UE 28
Architecture réseau

Mathieu BLANC

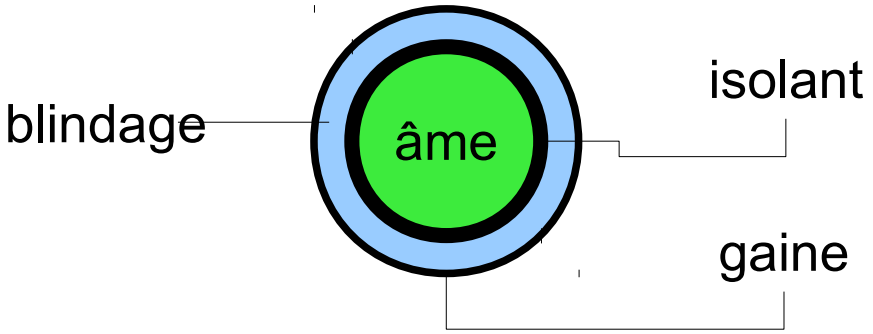
Architecture réseau

Composants réseau et utilisation courante

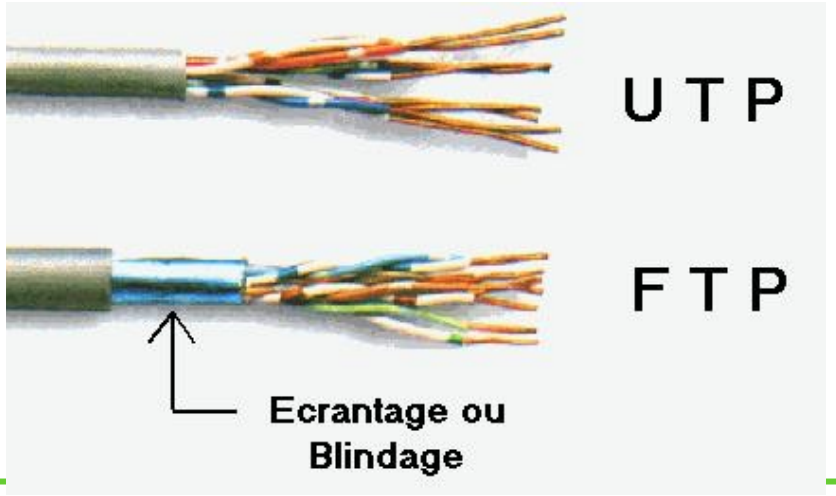
Architecture réseau

- **Câblage**
- **Interconnexion de niveau 2**
  - Répartiteurs
  - Commutateurs
  - Topologies physiques
- **Réseaux IP**
  - Routeurs
  - Adressage
  - DHCP
  - Architectures logiques
- **Commutateurs avancés**
  - VLANs
  - Sécurité du niveau 2

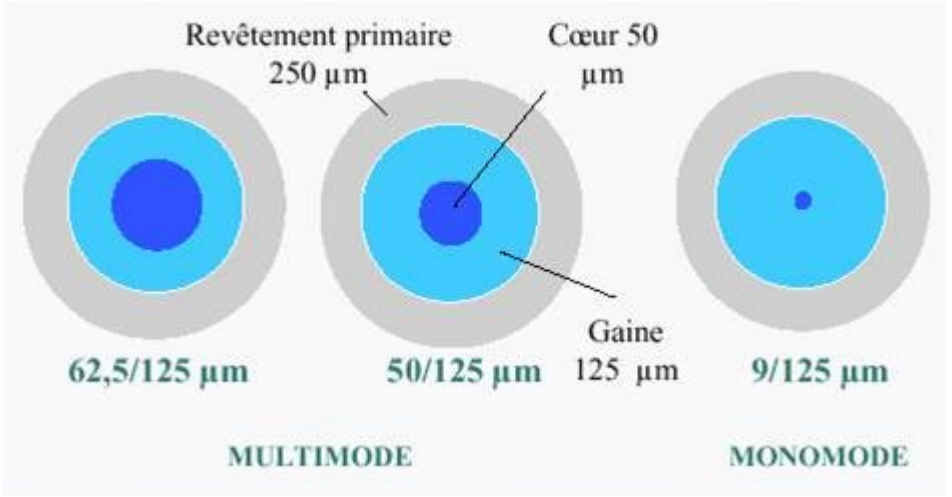
- **Câble coaxial**
  - âme
    - brin(s) de cuivre transportant les données
  - isolant
    - empêche toute interaction électrique néfaste
  - blindage
    - protège des parasites
  - gaine
    - protège de l'environnement exterieur



- **Paires torsadées :**
  - 3 types
    - STP (*Shielded Twisted Pair*) : blindage pour chaque paire de fil
    - S/STP (*Screened Shielded Twisted Pair*) : blindage autour de chaque paire *et* autour du cable
    - S/UTP (*Screened Unshielded Twisted Pair*) : aussi appelé FTP (Foiled Twisted Pair), blindage uniquement autour du cable
  - entrelacement de brins de cuivre
  - restrictions sur la longueur du câble : environ 100m
  - câbles réseau classiques, avec connecteurs RJ45
  - Ethernet : 4 paires torsadées, 8 fils



- **Fibre optique**
  - principalement utilisée au niveau des *backbones*
  - performante mais chère
    - peu de problèmes d'atténuation ou de dégradation du signal
    - gère les très hauts débits
  - Plusieurs modes
    - Rapport entre taille de la gaine et taille du coeur
    - Conditionne l'angle d'introduction de la lumière dans la fibre
    - Multimode : coeur très large, fréquences basses, courte portée
    - Monomode : coeur étroit, fréquences hautes, longue portée



Matériel réseau

- **Un réseau informatique repose sur des équipements d'infrastructure spécialisés dans des traitements spécifiques des flux réseau.**

- **Ces équipements sont :**
  - le plus souvent spécialisés dans le traitement d'une couche OSI
  - optimisés au niveau hardware pour leur fonction
  - dotés d'un OS spécifique, souvent minimal

- **L'interconnexion de ces équipements et des différentes autres composantes du réseau varie :**
  - câble classique (cuivre)
  - fibre optique

Répartiteur (*hub*)

- **Le répartiteur intervient au niveau 1 du modèle OSI : couche physique.**
- **Le répartiteur possède un nombre variable de ports, et répercute sur chacun le signal qu'il reçoit sur un port donné : cela permet de diffuser un même signal (une même trame) vers différentes machines rattachées aux différents ports.**
- **Un répartiteur ne possède pas d'implémentation d'une quelconque pile protocolaire, son action est purement électrique : il n'y aucune intelligence, aucun système d'exploitation interne.**
- **Ce type d'équipement se raréfie sur les réseaux d'entreprise**
  - Coût identique aux commutateurs
  - Performances mauvaises (division de la bande passante)
  - Problèmes de sécurité : possibilité d'épier le trafic facilement...

Commutateur *(switch) 1*

- **Le commutateur intervient au niveau 2 du modèle OSI : couche lien.**
- **Le commutateur possède également un nombre de ports variable. Son rôle consiste à envoyer les trames reçues sur un port vers le ou les équipement(s) destinataire(s), et uniquement celui-là, ou ceux-là. Il réalise cela en diffusant la trame reçue sur les ports adéquats.**
  - Broadcast/Unicast
- **Le commutateur détermine derrière quel port se trouve un équipement grâce à des tables qui peuvent être construites :**
  - dynamiquement
  - par une configuration statique
- **Le commutateur comprend donc le protocole de niveau 2 (typiquement Ethernet) qu'il gère.**

Commutateur *(switch) 2*

- **Généralement, un commutateur possède une série de ports à débit donné, et un port à débit plus important : l'*uplink*, qui remonte vers le *backbone* du réseau.**

- **Un commutateur peut proposer des fonctionnalités avancées selon le constructeur, l'OS :**
  - types d'administration (telnet, ssh, web, snmp)
    - cela se fait sur un port d'administration auquel est donc attribué une adresse, et non sur un port classique
  - fonctionnalités de sécurité (blocage de ports)
  - copie de port : possibilité de recopier le trafic passant par un port sur un autre port, pour des raisons de debug ou de sécurité

- **Ces équipements sont très courants sur les réseaux d'entreprise, la baisse des coûts a notamment favorisé leur utilisation au détriment des répartiteurs.**

