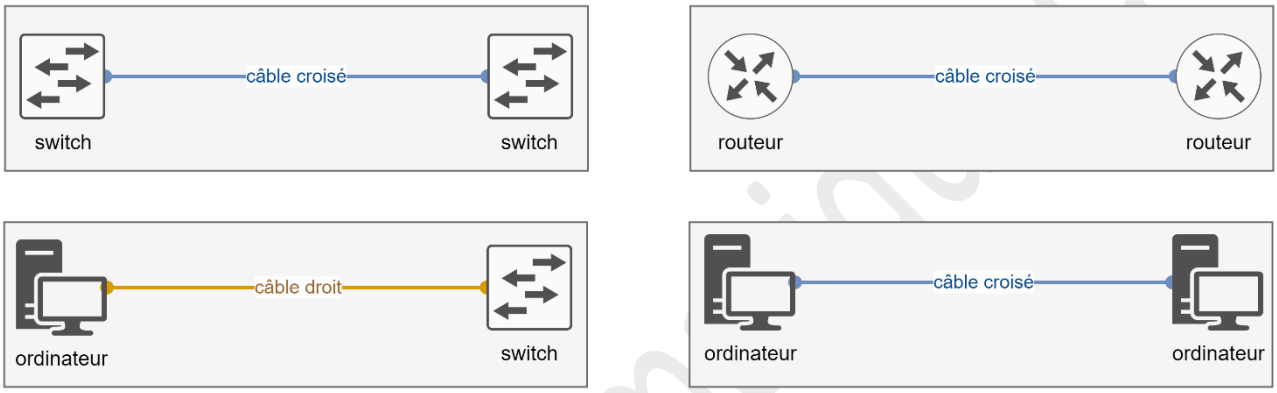
3 octets constructeur + 3 octets déterminés par le fabriquant.

Les 2 premiers bits de gauche du 1e octet constructeur sont à 00 si on s'adresse à une machine

A propos de la connectique

Les connecteurs RJ45 n'ont besoin que de 2 paires en 10/100 : 1 / 3 et 2 / 6. Les autres ne sont pas utilisées.

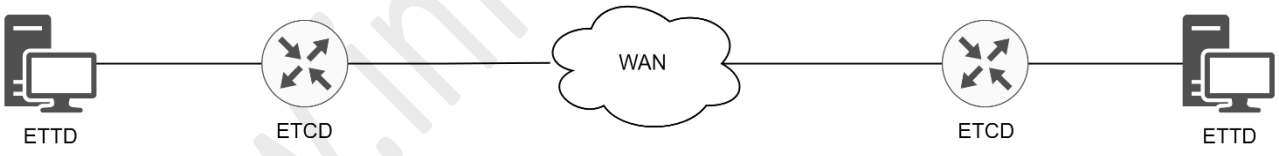
*Le fil **orange** est mis à la 2e prise : plus facile pour déterminer un câble droit / croisé*



Nota : 8 Mb/s = 1MB/s = 1Mo/s (8 megabits = 1 megaByte = 1 megaoctet)

Analogique / numérique

Codage des données : CODEC / MODEM – ETTD / ETCD et modes de fonctionnement

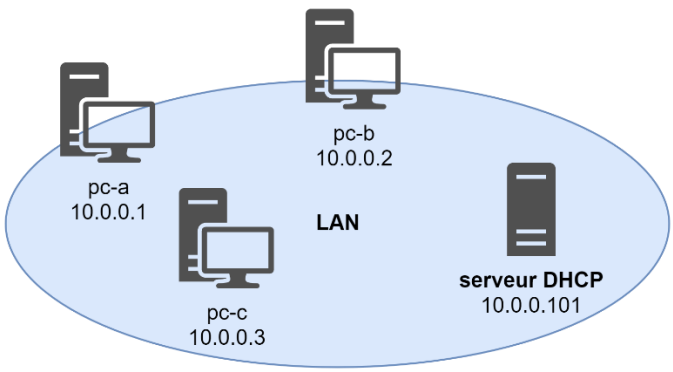


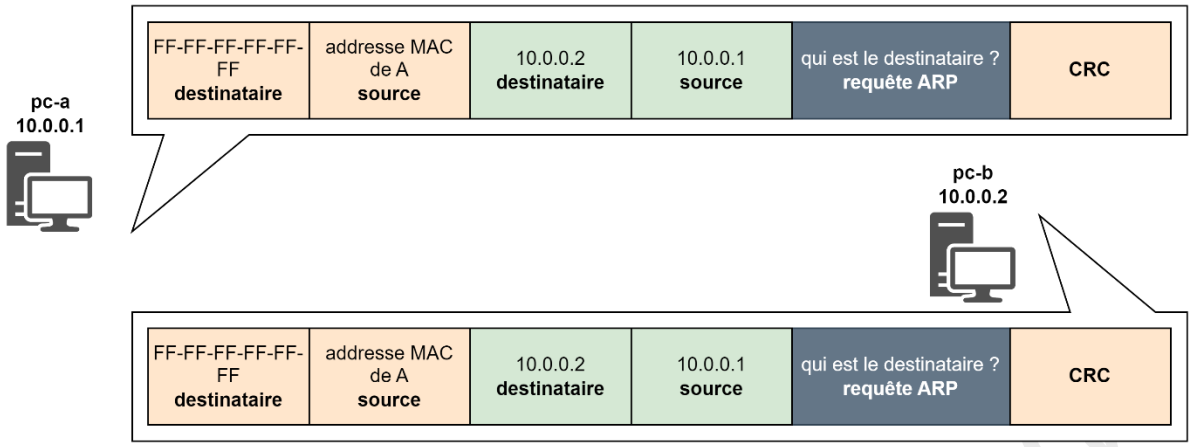
ETTD et ETCD

- ETCD (ou DCE) : Equipement Terminal de Circuit de Données
- ETTD (ou DTE) : Equipement Terminal de Traitement de Données

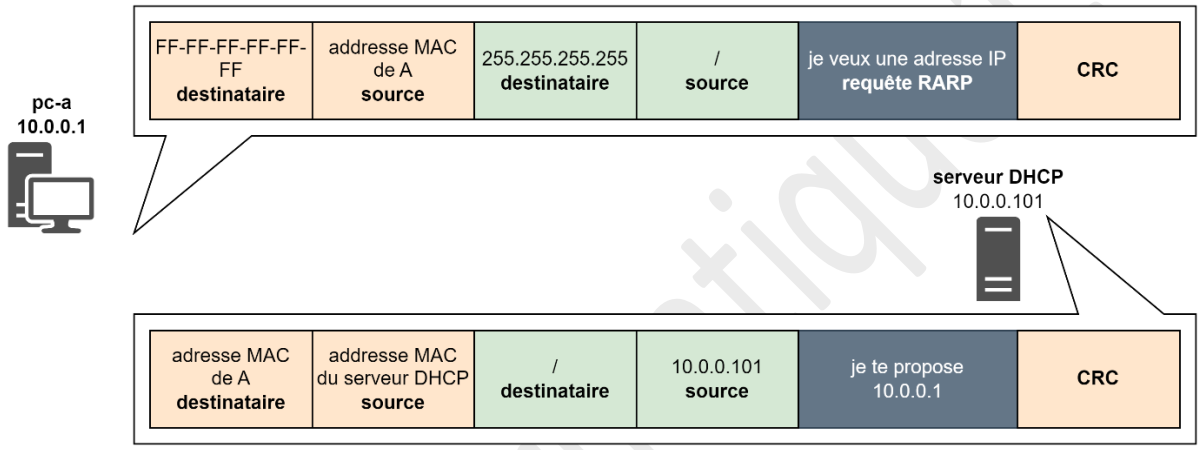
Les requêtes ARP et RARP

Pour les hôtes DHCP





Requête ARP : demande d'une adresse MAC



Requête RARP (demande d'adresse IP). Pc-a envoie ensuite une requête ARP pour savoir si 10.0.0.1 est libre

Support limité VS support non limité

Support limité :

1. Paire torsadée UDP (non blindé) ; STP (gaine + paires blindées une à une) ; FTP *folded twisted pair* (seule la gaine est blindée)
2. Fibre optique, etc.

Support non limité :

- WiFi
- Bluetooth
- Radio
- etc.

