Réseaux : 4° partie

Un réseau est un ensemble de noeuds reliés entre eux par des liens (canaux). Un réseau informatique est un ensemble d'équipements interconnectés pour échanger des informations.

On appelle noeud (node) l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions (un ordinateur, un routeur, un concentrateur, un commutateur).

Les réseaux informatiques filaires locaux existent depuis le milieu des années 1970 lorsque les universités américaines commencèrent à avoir besoin d'interconnexion entre les ordinateurs présents sur un même site.

Les réseaux informatiques filaires étendus sont apparus dans les années 1970 lorsque les fabricants de matériel informatique IBM et Digital equipment créèrent les architectures SNA et DECnet en conjonction avec le réseau de téléphone d'AT&T qui permit la mise en place de connexions dédiées à moyen débits entre sites distants.

Arpanet (le futur Internet) est le premier réseau à transfert de paquets développé aux États-Unis par la DARPA. Le projet fut lancé en 1969 et la première démonstration officielle date d'octobre 1972.

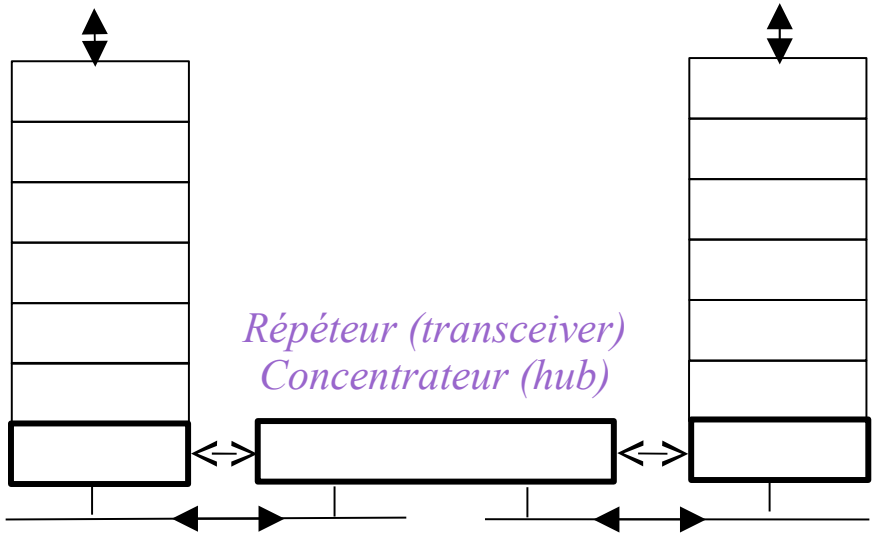
Bibliographie

- "TCP/IP sous Linux" de JF Bouchaudy - Formation Tsoft © Ed. Eyrolles
- "TCP/IP Administration de réseau" de Craig Hunt © Ed. O'Reilly
- "Les protocoles TCP/IP et Internet" d'Eric Lapaille © NetLine 1999
- "Technique des réseaux locaux sous Unix" de L. Toutain © Ed. Hermes
- "Pratique des réseaux locaux d'entreprise" de JL Montagnier © Ed. Eyrolles
- "Transmission et Réseaux" de S. Lohier et D. Present © ED. DUNOD
- Les sites www.frameip.com, fr.wikipedia.org, www.w3.org, etc ...

1. Interconnexion de niveau 1

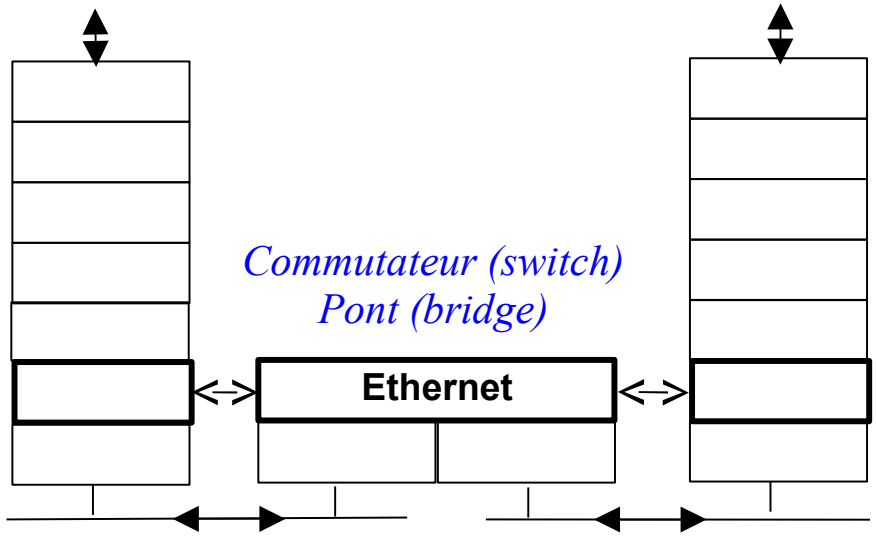
- ***Fonctions** d'un répéteur :*
  - la répétition des bits d'un segment sur l'autre (augmenter la distance)
  - la régération (amplification) du signal pour compenser l'affaiblissement
  - le changement du support physique
- Remarque : la trame n'est jamais modifiée lors de la traversée d'un répéteur.
- Le HUB se comporte comme un répéteur multi-ports. Avec HUB 100Mbps, on obtient un débit partagé de 100Mbps pour l'ensemble des équipements raccordés.

