Pratique des réseaux

Auteur
Carlos da Costa

GUIDE DE FORMATION

Guide de formation Tsoft
Pratique des réseaux
Référence : TS0083
Version 1 – septembre 2015

Table des matières

Avant-propos

Les réseaux sont le système nerveux de l'informatique actuelle. Il est indispensable d'en connaître et d'en maîtriser les aspects essentiels.

De simples médias statiques d'échange de données informatiques, ils ont vu leurs rôles croitre en complexité, en performance et en « intelligence ».

Le but de cet ouvrage est de vous permettre de maitriser les aspects essentiels des réseaux, de TCP/IP et des technologies actuelles qui leur sont liées.

Nous commencerons par étudier les différents types et les différentes catégories de réseaux, ainsi que le modèle de référence et d'analyse que constitue toujours OSI.

Ethernet est actuellement la technologie LAN la plus utilisée. Nous verrons les normes, les topologies, l'adressage et les formats de trames qui caractérisent Ethernet.

La commutation Ethernet est une évolution logique et importante des réseaux modernes. Nous étudierons le pontage, le protocole Spanning Tree, les VLANs ainsi que le trunking.

Le WiFi est devenu, en quelques années, la technologie informatique sans fil la plus répandue. Nous en étudierons les différentes normes, les composants, les contraintes, ainsi que les aspects sécuritaires.

TCP/IP est devenu le protocole réseau le plus utilisé et le plus répandu. Nous étudierons la pile TCP/IP : les principaux protocoles, l'adressage ainsi que les applications DNS et DHCP.

Enfin, la VoIP s'est déjà imposée chez les grands opérateurs et la plupart des grandes entreprises. Nous en étudierons les principes, les composants et les principaux protocoles.

Aujourd'hui, la sécurité est devenue une préoccupation majeure des entreprises et des gouvernements. Nous aborderons les aspects les plus importants de la sécurité réseau, tout ce qui permet de sécuriser les échanges entre les machines, ainsi que les principaux protocoles VPN.

Enfin, nous aborderons l'administration des réseaux. Quels sont les rôles et les fonctions liés à l'administration ? Quels protocoles permettent d'en faciliter le fonctionnement et l'efficacité ?

- *Types de réseaux*
- *Topologies*
- *ISO*
- *Modèle OSI*
- *Répéteur*
- *Hub*
- *Commutateur*

1

Présentation

Objectifs

Ce module présente les bases du réseau.

Connaissance

- Présentation des types de réseaux
- Les différents types de réseaux
- Les topologies réseaux usuelles
- Le modèle OSI et ses principes
- Les composants essentiels des réseaux

Progression

Principes de base	Classification des réseaux
Organismes importants	Le modèle OSI
Types de réseaux principaux	Composants d'un réseau
Topologies courantes	

Principes

- Le but des réseaux informatiques est de partager des ressources entre plusieurs utilisateurs
- Les ressources peuvent être des données, des applications, des périphériques, des services
- Cette centralisation des accès et cette mutualisation des ressources permettent :
  - Une gestion plus efficace des ressources
  - Une meilleure connaissance sur l'utilisation des ressources
  - Des coûts d'utilisation plus bas
  - Un niveau de sécurité plus élevé
  - Un meilleur niveau de communication
  - Des fonctionnalités nouvelles

PRINCIPES DES RESEAUX

Le but des réseaux informatiques est de partager des ressources entre plusieurs utilisateurs.

Les ressources peuvent être :

- Des données. Elles peuvent se trouver sur des machines dédiées, des serveurs, ou être mises à disposition, partagées, par un utilisateur sur sa propre machine.
- Des applications. L'utilisateur du réseau n'a besoin d'installer sur son poste de travail que la partie cliente d'une application. Selon le type d'application, une part plus ou moins grande du traitement sera effectuée par l'application serveur centralisée.
  De plus en plus d'applications ne sont plus distribuées en client/serveur, mais entièrement centralisées. C'est le cas des applications fonctionnant sous CITRIX ou Terminal Server. Seul le retour d'écran est traité sur le poste de travail de l'utilisateur, l'ensemble du traitement est effectué sur le ou les serveurs. Aucune installation applicative cliente n'est nécessaire.
- Des périphériques. Les imprimantes en sont l'archétype. Soit chaque utilisateur possède sa propre imprimante, qui généralement sera à faibles performances et représentera un coût global très important. Soit des imprimantes beaucoup plus performantes seront partagées sur le réseau. Elles seront moins nombreuses et individuellement plus chères, mais globalement le coût sera moindre.
- Des services. L'accès Internet est le service partagé le plus répandu. Si tout le monde possède son propre accès Internet, il sera lent et peu sécurisé. S'il est centralisé, il sera plus performant, globalement moins couteux et, surtout, beaucoup plus facile à sécuriser. Il est plus simple de sécuriser un point unique qu'une multitude.

AVANTAGES

Le réseau apporte les avantages suivants :

- Une gestion plus efficace des ressources. Ces ressources pourront être de meilleure qualité, plus performantes, pour un coût global moindre.
  Prenons l'exemple de l'accès Internet. Dans le cas d'un accès individuel, vous serez limité par le débit, souvent faible, disponible sur votre connexion.
  En revanche, dans le cas d'un accès mutualisé, si vous téléchargez, par exemple, à un moment où personne n'est connecté à Internet, vous profiterez de toute la bande passante disponible, qui est souvent beaucoup plus élevée que les abonnements individuels.
- Une meilleure connaissance de l'utilisation des ressources. Il est simple, pour un administrateur, de connaitre l'utilisation précise des ressources réseaux. C'est plus délicat dans le cas de ressources individuelles. Ce qui permet, au passage, de mieux anticiper les besoins des utilisateurs et les limites de ces ressources.
- Des coûts d'utilisation plus bas. Le but étant d'obtenir un coût par utilisateur acceptable financièrement.
  Prenons le cas des imprimantes. Il en existe une multitude qui est bon marché, avec des performances basiques. En équiper chaque utilisateur implique rapidement un budget conséquent et des performances qui resteront basiques. Une ou plusieurs imprimantes partagées en réseau, apporteront des performances sans commune mesure avec les imprimantes individuelles. Si vous devez effectuer une impression de 1000 pages, cette impression sera réalisée beaucoup plus rapidement sur une grosse imprimante partagée que sur une petite imprimante locale. Sans parler des imprimantes fort coûteuses qu'il n'est pas envisageable d'installer sur chaque poste de travail, mais qui partagées en réseau, reviennent à un coût par utilisateur acceptable.
- Un niveau de sécurité plus élevé. Il est illusoire de penser que les postes de travail hors réseau sont plus sécurisés. Les données doivent, d'une façon ou d'une autre, être accessibles. Or, les virus et autres chevaux de Troie sont très confortablement transportés sur les disquettes, les cédéroms et autres clés USB. La sécurité doit être définie de façon globale. Il est préférable de surveiller les éléments sensibles plutôt que de tenter de les isoler.
  Enfin, plus le nombre de points à surveiller est faible, plus efficaces seront les outils de sécurité.
- Un meilleur niveau de communication. Il est plus simple pour les utilisateurs de communiquer entre eux à travers le réseau. Par messagerie instantanée, par mail, par téléphone, par vidéo.
- Des fonctionnalités nouvelles. L'évolution des techniques et des performances permet d'offrir aux utilisateurs des services dont ils ne disposaient pas précédemment, ou avec des contraintes différentes.
  La voix et la téléphonie sur IP (VoIP / ToIP) en sont les exemples récents. Cette convergence des ressources est une tendance lourde des réseaux actuels.

INCONVENIENTS

Mais les réseaux ont également quelques inconvénients :

- La disponibilité du réseau est devenue un élément critique de l'entreprise. Sans réseau, l'accès aux données est impossible ou limité.

- La complexité croissante des technologies implique une spécialisation et donc une segmentation des compétences. Il est parfois plus difficile d'isoler un problème, car le champ des possibles a crû avec les performances et la complexité des réseaux
- La maturité insuffisante de certaines technologies et les évolutions permanentes ne favorisent pas toujours la fiabilité et l'efficacité du réseau.
- Des faiblesses dans la sécurité peuvent devenir catastrophiques en réseau. Il est donc nécessaire de mettre en place une politique de sécurité globale et efficace.

Organismes

- IEEE
- ISO
- IETF / IAB
- UIT
- FCC
- ETSI

Les principaux organismes de normalisation ou de validation sont les suivants :

IEEE

Institute of Electrical and Electronical Engineers. Institut américain chargé de normaliser et standardiser tout ce qui concerne l'électrique et l'électronique. D'un point de vue réseau, cet organisme est essentiellement en charge des couches PHYSIQUE et LIAISON DE DONNEES.

Notamment, toutes les normes 802 émanent de l'IEEE.

ISO

International Standard Organisation. Organisme international de standardisation. Son influence sur les réseaux informatiques est moindre que l'IEEE. Néanmoins, c'est l'ISO qui a développé le mode de référence OSI qui est toujours utilisé.

IETF / IAB

L'IAB (Internet Architecture Board) est en charge du développement et de la promotion d'Internet. L'IAB est constitué de fabricants, d'éditeurs, de FAI/ISP (Fournisseurs d'Accès Internet / Internet Service Provider), d'experts, de représentants gouvernementaux…

IAB gère plusieurs agences, dont deux sont plus particulièrement connues :

- L'IETF, Internet Engineering Task Force. Elle est en charge de la publication des RFCs (Request For Comment). Ces documents définissent et standardisent les différents protocoles et applications gravitant autour d'Internet et de TCP/IP. Son rôle est donc très important dans les réseaux actuels.

- L'ICANN, Internet Corporation for Assigned Names and Numbers. Anciennement IANA, cette agence est en charge de l'attribution des adresses publiques, des noms de domaine, des numéros de protocoles, des numéros de ports et des numéros d'AS (Autonomous System).

UIT

Union Internationale des Télécommunications. Son rôle est axé sur les accords de convergence entre les différents organismes de télécom mondiaux. L'exemple le plus connu est le plan d'adressage téléphonique international.

FCC

Federal Communications Commission. Cette agence fédérale américaine définit et normalise les communications aux Etats-Unis et sert de référence pour les Amériques et bien souvent le reste du monde. Son influence est très forte, notamment en ce qui concerne les réseaux sans fils.

ETSI

European Telecommunications Standards Institute. Son rôle est similaire à celui de la FCC pour l'Europe.

Types de réseaux

- Topologies :
  - Point-à-point
  - Point-multipoint
  - Multi-accès
- Broadcast / non broadcast
- Commutation :
  - Commutation de trames / cellules
  - Commutation de circuits
- Connecté / non connecté

Il existe différents types de réseaux. Les différences portent sur les topologies disponibles, le support ou non de la diffusion, le mode de commutation et de connexion.

TOPOLOGIES

Il existe trois grandes catégories de topologies réseau :

- Point-à-point. Les machines sont directement connectées entre elles, deux par deux. Elles peuvent l'être physiquement, virtuellement ou logiquement. Par exemple, le protocole PPP (Point-to-Point Protocol) ne fonctionne qu'en point-à-point.
- Point-multipoint. Une machine peut accéder, via une même interface, à plusieurs autres machines. Frame-relay, X25 et ATM peuvent utiliser ce genre de topologie.
- Multi-accès. Via une interface, une machine peut atteindre toutes les machines d'un même réseau physique, logique ou virtuel. Le réseau le plus connu en multi-accès est bien évidement Ethernet.

BROADCAST

Il y a deux possibilités :

- Le réseau supporte la diffusion, ce qui implique un système d'adressage physique permettant de le faire, généralement sous la forme d'une adresse spécialement réservée à cet usage. En adressage Ethernet MAC, par exemple, c'est l'adresse FF.FF.FF.FF.FF.FF. La plupart des protocoles réseau supporte la diffusion. L'exception est plutôt le fait de ne pas la supporter.
  Les réseaux broadcast supportent généralement aussi les multicasts.

Le réseau ne supporte par la diffusion. Dans ce cas, les trames échangées ont soit une adresse physique de destination univoque, soit le réseau est point-à-point. Parmi les réseaux ne supportant pas la diffusion : ATM et, dans certains cas, Frame-Relay.

COMMUTATION

Le mode de commutation détermine comment les trames sont acheminées sur le réseau.

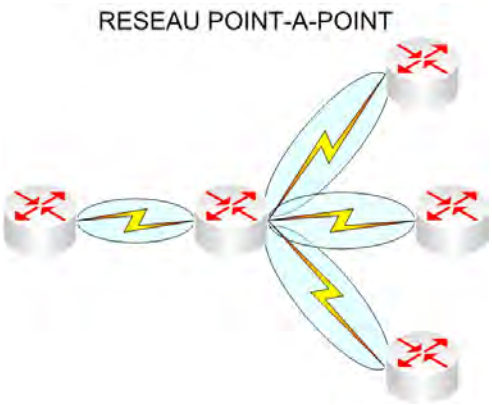
- La commutation de trames (souvent qualifiée à tort de commutation de paquets, qui existe également mais a une définition différente). Le principe est de traiter chaque trame indépendamment des autres. A chaque trame reçue, l'élément réseau chargé de son acheminement devra la traiter isolément de la précédente. Une cellule est simplement une trame de longueur fixe. Ethernet, Token Ring, FDDI et la plupart des réseaux de type LAN fonctionnent en commutation de trames.
- La commutation de circuit. Le principe consiste à établir un circuit, un chemin au préalable, avant toute émission de données. Une fois ce circuit établit, toutes les trames émises sur ce circuit virtuel seront acheminées de manière identique. Frame-Relay, ATM, X25, RNIS et RTC (Réseau Téléphonique Commuté) fonctionnent en commutation de circuit.