4 Eléments logiciels de communication

L'adresse de bouclage (loopback)

`ping 127.0.0.1` : teste de la pile IP

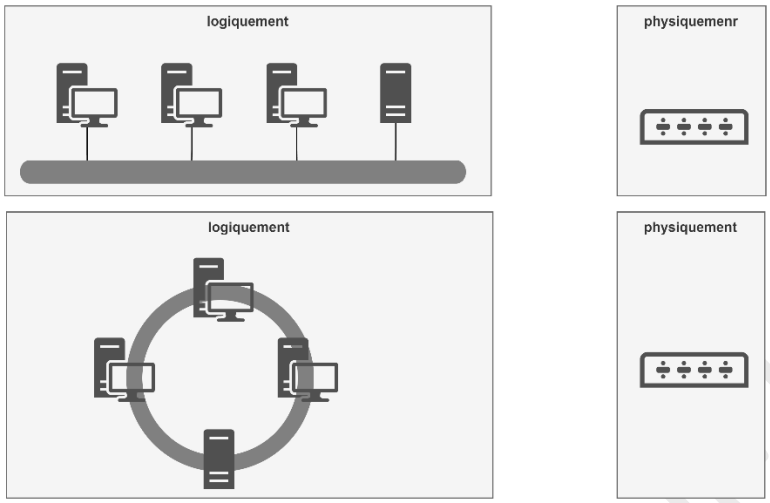
`ping 192.168.0.10` (adresse IP locale) : teste de la carte réseau / test du pilote

Nota : pour plus de commandes sur les éléments logiciels de communication, merci de se référer aux cours Unix et Windows sur les réseaux.

5 Topologies

Ethernet et token ring

On peut avoir un réseau Ethernet (fonctionnement logique du réseau) avec une infrastructure de type token ring.



Mode synchrone : on définit une ***horloge au départ*** et il y a un flot continu d'informations

Mode asynchrone : on envoie des données pour synchroniser. Les informations ne sont pas émises en continu

Plus sur l'Ethernet

Ethernet est une méthode d'accès au support.

Ethernet : CSMA/CD (Carrier Sense Multiple Access / Collision Detection)

1. Écoute de la porteuse (carrier sense) pour savoir s'il y a du bruit ;
2. La trame s'en va partout (multiple access) ;
3. En cas de problème de collision, si 2 postes émettent en même temps ou si le réseau fait une boucle → envoi d'un signal de collision (JAM)

Nota : pour chaque poste qui émet au moment du JAM (donc concerné par la collision) : attente normale + temps d'attente aléatoire (jusqu'à 16 fois) puis erreur si toujours du JAM.

Pour éviter les erreurs on définit une longueur max de réseau : **règle des 5-4-3**

- 5 segments
- 4 répéteurs
- 3 segments habités

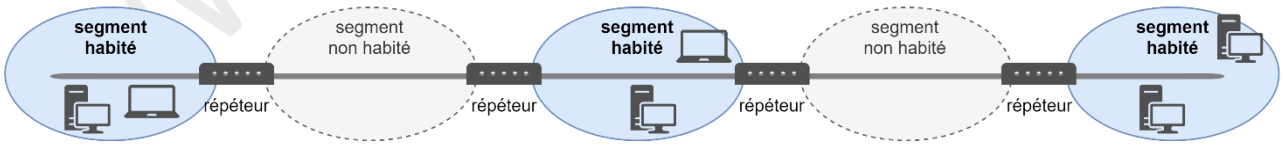


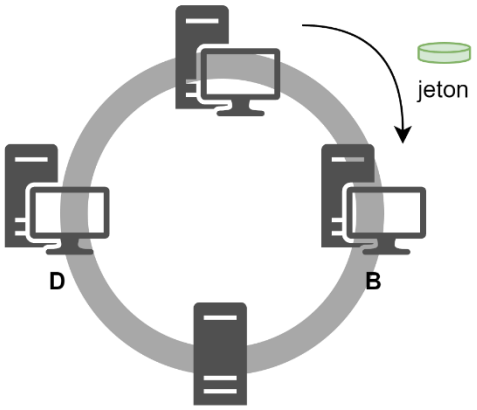
Illustration de la règle des 5-4-3

De plus la taille des trames doit être supérieure ou égale à 64 octets (encapsulation comprise) et inférieure à 1500 octets.

adresse MAC **destinataire**	adresse MAC **source**	adresse IP **destinataire**	adresse IP **source**	données	**bits de bourrage**	**CRC**

Les bits de bourrage remplissent les données de la trame pour qu'elle fasse toujours au moins 64o

Méthode du jeton passant



1. B récupère le jeton
2. B envoie la trame réseau à D
3. D réceptionne la trame et émet un flag
4. B rend le jeton après avoir reçu le flag

avantage : jamais de collision
inconvénient : coûte cher !!

Illustration de la méthode du jeton passant

Réseau FDDI

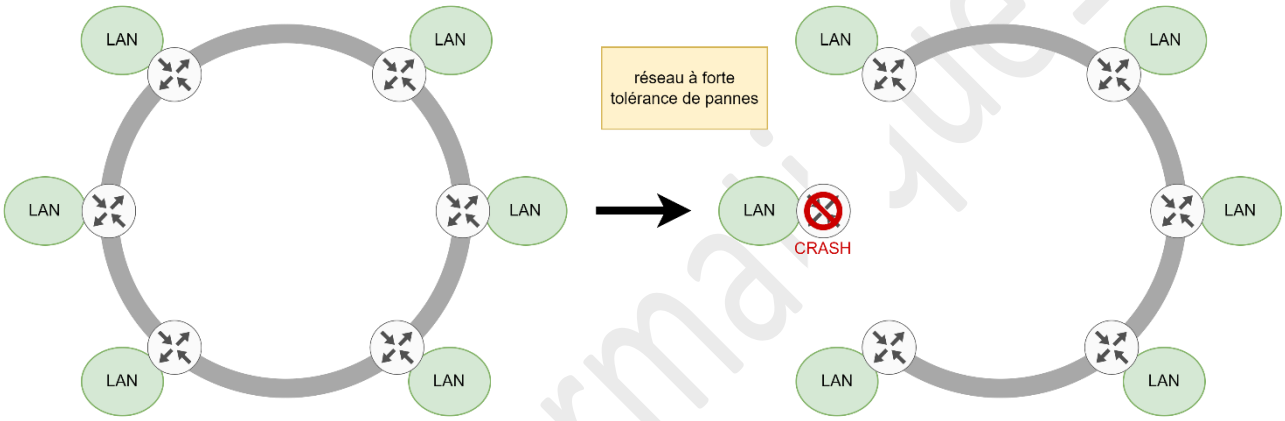
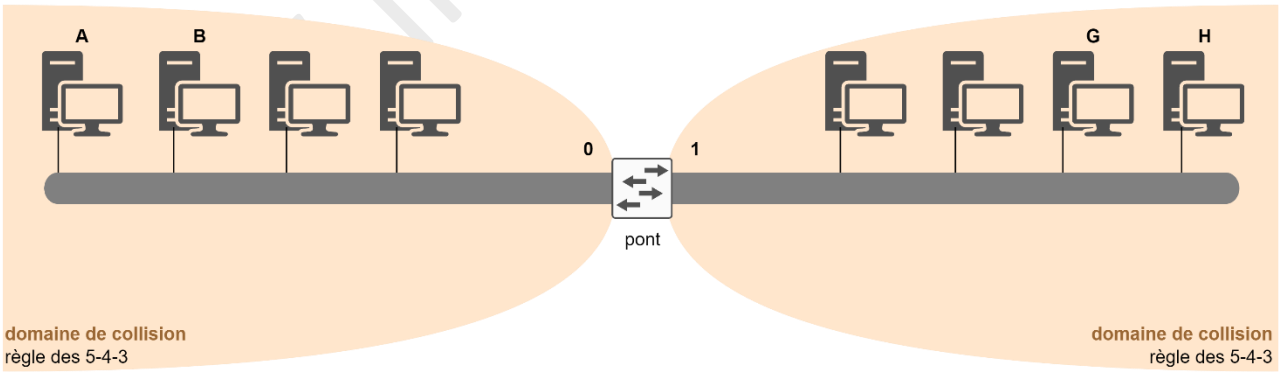


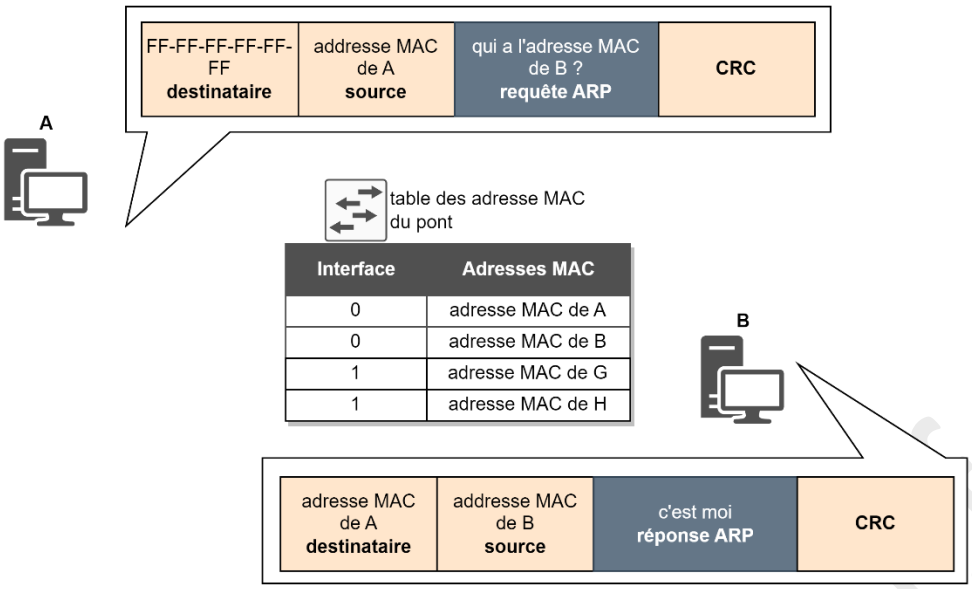
Illustration de réseau FDDI

Interconnexion des réseaux

Un répéteur ne fait que répéter le signal reçu (agit au niveau de la couche 1), et il le fait bien. Sur les schémas (en général), les répéteurs ne sont pas indiqués, ils sont implicites.