Remarque : dans un réseau Ethernet, une seule des machines connectées peut transmettre à la fois. Dans le cas contraire, une collision se produit, les machines concernées doivent retransmettre leurs trames après avoir attendu un temps calculé aléatoirement par chaque émetteur (méthode d'accès CSMA/CD).

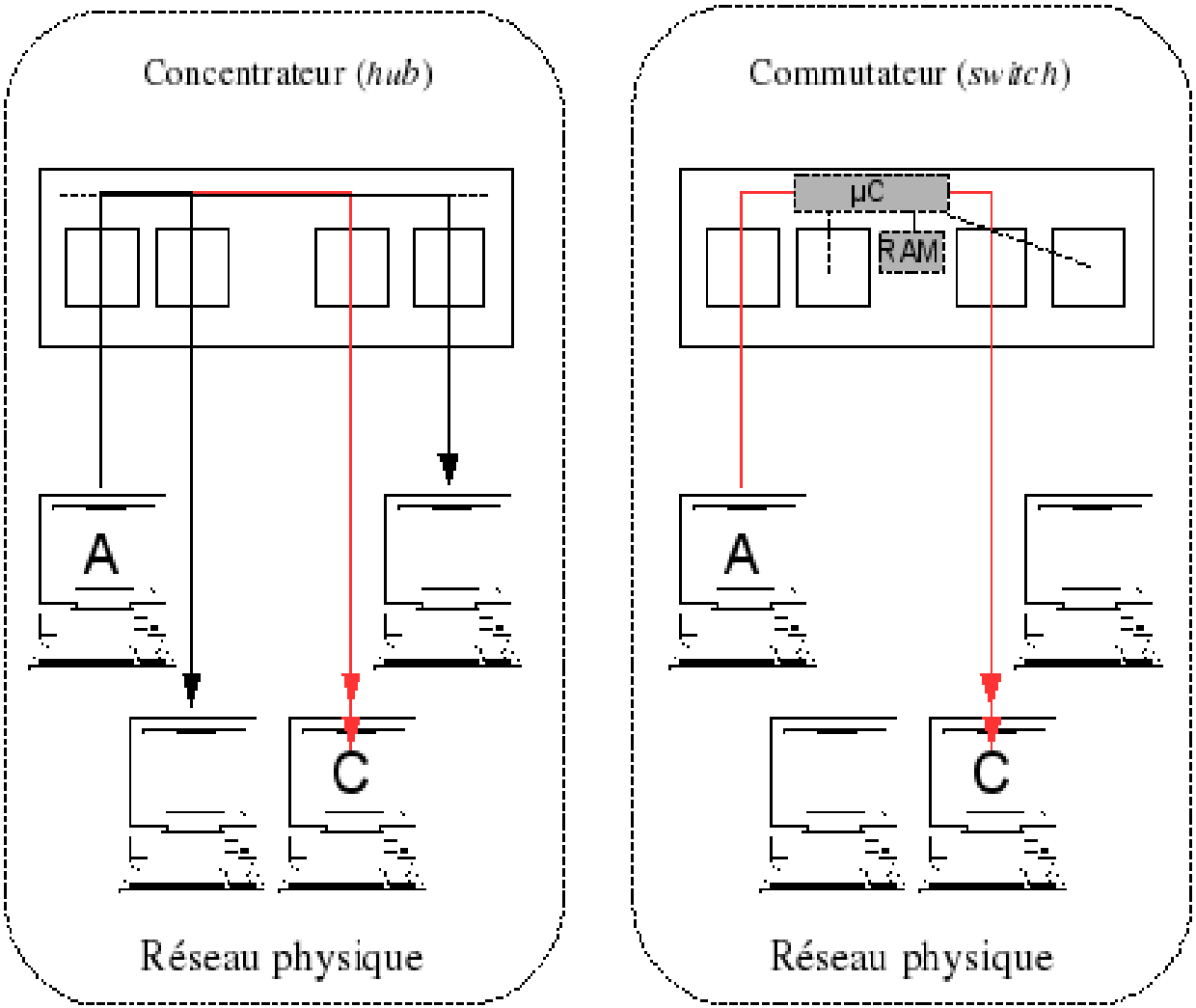


2. Interconnexion de niveau 2

- ***Fonctions** d'un pont ou d'un commutateur :*
  - analyser les trames qui circulent sur chaque segment ;
  - stocker et mettre à jour périodiquement la table de correspondance @ MAC/n°de port (possibilité de gérer des VLAN) ;
  - filtrer les trames en fonction de l'@ MAC du destinataire (segmentation de réseaux physiques)
  - assurer les fonctions d'un répéteur
- Dans le cadre d'un switch 100Mbps, on obtient un débit dédié de 100Mbps par port. Les caractéristiques principales à vérifier pour choisir un switch sont :
  - le nombre d'adresse MAC maximum qui peuvent mise en mémoire
  - le nombre de paquet par seconde (PPS) que la matrice de fond de panier peux commuter
  - manageable ou standard, supervision (SNMP)
- Le pont permet d'interconnecter deux réseaux de couche liaison différente. Par exemple, on trouvera des ponts permettant de relier des réseaux Ethernet et Token Ring.