Commutateur *(switch) 3*

- **Les cartes réseau sont connectés en *full duplex* : les communications entrantes et sortantes se font de façon indépendante.**
  - Cas des hubs : *half duplex*
  - Le canal qui relie une carte réseau au switch est dédié
  - Parfois les constructeurs jouent sur l'aspect full duplex : par exemple, annonce d'un débit max de 200 Mb/s pour un switch Fast Ethernet (en fait 100Mb/s dans chaque sens de communication)

- **Les performances sont bien meilleures : pas de division de la bande passante entre les ports**
  - Sauf si plusieurs ports sont répliqués sur un seul (trunking), on a alors une limitation à la bande passante disponible sur le port de trunk

Point d'accès WiFi *(access point)*

- **Le point d'accès WiFi intervient au niveau radio.**
- **Il s'agit d'un équipement gérant le protocole 802.11, configuré pour fonctionner en mode infrastructure (par opposition au mode ad hoc) et plus précisément fonctionnant comme maître. Les clients WiFi viennent ensuite s'y associer.**
- **Bien que l'essentiel des fonctions faisant la particularité de cet équipement se situent sur les couches basses du système OSI, il intègre le plus souvent des fonctionnalités de commutateur ou de pont (*bridge*), et éventuellement de routage.**
  - Pont : commutation de paquets entre différentes interfaces réseau séparées
- **On peut également trouver sur ces équipements des fonctionnalités telles que :**
  - serveur DHCP
  - serveur de nom (relais)
  - mécanismes de filtrage réseau

Autres équipements

- **Répéteur**
  - sur de trop grandes distances de câble, le signal a tendance à s'affaiblir : le répéteur sert à corriger cet affaiblissement.
  - le répéteur fonctionne au niveau 1 du modèle OSI : couche physique.

- **Pont (*bridge*)**
  - le pont fonctionne au niveau 2 du modèle OSI : couche lien.
  - le pont est comparable à un commutateur à 2 ports : il permet aux trames d'être transmises d'un brin réseau à un autre en se basant sur les adresses physiques, les 2 brins appartenant au même réseau.
  - il est principalement intéressant lorsque la couche physique diffère.
  - on trouve ce principe implémenté dans nombre de points d'accès pour permettre aux clients sans fils d'accéder au réseau filaire.

Topologies physiques 1

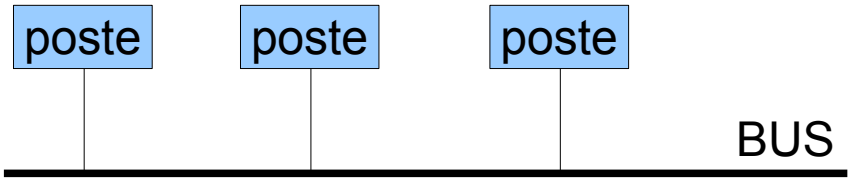
- **On distingue 5 types de topologie réseau physique**
  - en bus
  - en étoile
  - en anneau
  - en arbre
  - maillée

- **Ces topologies sont étroitement liées au type d'équipement utilisé pour relier les machines et aux protocoles des couches basses associés.**

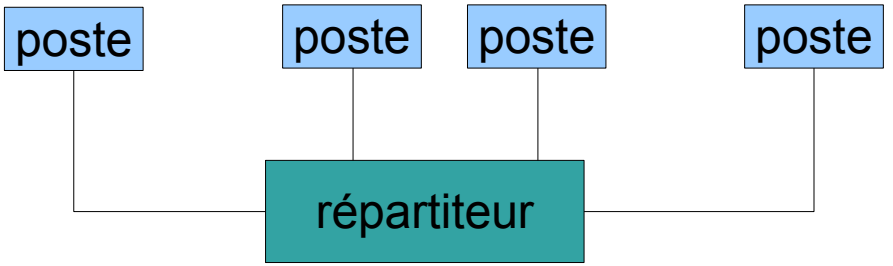
- **Les 3 premières peuvent être considérées comme obsolètes.**