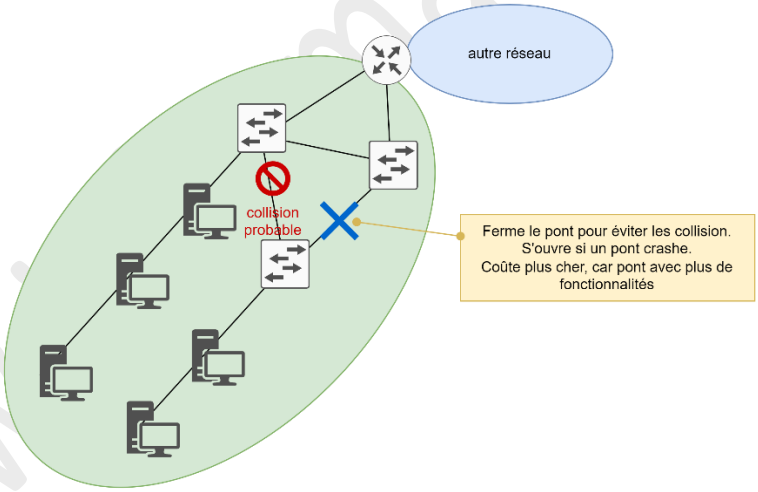
A/B et G/H sont dans des domaines de collision différents. Ils peuvent donc se parler en même temps

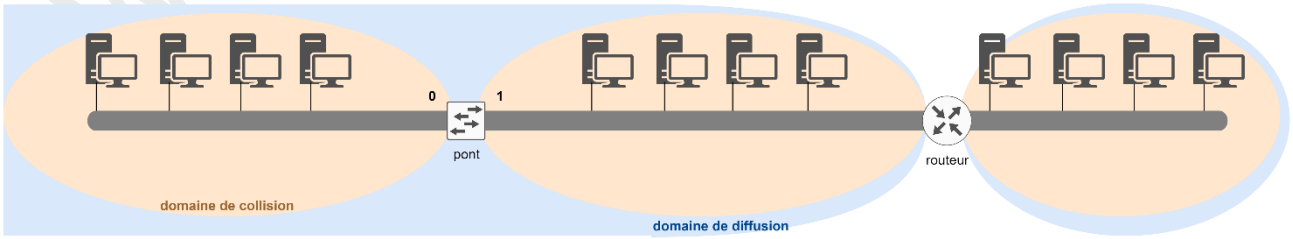


Le pont bloque les réponses ARP pour ne pas les laisser passer sur l'interface 1. En plus de ça, le pont ne laisse pas passer les collisions.

Le spanning tree

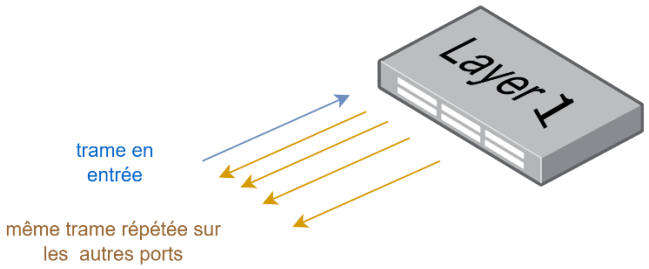
- Couche 1 - Transceiver : est capable de changer de type de signal (exemple : coaxial ⇔fibre optique) mais fait le même travail qu'un répéteur.
- Couche 2 - Pont : peut faire le lien entre Ethernet et Token Ring (exemple : taille des trames différentes)
- Inventeur : Edger DIJKSTRA



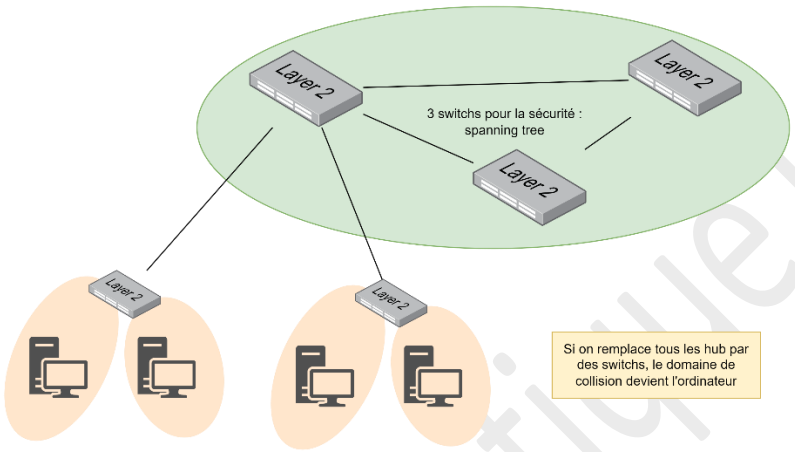


Domaine de diffusion et de collision des requêtes ARP

HUB : concentrateur = répéteur multiport (couche 1)



SWITCH : commutateur = pont multiport (couche 2)



Mode de fonctionnement des commutateurs

Store & Forward :

- Recalcule le CRC → si le CRC est erroné : ne retransmet pas
- Trame trop longue : ne retransmet pas
- Trame trop petite : ne retransmet pas
- Inconvénient : perte de vitesse

On the fly (à la volée) :

- Retransmet à la volée. Les SWITCH SISCO établissent des statistiques d'erreurs. Si il y a trop d'erreur, le SWITCH passe automatiquement en Store & Forward

Pour le token ring, le *spanning tree* est remplacé par le *source routing* (même principe).

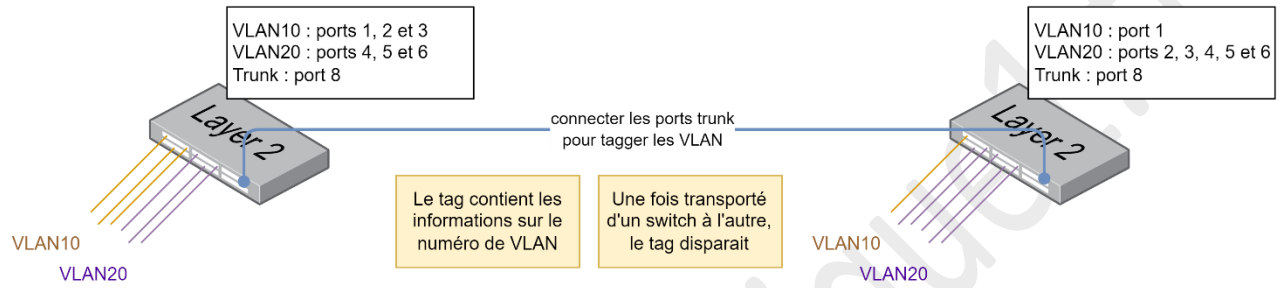
6 VLAN

VLAN (Virtual LAN) : principalement un réseau virtuel utilisant la norme IEEE 802.1d (trunking)

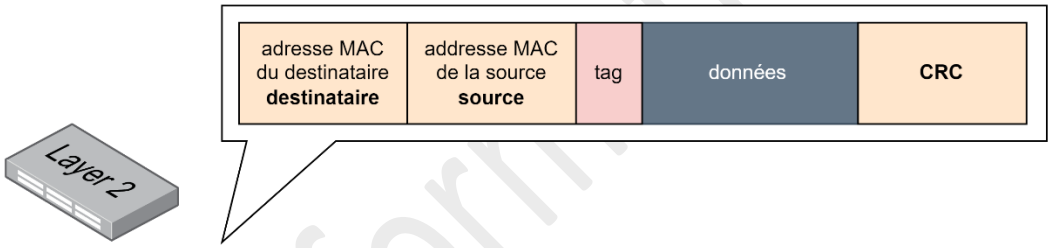
- Sécuriser,
- Séparer en domaines de diffusion,
- Mutualiser,
- S'affranchir des contraintes géographiques.

6.1 Types de VLAN

VLAN de niveau 1 (avec les numéros de ports)



Le port trunk ne se retrouve que sur les matériels CISCO



Le tag est ajouté par le port trunk et contient le numéro de VLAN

VLAN de niveau 2 (par adresses MAC)

Il faut un matériel particulier – de catégorie supérieure – pour stocker les adresses MAC

VLAN	Adresses MAC
10	22-0c-7b-88-f1-0d
10	0e-8c-dd-1a-8b-25

Exemple de stockage

Les adresses MAC changent souvent dans une entreprise (renouvellement du parc, pannes d'ordinateur, etc.). Cela demande donc beaucoup de maintenance.