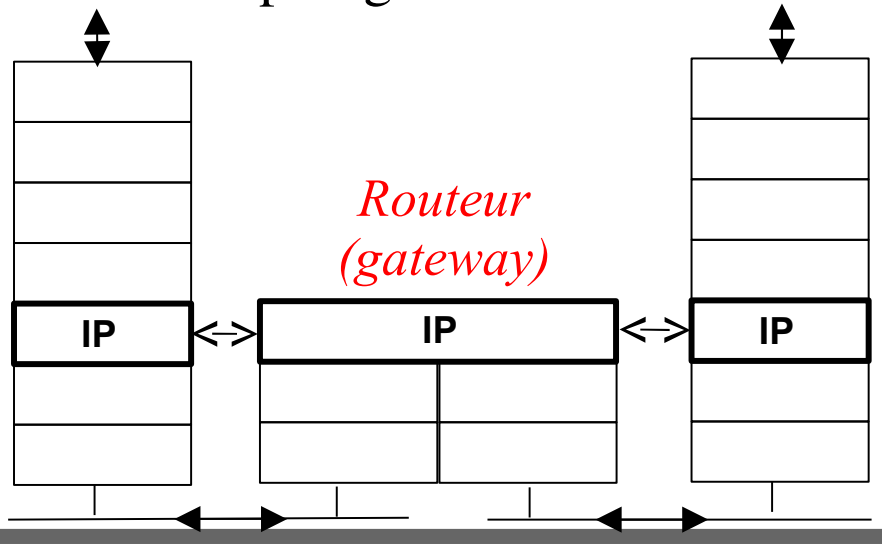
3. Réseau physique



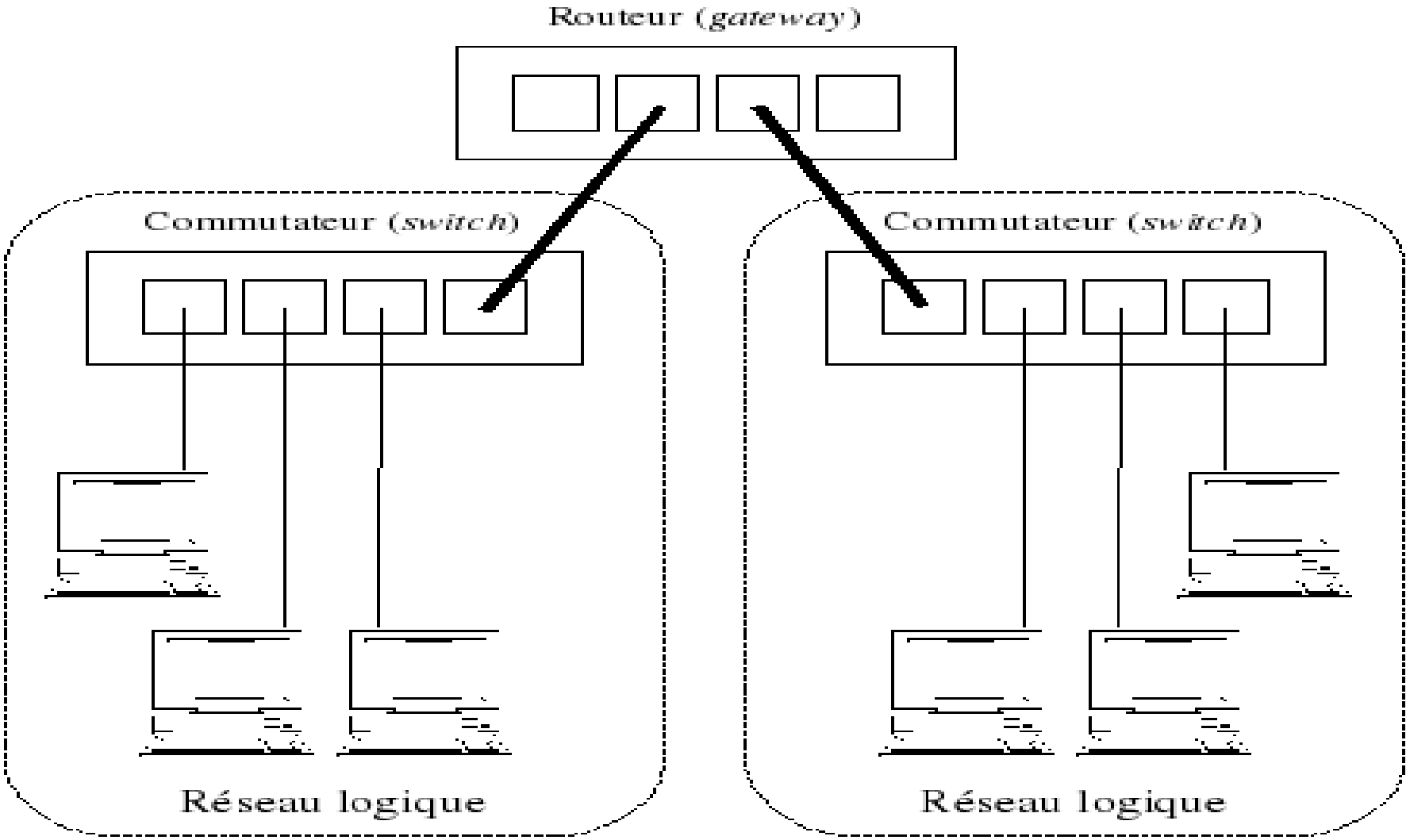
4. Interconnexion de niveau 3

- *Les **fonctions** assurés par le routeur sont :*
  - traiter et **router** les paquets des protocoles de niveau 3 (IP) ;
  - mettre à jour ses tables de routage (routage dynamique) en dialoguant avec d'autres routeurs et en utilisant des protocoles spécifiques (RIP, OSPF, EGP, BGP, …)
  - dialoguer avec d'autres routeurs (protocole ICMP) pour signaler des congestions, synchroniser des horloges, estimer les temps de transit, ...
  - interconnecter toutes les topologies.