Topologies physiques 2

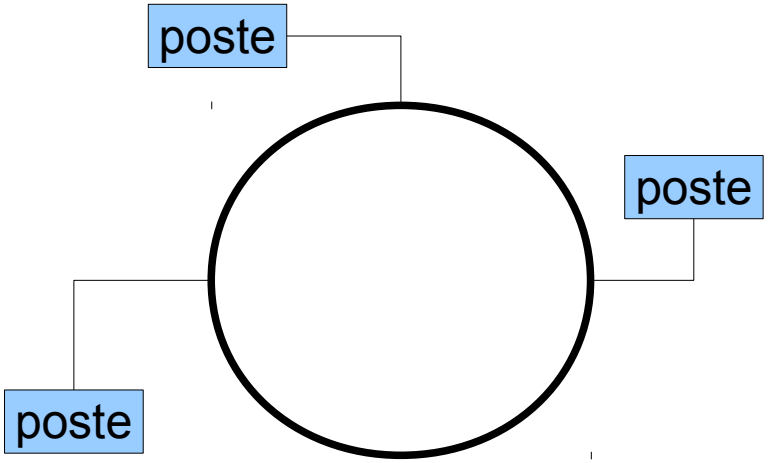
- **Topologie en Bus**



- **Topologie en étoile**

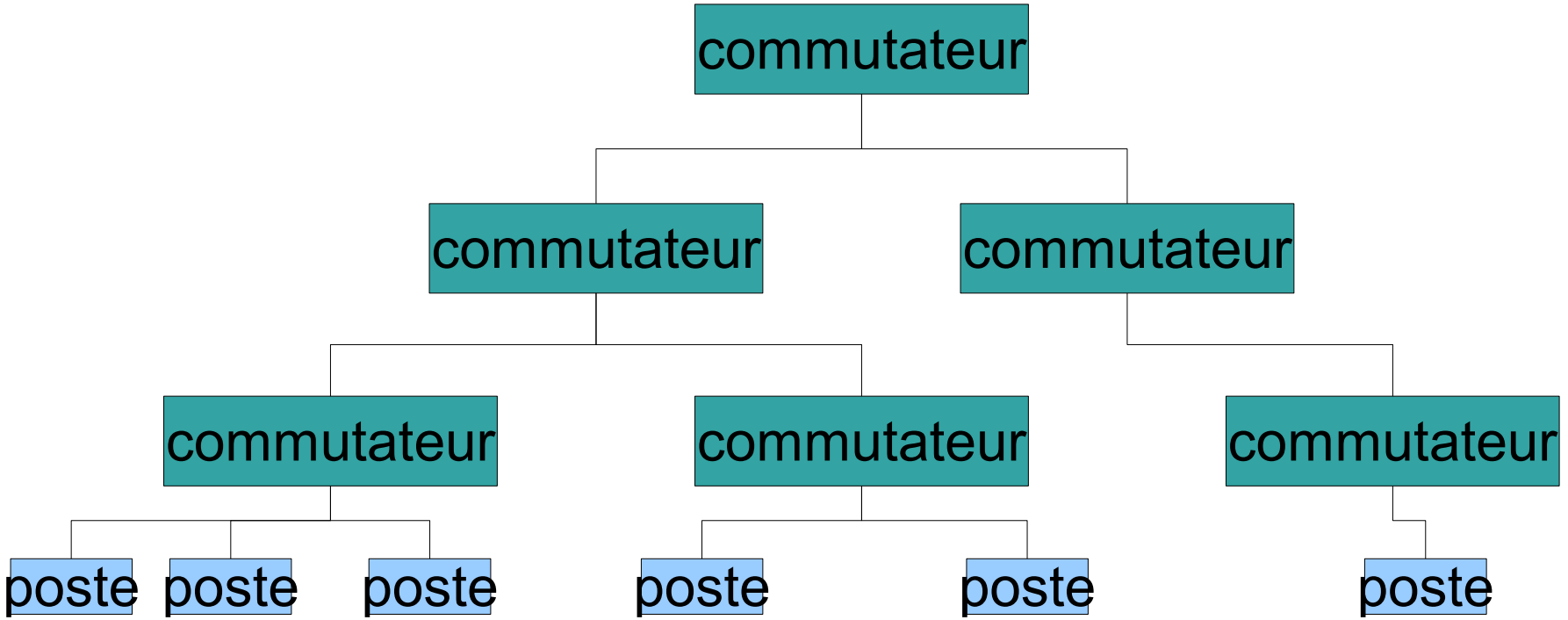


- **Topologie en anneau**
  - associée au *Token Ring*



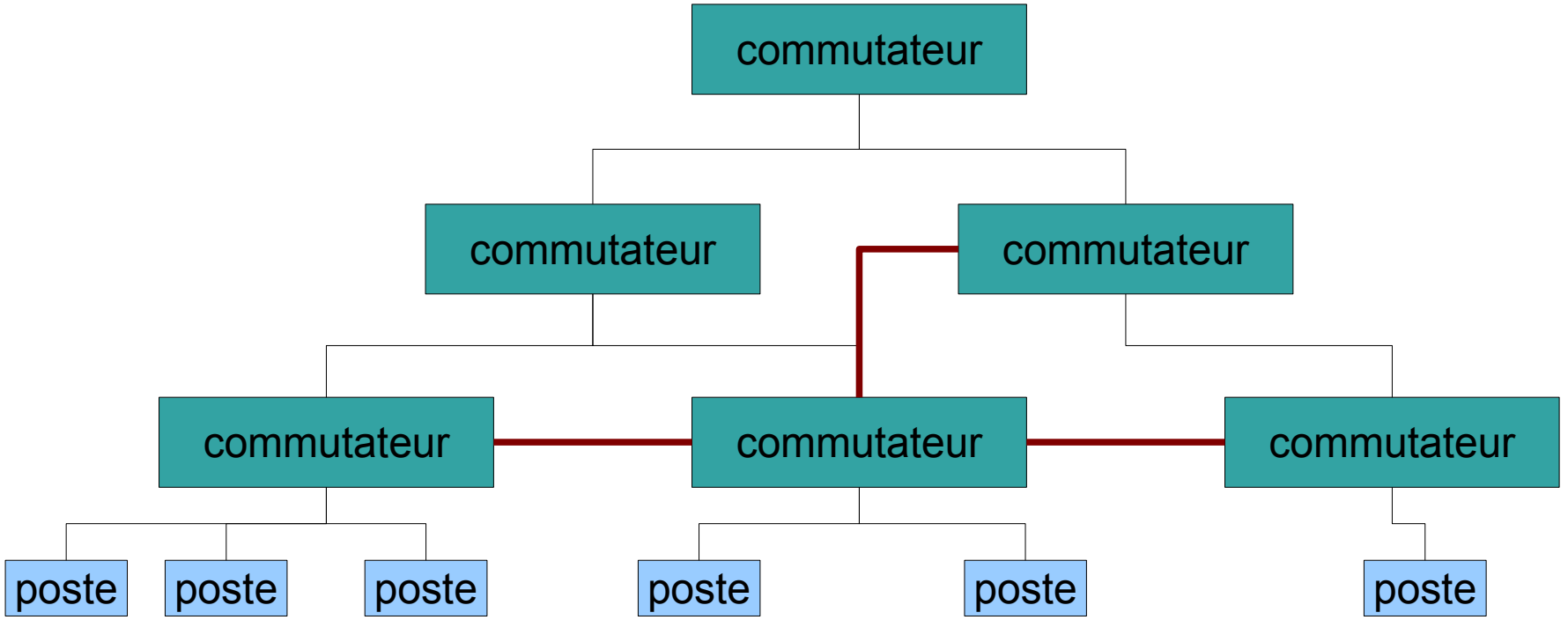
Topologies physiques 3

- **Topologie en arbre**
  - basée sur une arborescence de commutateurs
  - topologie la plus couramment rencontrée
  - classique sur les réseaux Ethernet



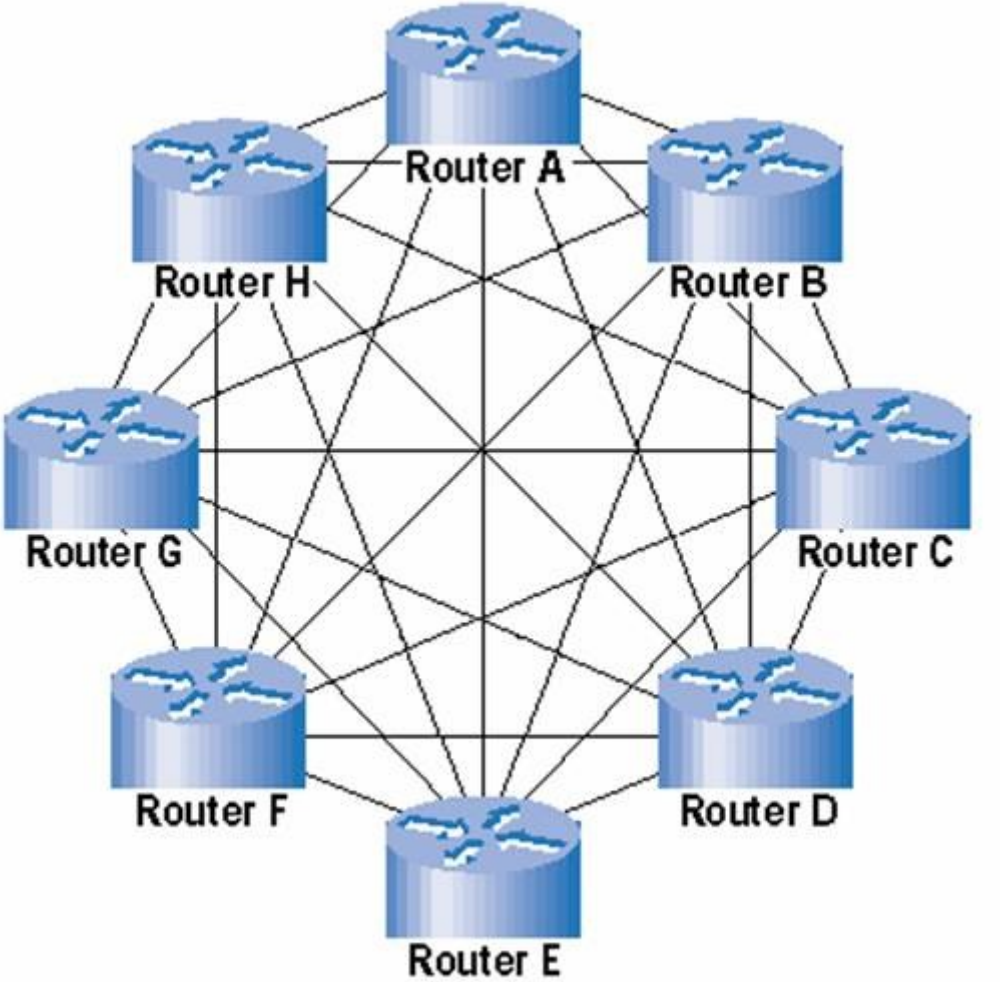
Topologies physiques 4

- **Topologie maillée**
  - reprend le principe de la topologie en arbre
  - mais des liens supplémentaires assurent une redondance



Topologies physiques 4

- **Topologie maillée : full mesh**
  - Chaque équipement est relié à tous les autres



Routeur 1

- **Le routeur intervient au niveau 3 du modèle OSI : couche réseau.**
- **Le routeur possède un nombre de ports variable. Ces ports sont en réalité des interfaces configurées avec des adresses de niveau 2 (MAC) et 3 (IP).**
- **Le routeur achemine les paquets IP qu'il reçoit vers leurs adresses de destination, en transmettant le paquet sur l'interface correspondante.**
- **Cette interface peut être déterminée**
  - statiquement
  - par des protocoles de routage dynamique

Routeur 2

- **Le paquet n'est pas transmis tel quel, il est modifié pour respecter les RFC, notamment :**
  - les adresses ethernet sont modifiées
  - le champ TTL (*time to live*) IP est décrémenté (s'il vaut 0, le paquet n'est pas transmis)

- **On retrouve la notion d'*uplink* au niveau du routeur.**

- **En fonction du constructeur, de l'OS, du modèle, différentes fonctionnalités sont disponibles :**
  - type d'administration (telnet, ssh, web, snmp, ftp, tftp...)
  - filtrage réseau (ACL : *Acces Control Lists*)
  - gestion d'IPsec

- **La fonction de routage simple peut cependant être assurée par d'autres types d'équipements à vocation de sécurité comme un pare-feu par exemple.**