VLAN de niveau 3 (par adresses IP) → le plus répandu

Si un matériel sait faire du niveau 3 alors il sait faire routeur.

VLAN	Adresses MAC
10	10.0.0.1
10	10.0.0.15
10	10.0.0.50 - 10.0.0.60

Exemple de stockage : soit par adresses IP, soit par plage d'IP (dans le cas de DHCP surtout)

6.2 Routage entre les VLANs : Inter VLAN

Moyen n°1 : on connecte des routeurs sur les switchs avec une patte dans chaque VLAN

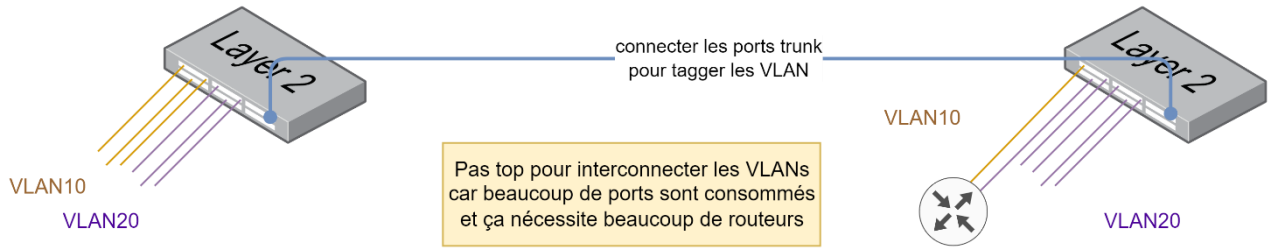


Illustration de la connexion de routeurs sur les switchs avec une patte dans chaque VLAN

Moyen n°2 : on utilise un routeur spécial qui a une patte sur un port dédié pour lui

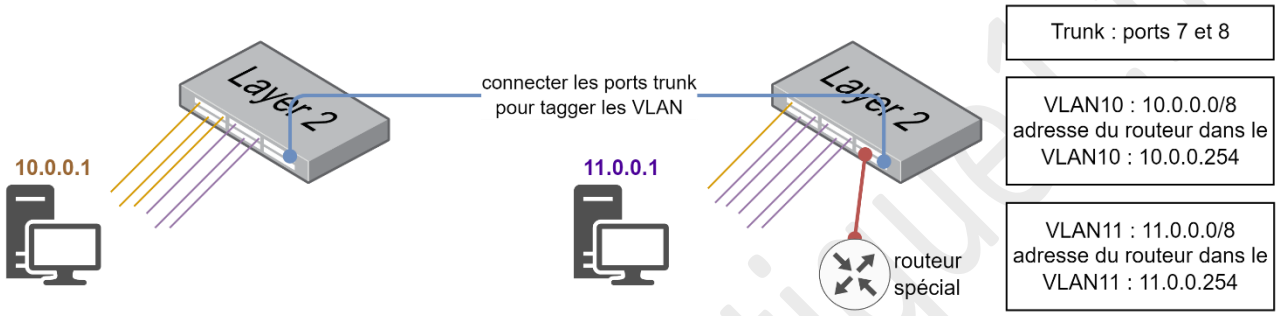


Illustration de la mise en place d'un routeur spécial sur un port dédié

Moyen n°3 : acheter un commutateur de niveau 3 (le top)

- Lui faire faire du VLAN de niveau 1 (physique)
- Configurer le routage inter VLAN (car il sait faire du niveau 3)

Illustration d'utilisation de commutateurs de niveau 3

6.3 Les routeurs

Rappel sur les tables de routage :

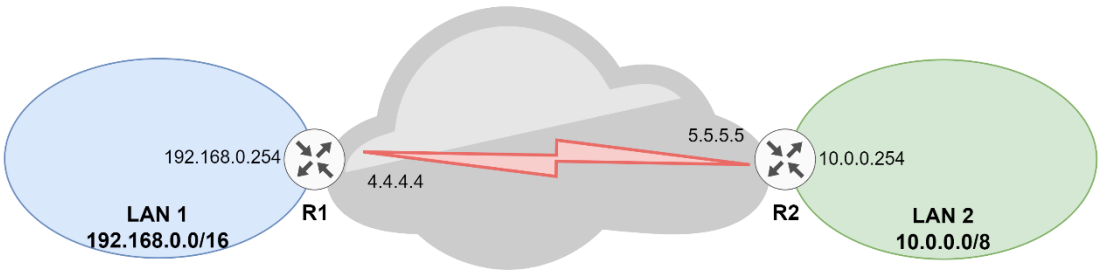


Table de routage de R1

Réseau	Adresse
192.168.0.0/16	connecté
10.0.0.0/8	5.5.5.5
0.0.0.0/0*	4.4.4.4

WAN (Internet)

Table de routage de R2

Réseau	Adresse
10.0.0.0/8	connecté
rien pour LAN1	
0.0.0.0/0*	5.5.5.5

* Le réseau 0.0.0.0/0 correspond à la route par défaut : chemin à prendre pour aller vers les autres réseau. Généralement la sortie vers Internet

Dans ce cas, R1 peut joindre R2, mais R2 ne peut pas joindre R1. Le ping est donc en échec

Routage dynamique (protocoles EIGRP / RIP / OSPF) : permet de construire les tables de routage automatiquement.

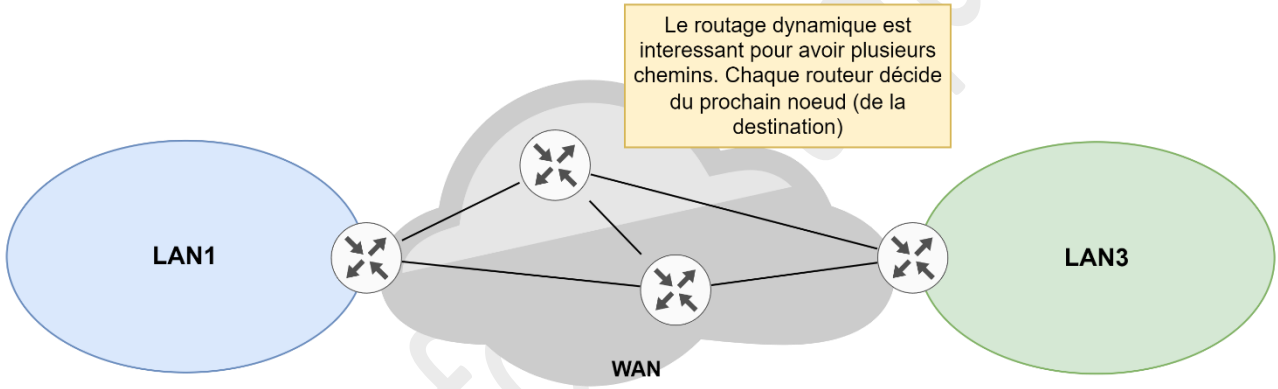


Illustration du routage dynamique

Comment un protocole de routage dynamique choisit-il le meilleur chemin :

Méthode	**Détail**	**Utilisable par Cisco**	**Activé par défaut (Cisco)**
Distance administrative	Degré de confiance accordé aux protocoles de routage		
Métrique	Représentation de la distance à parcourir		
Nombre de sauts	Nota : RIP n'utilise que cette méthode pour choisir le meilleur chemin		
Bande passante	(10Mb/s, 100Mb/s, etc.). Nota : OSPF n'utilise que cette mesure	X	X
Latence au ping		X	X
Charge sur le lien	Taux d'occupation	X	
Fiabilité	Taux d'erreurs sur la route	X	

6.4 Protocoles de routage :

A vecteur de distance (**RIP ; IGRP ; EIGRP**) → envoi de sa table de routage au voisin (t=30s) :

- Convergence lente (un saut -de routeur à routeur- toutes les 30 secondes)
- Peu de ressources utilisées
- Limitation du nombre de routeurs à traverser (éviter les boucles de routage)

A état de liaison (**OSPF ; IS-IS ; BGP**) → changement d'état = envoi du lien qui a changé :

- Convergence rapide
- Ressources du routeur importantes (processeur, RAM) car recalcule toute sa table
- Sujet au flaping (en cas de mauvais contact : renvoie plein de changements d'état)

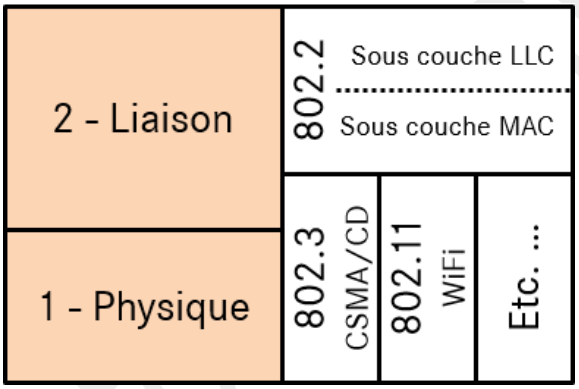
Passerelle

Au niveau réseau une passerelle sert à remonter puis redescendre de modèle OSI pour « traduire des données »

Normalisation des couches basses des PAN et LAN

Rappel : couches basses = couche 1 et couche 2 du modèle OSI

Des normalisations proviennent de l'IEEE (exemple : 802 pour les couches basses) :



Les normalisations IEEE des couches bases du modèle OSI

- Les normalisations du type 802.1 sont globales : pas affectées à un protocole particulier.