Remarque : une adresse IP par interface



5. Réseau logique



6. Synthèse des équipements d'interconnexion

- Une synthèse comparative des différents équipements Ethernet :

	Répéteur	HUB	Switch	Pont	Routeur
Agit sur la couche du modèle OSI	1	1	2	2	3
Permet de relier plusieurs équipements	Non	Oui	Oui	Oui	Oui
Fournit un débit dédié par interface	Non	Non	Oui	Oui	Oui
Sépare les domaine de braodcast niveau 2	Non	Non	Non	Oui	Oui
Sépare les domaine de braodcast niveau 3	Non	Non	Non	Non	Oui

www.frameip.com

7. Routage

- Le routage consiste à **déterminer la route qu'un paquet doit prendre pour atteindre une destination**.

- Cette tâche est réalisée au niveau de la **couche RESEAU** du modèle à couches : dans cette couche, on utilise un adressage qui permet de spécifier à quel réseau appartient un équipement (hôte ou routeur). Les équipement (hôtes ou routeurs) qui se situent sur des réseaux différents devront utiliser les services d'un **routeur** (*gateway* dans la terminologie IP) pour communiquer.

- Les **fonctions** au niveau de la **couche RESEAU** sont :
  - **Acheminer** (hôte ou routeur) : envoyer un paquet vers une destination (hôte ou routeur)
  - **Relayer** (routeur) : acheminer un paquet d'un réseau vers un autre réseau

- Chaque équipement (hôte ou routeur) achemine un paquet en fonction de l'**adresse IP destination** uniquement.

- Pour **déterminer la route** à prendre, le pilote IP utilise sa **table de routage** qui indique pour chaque destination (hôte, réseau ou sous-réseau), la route (interface ou passerelle) à prendre : c'est le routage de proche en proche.

8. Différents types de routage

- On distingue :
  - **Le routage statique** si les routes sont fixées manuellement par l'administrateur réseau
  - **Le routage dynamique** si les tables de routages sont automatiquement mises à jour pour tenir compte d'une modification du réseau global (panne de routeur, nouvelle route, …)
- Il y a deux types de routage :
  - Le routage direct : Délivrance d'un paquet à un hôte qui appartient au même réseau physique
  - Le routage indirect : Délivrance d'un paquet à un hôte qui appartient à un réseau physique différent
- Le routage s'effectue en consultant une table de routage (contenant des routes) et en appliquant un algorithme pour déterminer la route à prendre en fonction de l'adresse destination.
- Les tables de routage doivent être configurées sur l'ensemble des équipements (hôtes et routeurs) :
  - Cas des hôtes : les tables de routages des postes se limitent souvent à une route par défaut vers le routeur (*gateway*, donc souvent passerelle en français) qui permettra de sortir du réseau physique.
  - Cas des routeurs : les tables de routages sont donc configurées principalement au niveau des routeurs manuellement (routage statique) ou automatiquement acquises par dialogue entre routeurs (routage dynamique).

9. Algorithme de routage

- L'algorithme a évolué pour tenir compte l'abandon de la notion de classe. Ceci conduit à utiliser seulement le *netmask* pour déterminer la taille du réseau. On utilise aussi le terme **CIDR** (*Classless InterDomain Routing*).

```
POUR une adresse IP destination
 trouvé ← rechercher dans la table de routage le préfixe
 le plus long (netmask) qui correspond à l'adresse desti
 nation
 SI trouvé
  ALORS  envoyer le paquet
  SINON  renvoyer le message : "Destination unreacheable"
 FSI
FPOUR
```

Remarques : la route par défaut est notée 0.0.0.0, soit un masque de longueur nulle et toutes les adresses destinations correspondront. Les routes vers des hôtes utiliseront un masque de 255.255.255.255 pour obtenir une correspondance exacte.

10. Table de routage

- Une table de routage indique pour chaque destination (hôte, réseau ou sous-réseau) la route (interface ou passerelle) qu'il faut prendre. Les informations pour chaque route sont donc les suivantes :

Aller vers	*Passer par*
la destination (hôte ou réseau)	**la route**
Champs: Destination et Genmask	*Champs:* Passerelle et Iface

- Pour afficher une table de routage, on utilise les commandes **`nestat`** ou **`route`**. Il existe de nombreux champs supplémentaires dont :
  - Le champ Indic (*Flags*) qui indique si :
    - U (*Up*) : la route est active
    - H (*Host*) : la route conduit à un hôte
    - G (*Gateway*) : la route passe par une passerelle (voisine)
  - Le champ Métrique (*Metric*) indique la distance, en nombre de passerelles, pour atteindre la destination

11. Routage statique et dynamique

- Le routage statique, utilisé dans les réseaux de petite taille, est réalisé manuellement par l'administrateur réseau. On l'utilise notamment pour : les postes de travail (route par défaut) ou pour un routeur avec une route par défaut vers le Fournisseur d'Accès Internet (ou ISP: *Internet Service Provider*)

Avantages	***Inconvénients***
Utilisation de fichiers de configuration donc stabilité de la configuration	Si le réseau comporte de nombreux routeurs : - tâche fastidieuse - risque d'erreur important
	Impossibilité pour gérer les routes redondantes