CONNEXION

Enfin, un réseau peut fonctionner en mode connecté ou non connecté.

- Mode connecté. Dans ce mode, il faut que la machine émettrice entre en contact avec la machine destinatrice avant toute émission de données proprement dite. Eventuellement, un certain nombre de paramètres peuvent être négociés pour la durée de la connexion. Par exemple, la taille de la fenêtre en réception, les numéros de séquences initiaux…
  SDLC et 802.2/LLC2 utilisent ce mode.
- Mode non connecté. Les données sont émises dès que l'adresse du destinataire ou le circuit virtuel sont connus. Autrement dit, sans s'assurer de la disponibilité du destinataire et sans aucune négociation préalable. Ethernet et 802.2/LLC1 utilisent ce mode.

Réseaux point-à-point



- Les machines sont connectées directement
- Les connexions peuvent être physiques, logiques ou virtuelles Elles sont dans le même réseau IP
- Il y autant de réseaux IP que de connexions point-à-point
- Très utilisé en PAN, en WAN et en MAN
- Beaucoup moins utilisé en LAN

RESEAUX POINT-A-POINT

Dans un réseau point-à-point, les machines sont directement connectées entre elles, deux par deux.

Elles peuvent être connectées :

- Physiquement, via des câbles directement reliés aux machines.
- Virtuellement, à travers une encapsulation dans un autre protocole. C'est le cas notamment des tunnels.
- Logiquement, à travers l'utilisation de circuits virtuels.

Deux machines connectées en point-à-point sont forcément dans le même réseau IP.

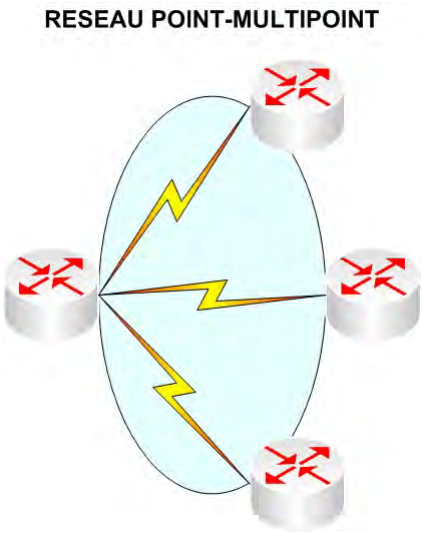
Il y a donc autant de réseaux IP que de connexions point-à-point.

Ce type de réseau est très utilisé :

- En PAN, les réseaux dits personnels. Par exemple les connexions Bluetooth.
- En WAN, les réseaux étendus. Par exemple en RNIS, RTC, X25 et Frame-Relay.
- En MAN, les réseaux métropolitains. Par exemple en ATM.

Beaucoup moins utilisé en LAN, les réseaux locaux.

Réseaux point-multipoint



- Les machines sont connectées directement
- Les connexions peuvent être logiques ou virtuelles
- Elles sont dans le même réseau IP
- Il y a un seul réseau IP
- Plutôt utilisé en WAN et en MAN
- Peu utilisé en LAN

RESEAUX POINT-MULTIPOINT

Dans un réseau point-multipoint, une machine peut atteindre directement plusieurs machines via la même interface.

Elles peuvent être connectées :

- Virtuellement, à travers une encapsulation dans un autre protocole. C'est le cas notamment des tunnels.
- Logiquement, à travers l'utilisation de circuits virtuels. C'est le cas le plus courant.

Toutes les machines connectées en point-multipoint sont toutes dans le même réseau IP.

Il y a donc un seul réseau IP pour un réseau point-multipoint donné.

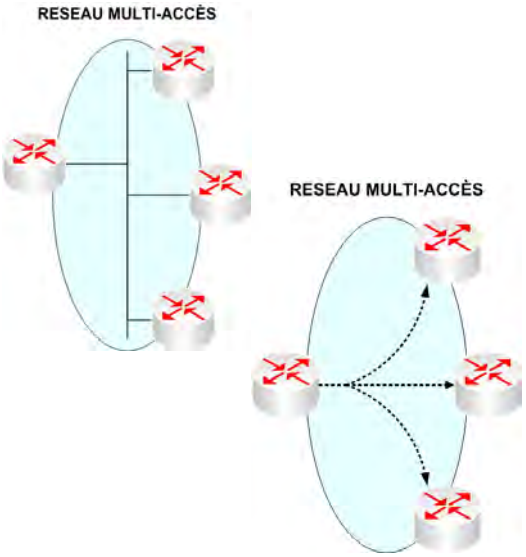
Ce type de réseau est plutôt utilisé :

- En WAN, les réseaux étendus. Par exemple Frame-Relay et X25.
- En MAN, les réseaux métropolitains. Par exemple en ATM.

Très peu utilisé en LAN, les réseaux locaux.

Une remarque d'ordre purement technique : les réseaux point-multipoint se différencient des réseaux multi-accès par leur topologie physique. En clair, un réseau point-multipoint est une juxtaposition de réseaux point-à-point utilisant un même réseau IP.
Par exemple, dans notre schéma, si le routeur de gauche veut diffuser une trame, il la répliquera sur chaque lien virtuel ou logique qui le connecte à chacun de ses voisins. En réseau multi-accès, une trame de diffusion suffira pour atteindre tous les destinataires.

Réseaux multi-accès



- Les machines ne sont pas forcément connectées directement
- Les connexions peuvent être physiques, logiques ou virtuelles. Elles sont dans le même réseau IP
- Il y a un seul réseau IP
- Très utilisé en LAN et en MAN
- Beaucoup moins utilisé en PAN et en WAN

RESEAUX MULTI-ACCES

Dans un réseau multi-accès, une machine peut atteindre directement plusieurs machines via la même interface.

Elles peuvent être connectées :

- Physiquement, généralement à un élément fédérateur de type hub ou commutateur.
- Virtuellement, à travers une encapsulation dans un autre protocole. C'est le cas notamment des tunnels.
- Logiquement, à travers l'utilisation des VLANs.

Toutes les machines connectées dans un réseau multi-accès sont généralement toutes dans le même réseau IP.

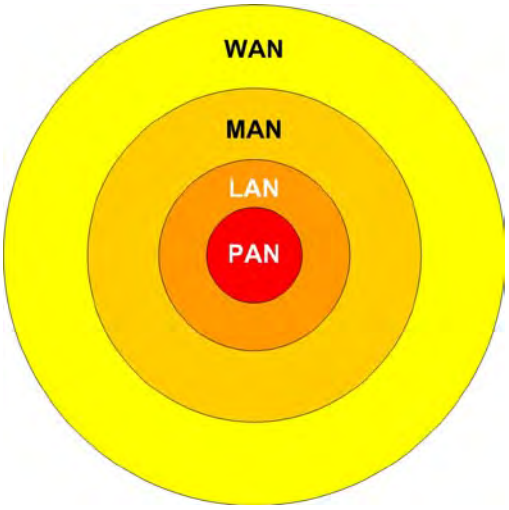
Il y a donc un seul réseau IP pour un réseau multi-accès donné.

Ce type de réseau est très utilisé :

- En LAN. Par exemple, Ethernet, Token Ring, FDDI…
- En MAN. Par exemple, 10G Ethernet, FDDI…

Très peu utilisé en PAN et en WAN.

Classification des réseaux



- PAN : Personal Area Network
  - Généralement point-à-point en homologue
  - Débits et distances faibles
- LAN : Local Area Network
  - Point-à-point ou centralisé
  - Débits élevés et distances moyennes
- MAN : Metropolitan Area Network
  - Point-à-point ou centralisé
  - Débits élévés et distances moyennes à longues
- WAN : Wide Area Network
  - Toute topologie
  - Débits faibles, longues distances

Les réseaux informatiques peuvent être classifiés en 4 grands groupes :

PAN

- Personal Area Network. Ce sont généralement des réseaux homologues point-à-point. Chaque intervenant joue un rôle identique, il n'y a pas de différentiation entre les machines.
- On utilise les PAN pour des connexions généralement ponctuelles et de courte durée.
- Les débits sont faibles, de l'ordre de quelques centaines de Kb au maximum.
- La technologie PAN la plus connue et la plus répandue est le Bluetooth.

LAN

- Local Area Network. Ce sont les réseaux les plus utilisés en entreprise. Ils sont généralement délimités physiquement sur un étage, un bâtiment ou un campus.
- La topologie peut être en point-à-point ou centralisée.
- Les distances sont faibles à moyennes. Quelques dizaines de mètres.
- Les débits sont plutôt élevés. Actuellement, les réseaux gigabit sont courants.
- Le rôle des LAN est de permettre aux utilisateurs d'accéder aux ressources partagées de l'entreprise.
- Généralement le matériel appartient à son utilisateur et il n'y a pas de facturation à l'usage.
- Aujourd'hui, Ethernet et WiFi représentent l'immense majorité des réseaux LAN déployés à travers le monde.

MAN

- Metropolitan Area Netwok. Tombés en quasi-désuétude il y a peu, ils sont revenus en force. Un MAN est un réseau à l'échelle d'une ville, d'un arrondissement, d'une zone industrielle ou commerciale.
- Le but d'un MAN est de permettre une interconnexion des réseaux d'entreprise plus performante et moins onéreuse que les WAN.
- La topologie peut être en point-à-point ou centralisée.
- Les distances sont faibles à moyennes. Quelques dizaines, quelques centaines de mètres.
- Les débits sont plutôt élevés. Actuellement, les réseaux gigabit et 10G sont courants.
- Généralement le matériel appartient ou est géré par un opérateur. Il y a facturation à l'usage.
    - Les réseaux MAN les plus répandus sont ATM et Gigabit/10G.

WAN

- Wide Area Network. Les WANs permettent d'interconnecter des réseaux d'entreprise à l'échelle d'un pays, d'un continent, de la planète.
- Tous les types de topologies existent.
- Les distances sont importantes, jusqu'à plusieurs milliers de kilomètres.
- Les débits sont généralement beaucoup plus faibles que ceux des MANs et des LANs. De l'ordre de quelques dizaines de Kb à plusieurs dizaines de Mb.
- Les réseaux WAN appartiennent et sont gérés par des opérateurs.
- Il y a facturation à l'usage. C'est en WAN que l'octet transporté est le plus cher.
- Parmi la myriade de technologies existantes citons : RNIS, RTC, X25, Frame-Relay, les liaisons satellites, GSM, GPRS, UMTS…

Présentation du modèle OSI

- ISO : International Standard Organisation
- Objectifs initiaux :
  - Formaliser le fonctionnement des couches réseaux
  - Fournir un modèle référentiel d'analyse pour tous les protocoles ou les applications fonctionnant sur un réseau
  - Permettre un fonctionnement inter-protocolaire

PRESENTATION DU MODELE OSI

L'ISO, International Standard Organisation, a élaboré le modèle OSI (Open Standards Interconnection) sous la référence ISO 7498. Même s'il est parfois critiqué et vilipendé, ce modèle reste une référence incontournable dans le monde des réseaux. Contrairement à des idées reçues, ce modèle a été inspiré par deux modèles antérieurs : TCP/IP et SNA d'IBM.

Le but était de proposer un modèle qui permettrait d'avoir une approche plus structurée et plus évolutive des réseaux.

Les objectifs initiaux étaient les suivants :

- Formaliser le fonctionnement des différentes couches, des différents composants d'un réseau.
- Fournir un modèle référentiel d'analyse pour tous les protocoles et les applications fonctionnant en réseau.
- Permettre un fonctionnement inter-protocolaire. Originellement, les couches devaient être interchangeables. Ce point, à de très rares exceptions, n'a jamais été respecté par aucun protocole réseau.