802.1D : spanning tree

802.1Q : TAG de trames (exemple : trunking)

Support physique

- **10base2** (10Mbps ; bande de base ; 2x100m ≈ 185m) *coaxial fin*
- **10base5** (idem mais 500m) *coaxial épais*
- **10baseT** (*torsadé*, distance maxi = 100m)
- **100baseT** (100Mbps) correspond au 100baseTX
- **100baseFX** (fibre optique)
- **1000baseT** (*torsadé*) / 1000baseFX (*fibre optique*)

Entête de trame Ethernet

Page wikipedia

préambule	adresses : **destinataire et source** (MAC et IP)	type, longueur	données	**CRC**

En-tête de trame Ethernet

Le Wi-Fi

Le Wifi est un label délivré par la wifi alliance

802.11 *: normalisation des réseaux sans fils*

Norme	Débit	Bande passante
802.11A	Jusqu'à 54 Mb/s	5 GHz
802.11B	Jusqu'à 11 Mb/s	2,4 GHz
802.11G	Jusqu'à 54 Mb/s	2,4 GHz
802.11N	Jusqu'à 300 Mb/s	2,4 GHz et 5 GHz

Mode AD HOC : connecter des machines de façon temporaire

Mode Infrastructure (point d'accès) : nécessite un point d'accès qui reçoit toutes les communications

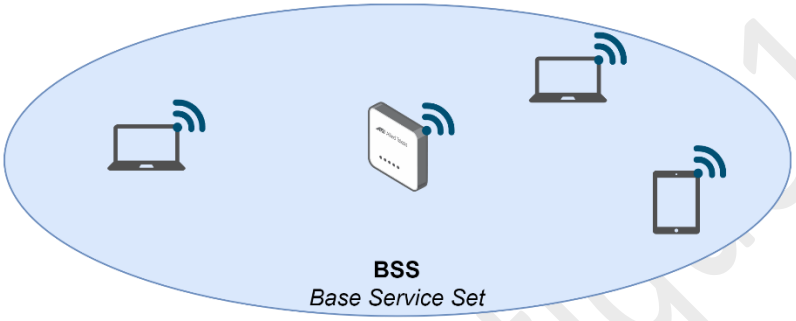


Illustration du BSS

Pas de CSMA/CD : trop de collisions. Utilisation du **CSMA/CA** : demande de temps de parole au point d'accès.

En wifi il y a beaucoup d'interférences et d'erreurs. On envoie donc des trames très petites

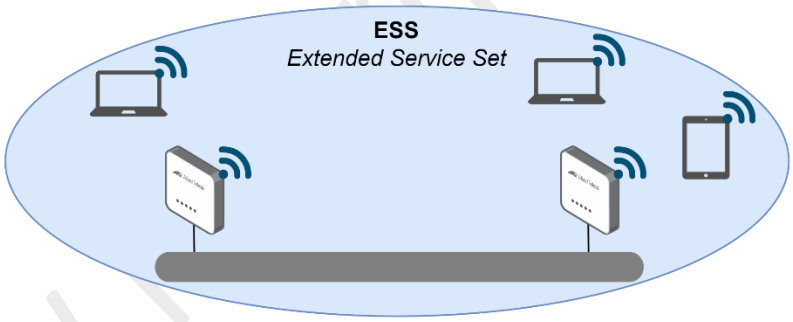


Illustration du ESS

Problème de la sécurité : IL FAUT PRENDRE LES DEVANTS !

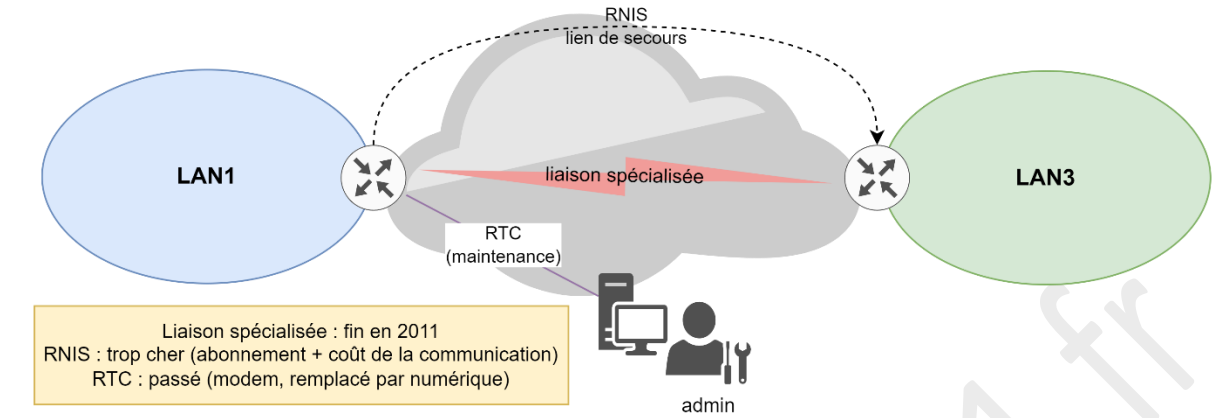
- Ne plus diffuser le SSID
- Changer le mot de passe (+login) de l'admin
- Filtrer les adresses MAC
- Chiffrer les données (WEP / WPA / WPA2 …) mais aussi serveur RADIUS

Courant porteur en ligne

- CPL (*Courant porteur en ligne*) : transporte des données informatiques en utilisant le courant électrique domestique comme support.
- Le boitier CPL est un genre de pont (transforme le signal Ethernet – CPL).
- Débits : ~~14 Mbps~~ ; 85 Mbps ; 200 Mbps

7 Protocoles des réseaux MAN et WAN

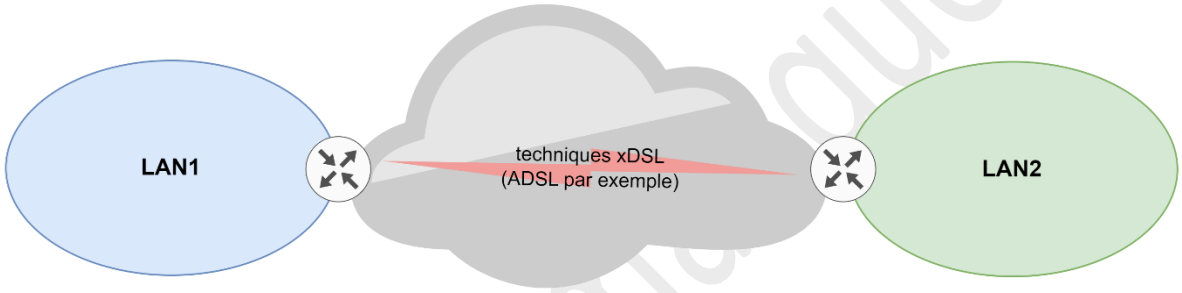
Rappels sur les méthodes en obsolescence



+

Méthodes obsolètes

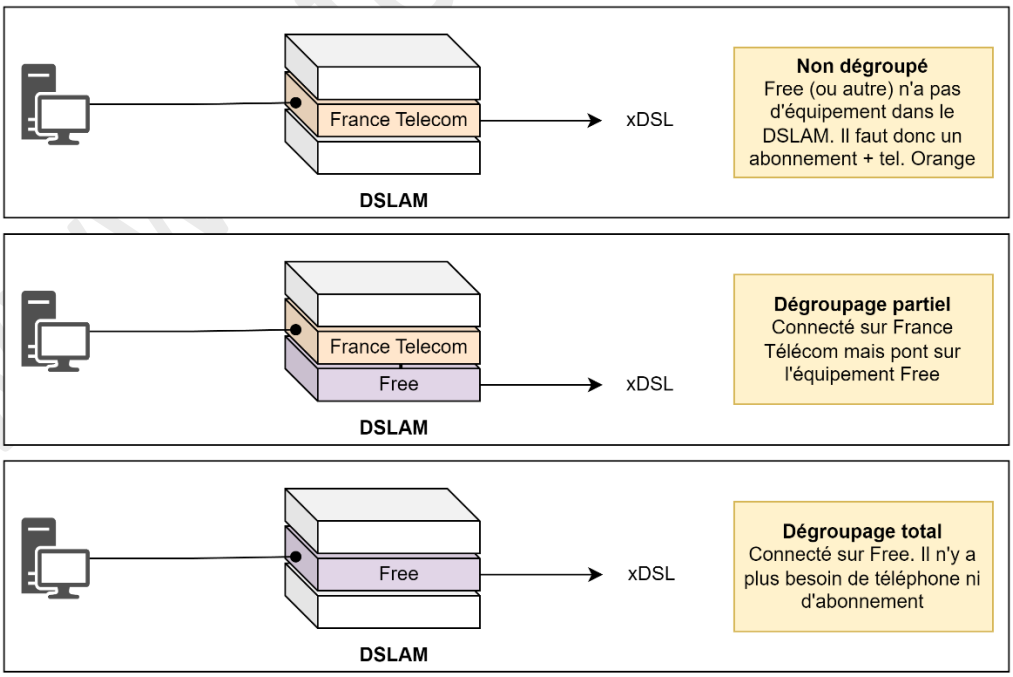
Méthodes d'aujourd'hui



ADSL = Asymetric Digital Subscriber Line

Le dégroupage

FT : France Télécom (Orange)



Plusieurs opérateurs peuvent se partager un DSLAM

Autre cas : **Abonnement nu.** Connecté sur FT mais FT sous-loue la ligne à un autre opérateur.