- Le routage dynamique est assuré par les routeurs eux-même en s'échangeant des informations sur leurs tables de routage et nécessite un protocole de routage

Avantages	***Inconvénients***
Simplicité de la configuration	Dépend du protocole de routage utilisé et de la taille du réseau : - consommation de la bande passante - temps de convergence - sécurité
Adaptabilité à l'évolution du réseau	
Optimisation (sélection des meilleurs routes)	
Elimination des boucles de routage	

12. Protocoles de routage

- Il faut distinguer deux types de domaine de routage :
  - **IGP** (*Interior Gateway Protocol*) : protocole de routage interne utilisé au sein d'une même unité administrative (AS) ;
  - **EGP** (*Exterior Gateway Protocol*) : protocole de routage externe utilisé entre passerelles appartenant à des unités administratives différentes (AS)

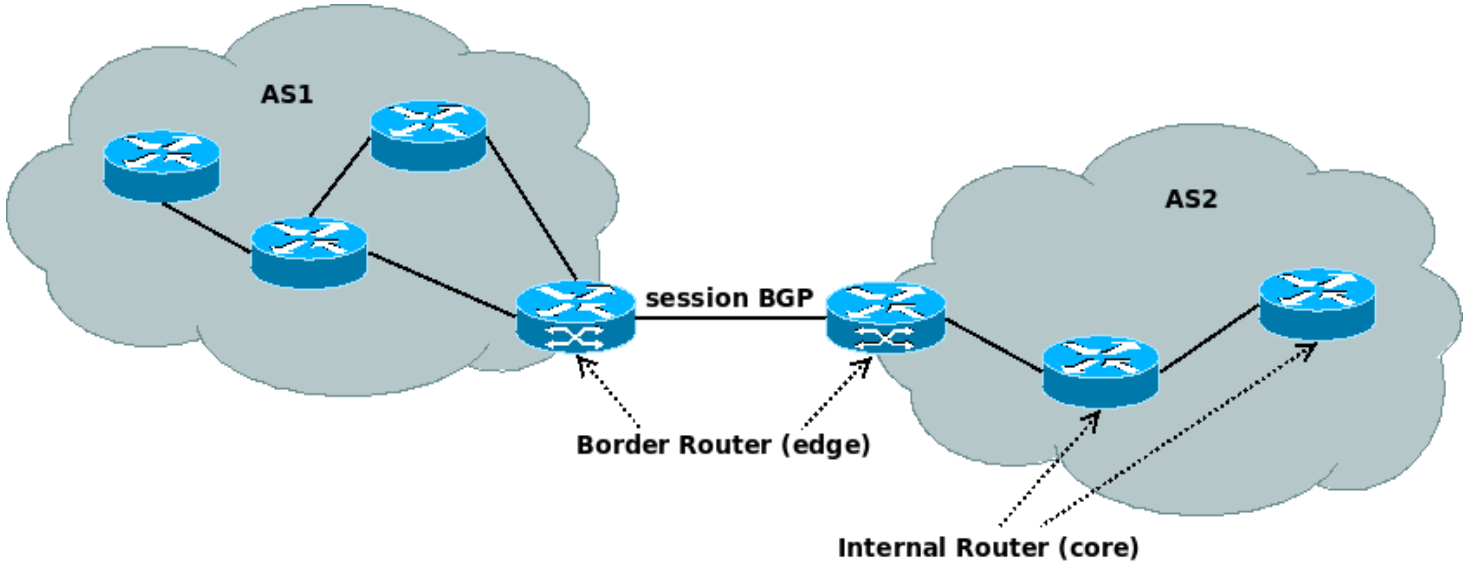
	Internet	***ISO***
Routage intra-domaines IGP Taille < 100 routeurs	On distingue deux types de protocoles : **- distance vecteur** (*distant vector*) : RIP (*Routing Information Protocol*), IGRP (*Internet Gateway Routing Protocol*) de la société CISCO (le protocole a été amélioré sous le nom EIGRP) **- état de liens** (*link state*) : OSPF (*Open Shortest Path First*)	IS-IS (*Intermediate System to Intermediate System*)
Routage inter-domaines EGP Taille = Internet	EGP (*Exterior Gateway Protocol*) : obsolète, remplacé par BGP (*Border Gateway Protocol*)	IDRP (*Inter Domain Routing Protocol*)
Entre équipement et routeur	ICMP *Redirect*	IS-ES

13. Réseaux autonomes (AS)

- Internet est un ensemble de réseaux autonomes (AS) qui sont reliés entre eux. Ces réseaux autonomes (AS) sont, par exemple, des Fournisseurs d'Accès Internet (Free, Wanadoo, ...) des hébergeurs (OVH, ...) ou fournisseurs de services (Google, ...), de grands réseaux Internet (Renater, ...) ou des opérateurs de télécommunication (France Telecom, Cegetel, Completel, ...).
- Sur Internet, un Système Autonome (Autonomous System ou AS) est un ensemble de réseaux IP sous le contrôle d'une seule et même entité, typiquement un fournisseur d'accès à Internet ou une plus grande organisation qui possède des connexions redondantes avec le reste du réseau Internet. La notion de système autonome est donc administrative et non technique.
- Au sein d'un système autonome, le protocole de routage est qualifié d'interne (par exemple, OSPF). Entre deux systèmes autonomes, le routage est externe (par exemple BGP).
- Chaque AS est identifié par un entier de 16 bits (passé récemment à 32 bits, avec le RFC 4893) qui est utilisé par le protocole de routage Border Gateway Protocol qui forme notamment le cœur du réseau Internet.