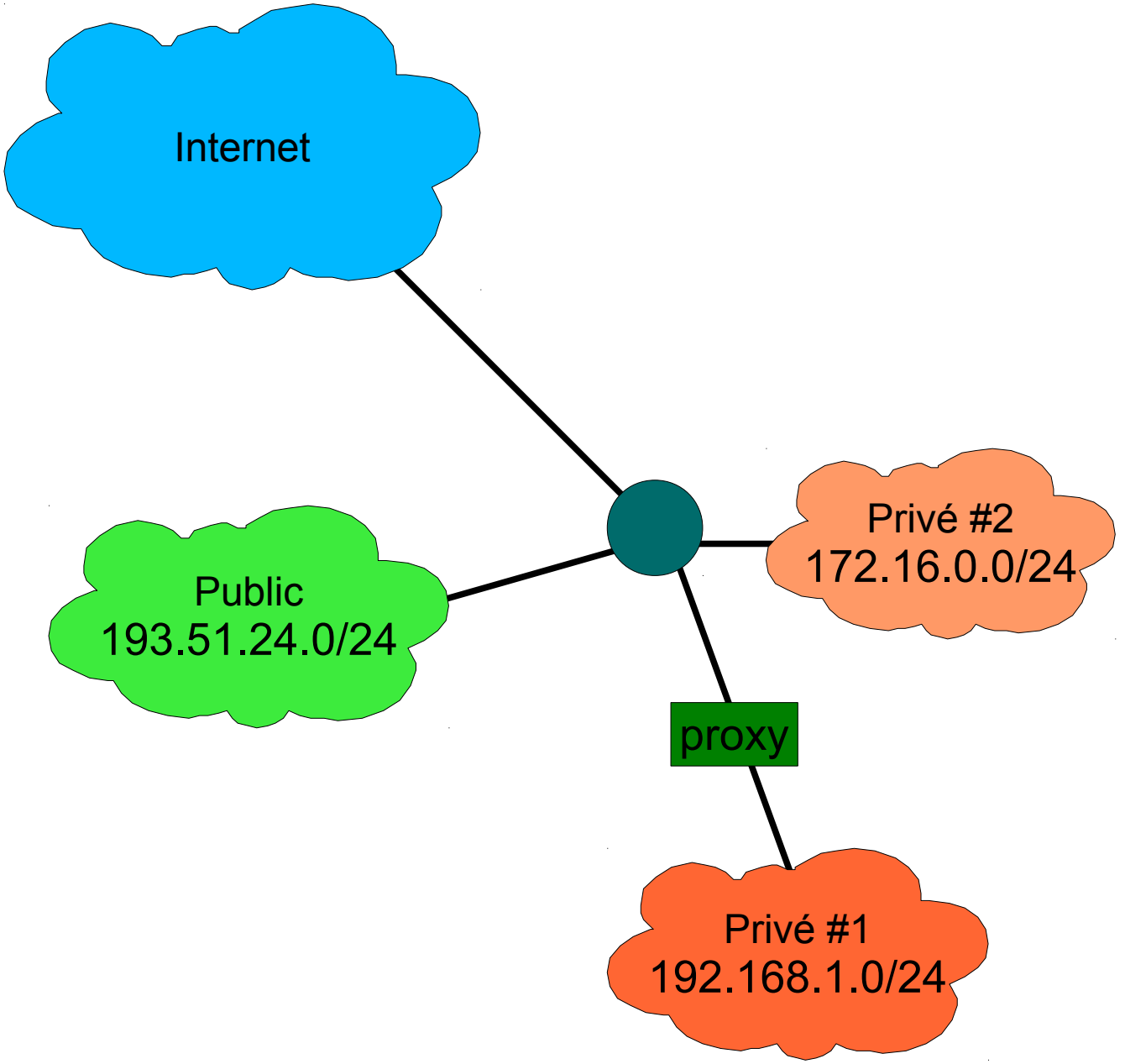
- **En IPv4, on distingue des types d'adresses particuliers, répertoriés dans la RFC 3330. Les principales singularités :**
  - la RFC 1918 définit les adresses suivantes comme privées :
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
  - la boucle locale : interface *lo*
    - 127.0.0.0/8 (on se contente souvent de définir 127.0.0.1)
  - lien local, adresses utilisées dans des phases d'autoconfiguration
    - 169.254.0.0/16
  - adresses de multicast
    - 224.0.0.0/4

- **Dans la perspective d'un réseau d'entreprise, on s'intéressera principalement aux spécificités des classes d'adresses privées définies par la rfc 1918.**
- **Dans un réseau, on peut distinguer 3 catégories de machines**
  - celles ne nécessitant aucun accès à Internet
  - celles nécessitant un accès à Internet pour un ou des services pouvant être mandatés (via l'utilisation d'un *proxy*)
  - celles nécessitant un accès direct à Internet

Les 2 premières catégories peuvent s'inclure dans un plan d'adressage privé, la troisième dans un plan d'adressage public.

- **Les adresses privées ne doivent pas être visibles sur/depuis Internet**
  - pas de routage de ces adresses
  - pas d'entrées pour ces machines dans les enregistrements DNS publiés à l'extérieur

- **Exemple**


Internet
Public
193.51.24.0/24
Privé #2
172.16.0.0/24
proxy
Privé #1
192.168.1.0/24

Bonnes pratiques

La définition d'une architecture réseau nécessite une certaine rigueur, notamment dans le cadre de réseaux de grande ampleur, c'est pourquoi il est bon de garder certains points à l'esprit :

- sur des sous-réseaux différents, des machines jouant le même rôle auront une adresse IP se terminant par les mêmes 8 octets
- la passerelle par défaut de **X.Y.Z.0/24** est généralement **X.Y.Z.254**
- l'utilisation de plages d'adresses privées doit être contrôlée : même si ces réseaux ne sont pas routés, éviter d'utiliser plusieurs fois la même plage
- penser à l'éventuelle utilisation de VPN dans des réseaux multi-sites : problématique du chevauchement des adresses
- bien sûr, un grand réseau « à plat » est rarement justifiable : découpage en sous-réseaux selon des critères variés :
  - fonctionnalités, populations, OS

Adressage statique ou dynamique

- **Il existe deux méthodes d'attribution de l'adresse IP à une machine sur un réseau :**
  - adresse statique : l'adresse IP est configurée *en dur* dans le système, et directement attribuée à l'interface par l'OS (au boot, par exemple).
    - exemple d'un fichier */etc/network/interfaces* sous Linux
      - iface eth0 inet **static**
  - adresse dynamique : l'adresse IP à attribuer à l'interface est a priori inconnue du système ; une requête DHCP est émise sur le réseau, et le serveur y répond avec une adresse IP pouvant être utilisée par la machine.

- **Cas particulier**
  - Sous Windows, lorsqu'une interface configurée pour utiliser DHCP ne reçoit aucune réponse, ou qu'elle est configurée en « automatique », une adresse du réseau 169.254.0.0/16 lui est assignée.

Le protocole DHCP 1

- **Ce protocole a pour but de permettre à une machine sans adresse IP de récupérer une configuration réseau : RFC 2131**
  - il se base sur UDP
  - les ports utilisés sont le 67 côté client et le 68 côté serveur

- **Principe de l'échange**
  - le client émet une requête (*dhcpdiscover*) pour trouver un serveur ; son adresse source est nulle : 0.0.0.0
  - le serveur répond (*dhcpoffer*) avec une adresse pouvant être utilisée par le client
  - le client renvoie une requête (*dhcprequest*) au serveur qu'il a choisi pour compléter sa configuration
  - le serveur répond (*dhcpack*)

Le protocole DHCP 2

- **Configurations de DHCP**
  - statique ou dynamique ?
    - statique : une adresse MAC donnée se verra toujours attribuer la même adresse IP
    - dynamique : une même adresse MAC pourra recevoir des adresses IP différentes au cours de requêtes successives

- **Informations fournies par DHCP**
  - les paramètres de configuration fournis par le serveur DHCP sont déterminés par des options définies dans la RFC 2132
  - On trouve notamment :
    - masque de réseau : 1
    - passerelle par défaut : 3
    - hostname : 12
    - des serveurs divers : de nom, ntp...
    - des paramètres réseau divers...