Le modèle OSI

- Le modèle OSI définit :
  - 7 couches représentant l'ensemble des entités de fonctionnement d'un réseau : Application, Présentation, Session, Transport, Réseau, Liaison de données, Physique
  - Le fonctionnement global de chacune de ces couches
  - Les règles de fonctionnement entre les couches
- Chaque couche possède une structure propre et des fonctions propres
- Les couches de même niveau dialoguent virtuellement directement entre elles en utilisant des PDUs (Physical Data Unit)
- Une couche doit pouvoir rendre des services aux couches supérieures

LE MODELE OSI

Le modèle OSI définit :

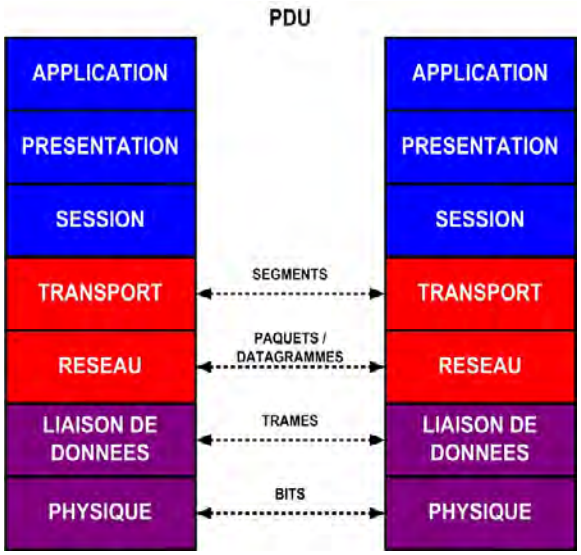
- 7 couches représentant l'ensemble des entités de fonctionnement d'un réseau :
  - ➔ Application
  - ➔ Présentation
  - ➔ Session
  - ➔ Transport
  - ➔ Réseau
  - ➔ Liaison de données
  - ➔ Physique.
- Le fonctionnement global de chacune de ces couches
- Les règles de fonctionnement entre les couches

Chaque couche possède une structure propre et des fonctions propres. Seul l'interfaçage avec les autres couches doit être standardisé.

Les couches de même niveau dialoguent virtuellement directement entre elles en utilisant des PDUs (Physical Data Unit).

Une couche doit pouvoir rendre des services aux couches supérieures. Celles-ci effectuent des appels de procédures standardisées.

Communication intra-couche

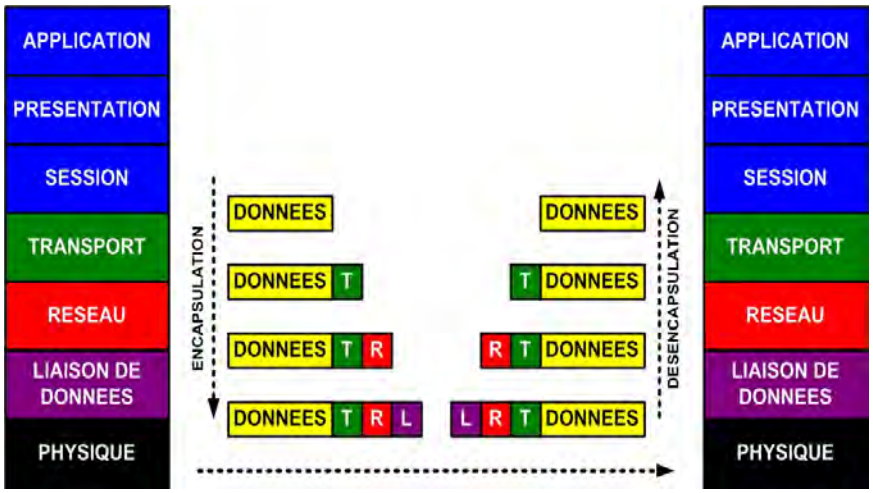


TERMINOLOGIE

Les couches réseaux de deux machines communiquent virtuellement directement entre elles. Pour cela elles utilisent des formats de données appelés PDU (Physical Data unit). La dénomination dépend de la couche OSI :

- Au niveau de la couche physique, on parle tout simplement de bits.
- Au niveau de la couche liaison de données, on parle de trames.
- Au niveau de la couche réseau on parle :
  - ➔ De datagrammes si le protocole fonctionne en mode non connecté. On parle de datagramme IP, par exemple.
  - ➔ De paquets si le protocole fonctionne en mode connecté. On parle ainsi de paquets X25.
    Il y a souvent un abus de langage à ce niveau. Même chez les éditeurs et les fabricants les plus sérieux on parle de paquets IP.
- Au niveau de la couche transport, on parle :
  - ➔ De datagrammes si le protocole fonctionne en mode non connecté. On parle de datagramme UDP.
  - ➔ De segments si le protocole fonctionne en mode connecté. On parle ainsi de segments TCP.
- Enfin, au niveau applicatif on parle simplement de données applicatives.

Encapsulation / désencapsulation



ENCAPSULATION

On procède à l'encapsulation quand les données « descendent » les couches. C'est-à-dire quand une machine émet des données. L'encapsulation peut avoir lieu à chaque traversée de couche.

Le principe est le suivant : une couche, lorsqu'elle transmet les données à la couche inférieure, ajoute un en-tête (header) et, éventuellement, un en-queue (trailer). Ces champs contiennent les informations nécessaires au traitement du PDU concerné. Autrement dit, les informations sont destinées à la couche homologue de la machine destinatrice.

DESENCAPSULATION

On procède à la désencapsulation quand les données « remontent » les couches. C'est-à-dire quand la machine reçoit des données. Elle a lieu à chaque traversée de couche.

Le principe est le suivant : une couche, lorsqu'elle reçoit les données de la couche inférieure, lit l'en-tête (header) et, éventuellement, l'en-queue (trailer). Ensuite, les données sont transmises à la couche supérieure.

EXEMPLE

Sur notre schéma les mécanismes suivants ont lieu :

ENCAPSULATION

- L'application transmet ses données à la couche transport.

- Celle-ci ajoute son en-tête et transmet le tout à la couche réseau.
- La couche réseau reçoit les données. Pour cette couche la charge utile est constituée des données de l'application et de l'en-tête de la couche transport.
- La couche réseau ajoute son en-tête et transmet le tout à la couche inférieure.
- La couche liaisons de données reçoit les données. Pour elle la charge utile est constituée des données applicatives et des deux en-têtes de la couche transport et de la couche réseau.
- La couche liaison de données ajoute son en-tête et transmet le tout à la couche inférieure, la couche physique.
- Cette dernière est la seule à ne jamais ajouter aucun champ à la trame qu'elle reçoit. Son rôle est de coder et de « déposer » sur le média les bits de données.

DESENCAPSULATION

- La couche physique du destinataire reçoit les bits, et les transmet à la couche liaison de données.
- Cette dernière lit l'en-tête et transmet uniquement les données, la charge utile, à la couche réseau appropriée…
- Qui procède de même : elle lit les champs qui lui sont destinés, les supprime et envoie le reliquat à la couche supérieure…
- Qui procède de même et ainsi de suite.

Couches « hautes »

- Application : Interface utilisateur
- Présentation : Représentation des données
  - Codage
  - Compression
  - Cryptage
- Session :
  - Connexion entre applications, client/serveur ou serveur/serveur
  - Négociation des paramètres de session
  - Fonctionnalités de sécurité

Les couches communément nommées « hautes » sont les trois couches les plus élevées dans le modèle OSI. Elles sont localisées au niveau des applications :

APPLICATION

La couche Application. Elle englobe tout ce qui est interfaçage avec l'utilisateur :

- CLI (Common Line Interface), les lignes de commandes.
- Les interfaces graphiques.
- Tout système permettant un échange interactif avec les utilisateurs.

PRESENTATION

La couche Présentation concerne toute représentation des données :

- Le codage des données. Les codages les plus connus sont ASCII et EBCDIC.
- La compression des données. Quelques exemples : ZIP, RAR.
- Le cryptage des données. Seul le destinataire pourra les lires en clair. Exemple : PGP.

SESSION

La couche Session fournit les fonctionnalités suivantes :

- Connexion entre les applications. Que ce soit en client/serveur ou en serveur/serveur. Cette couche en définit les modalités et les protocoles. Par exemple, pour accéder à une base de données SQL Server, il vous faut un client spécifique. Ce client inclut, entre autres, une couche session spécifique.

- Négociation des paramètres de session. Durée maximale de la validité d'une session, procédures de reconnexion, timers divers et variés…
- Sécurité. Par exemple, on peut choisir de crypter l'ensemble du trafic pour une application donnée entre deux machines. Certaines applications incluent leur propre protocoles de sécurité, d'autres utilisent le standard SSL/TLS.

Couches « réseau »

- Transport
  - Connexion hôte à hôte
  - Modes connecté et non connecté
  - Détection d'erreur
- Réseau
  - Adressage logique
  - Routage
  - Fragmentation / défragmentation des paquets
  - Détection d'erreur
  - Contrôle de flux

Les couches communément nommées « réseau » sont les deux couches intermédiaires dans le modèle OSI. Elles fonctionnent au niveau du système d'exploitation :

TRANSPORT

La couche Transport définit le mode de transport des données échangées entre les applications. Il existe deux modes principaux dans les réseaux informatiques :

- Le mode connecté. Un circuit est préalablement établi avant tout échange de données. Ce qui permet de s'assurer de la disponibilité du destinataire, de négocier des paramètres de session, de séquencer les segments et par voie de conséquence de fiabiliser les échanges. La détection d'erreur est quasi systématique dans ce mode. Enfin, certaines couches transports gèrent le contrôle de flux. TCP en est un bon exemple.
- Le mode non connecté. Les données sont expédiées dès que l'adresse du destinataire est connue. Souvent il n'y a pas de contrôle de flux, pas de séquencement des datagrammes, en conséquence, le mode est dit non fiable. La détection d'erreur n'est pas toujours implémentée dans ce mode.
  Toutefois, il existe un mode connecté avec accusé de réception et donc avec séquencement des datagrammes. Son usage reste très minoritaire.

RESEAU

La couche Réseau fournit les fonctionnalités suivantes :

- Adressage logique. Par opposition à l'adressage physique. Ce dernier est propre à une technologie, voire à une topologie donnée. Il est donc très complexe d'interconnecter des réseaux hétérogènes, puisque les systèmes d'adressage physiques ne sont pas compatibles entre eux.

La solution consiste à utiliser un adressage logique standard et normalisé. Il est ainsi possible d'interconnecter facilement des réseaux utilisant le même système d'adressage. L'adressage logique permet de faire abstraction de l'adressage physique pour l'acheminement des données entre les réseaux hétérogènes. L'adressage logique le plus utilisé est celui de TCP/IP.

- Routage. Le routage consiste à déterminer le meilleur chemin pour relier deux réseaux logiques. C'est un monde en soit.
- Fragmentation et défragmentation des paquets/datagrammes. Dans le cas où les données transmises par la couche transport excèderaient la charge utile maximale de la couche réseaux, celle-ci fragmente les données en autant de paquets ou de datagrammes que nécessaire.
- La détection d'erreur fait également partie de la panoplie de la plupart des protocoles de niveau 3. Il est à noter qu'IPv6 n'implémente justement plus cette fonctionnalité.
- Enfin, certaines couches réseau implémentent des mécanismes de contrôle de flux. C'est le cas de X25, par exemple. A contrario, IP laisse ce soin à TCP.

Couches « basses »

- Liaison de données
  - Adressage physique
  - Assemblage des bits en trames
  - Le mode : connecté ou non-connecté
  - Détection d'erreurs, correction optionnelle
  - Le contrôle de flux
  - Le protocole de couche supérieure destinataire des trames
- Physique
  - Spécifications physiques des médias
  - Codage des bits sur le média
  - Définition des interfaces

Les couches communément nommées « basses » sont les deux couches inférieures dans le modèle OSI.
Elles fonctionnent au niveau de la carte réseau :

LIAISON DE DONNEES

La couche liaison de données définit :

- L'adressage physique. Une adresse physique identifie de manière univoque une carte réseau. Deux machines communiquent réellement sur un réseau via ces adresses. Ethernet utilise les adresses MAC pour communiquer sur le réseau.
- L'assemblage des bits en trames. C'est à ce niveau que sont structurées les données.
- Le mode de communication. Il existe deux modes :
  - ➔ Le mode connecté. Un circuit est préalablement établi avant tout échange de données. Ce qui permet de s'assurer de la disponibilité du destinataire, de négocier des paramètres de session, de séquencer les trames et par voie de conséquence de fiabiliser les échanges. La détection d'erreur est quasi systématique dans ce mode. SDLC et 802.2/LLC2 fonctionnent selon ce mode.
  - ➔ Le mode non connecté. Les données sont expédiées dès que l'adresse du destinataire est connue. Souvent il n'y a pas de contrôle de flux, pas de séquencement des trames. En conséquence, le mode est dit non fiable. La détection d'erreur n'est pas toujours implémentée dans ce mode. Ethernet et 802.2/LLC1 fonctionnent dans ce mode.
    Il existe également un mode connecté avec accusé de réception et donc avec séquencement des trames. Il est réservé aux protocoles et applications temps réel et à l'informatique industrielle. 802.2/LLC3 fonctionne dans ce mode.

- La détection d'erreur. Elle est souvent implémentée sous la forme d'un calcul de redondance cyclique. En revanche, la correction d'erreur est beaucoup plus rare. Généralement la trame est simplement détruite. En mode connecté, l'émetteur en sera informé. En mode non connecté, l'émetteur ne le sera pas. La suppression sera dite silencieuse. C'est le cas d'Ethernet et de 802.3.
- Le contrôle de flux. Il est généralement associé au mode connecté, bien que ce ne soit pas une obligation absolue. Le contrôle de flux consiste à adapter le débit d'émission à la machine réceptrice ou aux performances du réseau. Dans les réseaux actuels, cette fonctionnalité est plutôt utilisée au niveau de la couche Transport. Ethernet et 802.2/LLC1 n'implémentent aucun contrôle de flux. C'est en revanche le cas pour 802.2/LL2 et 802.2/LL3.