14. BGP (Border Gateway Protocol)

- BGP (Border Gateway Protocol) est un protocole d'échange de route utilisé notamment sur le réseau Internet. Son objectif est d'échanger des informations d'accessibilité de réseaux (appelés préfixes) entre routeurs.
- BGP est principalement utilisé entre les opérateurs et fournisseurs d'accès à Internet pour l'échange de routes entre Autonomous Systems (AS).
- Les connexions entre deux voisins BGP (neighbours ou peers) sont configurées manuellement entre deux routeurs (border routeur ou edge).



15. Interconnexion d'opérateurs

- On distingue donc deux types de raccordement entre opérateurs :
- le transit : il permet l'échange de données entre deux opérateurs, via le réseau d'un opérateur tiers. Il n'y a pas de connexion directe possible entre les réseaux des deux fournisseurs de services qui, pour échanger leur données, doivent passer par le réseau d'un troisième opérateur. Dans ce cas, le transport est le plus souvent facturé par l'opérateur tiers.

- l'échange entre pairs (peering) : c'est une alternative au transit et il permet à des opérateurs ou aux différents fournisseurs d'accès Internet (ou FAI ou ISP) d'échanger du trafic Internet entre leurs réseaux de systèmes autonomes grâce à des accords mutuels dits de «peering». Le peering est souvent gratuit : on est dans une configuration d'égal à égal, souvent utilisée par des réseaux de tailles comparables.

16. Pare-feu (*firewall*)

- Un système pare-feu (*firewall*) est un dispositif conçu pour examiner et éventuellement bloquer les échanges de données entre réseaux. C'est donc un élément de sécurité.
- Le pare-feu joue le rôle de filtre et peut donc intervenir à plusieurs niveaux du modèle DoD ou OSI (analyse des en-têtes des protocoles).
- Il existe trois types principaux de pare-feu :
  - filtrage de paquets : adresse source et destination, protocole et numéro de ports
  - filtrage de paquets avec état (*firewall stateful*) : assure un suivi de session et de connexion
  - proxy : jusqu'à la couche application

- Les fabricants de pare-feu ont tendance à intégrer un maximum de fonctionnalités :
  - filtrage de contenu (URL, *spam* mails, code ActiveX, applets Java, …), réseau virtuel privé (VPN), détection d'intrusions (IDS), tolérance de pannes (haute disponibilité, équilibrage de charge, NAT, ...

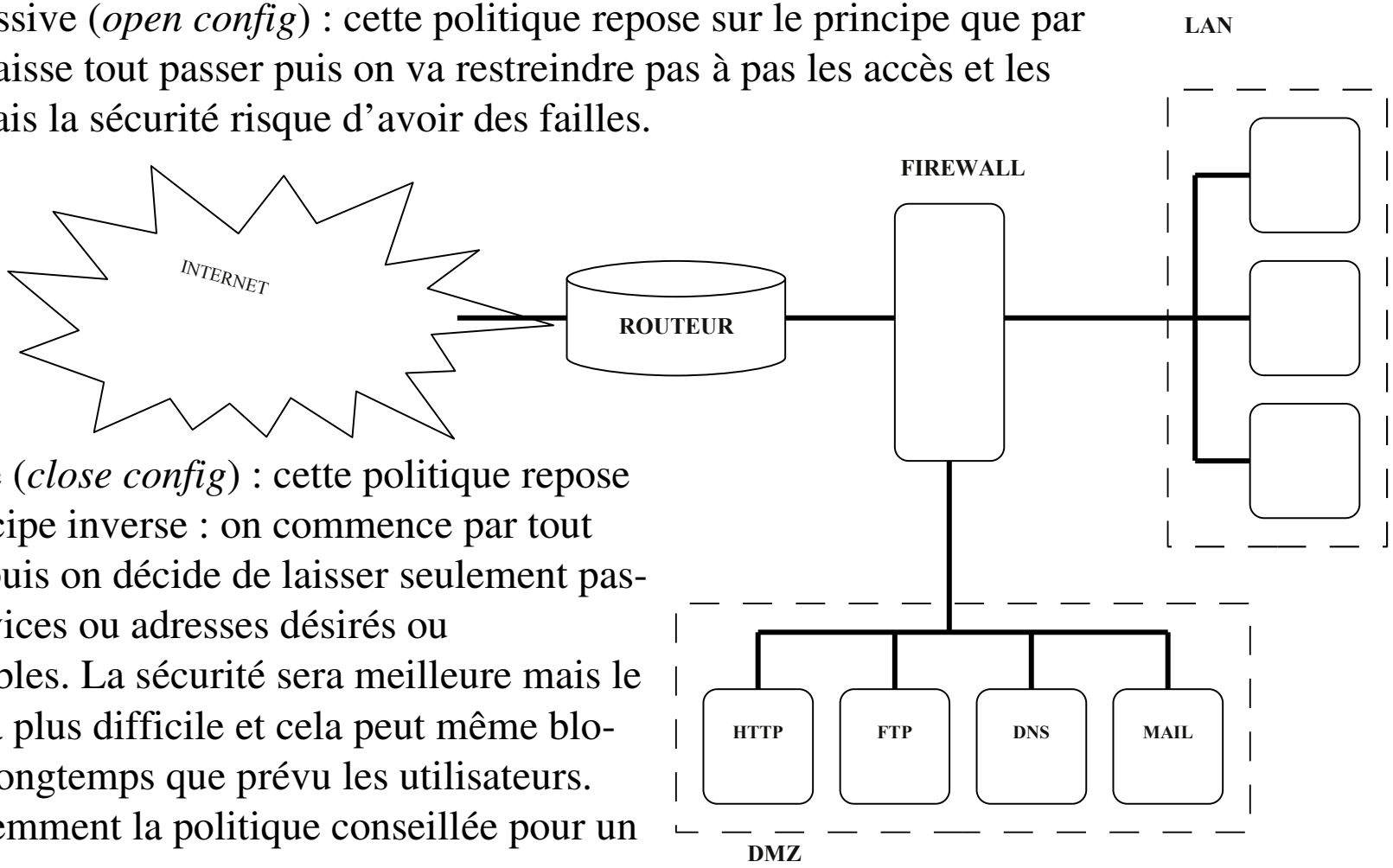
17. DMZ (*De-Militarized Zone*)