Architecture

- **Au niveau des méthodes de communication des équipements, on distingue différentes catégories, selon**
  - la nature de la couche physique dans certains cas
  - les équipements utilisés
  - les services (applicatifs) souhaités

- **Ces méthodes de communication sont indépendantes de la topologie physique du réseau (indépendance des couches dans le modèle OSI)**

- **On distingue**
  - le modèle client(s)/serveur
  - le modèle distribué

Architecture client(s)/serveur 1

- **C'est une architecture centralisée**
  - un serveur met à disposition une ressource (données, service)
    - la ressource n'est pas nécessairement disponible sur un unique serveur : notions de redondance et d'équilibrage de charge
  - les clients voulant utiliser cette ressource en font la demande au serveur

- **Le serveur est donc l'élément clé de cette architecture**
  - nécessité d'une bonne sécurisation
  - la disponibilité est souvent cruciale
    - sauvegarde, redondance, tolérance aux pannes
  - Spécificités d'administration
    - hardware
    - système d'exploitation
    - outils/applications installés
    - comptes utilisateurs

Architecture client(s)/serveur 2

- **Cas typique : services TCP ou UDP**
  - le serveur écoute sur un port donné
    - cf */etc/services* sous Unix pour les ports bien connus
  - le client envoie une requête (niveau applicatif) sur ce port
    - sauf cas particuliers, le port source est un port > 1023
  - le serveur répond en accord avec le protocole applicatif concerné

- **Exemples : mail, DNS, web...**

Architecture distribuée

- **Par opposition à l'architecture clients/serveur, dans une architecture distribuée, tous les éléments sont sur un pied d'égalité :**
  - pas de serveur unique
  - tous les éléments sont aptes à fournir la fonctionnalité souhaitée
  - tous les éléments sont également des clients potentiels
- **On retrouve ce principe dans des cas variés d'utilisation**
  - calcul parallèle
  - technologies distribuées type CORBA
  - *peer-to-peer*
  - réseaux WiFi en mode *ad hoc*

Implications

- fiabilité des éléments ?
- plus de point central représentant la clé de voûte de l'architecture
- problématique pour l'administration !

Les VLANs 1

- **VLAN : Virtual LAN**
- **Les VLANs permettent de créer des réseaux logiques indépendants au sein d'un même réseau physique**
- **L'implémentation passe par le protocole 802.1Q (niveau 2)**
  - les commutateurs peuvent associer un port à un VLAN donné
  - les paquets sont tagués pour identifier leur VLAN
  - sur un brin regroupant plusieurs VLANs (*trunk*), on peut ainsi les identifier
- **Avantages :**
  - réduit le domaine de broadcast
  - réduit les besoins en terme de matériel (séparation logique)
  - facilite certains aspects de l'administration réseau

Les VLANs 2

- **Plusieurs critères peuvent servir à regrouper les machines au sein d'un même VLAN**
  - le protocole de niveau 3 (IP, IPv4 ou IPv6, Appletalk)
    - peu voire plus utilisé
  - notion d'authentification avec le protocole 802.1x
  - adresse MAC
  - port associé sur le commutateur

- **Dans la pratique**
  - un VLAN est souvent associé à un sous-réseau IP
    - possibilité de le distribuer (logiquement) sur un vaste réseau (physique)
    - possibilités de filtrages selon l'appartenance à un VLAN

Sécurité niveau 2 (1)

- **Dynamic Trunking Protocol (DTP)**
  - Négotiation automatique du *trunking mode*
  - Configure chaque port en trunking ou accès simple
  - Problème : une station peut émuler le protocole DTP
  - Solution : configurer statiquement les ports des stations
- **Spanning Tree Protocol**
  - Détection des boucles dans les réseaux
  - Création automatique d'une structure d'arbre pour l'envoi des trames
  - Problème : une station peut émuler le protocole STP
    - Pour forcer un recalcul de la structure de l'arbre (DoS)
    - Pour intercepter le trafic en devenant la racine
  - Solution : refuser le trafic STP sur les ports des stations

Sécurité niveau 2 (2)

- **Hot Standby Router Protocol**
  - Autorise la configuration de routeurs multiples en redondance
  - 1 routeur *actif*, les autres en *standby*
  - Election automatique en cas de panne du routeur actif
  - Problème : une station peut tenter de devenir le routeur actif
    - Détournement du trafic
    - Déni de service si la station ne retransmet pas les paquets
  - Solution : Désactiver le protocole HSRP sur les ports des stations
- **Dynamic ARP inspection (DAI)**
  - Problème : attaques par ARP spoofing
  - Solution : DAI associe les adresses IP aux adresses MAC
    - Détection immédiate d'un changement de couple IP/MAC
    - Blocage des paquets ARP anormaux
    - Possibilité de fermer le port incriminé

Sécurité niveau 2 (3)

- **VLAN Hopping (saut de VLAN)**
  - Problème : Possibilité pour une station de communiquer avec un autre VLAN que le sien
  - Solution : configurer les ports des stations en accès simple
    - Attention également au Dynamic Trunking
- **Private VLAN**
  - Idée : restreindre les communications au sein d'un VLAN
  - Les stations d'un VLAN ne peuvent communiquer que vers le port du routeur
  - Reprend l'idée du cloisonnement entre stations en WiFi

Architecture réseau

Architecture, cloisonnement et redondance

Architecture, cloisonnement et redondance

- Architecture
- Découpage du réseau
- Firewalls, proxies, DMZ
- Cloisonnement
- Pare-feu
- Redondance

Architecture réseau

- **Architecture au sens large : comment organiser son réseau pour en tirer le meilleur parti en terme**
  - de fonctionnalités
  - de performances
  - d'administration
  - de sécurité

- **L'architecture ainsi déterminée n'est pas restreinte à un niveau du système OSI mais au contraire influera sur**
  - l'architecture logique
  - l'architecture physique

- **Cependant elle est conditionnée par des critères**
  - financiers : l'architecture idéale peut être très onéreuse
  - matériels : équipements disponibles, dimension du site...
  - humains : technicité, difficultés d'exploitation

Principes d'une architecture réseau

- **Un réseau présente des machines aux rôles et aux fonctionnements divers : pourquoi toutes les laisser sur le même plan ?**
- **Plutôt qu'une architecture « à plat » (ie une seule plage d'adresse, pas de routage interne), on préférera un agencement prenant en compte ces diversités.**
- **Ce type d'architecture facilite ensuite**
  - l'administration
    - exemple : les administrateurs des stations ne seront pas les mêmes que ceux des serveurs de base de données
  - la mise en place de mesures de sécurité
    - contrôle des flux entre les zones
- **Mais il est plus complexe**
  - plus d'équipements à gérer
  - ces architectures peuvent rapidement devenir très compliquées

Découpage en sous-réseaux

- **La base de l'architecture va être un découpage du réseau global en zones, le plus souvent associées à un sous-réseau ou à un ensemble de sous-réseaux IP.**

- **Les critères de découpage sont multiples**
  - accessibilité de la zone
  - fonctions des machines
  - population de la zone
  - autres : systèmes d'exploitation, flux spéciaux

- **L'implémentation est possible**
  - via des sous-réseaux IP
  - mais aussi des VLANs spécifiques, généralement calqués sur le découpage effectué au niveau 3
  - des outils de filtrage et de routage adaptés

Découpage selon l'accessibilité

- **Dans un réseau, toutes les machines n'ont pas les mêmes besoins en terme d'accessibilité : pour une machine donnée, on se posera les questions suivantes :**
  - doit-elle être accessible depuis l'extérieur ? (serveurs publics)
  - doit-elle être accessible pour les autres machines du réseau local ? (serveurs internes, intranets)
  - a-t-elle besoin d'accéder à Internet ? ou à d'autres zones extérieures au réseau ?
  - a-t-elle besoin d'accéder à des services spécifiques du réseau local ?
  - des précautions particulières doivent-elles être considérées pour sa sécurité ?
- **De ces réponses vont découler des contraintes techniques**
  - adressage spécifique : public ou privé ?
  - positionnement derrière un proxy, un pare-feu, un reverse-proxy ?
- **Ces besoins sont être étroitement liés à la fonction de la machine.**

Découpage selon la fonction 1

- **La première distinction à considérer concerne :**
  - les serveurs d'une part
  - les stations d'autre part
- **On peut cependant ajouter d'autres catégories**
  - les équipements réseau (routeurs, commutateurs...)
  - les équipements de sécurité (pare-feu, proxies...)
- **Les serveurs peuvent (doivent !) également être distingués**
  - serveurs d'authentification (NIS, kerberos, radius...)
  - serveurs de fichiers (NFS, samba...)
  - serveurs mail, DNS
    - internes
    - publics
  - serveurs de sauvegarde : souvent une architecture spécifique !