Exemple : 4 habitants isolés donc trop cher de mettre le dégroupage Free sur le DSLAM.

FDDI

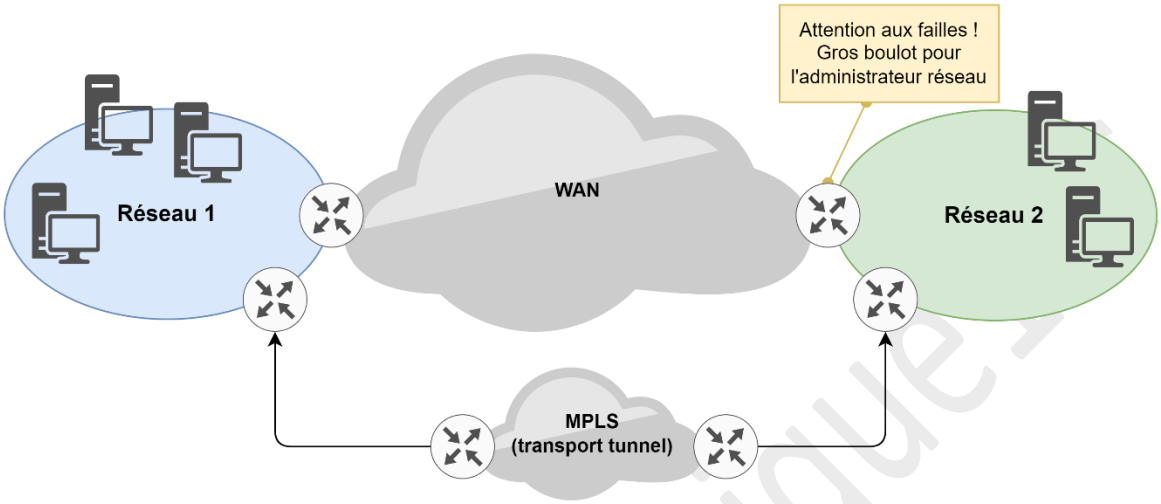
FDDI : fibre. Fonctionne sur les couches 1 à 3 du modèle OSI.

ATM

ATM : Asynchronous Transfer Mode. Fonctionne sur les couches 1 à 3 du modèle OSI.

MPLS

MPSL : *MultiProtocol Label Switching*. De plus en plus répandu.



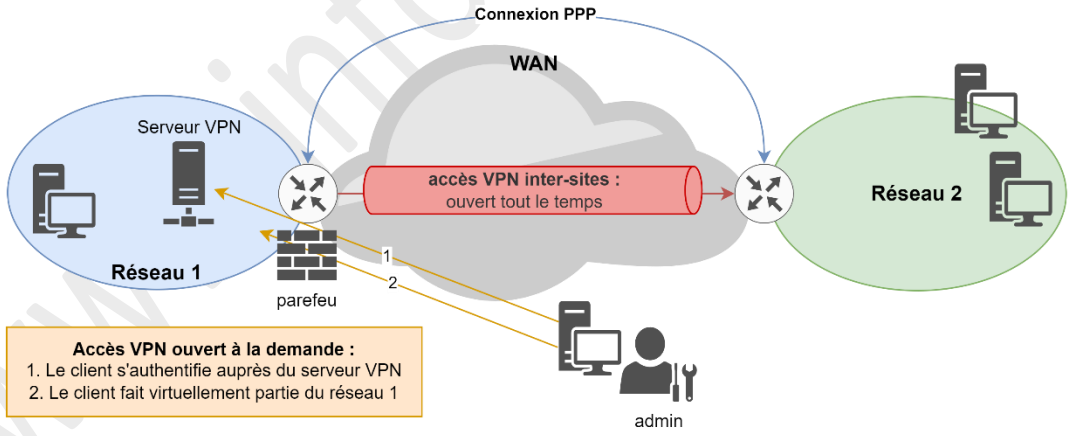
*En MPLS on passe **hors Internet**. C'est le même principe qu'un VLAN*

Les trames MPLS sont taguées aux niveaux 1 et 2 du modèle OSI. C'est donc rapide.

Avantages :

- On peut aussi ajouter ou interdire des services (VoIP ...)
- Les informations qui passent dans le MPLS sont confidentielles
- L'accès internet est fourni (la sécurité repose sur le Fournisseur d'Accès Internet. On se sent donc mieux)

Accès distant et VPN



Les différents types d'accès distants

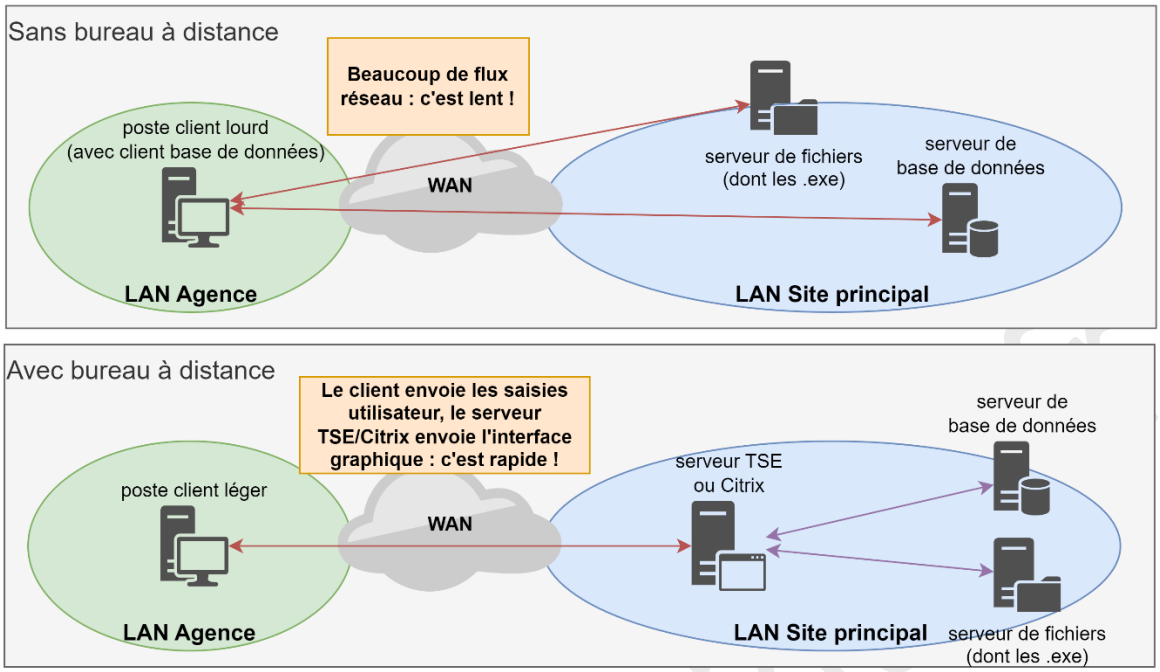
- Le VPN c'est du PPP chiffré
- PPP = connexion directe à un poste distant

VPN SSL

VPN SSL : Connexion VPN utilisant un certificat pour chiffrer les connexions entre le client et le serveur.