PHYSIQUE

La couche Physique fournit les fonctionnalités suivantes :

- Spécifications des médias. Quel support pour transporter les bits ? Avec quelles caractéristiques ? L'air, le cuivre, la fibre optique sont les médias les plus usuels.
- Le codage des bits. Comment est codé un 1 ? Comment est codé un 0 ? Il existe plusieurs méthodes :
  - ➔ Par différents voltages électriques. Par exemple, +5v représente un 0 et -5v un 1. Ou inversement…
  - ➔ Par transition de tension électrique. Par exemple, une tension constante représente un 0 et un changement de tension un 1. Ou inversement…
  - ➔ Par impulsions lumineuses. Par changement de phases ou par niveau d'amplitude.
  - ➔ Par ondes radios. Par changement de phase ou niveau d'amplitude.
- Définition des interfaces. Quelles interfaces seront utilisées avec quels médias ? Par exemple, les interfaces les plus utilisées actuellement pour Ethernet sont : RJ 45 en cuivre et MIC ST en fibre optique.

Composants d'un réseau

- Carte réseau
- Répéteur
- Hub
- Pont
- Commutateur
- Routeur

Que faut-il pour constituer un réseau ? Quels en sont les composants ?
Nous allons aborder un bref descriptif de chacun de ces éléments.

Certaines interfaces et les hubs seront détaillés plus spécifiquement dans le chapitre suivant consacré à Ethernet.

Les ponts et les commutateurs seront détaillés dans le chapitre consacré à la commutation.

Enfin, le chapitre sur TCP/IP précisera le rôle des routeurs en IP.

Carte réseau

- Permet aux périphériques d'accéder au réseau
- Spécifique à chaque technologie réseau
- Formats disponibles : PCI, USB, PCMCIA…
- Certaines cartes sont multiports

CARTE RESEAU

Une carte réseau, ou adaptateur réseau, permet aux périphériques d'accéder au réseau.

Une carte réseau est spécifique à une technologie réseau : Ethernet, Token Ring, WiFi, ATM…

Les cartes réseaux sont disponibles sous différents formats :

- Intégrées à la carte mère. C'est quasiment systématique actuellement.
- PCI/PCIe est le format le plus répandu sur les postes fixes.
- USB. Plutôt adapté pour les portables.
- PCMCIA. Dédié au portable.

Il faut bien distinguer la carte réseau de son interface ou port. Le port n'est qu'un composant de la carte réseau.

Une carte simple possède une seule interface, un seul port. Certaines cartes peuvent gérer plusieurs ports. Ils peuvent être identiques ou différenciés.

Un poste de travail possède généralement une seule carte réseau avec un seul port.

Les serveurs ont de plus en plus des cartes multiports, ce qui permet de répartir la charge et de disposer de tolérance de panne.

Un routeur possède généralement plusieurs cartes réseaux simple ou multiport.

Répéteur

- Répète (amplifie) les signaux qu'il reçoit
- Fonctionne au niveau physique
- Elément « discret », n'a aucune action sur les trames
- Utilisation :
  - Dans les environnements hostiles
  - Quand les distances d'utilisation sont importantes

REPETEUR

Un répéteur est un élément très simple du réseau. Son rôle est de répéter, en l'amplifiant, les signaux qu'il reçoit. Il en existe de toutes sortes : électriques, radio, lumineux. On utilise également parfois le terme relais.

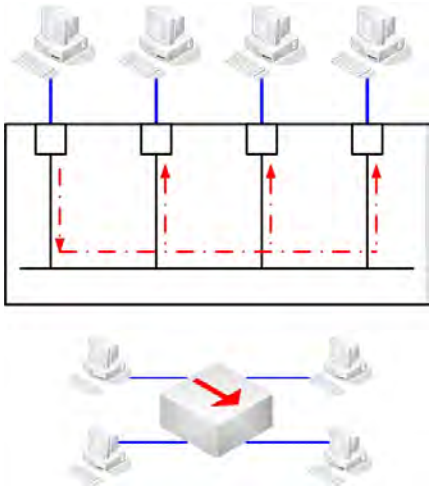
Un répéteur fonctionne purement au niveau physique. Il se contente d'amplifier les signaux qu'il reçoit. Si une trame est erronée, elle sera amplifiée telle quelle.

C'est un élément dit « discret », il n'a aucune action sur les trames. Il n'est donc normalement pas détectable sur le réseau.

On utilise un répéteur dans les cas suivants :

- Dans les environnements hostiles, très perturbés, quand des interférences affaibliront le signal, réduisant sa distance de propagation.
- Quand les distances d'utilisation sont importantes. Quand deux points sur le réseau sont séparés par une distance supérieure au maximum toléré par le média.

HUB



- Fonctionne au niveau physique
- Un hub constitue un domaine de collision
- Un hub définit un domaine de broadcast
- Un broadcast touche toutes les machines connectées
- Tous les périphériques partagent la même bande passante

HUB

Un hub est un composant d'infrastructure du réseau.

Il fonctionne au niveau physique.

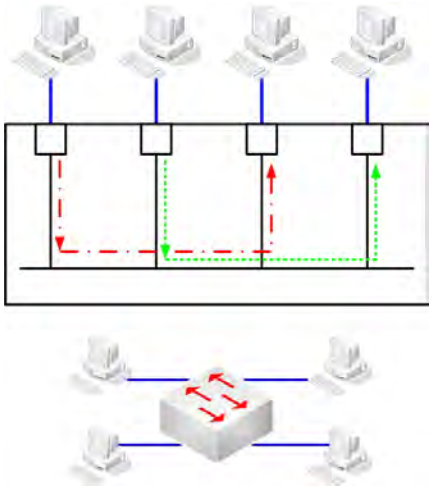
Tous les périphériques connectés à un hub sont dans le même domaine de collision. Autrement dit, le hub constitue un domaine de collision. Cela signifie qu'une seule des machines connectées peut émettre à un instant t. Quant une machine émet, les autres machines sont en réception.

Tous les périphériques connectés au hub sont dans le même domaine de diffusion. Ce qui implique que lorsqu'une machine émet une diffusion, l'ensemble des machines connectées au hub reçoivent cette diffusion.

Tous les périphériques connectés au hub partagent la même bande passante. Un hub 10 Mb/s signifie que son fond de panier fonctionne à 10 Mb/s.

Souvent, un hub fait également office de répéteur.

Pont & commutateur



- Fonctionnent au niveau de la couche liaison de données
- Commun :
  - Chaque port définit un domaine de collision
  - Un seul domaine de broadcasts
- Commutateur :
  - Bande passante garantie par port
  - Fond de panier beaucoup plus élevé
  - ASICs

PONT & COMMUTATEUR

Propriétés communes

Un pont ou un commutateur fonctionnent au niveau de la couche liaison de données. Ils font partie de l'infrastructure d'un réseau.

Les commutateurs sont une évolution des ponts.

Chaque port définit un domaine de collision. Autrement dit, plusieurs machines peuvent émettre simultanément sur un pont ou un commutateur.

Tous les périphériques connectés sont dans le même domaine de diffusion. Un pont ou un commutateur définissent un seul domaine de diffusion.

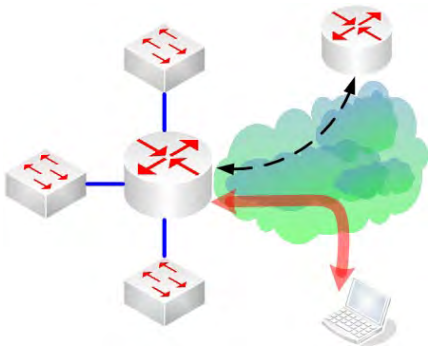
Spécificités des commutateurs

La bande passante est garantie par port sur un commutateur. Un commutateur fonctionnant à 100 Mb/s signifie que chaque port fonctionne à 100 Mb/s.

En conséquence, le fond de panier d'un commutateur est évidemment beaucoup plus performant que celui d'un pont.

Enfin, les commutateurs effectuent le maximum de tâches via des composants spécifiques dédiés, les ASICs.

Routeur



- Fonctionne au niveau de la couche réseau
- Un domaine de collision et de broadcast par port
- Adressage & routage logique
- Gestion du trafic
- Connexions WAN
- Accès des utilisateurs distants

ROUTEUR

Un routeur fonctionne au niveau de la couche réseau.

Un routeur définit un domaine de collision par port. Ce qui signifie qu'un routeur peut gérer plusieurs flux de données simultanément, sans collision.

Un routeur définit également un domaine de broadcast par port. Autrement dit, un routeur ne transmet pas un broadcast reçu sur une de ses interfaces sur les autres interfaces.

Il gère l'adressage logique, notamment celui de TCP/IP.

Un des rôles essentiels d'un routeur est le routage logique qui permet au routeur de déterminer le chemin optimum pour chaque réseau de destination.

La plupart des routeurs actuels permet également le routage des multicasts.

De plus en plus, les routeurs gèrent la qualité de service ou QoS, Quality of Service. La QoS permet de classifier et de définir les niveaux de priorité des différents flux applicatifs en tenant compte de leurs spécificités.

Ce sont également les routeurs qui généralement gèrent les connexions WAN.

Enfin, ils permettent les accès distants des utilisateurs, que ce soit via des connexions logiques ou des connexions VPN (Virtual Private Network).

- *Ethernet*
- *CSMA/CD*
- *Adressage MAC*
- *Topologies*
- *802.3*
- *802.2*

2

Ethernet

Objectifs

Ce module traite d'Ethernet.

Connaissance

- Présentation générale d'Ethernet
- La méthode d'accès réseau CSMA/CD
- L'adressage MAC
- Les topologies Ethernet
- Le câblage Ethernet
- Les formats de trames Ethernet II et 802.3/802.2

Progression

Présentation	Câblage cuivre
CSMA/CD	Câblage fibre
Adressage MAC	Normes IEEE
Topologies Ethernet	Format de trames

Présentation

- Ethernet a été défini par le « DIX » : Digital Intel Xerox
- C'est un réseau local s'appuyant sur un bus à diffusion : toutes les machines connectées au réseau partagent le même câble
- La gestion est répartie entre les postes connectés au réseau
- Fonctionnement en « Best-effort Delivery »
- Chaque carte réseau est identifiée par une adresse MAC
- Mécanisme d'accès au réseau : CSMA/CD

Ethernet est actuellement la technologie de réseau local informatique (LAN) la plus répandue. Elle a été développée par Xerox au début des années 70'. En 1978, elle a été standardisée par le groupe communément appelé DIX, pour Digital Intel Xerox.

Dans les années 80', l'IEEE l'a fait évoluer et l'a normalisée en 802.2/802.3.

PRINCIPES

- Ethernet est basé sur un bus à diffusion. Toutes les machines connectées au réseau partagent le même câble, la même bande passante. Ce qui signifie que toute trame émise par une machine est reçue par tous les éléments connectés au réseau.
- La gestion du réseau n'est pas centralisée, elle est répartie entre les postes connectés au réseau. Chaque machine gère donc son propre accès au réseau.
- Le fonctionnement est dit en « Best-effort Delivery », au mieux, sans garantie de remise. Ethernet ne fournit aucun mécanisme permettant à l'émetteur de savoir si les trames sont correctement transmises et traitées.
- Si une trame reçue est erronée, elle est simplement détruite. L'expéditeur n'en est pas informé.
- Chaque carte réseau est identifiée de manière unique par une adresse MAC.
- Le mécanisme d'accès au réseau est CSMA/CD.

CSMA/CD

- Ethernet utilise la technique CSMA/CD (Carrier Sense Multiple Access / Collision Detect) pour l'accès au réseau
- Fonctionnement :
  - L'émetteur écoute le réseau
  - Si le réseau semble libre, il émet, sinon, il attend jusqu'à ce que ce soit le cas
  - Il continue à écouter après l'émission de la trame
  - S'il détecte une collision, émission simultanée de deux postes, il réémettra après un temps aléatoire t
  - S'il y a toujours collision, il réémettra après 2t, puis 4t etc. jusqu'à 512t

Ethernet utilise la technique du CSMA/CD (Carrier Sense Multiple Access / Collision Detect) pour l'accès au réseau. Le principe est de détecter les éventuelles collisions. Une collision a lieu sur un réseau Ethernet lorsque deux machines émettent simultanément.

FONCTIONNEMENT DE CSMA/CD

- Lorsqu'une machine veut émettre sur le réseau, elle commence par écouter le réseau. C'est-à-dire détecter un signal émis par une autre machine. Le temps d'écoute dépend de la topologie Ethernet utilisée et du débit.
- Si le réseau semble libre, la machine émet sa trame. Si ce n'est pas le cas, elle attend jusqu'à ce qu'il le soit.
- Une fois la trame émise, la machine continue d'écouter afin de détecter une éventuelle collision.
- S'il y a collision, la machine attendra un temps aléatoire t avant de réémettre la trame.
- S'il y a toujours collision, la trame sera réémise après 2t. S'il y a toujours collision, elle sera réémise après 4t. Et ainsi de suite jusqu'à 512t.
- En cas d'échec final, l'accès au réseau sera désactivé sur la carte réseau par le pilote de la carte. Il sera réactivé automatiquement au bout d'un certains laps de temps, ou manuellement par l'utilisateur.