Découpage selon la fonction 2

- **Au niveau stations, une discrimination plus fine peut être établie en fonction des populations d'utilisateurs, ce qui n'est pas le cas des autres machines, qui de par leur fonction même sont déjà restreintes à un type d'administrateur.**
- **Pour les équipements réseau et de sécurité, on trouvera souvent une architecture spécifique avec**
  - une ou plusieurs interfaces (ou ports) en prise directe avec le réseau classique
  - une interface d'administration sur un réseau dédié
    - notion de VLAN d'administration
    - fonctionnalités non disponibles sur les autres interfaces
      - serveur ssh
      - interface web d'administration...
- **Tant pour les serveurs que pour ces équipements spécifiques, il est souhaitable que l'architecture permette un bon contrôle des accès.**

Découpage selon la population

- **Il peut être directement lié à la fonction (serveurs, équipements réseau, de sécurité).**

- **La distinction selon la population d'utilisateurs prend son sens au niveau des stations. On différencie alors :**
  - les administrateurs
    - réseau
    - système
    - de sécurité
  - les utilisateurs classiques
  - le personnel administratif (secrétaires...)
    - utilisation souvent restreinte aux suites bureautiques
  - les stagiaires, thésards, prestataires

- **A chacune de ces populations peut donc être attribué un sous-réseau, avec accès aux serveurs et applications nécessaires à leur fonction.**

Découpage selon des critères divers

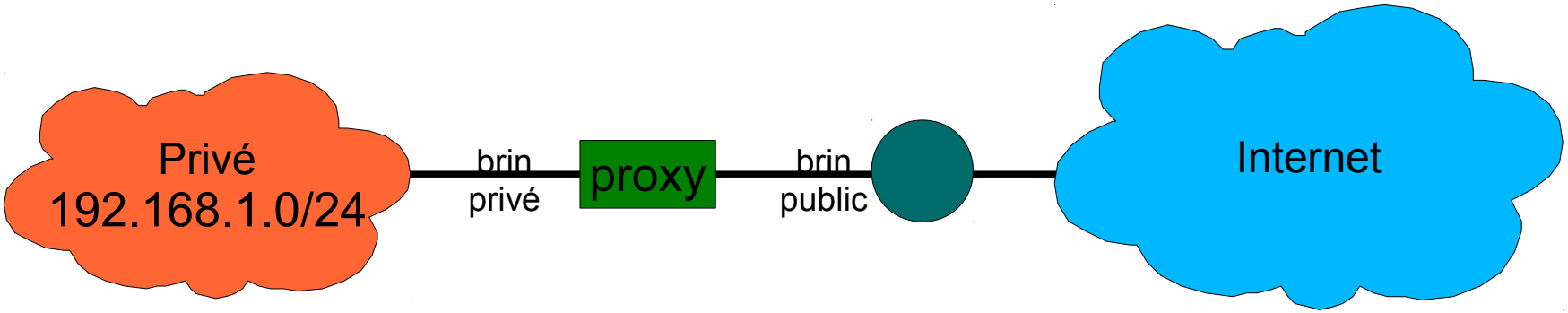
- **La segmentation du réseau en zones peut se faire de manière totalement progressive, en enchaînant les critères de découpage précédemment évoqués pour ramifier le réseau.**

- **De nouveaux critères peuvent ensuite être invoqués pour résoudre ou faciliter des problèmes d'administration :**
  - système d'exploitation
    - Windows, Unix
    - flux distincts
    - administration différente !
  - besoin de flux spécifiques
    - IPsec
    - zones expérimentales
  - accueil de personnels extérieurs
    - postes dédiés
    - Hot spots WiFi

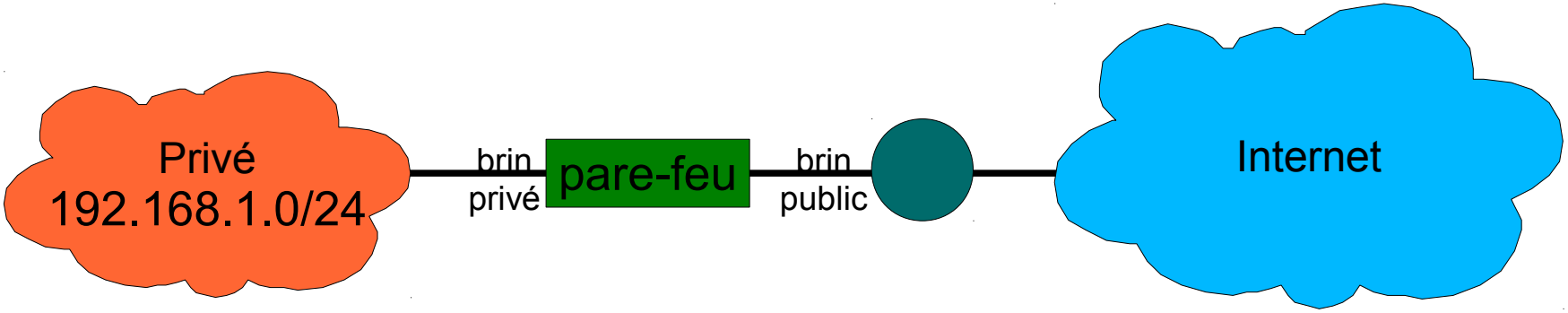
Firewalls, proxies 1

- **Un découpage logique basé sur des sous-réseaux IP, renforcé par l'utilisation de VLANs, est un bon départ pour définir une architecture.**
- **L'utilisation adaptée de pare-feu (*firewalls*) et de mandataires (*proxies*) apporte un plus pour**
  - la sécurité
  - les performances
- **Le pare-feu permet**
  - de contrôler les flux entrant et sortant d'une ou plusieurs zones
  - d'implémenter de la translation d'adresse (NAT)
    - possibilité pour un réseau non routé d'atteindre l'extérieur
- **le mandataire permet**
  - de donner accès à certains services réseau
  - d'implémenter du contrôle au niveau applicatif (http par exemple)
  - d'améliorer les performances (cache...)

- **Utilisation avec des réseaux privés**
  - proxy : travaille au niveau applicatif

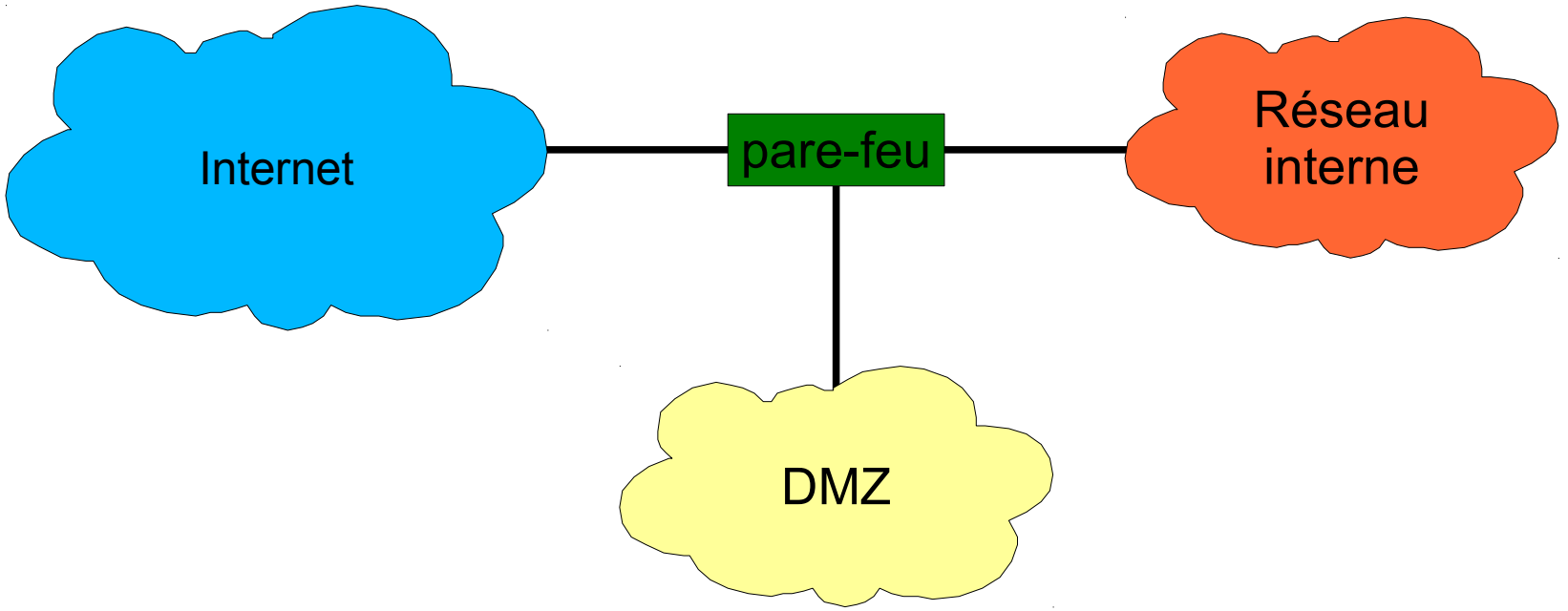


  - pare-feu : travaille au niveau réseau



DMZ : zone démilitarisée 1

- **Au sein du réseau, certains serveurs (mail, DNS, web) doivent être accessibles depuis l'extérieur pour offrir un service sur Internet.**
- **Ils occupent une place particulière dans la politique de sécurité du réseau : la zone qui leur est réservée est appelée DMZ (*DeMilitarized Zone*).**
- **On représente alors le réseau comme suit :**