Bureau à distance

TSE – CITRIX :



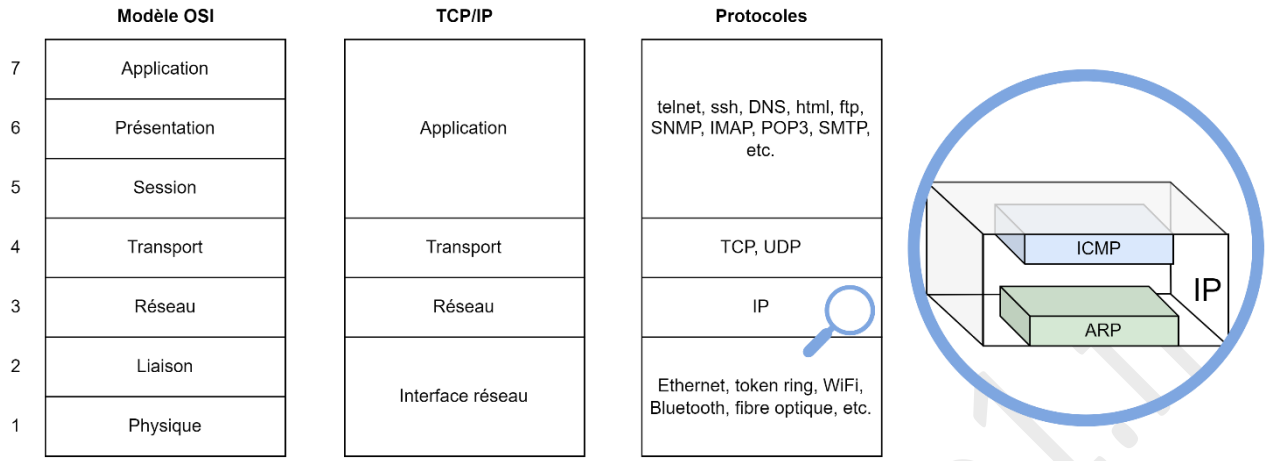
Le serveur TSE/Citrix et les autres serveurs communiquants avec doivent être proches

Avantages :

- Si on installe TSE avec le client du progiciel (exemple word2010), le client n'a plus besoin d'avoir Word2010. Ça fonctionne même s'il a Word2013.
- Ça fonctionne aussi avec des OS différents sur les postes du réseau.
- Ça fonctionne aussi avec des machines obsolètes (peu de travail du processeur).
- Plus besoin de progiciel spécifique.

8 Protocoles des couches moyennes et hautes

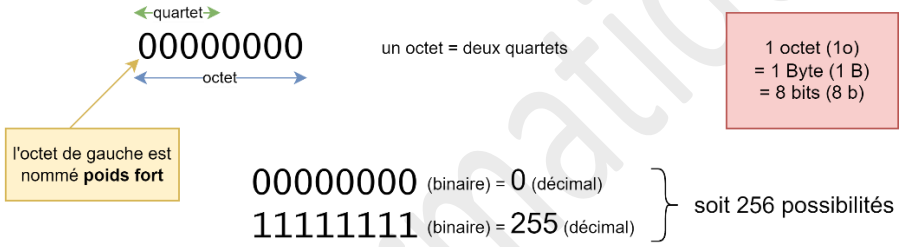
TCP/IP



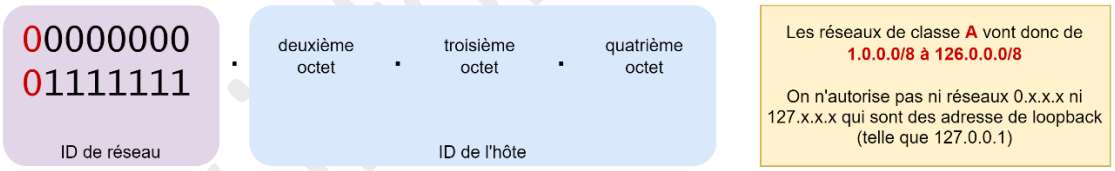
La couche 3 est celle qu'on connait le mieux : celle avec les adresses IP

Présentation de l'octet

Le protocole IPv4 est codé sur 4 octets séparés par des points (exemple : 192.168.1.101).



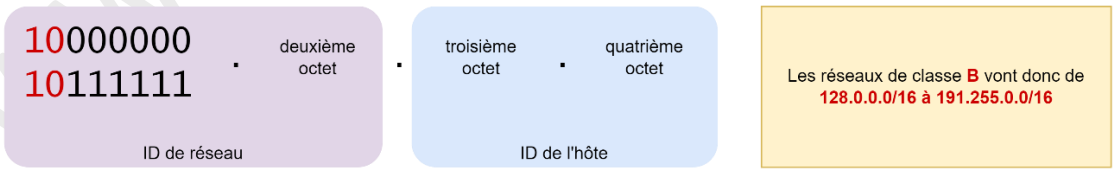
Les classes de réseaux



masque = **255.0.0.0** ou **/8** en notation CIDR (on prend les **8** octets les plus à gauche pour l'ID de réseau)

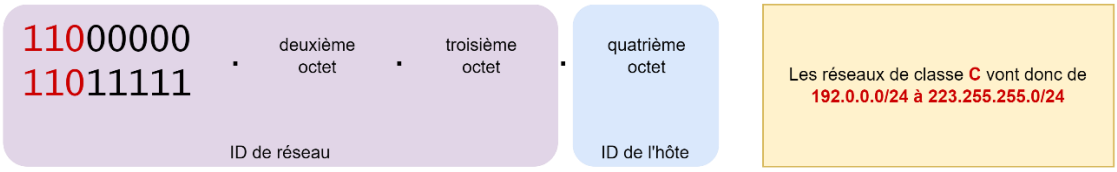
Par exemple, pour une machine ayant l'adresse IP 115.8.8.101 : l'ID de Réseau = 115 ; l'ID de l'hôte = 8.8.101

Réseau de classe A



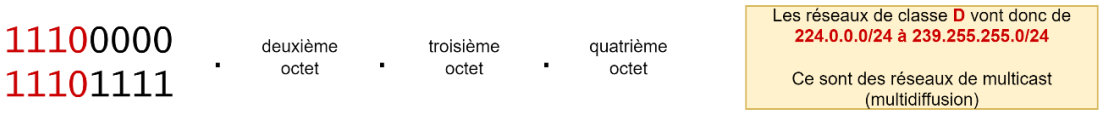
masque = **255.255.0.0** ou **/16** en notation CIDR (on prend les **16** octets les plus à gauche pour l'ID de réseau

Réseau de classe B

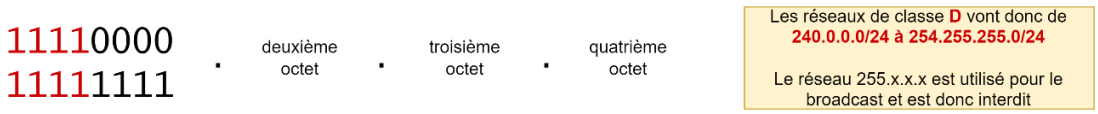


masque = **255.255.255.0** ou **/24** en notation CIDR (on prend les **24** octets les plus à gauche pour l'ID de réseau

Réseau de classe C



Classe D – multidiffusion



Classe E - Expérimental

Si pour l'ordinateur (selon son Masque) l'adresse IP_A est sur le même réseau que l'adresse IP_B alors A peut envoyer à B sans passer par un routeur.

- Adresse IPa = 162.40.10.1/16 (masque : 255.255.0.0)
- Adresse IPb = 162.40.11.2/24 (masque : 255.255.255.0)

Selon a, l'adresse du réseau est 162.40.0.0/16. L'adresse IP de a et l'adresse IP de b sont sur le même RSO. a envoi donc à b

Selon b, l'adresse du RSO = 162.40.11.0/24. L'addrese IP de a et l'adresse IP de b ne sont pas sur le même RSO. b n'envoie pas à a

La conversion binaire – décimal

Il est important de savoir convertir le binaire en décimal puisque l'ordinateur réfléchit en binaire.

Lorsqu'on parle d'une adresse IP : 192.168.1.101, il faut savoir la convertir en 4 octets :

`192.168.1.101` = `11000000.10101000.00000001.01100101`

C'est notamment très utile pour savoir de quel réseau fait partie une adresse IP ou de savoir combien d'hotes peut contenir un réseau.

Le masque de réseau – méthodologie

Adresse IP = 10.11.12.1. Le masque est 255.0.0.0. Avec l'adresse IP et le masque, on peut trouver l'adresse réseau :

- Adresse IP : 10.11.12.1 = 00001010.00001011.00001100.00000001
- Masque : 255.0.0.0 = 11111111.00000000.00000000.00000000

On applique ensuite un ET logique entre l'adresse IP et le masque pour trouver l'adresse du réseau :

- Adresse réseau : 00001010.00000000.00000000.00000000, soit 10.0.0.0 (Id réseau : 00001010)

Dans le cas présent c'était facile. Calculer l'adresse réseau pour 172.127.0.10/12 par exemple.