Trames Ethernet

- Il existe trois types de trames Ethernet :
  - Unicast : un à un. La source est unique, la destination est unique.
  - Broadcast : un à tous. La source est unique, la destination est FF.FF.FF.FF.FF.FF. Cette adresse signifie « toute machine du réseau ».
  - Multicast : un à certains. C'est de la diffusion sélective. La source est unique, la destination est une adresse de groupe.
- Règles d'adressage :
  - Une adresse source ne peut être ni une adresse de diffusion ni une adresse de groupe
  - Une carte réseau accepte par défaut le trafic Ethernet à destination de deux adresses MAC :

    Sa propre adresse MAC

    L'adresse de diffusion FF.FF.FF.FF.FF.FF

TYPES DE TRAMES ETHERNET

Il existe trois types de trames Ethernet :

- Les trames unicast, ou monodiffusion. L'adresse est unique, la destination est également unique. C'est le type de trame le plus utilisé. Il est utilisé pour les échanges entre deux machines clairement identifiées.
- Les trames broadcast, ou de diffusion. L'adresse source est unique, l'adresse destination est FF.FF.FF.FF.FF.FF. Cette adresse signifie « toute machine de ce réseau », elle est réservée à cet usage.
  Ce type de trame est utilisé :
  - ➔ Lorsque le destinataire n'est pas, ou pas encore, identifié par son adresse MAC. Par exemple, une machine connait l'adresse IP de la destinatrice, mais pas son adresse MAC. Elle va alors utiliser ARP afin de résoudre celle-ci, c'est-à-dire trouver l'adresse MAC associée à cette adresse IP. Pour cela, ARP envoie une diffusion à laquelle la machine destinatrice sera la seule à répondre.
  - ➔ Quand des données sont à destination de plusieurs machines. Cela permet de n'utiliser qu'une seule trame et évite de devoir résoudre les différentes adresses MAC des destinataires.
    Par exemple, une machine NetBIOS qui démarre. Elle va s'annoncer à toutes les autres machines déjà présentes. Il n'est pas nécessaire de connaitre leurs adresses MAC, ni leurs adresses IP d'ailleurs, au préalable. Le message est simplement informatif.

➔ Pour localiser dynamiquement certaines applications. L'identification se fera via le port utilisé au niveau de la couche transport.
Par exemple, un client DHCP envoyant une requête afin d'obtenir un bail d'adresse IP. Comme il ne connait pas l'adresse des serveurs, sa requête est envoyée en broadcast sur le port UDP 67.

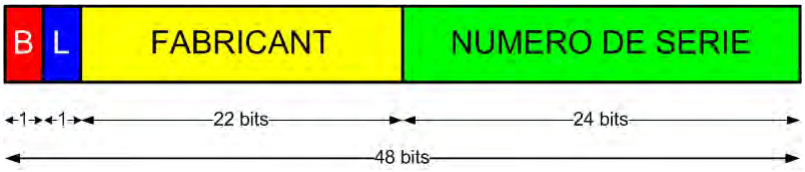
- Les trames multicast ou multidiffusion. L'adresse source est unique, la destination est une adresse de groupe. Une trame multicast ne sera traitée que par les machines ayant préalablement adhéré au groupe de destination. Les adresses de multicast utilisent une OUI spéciale : 01.00.5E. Le multicasting est surtout utilisé avec TCP/IP. La diffusion sélective permet d'obtenir le même dynamisme que les diffusions sans leurs inconvénients. Elle génère moins de pollution pour la pile IP, elle est contrôlable et elle est routable.

REGLES D'ADRESSAGE

Il existe un certain nombre de règles de base pour l'adressage MAC :

- Une adresse MAC source ne peut être ni une adresse de diffusion, ni une adresse de groupe. Ce qui parait logique et cohérent, une source ne pouvant être un groupe.
- Une carte réseau accepte par défaut le trafic Ethernet à destination de deux adresses MAC :
  - ➔ La propre adresse MAC de la machine (sa BIA)
  - ➔ L'adresse réservée de diffusion FF.FF.FF.FF.FF.FF.

Adressage MAC



- Adressage sur 48 bits en notation hexadécimale : XX.XX.XX.XX.XX.XX
- Unicité des adresses
- Le bit B (broadcast ?) positionné à 1 indique une diffusion ou une multidiffusion
- Le bit L (Local ?) positionné à 1 indique une adresse locale
- Le champ FABRICANT identifie le fabricant de la carte
- Le champ suivant indique le numéro de série de la carte réseau

---

Ethernet utilise comme adresses physiques les adresses MAC (Media Access Control).

TYPES D'ADRESSES MAC

Une adresse MAC est codée sur 48 bits, 6 octets. Elle permet d'identifier de manière unique une carte réseau. Il existe deux sortes d'adresses MAC :

- Les BIA, Burned In Address, qui sont enregistrées en « dur » sur la carte réseau par le fabricant. Cette adresse ne peut être modifiée et sa valeur est universelle. Cela signifie qu'aucune autre carte dans le monde n'aura la même adresse.
- Les adresses locales. Sur certaines cartes, il est possible d'indiquer une ou plusieurs adresses MAC supplémentaires gérées localement. Ces adresses ont une valeur uniquement locale.

NOMENCLATURE D'UNE ADRESSE MAC

Une adresse MAC a la structure suivante :

- 22 bits sont utilisés pour identifier le fabricant de la carte. Ce code, l'OUI, est fournit par l'IEEE.
- 24 bits sont utilisés pour le numéro de série de carte. Pour chaque code fabricant, un numéro de série ne peut être utilisé qu'une seule fois, ce qui donne l'unicité globale de l'adresse MAC du fabricant. Un fabricant peut donc, en théorie, produire avec un code OUI 2^24=16 millions de cartes. Pour en produire d'avantage, il devra obtenir un autre code OUI.
- Un bit BROADCAST. S'il est positionné à 1, cela signifie que l'adresse est de type diffusion ou multidiffusion.
- Un bit LOCAL. Il est positionné à 1 pour une adresse gérée localement.

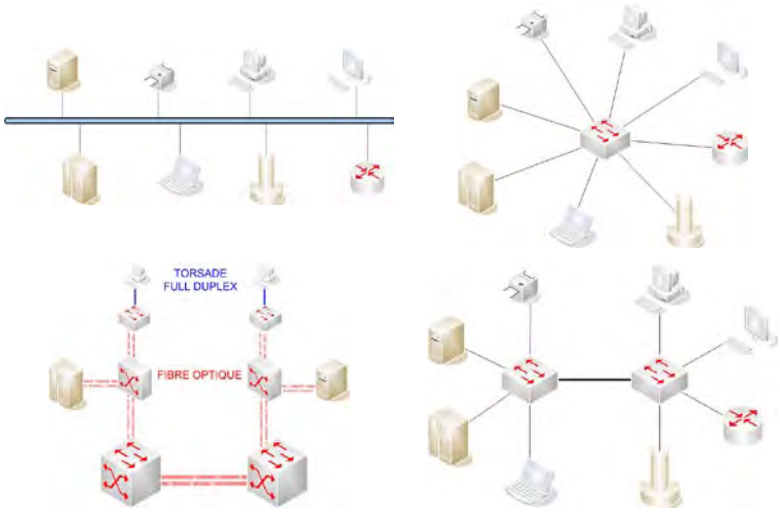
Topologies

- Il existe essentiellement quatre variantes de Ethernet :
  - Thick Ethernet, utilisant du câble coaxial épais
  - Thin Ethernet, utilisant du câble coaxial fin
  - A paires torsadées
  - Fibre optique
- La topologie logique de Ethernet est unique : bus à diffusion
- Il existe, en revanche, trois topologies physiques :
  - Bus, utilisée en Thick Ethernet et Thin Ethernet
  - Etoile, utilisée en paire torsadées
  - Point à point, utilisée en fibre optique

Il existe quatre variantes d'Ethernet :

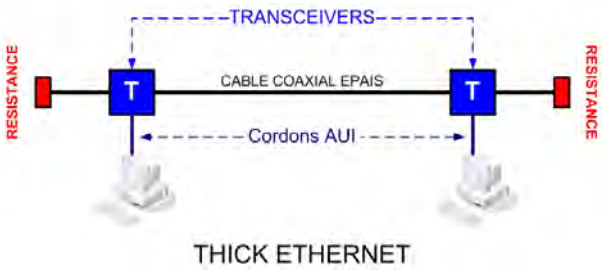
- Thick Ethernet, ou en Base5, qui utilise du câble coaxial épais.
- Thin Ethernet, ou en Base2, qui utilise du câble coaxial fin.
- Ethernet en BaseT, ou à paire torsadées.
- En fibre optique, en monomode et multimode.

Ethernet fonctionne selon une topologie logique de bus à diffusion. En revanche, il existe trois topologies physiques associées à Ethernet :



- Topologie bus. Elle est utilisée notamment par Thick Ethernet et Thin Ethernet. Le bus est matérialisé par le câble lui-même.
- Topologie en étoile. Elle est utilisée par Ethernet en paires torsadées. Le bus, dans ce cas, est localisé à l'intérieur du hub, auquel se connectent les machines.
- Point à point. Dans cette topologie, la détection de collision est désactivée. Elle est utilisée dans deux cas :
  - ➔ Avec la fibre optique. Pour relier deux machines, on utilise deux fibres unidirectionnelles. Aucun risque de collision. Les machines peuvent être deux commutateurs, deux ponts ou deux routeurs. On relie également les gros serveurs aux commutateurs avec de la fibre.
  - ➔ Paire torsadée en full duplex. Pour relier deux machines entre elles on utilise un câble croisé. Pour relier une machine, PC ou serveur, à un commutateur on utilise un câble droit. Là encore, il n'y a aucun risque de collision.

Thick Ethernet



THICK ETHERNET

- Standard 10Base5
- Fonctionne à 10Mb/s
- Utilise du câble coaxial épais
- Les cartes réseaux utilisent des prises AUI (15 broches)
- Les transceivers sont externes et permettent le raccordement au câble

Thick Ethernert est défini par le standard 10Base5. Il utilise du câble coaxial épais. Son débit nominal est de 10Mb/s.
Les cartes réseaux utilisent des prises AUI 15 broches et un cordon pour se connecter au transceiver. Celui-ci est externe et permet la connexion au réseau. Le transceiver utilisait souvent des prises dites vampire que l'on enfichait directement dans l'âme du câble. L'usage de cette topologie s'est rapidement limité aux interconnexions d'étages ou de bâtiments.

AVANTAGES

Les avantages du Thick Ethernet sont les suivants :

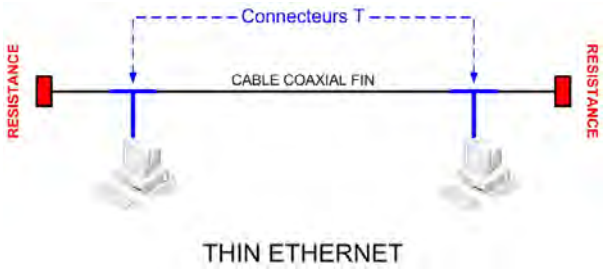
- La longueur maximale du câble est de 500m
- Peu sensible aux perturbations électromagnétiques
- Peu sensible aux vibrations (usage militaire ou aéroporté)
- Facile à installer

INCONVENIENTS

Les inconvénients du Thick Ethernet sont les suivants :

- Débit limité
- Evolutivité des connexions problématique. Les connexions par prises vampires ne sont pas adaptées à un changement fréquent de la topologie du réseau.
- Etendue du réseau limitée. Il est difficile d'entendre efficacement le réseau.

Thin Ethernet



THIN ETHERNET

- Standard 10Base2
- Fonctionne à 10Mb/s
- Utilise du câble coaxial fin
- Les cartes réseaux utilisent des prises coaxiales (connecteurs BNC)
- Les transceivers sont internes
- Des connecteurs, dit en T, permettent le raccordement au réseau

---

Thin Ethernert est défini par le standard 10Base2. Il utilise du câble coaxial fin. Son débit nominal est de 10Mb/s.
Les cartes réseaux utilisent des prises coaxiales de type BNC. Le transceiver est interne à la carte réseau.

AVANTAGES

Les avantages du Thin Ethernet sont les suivants :

- La longueur maximale du câble est de 186m
- Peu sensible aux perturbations électromagnétiques
- Facile à installer

INCONVENIENTS

Les inconvénients du Thin Ethernet sont les suivants :

- Débit limité
- Fonctionnement du réseau dépendant de tous les éléments connectés : câbles, connecteurs T, cartes réseaux, etc.
- Etendue du réseau limitée. Il est difficile d'entendre efficacement le réseau

Paires torsadées

- xBaseT : 10BaseT, 100BaseT, 1000BaseT et 10GBaseT
- Composants d'un réseau à paires torsadées :
  - Eléments passifs : les câbles, en 2 ou 4 paires torsadées
  - Eléments actifs : cartes réseau, hubs, ponts et commutateurs, routeurs
- Topologie physique en étoile
- Les connecteurs sont de type RJ45
- Longueur maximale entre deux points : 100m
- Deux modes duplex : half et full

La topologie Ethernet en paire torsadée est de loin la plus utilisée aujourd'hui. Elle est définie par les normes IEEE xBaseT. X désigne le débit supporté : 10, 100, 1000 et 10.000 Mb/s.