DMZ : zone démilitarisée 2

- **La politique de sécurité définit traditionnellement, et succinctement, les règles sur les flux comme suit :**
  - Depuis le réseau interne
    - vers l'extérieur : autorisé, ou soumis à restrictions (proxy...)
    - vers la DMZ : autorisé
  - Depuis l'extérieur
    - vers la DMZ : autorisé
    - vers le réseau interne : interdit
  - Depuis la DMZ
    - vers le réseau interne : interdit
    - vers l'extérieur : interdit
- **Le fait que les serveurs en DMZ soient exposés au monde extérieur nécessite qu'ils soient renforcés au niveau sécurité**
  - blindage système
  - surveillance (IDS, logs)

Cloisonnement : motivations

- **Le découpage du réseau en zones distinctes a de nombreux avantages, notamment en termes de sécurité.**
- **Parmi les rôles de la politique de sécurité d'un réseau, ou peut citer :**
  - la définition du rôle de chaque zone
  - les flux qui peuvent transiter entre chaque zone (cf DMZ)
  - les moyens à mettre en place pour
    - assurer ce cloisonnement (pare-feu, ACLs...)
    - vérifier son bon fonctionnement (outils de supervision réseau)
- **Le cloisonnement permet**
  - de restreindre les accès et donc les risques de compromission
  - de limiter les risques de propagation de malware entre les zones
  - de définir des politiques plus fines selon chaque zone
    - accès aux services
    - surveillance

Cloisonnement : principes

- **Les grands principes de sécurisation d'un système d'information sont applicables au cas particulier du réseau et de son cloisonnement en zones.**

- **Principe de l'unicité des rôles**
  - une machine assure une fonction et une seule
    - serveurs dédiés
  - une zone réseau est constituée de machines ayant
    - des rôles similaires
    - des besoins comparables en terme de flux

- **Principe du moindre privilège**
  - les flux strictement nécessaires entre les zones sont autorisés
  - tous les autres sont interdits

Pare-feu 1

- **Du point de vue fonctionnel, on distingue deux types de pare-feu :**
  - stateless : pas de notion d'état, les paquets sont tous traités indépendamment les uns des autres.
  - stateful : gestion (plus ou moins précise selon l'implémentation) des états : connexions TCP, certains protocoles basés sur UDP, fragmentation IP...

- **Du point de vue stratégie, on distingue deux types de politique :**
  - Permis par défaut : on autorise tout par défaut, on interdit simplement ce que l'on sait être dangereux.
  - Interdit par défaut : on interdit tout par défaut, on autorise ensuite explicitement ce dont on a besoin.

- **En pratique on utilise**
  - un pare-feu stateful
  - avec une politique de type *interdit par défaut*

Pare-feu 2

- **Classiquement, le filtrage de paquet s'effectue aux niveaux 3 et 4 du système OSI. Les règles prennent dès lors en compte des paramètres tels que :**
  - une interface réseau
  - les adresses IP source/destination (machines ou réseaux)
  - un protocole (TCP, UDP, ICMP, voire dans certains cas un numéro de protocole)
  - les ports source/destination (pour TCP et UDP)
- **C'est le minimum que l'on est en droit d'attendre d'un filtre de paquet.**
- **On trouve assez souvent des paramètres plus spécifiques :**
  - champ IP (fragmentation, TTL...)
  - flags ou options TCP
  - type ICMP
- **Egalement, on dispose de possibilités de logger les flux bloqués ou autorisés...**
- **On peut alors contrôler les paquets reçus, émis, ou routés.**

Pare-feu 3

- **Depuis le noyau 2.4, Linux intègre Netfilter**
  - Netfilter est la partie Kernel du firewall
  - Iptables est l'outil de configuration en espace utilisateur

- **Quelques caractéristiques :**
  - firewall stateful (en IPv4)
  - gestion du NAT (Network Address Translation)
  - architecture modulaire
    - possibilité de ne compiler/charger que les composants utiles
    - possède de nombreuses extensions disponibles via patch-o-matic
  - possibilité de passer les paquets en user space pour un traitement quelconque
  - système de log évolué

Pare-feu 4

- **Architecture :**
  - Netfilter se découpe en 3 tables
    - filter : traite les paquets émis vers ou depuis la machine, ou pour lesquels la machine effectue du routage (IP forwarding)
    - nat : gère la translation d'adresse (source, ou SNAT, et port forwarding)
    - mangle : permet la modification de paquets
  - Chaque table est ensuite divisée en chaînes
    - les chaînes builtins correspondent à des hooks dans le noyau : à un moment de son traitement par le kernel, le paquet est passé à Netfilter pour inspection
    - il est possible de créer ses propres chaînes, pour structurer son firewall
  - Chaque chaîne possède
    - une série de règles : pour un paquet donné, la première règle à lui correspondre décide de son destin
    - une politique par défaut à appliquer aux paquets n'ayant rencontré aucune règle adéquate

- **Commandes utiles**
  - iptables -t table -L -n -v
    - -L pour lister les règles d'une table (affiche toutes les chaînes)
    - -n pour ne pas résoudre les noms, -v pour verbose
  - iptables -t table -F [chaîne]
    - -F pour flusher une table entière, une seule chaîne si elle est précisée
  - iptables -t table -P chaîne cible
    - -P pour attribuer à la chaîne en argument une politique par défaut définie par la cible (target) ; une cible peut valoir ACCEPT, DROP, REJECT...
  - iptables -t table -A chaîne <règle> -j cible
    - -A pour ajouter la règle définie en fin de chaîne (-I chaîne rang permet d'insérer la règle à la position définie par le rang)
  - iptables -t table -D chaîne rang
    - -D pour supprimer la règle à la position définie par rang dans la chaîne donnée
- **man iptables est votre ami**

Pare-feu 6

- **Packet Filter, communément appelé PF, est le firewall intégré à OpenBSD depuis la version 3.0**
  - PF est contrôlé en espace utilisateur par la commande pfctl

- **PF offre :**
  - du filtrage stateful
  - de la translation d'adresse
  - de la normalisation de trafic
  - de la qualité de service (QoS)
  - un système de règles dynamiques

- **Contrairement à Netfilter, PF**
  - a une structure monolithique
  - ne rentre pas dans les détails de protocoles applicatifs

Pare-feu 7

- **La configuration se définit classiquement dans /etc/pf.conf**
  - possibilité de définir des variables

    ```
    interface_interne="rl0"
    interface_externe="rl1"
    ```

  - normaliser le trafic entrant

    ```
    scrub in all
    ```

  - exemples de règles de filtrage

    ```
    block in on $interface_externe all
    pass in quick on $interface_externe proto tcp from any \
            to $interface_externe port {80, 443} flags S/SA keep state
    ```

  - positionnement d'une ancre pour des règles dynamiques

    ```
    anchor dyn-rules
    ```

- **Utilisation de pfctl**
  - activation du pare-feu et chargement du fichier de configuration

    ```
    pfctl -e
    pfctl -f /etc/pf.conf
    ```

  - chargement d'un fichier de règles dynamiques

    ```
    pfctl -a dyn-rules:all -f /etc/pf/dyn-rules.conf
    ```

Pare-feu 8

- **PF offre de riches possibilités au niveau grammaire**
  - variables
  - tables d'hôtes modifiables dynamiquement

- **Le parcours des règles pour savoir laquelle appliquer :**
  - quand on rencontre une règle correspondant au paquet traité
    - elle est appliquée si elle contient le mot-clé quick
    - sinon, elle est conservée comme règle à appliquer par défaut si aucune règle adéquate n'est rencontrée par la suite

- **Les règles dynamiques (système d'ancres)**
  - PF permet de laisser des points d'entrée dans le jeu de règles principal
  - on peut ensuite manipuler dynamiquement des règles au sein de cet espace réservé (par exemple les charger dans des circonstances particulières, cf authpf)

Pare-feu 9

- **Quelques pare-feu commerciaux :**
  - Cisco Pix
  - Checkpoint Firewall-1
  - Netasq
  - Juniper