- Il existe plusieurs **zones de sécurité** commune aux réseaux. Ces zones déterminent un niveau de sécurité en fonction des accès réseaux et donnent les bases de l'architecture.

- On considère en général trois zones ou réseaux :
  - Réseaux externes : c'est le réseau généralement le plus ouvert. L'entreprise n'a pas ou très peu de contrôle sur les informations, les systèmes et les équipements qui se trouvent dans ce domaine.
  - Réseaux internes : les éléments de ce réseau doivent être sérieusement protégés. C'est souvent dans cette zone que l'on trouve les mesures de sécurité les plus restrictives et c'est donc le réseau le moins ouvert.
  - Réseaux intermédiaires : cette zone est un compromis entre les deux précédentes. Ce réseau est composé de services fournis aux réseaux internes et externes. Les services publiquement accessibles (serveurs de messagerie, Web, FTP et DNS le plus souvent) sont destinés aux utilisateurs internes et aux utilisateurs par Internet. Cette zone, appelée **réseau de service** ou de **zone démilitarisée** (**DMZ** *De-Militarized Zone*), est considérée comme la zone moins protégée de tout le réseau de l'entreprise.

18. Politique de sécurité

- Politique de sécurité
  - Politique permissive (*open config*) : cette politique repose sur le principe que par défaut on laisse tout passer puis on va restreindre pas à pas les accès et les services mais la sécurité risque d'avoir des failles.



  - Politique stricte (*close config*) : cette politique repose sur le principe inverse : on commence par tout interdire, puis on décide de laisser seulement passer les services ou adresses désirés ou indispensables. La sécurité sera meilleure mais le travail sera plus difficile et cela peut même bloquer plus longtemps que prévu les utilisateurs. C'est évidemment la politique conseillée pour un pare-feu.

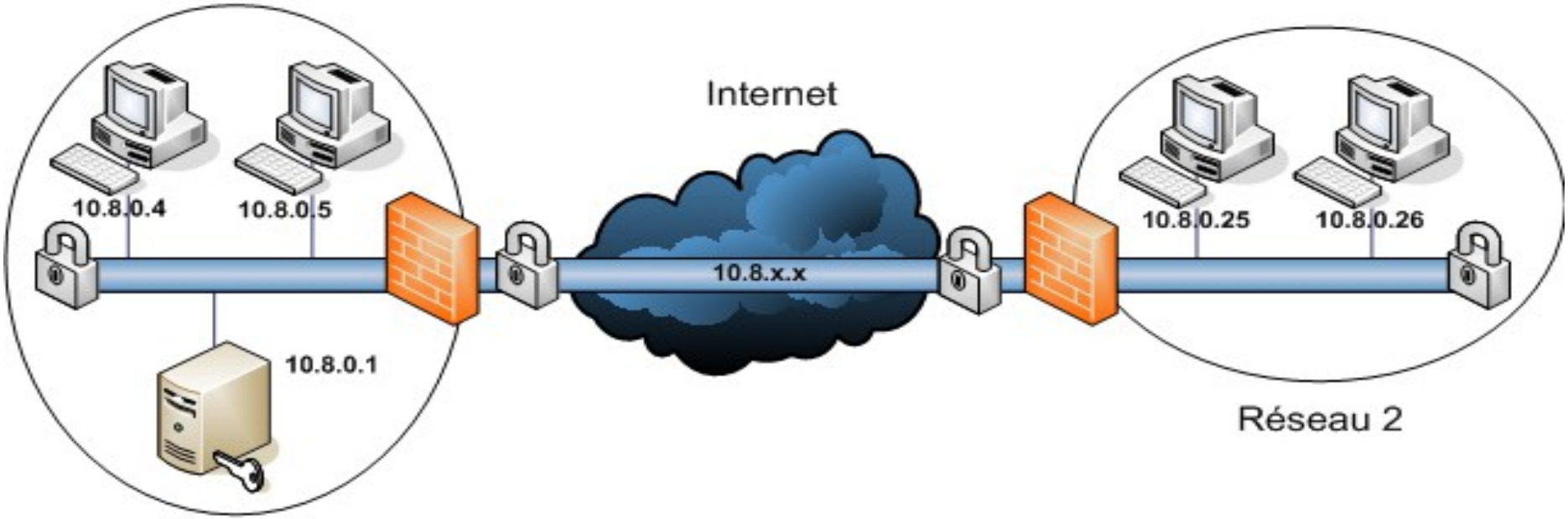
19. Serveur mandataire (*proxy*)

- Un serveur mandataire ou *proxy* est un serveur qui a pour fonction de relayer des requêtes entre un poste client et un serveur d'application.