COMPOSANTS

Un réseau xBaseT est composé des éléments suivants :

- Les éléments passifs. Les câbles utilisent 2 ou 4 paires torsadées selon la catégorie utilisée. Les câbles utilisent des prises RJ45.
- Les éléments actifs, d'infrastructure :
  - ➔ Les cartes réseaux, dont le rôle est l'interfaçage entre le réseau et la machine.
  - ➔ Les hubs, qui hébergent le bus à diffusion.
  - ➔ Les ponts, qui permettent l'interconnexion de hubs et la segmentation des domaines de collision.
  - ➔ Les commutateurs, qui sont les successeurs des ponts dont ils reprennent les fonctionnalités en les améliorant et en y ajoutant de nouvelles, notamment les VLANs.
  - ➔ Les routeurs, qui apportent les fonctionnalités logiques de niveau 3 et permettent la segmentation des domaines de broadcast.

TOPOLOGIE

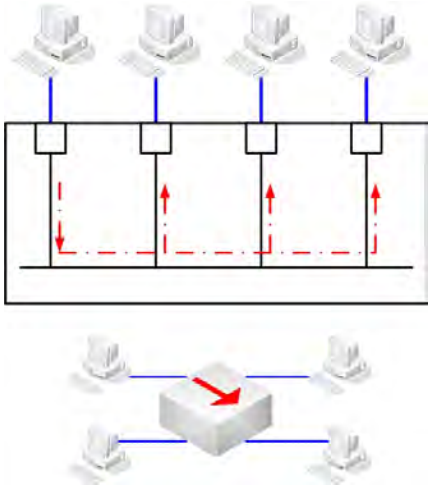
- La topologie physique est en étoile. Les machines sont connectées à un hub. Ce hub permet l'accès à un bus interne partagé entre toutes les machines qui y sont reliées.
- La longueur maximale entre deux points est de 100m.

DUPLEX

Il existe deux modes de connexion :

- Half duplex : fonctionnement normal entre des entités Ethernet. Une machine ne peut émettre et recevoir simultanément. Toute connexion à un hub utilise obligatoirement ce mode.
- Full duplex : fonctionnement en point-à-point. Une machine peut simultanément émettre et recevoir. Dans ce cas, la détection de collision est désactivée. Ce mode peut être utilisé :
  - ➔ Quand deux PCs ou deux serveurs sont directement connectés l'un à l'autre.
  - ➔ Quand deux commutateurs sont directement connectés l'un à l'autre.
  - ➔ Quand deux routeurs sont directement connectés l'un à l'autre.

Topologie en étoile



- Chaque élément utilisateur du réseau est connecté directement au hub
- Le hub héberge le bus à diffusion partagé
- Lorsqu'une machine émet, le trafic est dupliqué sur tous les ports, sauf celui de l'émetteur
- Un seul port, à un instant t, peut être émetteur sur un hub, les autres sont en réception
- Le seul mode accepté sur un hub est le half duplex

CARACTERISTIQUES

La topologie en étoile utilisée par xBaseT a les caractéristiques suivantes :

- Chaque élément utilisateur (PC, serveur, imprimante, routeur…) est connecté directement au hub.
- Le hub héberge le bus à diffusion partagé.
- Lorsqu'une machine émet, le trafic est dupliqué sur tous les ports, à l'exception du port émetteur.
- Donc, un seul port peut, à un instant t, être émetteur sur un hub. Tous les autres ports seront en réception.
- Un seul mode duplex est utilisable sur un hub : le half. En effet, une machine connectée à un hub ne peut à la fois émettre et recevoir.

AVANTAGES & INCONVENIENTS

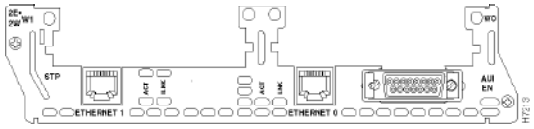
Avantages :

- Si un câble ou une carte réseau sont défaillants, cela n'impacte pas les autres éléments du réseau.
- Le câblage est très simple à réaliser.
- Le dépannage est facilité, on peut plus facilement isoler et localiser un problème.
- Le coût du matériel est faible.
- Les débits atteints sont beaucoup plus élevés que ceux des topologies physiques bus.

Inconvénients :

- La centralisation des connexions sur le hub en fait le point de faiblesse du réseau. En cas de défaillance de ce dernier, l'ensemble des machines est impacté.
- La sensibilité initiale aux perturbations.

Câblage cuivre



- Câbles RJ45 utilisés :
  - UTP, non blindés. Sensibles aux perturbations.
  - STP, blindés. Moins sensibles aux perturbations.
- Catégories de câbles : seules les catégories 3 à 7 sont utilisables pour Ethernet :
  - CAT3 permet d'atteindre 10Mb/s
  - CAT5 pour le 100Mb/s
  - CAT6 pour le Gbit/s
  - CAT7 pour le 10Gbit/s

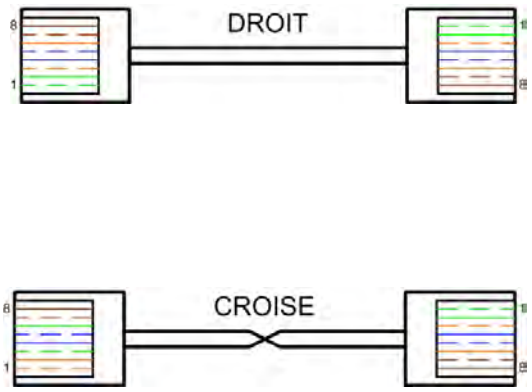
Il existe deux types de câbles en BaseT :

- UTP, (Unshielded Twisted-Pair), non blindés. Sensibles aux perturbations. Ils sont surtout utilisés pour les débits inférieurs au Gigabit Ethernet.
- STP, (Shielded Twisted-Pair), blindés. Moins sensibles aux perturbations. Ils sont utilisés à partir du Gigabit et dans les environnements très perturbés.

L'EIA/TIA (Electronic Industries Alliance / Telecommunications Industry Association) normalise les catégories de câbles. Il y a, actuellement, 7 catégories de câbles cuivre :

- CAT1, catégorie 1 : voix uniquement, inutilisable pour les données. Deux paires non blindées.
- CAT2, catégorie 2 : Quatre paires non blindées. Maximum 4Mb/s.
- CAT3, catégorie 3 : Quatre paires non blindées. 10Mb/s maximum.
- CAT4 : Quatre paires non blindées. 16 Mb/s maximum.
- CAT5 : Quatre paires blindées ou non. Surtout utilisé pour le 100Mb/s.
- CAT5E : Enhanced. Supporte le Gb/s.
- CAT6 : Quatre paires, chacune enveloppée d'un feuillard d'isolation. Un feuillard isolant supplémentaire est utilisé en plus pour chaque groupe de paires. Enfin, une gaine de plastique ignifugée recouvre cette deuxième couche isolante. Catégorie privilégiée recommandée pour le Gb/s. Il existe des améliorations en versions A et E.
- CAT7 : Chaque paire est enveloppée dans son propre blindage. Un blindage supplémentaire est utilisé pour chaque groupe de paires. Enfin, une gaine de plastique ignifugée recouvre cette deuxième couche de blindage. Catégorie préconisée pour le 10Gb/s.

Connectique



- Connectique des câbles :
  - Câble droit : les couleurs aux deux extrémités du câble sont agencées de la même façon. Utilisé pour connecter des machines ayant des rôles différents dans un réseau Ethernet.
  - Câble croisé : les couleurs aux deux extrémités du câble sont agencées de façon différente. Utilisé pour connecter entre elles des machines ayant des rôles similaires dans un réseau Ethernet.

Les câbles utilisés en Ethernet BaseT peuvent être droits ou croisés selon la connectique.

CABLES DROITS

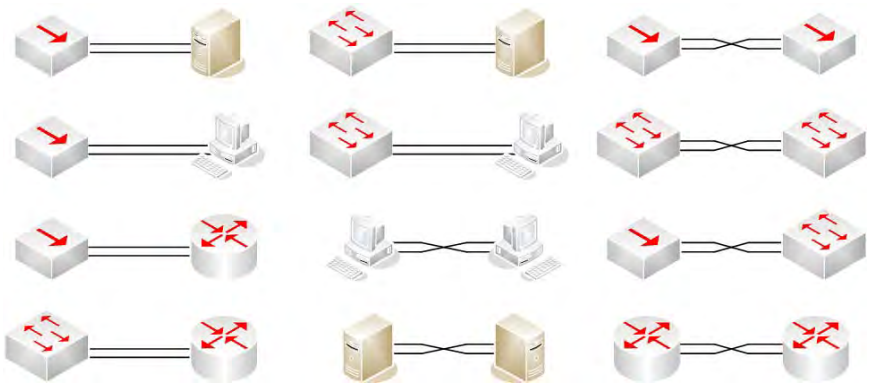
Les couleurs aux extrémités du câble sont agencées de la même façon. Les câbles droits sont les câbles les plus utilisés. Ils permettent de connecter des machines ayant des rôles différents dans un réseau Ethernet.
Par exemple :

- Un PC ou un serveur à un hub ou un switch
- Un routeur à un hub ou un switch

CABLES CROISES

Les couleurs aux extrémités du câble sont agencées de façon différente. Les câbles croisés sont utilisés pour connecter des machines ayant des rôles différents dans un réseau Ethernet.
Par exemple :

- Deux PCs ou deux serveurs entre eux
- Deux routeurs entre eux
- Deux hubs ou deux commutateurs entre eux

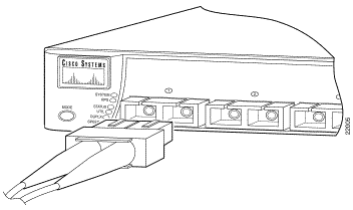


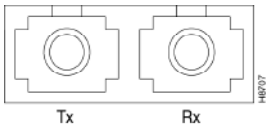
Normes Ethernet cuivre

	10Base2	10Base5	10BaseT	100BaseT	1000BaseT	10GBaseT
MEDIA	50Ω	50Ω	EIA/TIA CAT3-5 UTP 2 paires	EIA/TIA CAT5 UTP 2 paires	EIA/TIA CAT5-7 4 paires	EIA/TIA CAT6A & 7 4 paires
LONGUEUR MAX D'UN SEGMENT	186m	500m	100	100	100	100
TOPOLOGIE	BUS	BUS	ETOILE	ETOILE	ETOILE	ETOILE
CONNECTEUR	BNC	AUI	ISO 8877 (RJ45)	ISO 8877 (RJ45)	ISO 8877 (RJ45)	ISO 8877 (RJ45)

Ce tableau récapitule les principales normes physiques en câblage cuivre associées à Ethernet.

Fibre optique





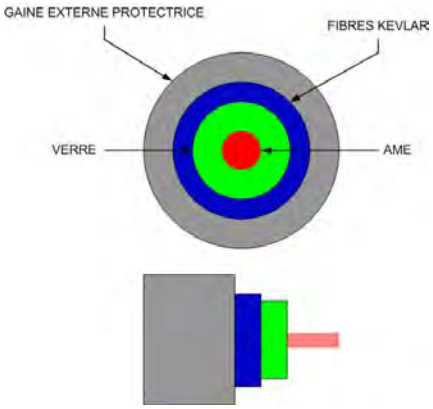
Connecteur Fibre

- Utilise un LED ou un LASER
- La fibre optique est disponible en deux modes : monomode ou multimode
- Full duplex en natif : on utilise deux fibres, une dans chaque sens
- Très grande évolutivité
- Très peu sensible aux perturbations
- Connecteurs : les plus répandus sont ST et SC

Ethernet est également utilisable sur fibre optique. La fibre optique transporte les bits informatiques sous forme d'impulsions lumineuses.
Les principales caractéristiques de la fibre optique sont les suivantes :

- Elle utilise comme source lumineuse un LED ou un LASER.
- Elle existe en deux modes : monomode et multimode.
- Elle fonctionne nativement en full duplex. Une fibre ne fonctionne que dans un seul sens. De fait, on connecte les machines entre elles en utilisant deux fibres, une dans chaque sens. La détection de collision est donc désactivée.
- Elle permet une très grande évolutivité. Il est possible de faire évoluer les éléments actifs, commutateurs, routeurs et cartes réseaux, tout en conservant le câblage fibre. La limite théorique, en débit propre à la fibre, est très loin d'être atteinte.
- La fibre optique est également très peu sensible aux perturbations électromagnétiques et environnementales.
- Enfin, proportionnellement au cuivre, le poids est nettement moindre.
- Les principaux connecteurs utilisés sont ST et SC.