A propos du 0 et du 255

Prenons l'exemple d'une adresse IP : 192.5.5.3/24 :

- Si on met 0 (binaire) pour toute la partie hôte on obtient le réseau : 11000000.00000101.00000101.00000000 soit 192.5.5.**0**.
- Si on met 1 (binaire) pour toute la partie hôte on obtient l'adresse de broadcast : 11000000.00000101.00000101.11111111 soit 192.5.5.255
- Toutes les autres IP peuvent être assignées à des hôtes : de 192.5.5.1 à 192.5.5.254
- L'adresse IP 192.5.5.3/24 est donc autorisée

Pour le cas de l'adresse IP 172.127.0.10/12 :

- Réseau : 172.112.0.0
- Adresse de broadcast : 172.127.255.255
- Adresses IP autorisées : 172.112.0.1 à 172.127.255.254
- L'adresse IP 172.127.0.10/12 est donc autorisée

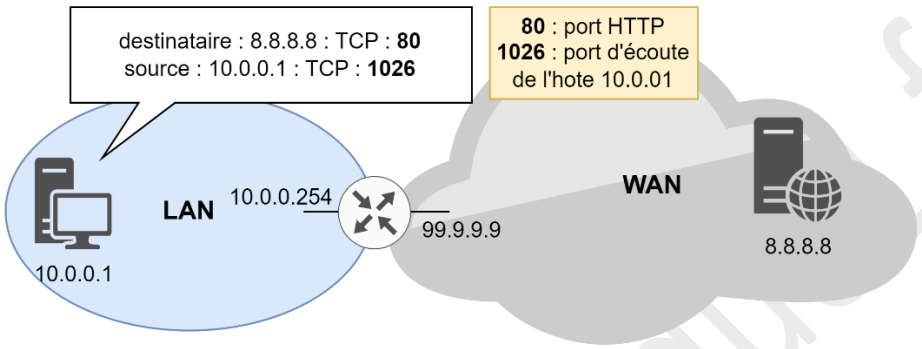
Partie réseau : définit le réseau

Partie hôte : utilisable pour définir les adresses de hôtes de ce réseau. Le « tous les bits à 0 » est interdit (car il définit le réseau), le « tous les bits à 1 » est interdit (car il définit le domaine de diffusion/broadcast)

Méthode pour retrouver les classes de réseau

Classe	Bits de poids fort	Décimal	Plage théorique	Exceptions	Plage réelle
A	0xxxxxxx	0	0 à 127	0 et 127 sont interdits	1 à 126
B	10xxxxxx	128	128 à 191		128 à 191
C	110xxxxx	192	192 à 223		192 à 223
D	1110xxxx	224	224 à 239		224 à 239
E	1111xxxx	240	240 à 255	255 est interdit	240 à 254

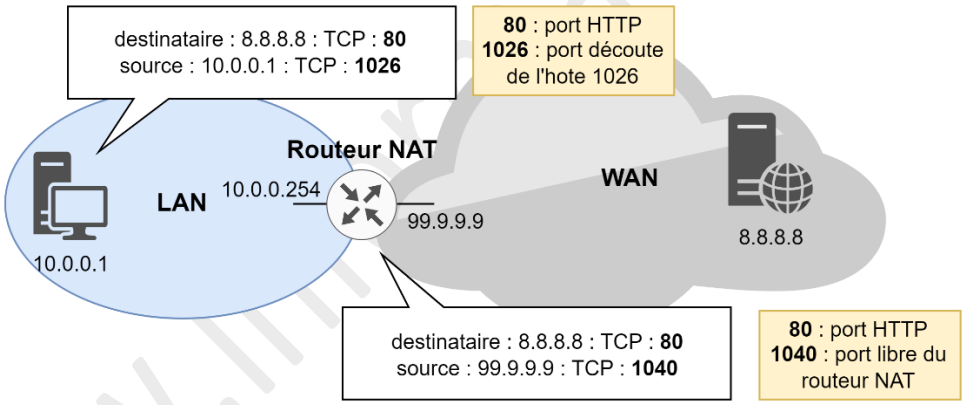
Le NAT et le socket



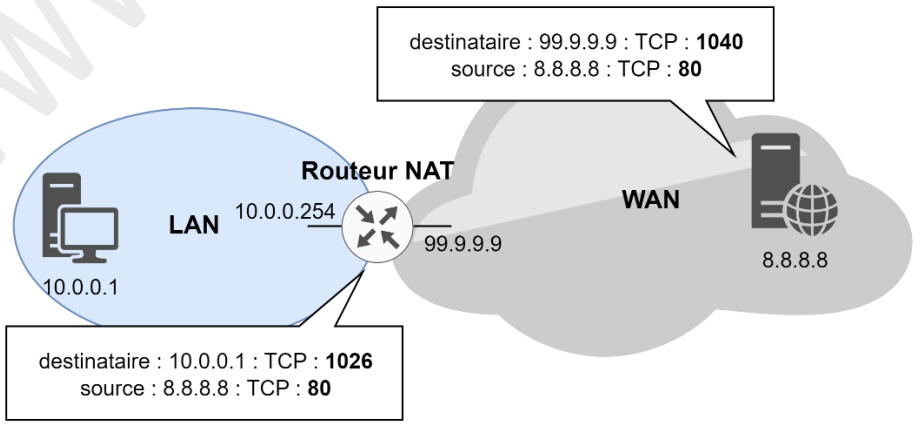
Problème : le 10.0.0.1 est inconnu d'internet (il y a des adresses IP autorisées !!). La trame ne revient donc pas !

Solution : on fait du NAT (*Network Address Translation*) :

99.9.9.9* : adresse IP publique (déclarée pour aller sur Internet)



Envoi de la requête vers le site web 8.8.8.8 – en blanc, ce sont les sockets



Retour de la requête depuis le site web 8.8.8.8 – en blanc, ce sont les sockets

Quelques ports de TCP et UDP :

- http : tcp 80, https : tcp 443
- ftp : tcp 20/21
- telnet : tcp 23
- dns : udp 53

Liste des ports bien connus (wikipedia)

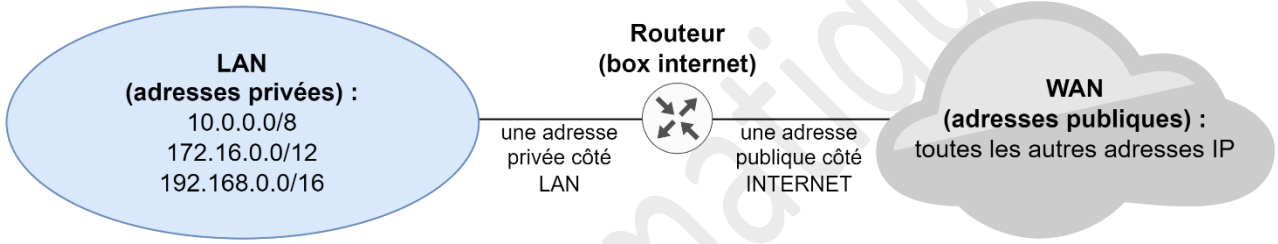
Nota : les ports peuvent aller jusqu'à 65535 :

- de 0 à 1023, ce sont les ports bien connus (exemples plus haut)
- au-delà de 1024, ce sont les ports « aléatoires »

Les plages d'adresses privées :

Certaines plages d'adresses ne se retrouvent pas sur les serveurs internet. On peut donc les utiliser pour des machines voulant se connecter à internet.

Dans le cas où on donnerait une adresse publique à un hôte, il ne pourrait pas contacter le serveur ayant la même adresse IP que lui. Exemple pour 88.8.8.8 qui correspond à 8.red-88-8-8.dynamicip.rima-tde.net (je ne sais pas à quoi ça correspond, c'est juste pour l'exemple). Si notre machine fait partie du même réseau (exemple : 88.8.8.1/24, l'hôte crois que c'est le même réseau et n'envoie donc pas sur le routeur internet. Le site est donc injoignable).



Liste des adresses privées. Le routeur a une adresse privée et une adresse publique

Le CIDR (Classless InterDomain Routing)

Equivalent au Subnetting similaire au VLSM (Very Lenght Subnet Mask)

CIDR : sur internet / VLSM : réseaux locaux

Exemple :

192.168.4.3 – masque 255.255.255.0 → 192.168.4.3/24 nombre de bits à 1 du mask de réseau. /24 correspond à la notation CIDR

Un masque contient d'un côté que des 1, de l'autre côté que des 0 :

Masque 255.255.255.0 = 11111111.11111111.11111111.00000000 (il y a vingt-quatre 1) = /24

Adressage DHCP

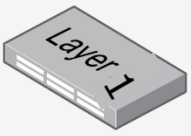
Page wikipedia

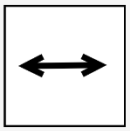
Lorsqu'une machine doit définir une adresse IP automatique, elle essaye de contacter un serveur DHCP pour lui attribuer une adresse IP. Si elle ne trouve pas de serveur DHCP, elle utilise un protocole en fonction du système d'exploitation pour s'auto-attribuer une adresse IP :

- Microsoft utilise APIPA qui est le nom donné par Microsoft au protocole IPV4 LL (IPv4 link layer)
- Unix/Linux utilise AVAHI (qui utilise Zeroconf)
- Coté MacOS le protocole utilisé est BONJOUR

9 Résumé sur les hub, switches et routeurs

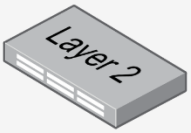
HUB (répéteur / concentrateur)





Il répête le signal réseau
Il n'a pas d'incidence sur l'architecture réseau

Switch (commutateur)



Il sépare les domaines de collision et joue le rôle de pont.
Il peut faire du spanning tree.
Il peut faire du VLAN et répète le signal

Routeur (répartiteur)

Il route l'information
Il sait faire la même chose qu'un HUB et qu'un SWITCH