- **Ils intègrent souvent de nombreuses fonctionnalités supplémentaires**
  - IPS
  - interfaces diverses
  - fonctions de filtrage applicatif ou possibilités d'ajouts de modules

- **Le plus souvent on les trouve sous forme d'appliance**

Le filtrage applicatif (proxies)

- **Le rôle est similaire à celui d'un pare-feu stateful de niveau 3-4**
  - Autoriser ou interdire les accès entre différents réseaux selon la politique de sécurité en vigueur
  - Seule la méthode est différente
- **Un proxy se positionne comme intermédiaire entre chaque connexion réseau**
  - Les clients se connectent au proxy au lieu de se connecter directement à la destination finale, le proxy initie la seconde moitié de la connexion
  - Intérêt : aucune **connexion directe** entre les systèmes situés de part et d'autre du pare-feu
- **Les proxies sont généralement mis en oeuvre par des programmes de confiance, petits, robustes et spécialisés pour une protocole donné**
  - Chaque proxy a une connaissance exhaustive du protocole qu'il véhicule → analyse de sécurité complète
- **Solution du pauvre : proxies génériques**

Fonctionnement d'un proxy applicatif

- **Un proxy se comporte à la la fois comme client et serveur**
  - Un client souhaitant se connecter vers un serveur initie d'abord une connexion vers le proxy
  - Ce dernier ouvre alors une connexion vers le serveur destinataire
  - Les données envoyées par le client sont retransmise vers le serveur, et les données reçues du serveur sont renvoyées vers le client
- **Chaque requête/réponse est analysée afin de vérifier son adéquation avec la politique de sécurité**
- **Notion de proxy transparent**
  - Le client ne sait pas qu'il utilise un proxy pour se connecter au serveur
  - Nécessite de modifier l'entête IP
- **« Firewall proxy »**
  - Machine blindée (« bastion ») possédant plusieurs interfaces réseaux et un ensemble de proxies spécialisés
  - Les produits commerciaux supportent souvent un très grand nombre de protocoles
    - Etendue réelle des vérifications protocolaires ?

Avantages et inconvénients des proxies

- **Analyse plus ou moins complète de la couche applicative**
  - Les jounaux de logs sont en général nbeaucoup plus complets et facilitent les résolutions d'incidents
- **Masquage de la topologie interne du réseau**
  - Le NAT peut fournir la même fonctionnalité mais dans une moindre mesure (TTL, IPID, OS fingerprinting, etc.)
- **Les proxies ne sont pas toujours compatibles avec les clients ou les implémentations d'un protocole donné**
  - Nouvelle application == nouveau proxy
- **Performances**
  - Plus l'analyse protocolaire est évoluée, plus l'impact sur les performances est important
- **Difficultés de configuration ou de mise en place**
  - On trouve de moins en moins de véritables proxies dans les produits commerciaux, la tendance s'oriente plus vers du NAT avec un contrôle (simplifié) de la couche applicative

Quelques exemples de proxies

- **Proxy web**
  - Souvent associé avec un cache pour optimiser les accès des utilisateurs
  - Contrôle des sites auxquels accèdent les utilisateurs
    - {White,Black}-lists, mots-clés, etc.
  - Importance des logs d'accès
  - « Reverse proxy »
    - Contrôle des accès à un serveur web (granularité très fine)
    - Sécurisation des accès (SSL et/ou authentification)
- **Proxy FTP**
  - Souvent utilisé conjointement avec un pare-feu de niveau 3-4 (pf)

Monitoring et Surveillance

- **Monitoring système et réseau**
  - Objectif principal : donner aux administrateurs un aperçu de l'état de la protection du système d'informations
  - Différent de la détection d'intrusions
    - Périmètre plus large incluant la disponibilité et les performances
- **La surveillance des paramètres de base systèmes et réseau est importante même pour des administrateurs de sécurité**
  - Exemples de paramètres de base : espace disque, bande passante, uptime, temps de réponse des services, etc.
  - La disponibilité peut être un paramètre très important
  - Détection des anomalies :
    - Détection des changements de comportement d'un système
    - ... mais également des changement de configuration
    - ... ou des changement d'utilisation

Objet de la surveillance

- **Exemples d'outils :**
  - BigBrother, HPOV, Nagios, etc.
- **Surveillance de base**
  - Ce sont les indicateurs que l'on doit toujours surveiller
  - Charge machine, accessibilité réseau, espace disque, etc.
- **Les éléments à surveiller dépendent également de la finalité du système et de ce qui est « vital » pour l'entreprise**
  - Pour un site web de commerce électronique, on s'intéressera par exemple à l'utilisation de la bande passante, au nombre de hits par seconde, au pourcentage d'achat réalisés, etc.
  - Si la messagerie est un outil de travail important, le service doit être surveillé à tous les niveaux
- **Les outils de surveillance peuvent également être spécialisés en fonction des services**
  - Simulation du parcours d'un client pour un site web
  - Envois de mails à echo@...
  - ...

Intégration de la surveillance dans le SI

- **En principe, la surveillance locale reste simple**
  - Veiller toutefois à ce que les processus de surveillance ne consomment pas trop de ressources des systèmes surveillés
- **Problème des remontés d'informations ou d'alertes**
  - Cloisonnement réseau
  - Authentification
  - Confidentialité des informations
  - Sécurité intrinsèque des outils de monitoring

Réponse aux incidents

- **Différents moyens pour alerter**
  - Envoi de mails ou de SMS, pager, etc.
    - Quels sont les garanties que les alertes soit livrées ?
  - Qui sont les destinataires ?
    - Gérer les problèmes de communication en cas de crise
  - Souplesse générale du mécanisme
    - Horaires différents, week-end, congés, etc.
- **Centralisation des envois**
- **La réponse aux incidents doit être documentée dans la politique de sécurité de l'entreprise**
  - Qui doit traiter les alertes, quelles sont les différents niveaux en cas d'escalade, quelles sont les premières actions à faire par les différents niveaux, etc.

Réponse aux incidents

- **Préparer**
  - Entraîner les gens : formation, documentation, etc.
- **Identifier**
  - Indicateurs, messages, analyse
- **Maitriser (« containment »)**
  - Ne pas oublier les « preuves »
- **Eradiquer**
- **Réparer**
- **Poursuivre**

Redondance

- **Objectif : améliorer la disponibilité d'un service**

- **La redondance peut être assurée à divers niveaux :**
  - redondance électrique pour un serveur sensible
    - 2 alimentations
    - chaque alimentation reliée à un réseau électrique distinct
  - redondance du service en soi
    - plusieurs serveurs assurent la même fonctionnalité
    - ce sont quasiment des clônes

- **La redondance ne doit pas être confondue avec la répartition de charge**
  - même si l'implémentation peut être proche, le but est différent !

Exemples de redondance

- **Redondance électrique**
  - n'est possible que sur certains matériels
  - ne doit pas être négligée, c'est le premier niveau du système
- **Redondance réseau**
  - infrastructure : réseaux de backup
  - redondance des routeurs
    - protocole VRRP et assimilés
- **Redondance de serveurs**
  - certains services fonctionnent avec des notions de maître/esclave
    - exemple : DNS
  - lorsque le maître ne peut fournir l'information, un esclave est interrogé

CARP, la redondance au sein de PF

- **Le pare-feu PF d'OpenBSD intègre un mécanisme de redondance : CARP, ou Common Address Redundancy Protocol.**
- **Grâce à ce mécanisme, plusieurs machines peuvent être placées en redondance pour assurer le filtrage, et assurer un système failsafe.**
- **Le protocole est similaire à VRRP**
  - élection d'un Master
  - machines en backup
  - protocole d'élection via une adresse multicast
- **pfsync assure la transmission des états pour que ceux-ci soient cohérents d'une machine à l'autre en cas de bascule.**

Architecture Réseau

Conclusion

Conclusion

- **Différents types de cablage et d'interconnexion**
  - Cuivre / Fibre : coûts très différents
    - Transpondeurs, boîtiers TAP
  - Commutateurs : premier niveau de cloisonnement
  - VLAN : cloisonnement inter-commutateurs

- **Attribution des adresses IP**
  - Regroupement des ressources similaires (serveurs, stations)
  - Adresses statiques / dynamiques
  - Cloisonnement par la configuration du routage

- **Architectures réseau**
  - Séparation en zones logiques = identification des flux réseau
    - Meilleur découpage = règles de filtrage simples
    - Mise en place de serveurs proxy = suppression du routage
  - Bien étudier son réseau !