Structure

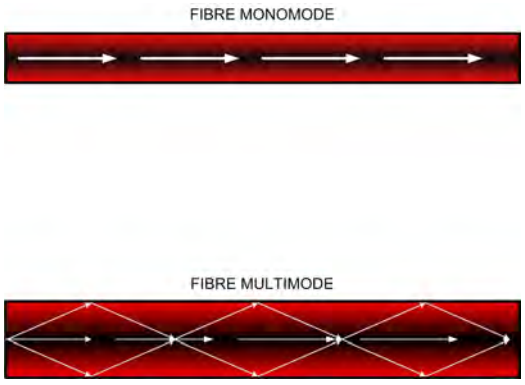


- L'âme, ou le cœur, contient la ou les fibre elles-mêmes
- Le verre protège le cœur et reflète les faisceaux lumineux
- Les fibres en Kevlar assurent un protection supplémentaire du cœur
- La gaine externe protège le câble des agressions physiques extérieures

Une fibre est composée des éléments suivants :

- L'âme centrale du câble ou cœur. C'est-à-dire la fibre optique elle-même. Il peut y en avoir plusieurs, selon le mode utilisé.
- Une couche de verre qui possède une densité différente de celle du cœur. Son rôle est de réfléchir les signaux lumineux transportés par le cœur. Une gaine intermédiaire en plastique opaque, enrobant le verre, assure l'absorption des éventuels faisceaux lumineux qui parviendraient à traverser la couche de verre.
- Des brins de fibres d'aramide en Kevlar. Ces brins de polymère évitent au câble d'être étiré et assurent une protection supplémentaire du cœur.
- Une gaine plastique extérieure protectrice, ou finale. Cette gaine protège le câble des agressions physiques extérieures de toute nature.

Mode



- Monomode :
  - Un seul faisceau en trajet direct
  - Très longues distances supportées
  - Performant mais cher
  - Utilise le LASER comme source lumineuse
- Multimode
  - Plusieurs chemins possibles pour le faisceau
  - Longues distances
  - Moins performant mais moins cher que le monomode
  - Utilise des LEDs comme source lumineuse

Deux types de fibres sont utilisées dans les réseaux informatiques : la fibre monomode et la fibre multimode.
Le mode est défini comme le nombre de chemins possible que peut emprunter un signal lumineux à travers une fibre.

MONOMODE

On parle également de SMF, Single Mode Fiber. Le signal lumineux ne peut emprunter qu'un seul chemin, il utilise un trajet direct. La fibre monomode est plus performante que la fibre multimode. En revanche, cela nécessite l'utilisation d'une source lumineuse très puissante. Généralement, ce sont des LASER qui sont utilisés. Actuellement, on atteint des distances de plusieurs dizaines de kilomètres entre deux points.

La fibre monomode est plutôt utilisée pour les longues distances. Ce sont généralement les opérateurs et les FAI/ISP qui les utilisent.

MULTIMODE

On parle également de MMF, Multi Mode Fiber. Dans ce mode, le signal lumineux peut emprunter plusieurs chemins. Ce type de fibre est moins performant que le monomode, mais beaucoup moins onéreux et plus souple d'utilisation. Ce sont des LEDs qui sont utilisés comme sources lumineuses. Les distances sont plus courtes que celles supportées par le monomode.

La fibre multimode est particulièrement utilisée dans les réseaux d'entreprise.

Connecteurs

- Connecteur SC :
  - Verrouillage coulissant
  - Adapté aux usages bureautiques et particuliers
  - Plutôt associé au multimode

- Connecteur ST :
  - Verrouillage à baïonnette
  - Adapté aux réseaux hautes performances
  - Utilisé en mono comme en multimode

Deux connecteurs sont majoritairement utilisés en fibre optique Ethernet :

CONNECTEUR SC

Le connecteur le plus simple. Il est souvent associé à de la fibre en multimode. Il intègre un verrouillage coulissant.
Il est adapté :

- Aux usages bureautiques, pour la connexion des postes de travail
- Aux connexions audio/vidéo domestiques
- Aux connexions pour le câble et le satellite

CONNECTEUR ST

C'est un connecteur plus évolué que le SC. Il peut aussi bien être associé à la fibre monomode que multimode. Le verrouillage est de type baïonnette.
Il est adapté aux exigences hautes performances :

- En usage réseau : interconnexion des commutateurs, liens intersites, liens SAN…
- En connexion des serveurs hautes performances
- Au cœur des réseaux opérateurs

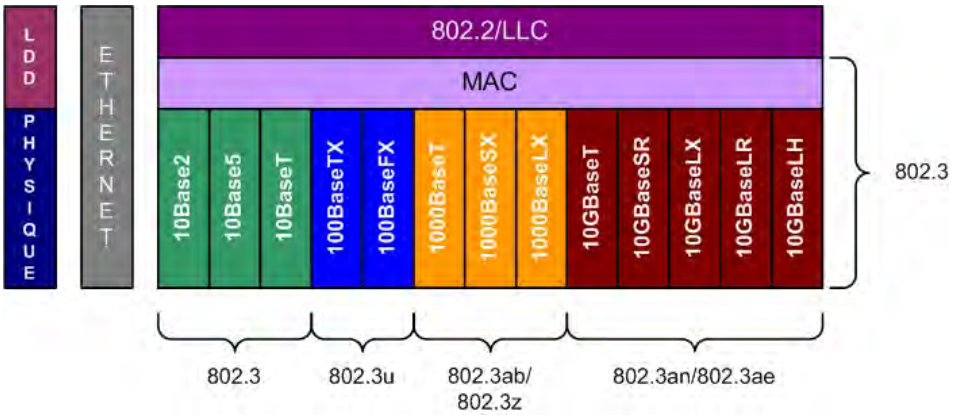
Normes Ethernet fibre

	100BaseFX	1000BaseSX	1000BaseLX	1000BaseLX	1000BaseLH	10GBaseSR	10GBaseLX4	10GBaseLX4	10GBaseLR
MEDIA	62,5/128µ multimode	62,5/128µ multimode	62,5/128µ multimode	9µ monomode	9µ monomode	62,5/128µ multimode	62,5/128µ multimode	9µ monomode	9µ monomode
LONGUEUR MAX D'UN SEGMENT	>2km	275-550m	550m	3-10km	70km	26-82m	240-300m	10km	10-40km
TOPOLOGIE	Pt-à-pt	Pt-à-pt	Pt-à-pt	Pt-à-pt	Pt-à-pt	Pt-à-pt	Pt-à-pt	Pt-à-pt	Pt-à-pt
CONNECTEUR	MIC ST	MIC ST	MIC ST	MIC ST	MIC ST	MIC ST	MIC ST	MIC ST	MIC ST

Le tableau récapitule les principales normes Ethernet en fibre optique :

- 100BaseFX : multimode, vitesse de 100Mbps, portée de 2 km.
- 1000BaseLX : monomode, vitesse de 1Gbps, portée de 3 km.
- 1000BaseLX : multimode, vitesse de 1Gbps, portée de 550 m.
- 1000BaseSX : multimode, diamètre de 50 micromètres, vitesse de 1Gbps, portée de 550 m.
- 1000BaseSX : multimode, diamètre de 64 micromètres, vitesse de 1Gbps, portée de 275 m.
- 1000BaseLH : vitesse de 1Gbps, portée de 70 km.
- 10GBaseSR : multimode, vitesse de 10Gbps, portée de 26 à 82 m.
- 10GBaseLX4 : multimode, vitesse de 10Gbps, portée de 240 à 300 m.
- 10GBaseLX4 : monomode, vitesse de 10Gbps, portée de 10 Km.
- 10GBaseLR et 10GBaseER : monomode, vitesse de 10Gbps, portée de 10 à 40 Km.

Implémentations de la couche Physique



Ce tableur récapitule les principales normes de l'IEEE concernant les implémentations de la couche Physique liées à Ethernet :

- 802.3 définit Ethernet en 10Mbps avec les normes cuivre 10Base2, 10Base5 et 10BaseT.
- 802.3u définit Ethernet en 100Mbps, ou FastEthernet, avec les normes :
- 100BaseTX en cuivre
- 100baseFX en fibre
- 802.3ab (cuivre) et 802.3z (fibre) définissent Gigabit Ethernet avec les normes :
- 1000BaseT en cuivre
- 1000BaseSX et 1000BaseLX en fibre
- 802.3an (cuivre) et 802.3ae (fibre) définissent 10G Ethernet avec les normes :
- 10GBaseT en cuivre
- 10GBaseSR/LX/LR/LH en fibre

Il est à noter qu'en 10G, le mode half duplex n'est plus supporté. Toutes les connexions se font obligatoirement en full duplex.

Trames Ethernet

- Il existe deux formats de trames Ethernet :
  - Ethernet proprement dit ou Ethernet DIX (Digital Intel Xerox), actuellement en version II, qui ne supporte qu'un seul mode de fonctionnement : non connecté, sans accusé de réception
  - La version normalisée par l'IEEE, 802.2/802.3, qui permet de définir au travers de sa couche 802.2/LLC différents modes de fonctionnement :

    LLC1 : mode non connecté, sans accusé de réception.

    LLC2 : mode connecté, avec accusé de réception.

    LLC3 : mode non connecté, avec accusé de réception.
- Les cartes réseaux modernes supportent les deux formats de trames

---

Il existe deux formats de trames Ethernet :

ETHERNET DIX

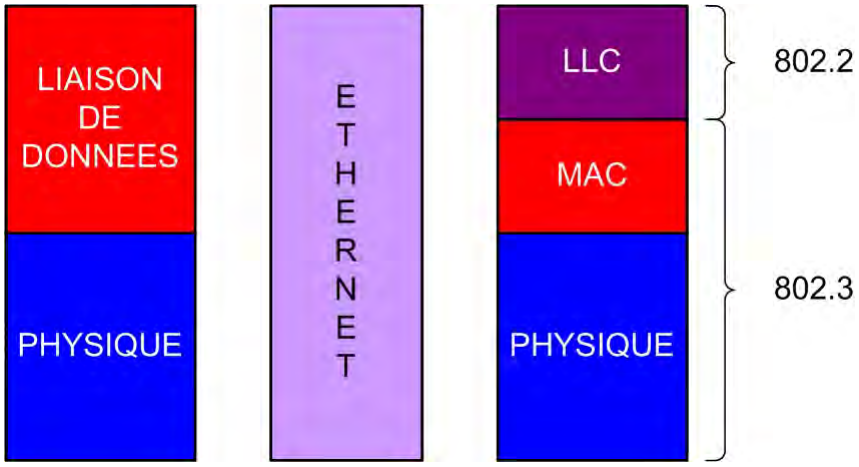
C'est le format d'origine, actuellement en version II. Il a été légèrement modifié, notamment en ce qui concerne le champ TYPE. Dans ce format, Ethernet ne supporte qu'un seul mode de fonctionnement : non connecté sans accusé de réception. Autrement dit, le mode non fiable d'origine.
Ce format de trame est encore très utilisé car très facile à implémenter et, surtout, en adéquation avec le fonctionnement de TCP/IP. Ce dernier fonctionne lui-même en mode non fiable. Pourquoi fiabiliser la couche 2 si la couche 3 ne l'est pas ?
La fiabilité est assurée soit par l'utilisation de TCP, soit par l'application elle-même dans le cas de l'utilisation d'UDP.

802.2/802.3

C'est la version standardisée de l'IEEE. Dans ce format, trois modes sont supportés :

- LLC1 : mode non connecté, sans accusé de réception. Fonctionnement identique à Ethernet II. Utilisé par défaut par IP et la plupart des protocoles réseau en mode non connecté.
- LLC2 : mode connecté, avec accusé de réception. Prévu à l'origine pour le transport du protocole SNA de IBM.
- LLC3 : mode non connecté, avec accusé de réception. Utilisé surtout en informatique industrielle et en environnement temps réel.

802.2/802.3



La norme Ethernet définit une seule couche, monolithique. Cette couche assure les fonctions correspondantes à celles des couches PHYSIQUE et LAISON DE DONNEES du modèle OSI.

La norme IEEE 802.2/802.3 définit, elle, trois couches : PHYSIQUE, MAC et LLC (Logical Link Control). Afin de ne pas avoir 8 couches en OSI, les couches PHYSIQUE et MAC sont regroupées sous le terme 802.3. La couche LLC est désignée par 802.2.

Cette évolution est née du besoin d'IBM de pouvoir transporter du trafic SNA sur les réseaux locaux. SNA est à la fois une architecture et une pile de protocoles propriétaires IBM. Or, SNA ne peut être transporté que sur deux types de réseaux : les réseaux dédiés SNA sur du matériel spécifique et dédié, et sur les réseaux supportant le protocole de niveau deux SDLC (Synchronous Data Link Control). IBM avait en effet précédemment adapté SNA pour pouvoir le transporter sur les réseaux WAN. Comme il était beaucoup trop compliqué d'adapter directement SNA sur Ethernet et sur les autres topologies locales, IBM a préféré faire évoluer Ethernet. Cette évolution a donné, après normalisation, le 802.2/802.3.

802.3

La couche physique assure les mêmes fonctions que celles définies dans le modèle OSI :

- Codage des bits
- Spécification des médias
- Définition des interfaces

La couche MAC assure les fonctions essentielles de la couche liaisons de données :

- Adressage physique. La couche MAC utilise les adresses éponymes identiques à celle de Ethernet.
- Identification de la couche supérieure. Elle est implicite, en 802.3 on transporte toujours du 802.2.