- Les serveurs proxy sont notamment utilisés pour assurer les fonctions suivantes :
  - mémoire cache (amélioration des performances)
  - la journalisation des requêtes (« logging »)
  - la sécurité du réseau local
  - le filtrage et l'anonymat
  - l'authentification pour autoriser ou non l'accès au service

20. Réseau privé virtuel

- Le réseau privé virtuel VPN (*Virtual Private Network*) est vu comme une extension des réseaux locaux et préserve la sécurité que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel » (*tunneling*), c'est-à-dire en encapsulant les données à transmettre de façon chiffrée. Les principaux protocoles de tunnelisation sont : L2TP, IPsec et aussi SSH.



21. RFC

- Les *Requests For Comment* (RFC), littéralement demande de commentaires, sont une série numérotée de documents électroniques documentant les aspects techniques d'Internet.
- Peu de RFC sont des standards, mais tous les standards d'Internet sont des RFC.
- Les RFC sont rédigées pas des experts techniques. En mai 2008, le nombre de RFC a atteint les 5 000.
- La première RFC (RFC 1), titrée "Logiciel hôte", a été publiée le 7 avril 1969 par Steve Crocker.

22. Terminologie Internet

- Une passerelle (*gateway*) est un dispositif permettant de relier deux réseaux informatiques, comme par exemple un réseau local et Internet. Cependant, le terme passerelle (sans autre précision) est couramment employé comme exact synonyme du terme routeur. Par exemple, on parle de passerelle par défaut (*default gateway*) ou ***gateway IP*** pour désigner un routeur qui interconnecte deux réseaux IP. Le routeur est un équipement réseau qui permet de relayer les paquets d'un réseau vers un autre.
- **Internet** est le réseau informatique mondial qui rend accessibles au public des services (comme le courrier électronique et le World Wide Web). Ses utilisateurs sont désignés par le néologisme « **internaute** ». Techniquement, Internet se définit comme le réseau public mondial utilisant le protocole de communication « TCP/IP » (au sens les protocoles de la famille TCP/IP).
- Lorsque les technologies Internet (TCP/IP, services, etc.) sont mises en oeuvre au sein de réseaux privés (entreprises, administrations, etc ...), on parle alors d'**intranet**.

23. Découpage fonctionnel

- Un réseau peut être classé en fonction de son utilisation et des services qu'il offre. Ainsi, pour les réseaux utilisant les protocoles **TCP/IP**, la nomenclature est la suivante :
  - Intranet : le réseau interne d'une entité organisationnelle
  - Extranet : le réseau externe d'une entité organisationnelle
  - Internet : le réseau des réseaux interconnectés à l'échelle de la planète

24. ICANN

- ICANN (Internet Corporation for Assigned Names and Numbers) est une organisation internationale sans but lucratif dont le rôle premier est d'allouer l'espace des adresses de protocole Internet (IP), d'attribuer les identificateurs de protocole, de gérer le système de nom de domaine de premier niveau pour les codes génériques (gTLD) et les codes nationaux (ccTLD), et d'assurer les fonctions de gestion du système de serveurs DNS racines.

- C'est une autorité de régulation de l'Internet.

25. IANA (Internet Assigned Numbers Authority)

- IANA (Internet Assigned Numbers Authority) est une organisation dont le rôle est la gestion de l'espace d'adressage IP d'Internet, et des autres ressources partagées sur Internet. Depuis 1998, elle est une composante de l'ICANN, l'autorité suprême de régulation de l'Internet. De manière générale, les ressources à gérer "mondialement" au niveau d'Internet sont :

  - Noms de domaine : l'IANA gère la zone racine du DNS (assignations de domaines de premier niveau) ainsi que les délégations dans les zones .int et .arpa.
  - Numéros d'AS : l'IANA assigne des blocs de AS aux RIR (Registres Internet Régionaux).
  - Adresses IP : l'IANA a découpé l'espace d'adressage IPv4 en 256 blocs (/8). Chacun de ces blocs est libre, réservé, assigné dans le passé ou alloué à un RIR (Registre Internet Régional). Pour IPv6, l'IANA assigne des blocs de taille /12 à 13 aux RIR.
  - Numéros de protocoles et de port : l'IANA gère également les numéros de protocoles de nombreux protocoles différents sur IP. L'IANA publie notamment la liste des numéros de ports TCP et UDP.

26. RIR et LIR

- Un RIR (Regional Internet Registry) est un organisme qui alloue les blocs d'adresses IP (adressage IPv4, IPv6) et des numéros d'Autonomous System dans sa zone géographique. Il existe aujourd'hui cinq RIR :
  - RIPE-NCC (Réseaux IP Européens) pour l'Europe et le Moyen-Orient ;
  - ARIN (American Registry for Internet Numbers) pour l'Amérique du Nord ;
  - APNIC (Asia Pacific Network Information Center) pour l'Asie et le Pacifique ;
  - LACNIC (Latin American and Caribbean IP address Regional Registry) pour l'Amérique latine et les îles des Caraïbes ;
  - AfriNIC (African Network Information Center) pour l'Afrique

- Un LIR (Local Internet Registry) est un organisme qui a reçu une allocation d'adresse IP d'un registre Internet régional (RIR) en vue d'assigner ces adresses à des tiers (en général, ses clients) ou pour ses besoins propres. Un LIR est généralement un fournisseur d'accès à Internet.