802.2

Cette couche permet l'interfaçage avec les couches supérieures, les couches réseaux. Elle définit également le mode de fonctionnement utilisé pour l'échange des données entre l'émetteur et le récepteur. Il y a, comme nous l'avons vu, trois modes de fonctionnement :

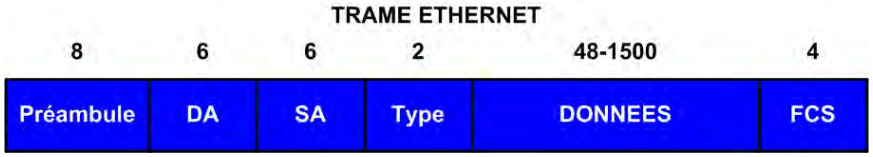
- LLC1. Ce mode reprend le mode de fonctionnement d'Ethernet II, le mode non connecté. Aucune fiabilité n'est assurée. Pas de séquencement des trames, pas d'accusé de réception, pas de contrôle de flux, pas de retransmission. C'est le mode privilégié pour le transport de datagrammes IP et des principaux protocoles réseau.
- LLC2. Ce mode fonctionne en mode connecté fiable. Il émule le fonctionnement de SDLC. Les trames sont séquencées et acquittées. Le contrôle flux est possible. C'est le mode utilisé pour transporter SNA d'IBM.
- LLC3. Ce mode fonctionne en mode non connecté mais avec accusé de réception. Ce mode « intermédiaire » entre les deux précédents permet d'obtenir des temps d'acheminement courts et surtout offrant peu de variation, peu de décalage dans les délais de transmission. Ce qui est idéal pour le transport des données en temps réel ou les réseaux industriels.

Il est donc possible grâce à 802.2 de pouvoir choisir le mode de fonctionnement réseau de la couche deux adapté aux besoins d'un protocole ou d'une application.

Il est à noter également que la norme 802.2/802.3 offre une évolutivité plus importe que Ethernet II. Il est en effet possible de faire évoluer la couche LLC sans réécrire la couche MAC, et réciproquement.

Enfin, la quasi-totalité des cartes réseaux actuelles supporte les deux formats de trames.

Trame Ethernet II



- DA : Adresse MAC du destinataire
- SA : Adresse MAC de l'émetteur
- Type : Code du protocole de niveau 3 destinataire des données transportées
- Données : Contient les données transportées
- FCS : Calcul de redondance cyclique permettant de vérifier l'intégrité de la trame

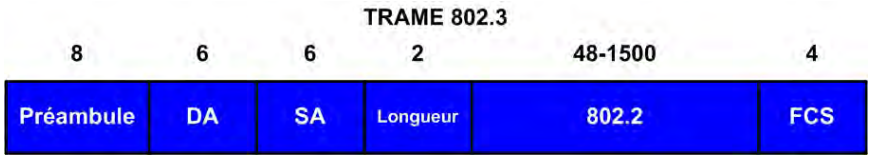
---

Le format d'une trame Ethernet II est le suivant :

- Un préambule sur 8 octets. Ce préambule est constitué d'une suite alternée de 0 et de 1. Il sert à synchroniser les horloges en lecture.
- Le champ DA, pour Destination Address, sur 6 octets. Il contient l'adresse MAC du destinataire.
- Le champ SA, pour Source Address, sur 6 octets. Il contient l'adresse MAC source, celle de l'émetteur de la trame.
- Le champ type, sur deux octets, contient le code du protocole réseau destinataire des données transportées par Ethernet. Par exemple 0x800 pour IP, 0x806 pour ARP.
- Le champ données est variable, compris entre 48 et 1500 octets.
- Le champ FCS, pour Frame Check Sequence, sur 4 octets. Il contient la somme de contrôle de la trame. Ce qui permet au destinataire de vérifier l'intégrité de la trame en refaisant le même calcul et de comparer le résultat à la valeur contenue dans ce champ.

Il est à noter ici que le destinataire ne connait pas, a priori, la longueur de la trame puisque rien n'indique la longueur du champ DONNEES. Ce ne sera possible qu'une fois la trame reçue dans son intégralité. Il n'est donc pas possible d'enchainer les trames, comme on le faisait en SDLC par exemple.

Trame 802.3



- DA : Adresse MAC du destinataire
- SA : adresse MAC de l'émetteur
- Longueur : indique la longueur totale de la trame
- 802.2 : contient l'en-tête 802.2 et les données transportées par celui-ci
- FCS : Calcul de redondance cyclique permettant de vérifier l'intégrité de la trame

Le format d'une trame 802.3 est le suivant :

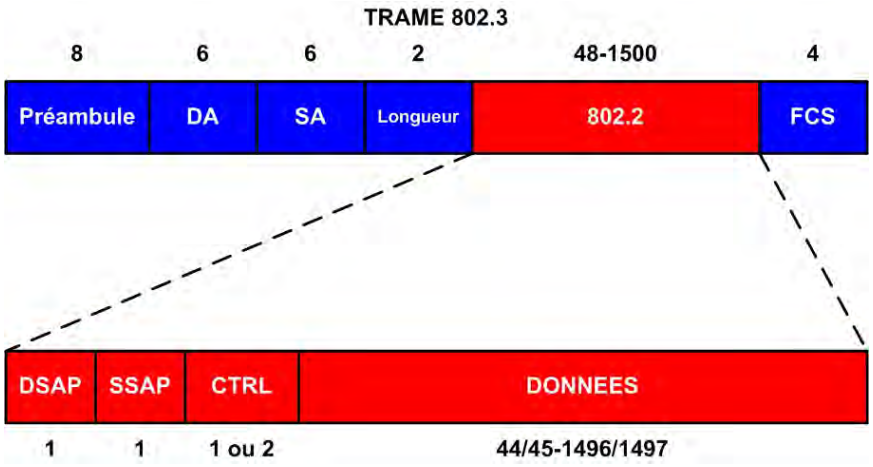
- Un préambule sur 8 octets. Ce préambule est constitué d'une suite alternée de 0 et de 1. Il sert à synchroniser les horloges en lecture.
- Le champ DA, pour Destination Address, sur 6 octets. Il contient l'adresse MAC du destinataire.
- Le champ SA, pour Source Address, sur 6 octets. Il contient l'adresse MAC source, celle de l'émetteur de la trame.
- Le champ longueur, sur deux octets. La valeur maximale est de 1518, ce qui correspond à la longueur maximale d'une trame Ethernet (on ne compte pas le préambule).
- Le champ 802.2 est variable, compris entre 48 et 1500 octets.
- Le champ FCS, pour Frame Check Sequence, sur 4 octets. Il contient la somme de contrôle de la trame. Ce qui permet au destinataire de vérifier l'intégrité de la trame en refaisant le même calcul et de comparer le résultat à la valeur contenue dans ce champ.

Il est à noter ici que le destinataire connait la longueur de la trame puisque qu'elle est indiquée. Il est donc possible d'enchainer les trames, comme on le faisait en SDLC. De plus, on ne donne aucune indication sur le protocole de niveau supérieur transporté puisqu'en 802.3 c'est obligatoirement du 802.2. Il existe deux formats de trames 802.2 : SAP et SNAP.

Une question pertinente peut se poser ici : comment une carte réseau fait la distinction entre une trame Ethernet II et 802.3 ? Selon la valeur contenue dans le champ longueur/type :

- Si la valeur est strictement supérieure à 1518, cela signifie que le champ lu est le champ type. On est donc en présence d'une trame Ethernet II.
- Si la valeur est inférieure ou égale à 1518, cela signifie que le champ lu est le champ longueur. C'est donc une trame au format 802.3.

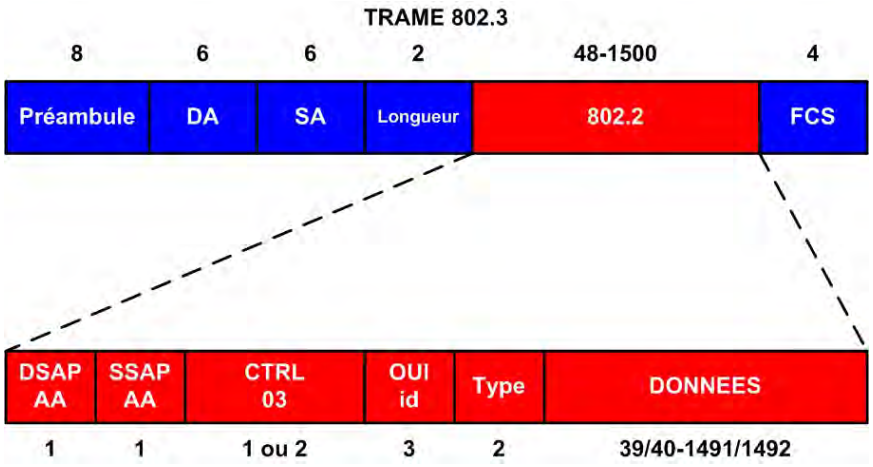
Trame 802.2/SAP



Le format d'une trame 802.2/SAP est le suivant :

- Le champ DSAP, pour Destination SAP sur 1 octet. Le SAP, Service Access Point, est le protocole destinataire de la trame. Les valeurs facteur de 4 sont réservées pour SNA.
- Le champ SSAP, pour Source SAP sur 1 octet. Il peut paraître étonnant de devoir préciser le protocole destination et source. En Ethernet II, le protocole destinataire est aussi le protocole émetteur, ce qui est indubitablement logique.
  Mais en SNA rien de tel, les mécanismes et les protocoles ne sont pas symétriques. SNA est une architecture entièrement centralisée : un maître ne communique pas avec un esclave de la même manière que celui-ci communique avec lui.
  Pour les autres protocoles, et notamment TCP/IP, les champs DSAP et SSAP sont identiques.
- Le champ CONTROL sur 1 ou 2 octets. Ce champ est utilisé pour la signalisation réseau de Ethernet. Dans le cas du LLC1, ce champ a une longueur de 1 octet. Dans le cas des LLC2 et LLC3, il a une longueur de 2 octets. Ce qui est logique, car pour ces deux modes, il faut séquencer les trames et les acquitter.

Trame 802.2/SNAP



Le format SNAP (Sub-Network Acces Point) a été développé pour permettre à un éditeur ou à un fabricant de matériel de définir et utiliser ses propres protocoles.
Avec Ethernet II, pour chaque protocole réseau de niveau 3, il faut demander à l'IEEE un code TYPE. Idem pour 802.2/SAP, il faut obtenir un code DSAP/SSAP.
Avec SNAP les choses sont plus simples : il « suffit » d'obtenir un code OUI identifiant spécifiquement l'éditeur ou le constructeur. Ainsi, par exemple, CISCO dispose du code 00.00.0C. Il peut donc ainsi définir, grâce au champ TYPE, 65536 protocoles propriétaires. Et, à chaque nouvelle création de protocole, inutile d'en référer à l'IEEE. Souvent les codes OUI fournis sont les mêmes que ceux attribués pour l'adressage MAC.

Le format d'une trame 802.2/SNAP est le suivant :

- Le champ DSAP est égal à AA, qui est une valeur réservée pour identifier les trames SNAP.
- Le champ SSAP est égal à AA, qui est une valeur réservée pour identifier les trames SNAP.
- Le champ CONTROL est égal à 0x03 pour les trames SNAP.
- Le champ OUI contient le code, fourni par l'IEEE, identifiant un fabricant ou un éditeur.
- Le champ TYPE permet de définir le code spécifique d'un protocole du propriétaire de l'OUI.

- *Pontage*
- *Spanning-Tree*
- *Commutation L2*
- *VLAN*
- *802.1q*
- *GVRP*
- *LACP*

3

Commutation

Objectifs

Ce module traite des extensions Ethernet, de Spanning-Tree et la commutation.

Connaissances

- Pontage
- STP
- RSTP
- PVST
- VLANs
- 802.1q
- GVRP
- LACP / LAG
- Commutation L3 & L4

Progression

Extensions Ethernet	VLANs
Pontage	GVRP
Spanning-Tree	LACP
Commutation de niveau 2	Commutation de niveaux 3 et 4

Extension d'un réseau Ethernet

- Un réseau physique, quelque soit la topologie utilisée ne peut supporter qu'un nombre limité de machines
- Il faut donc utiliser plusieurs réseaux physiques dès que le nombre de machines maximal est atteint
- Problème : relier les réseaux physiques
- Différentes méthodes existent
  - Pontage
  - Commutation
  - Routage

PROBLEMATIQUE

L'extension d'un réseau Ethernet pose plusieurs problèmes :

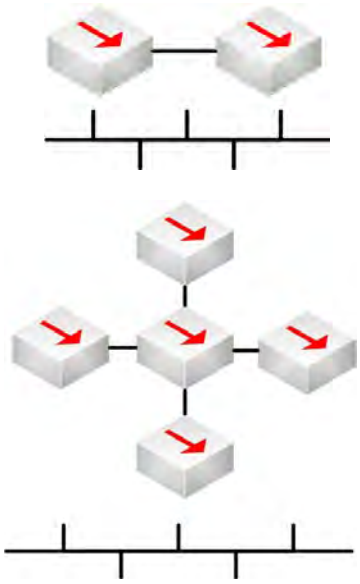
- Tout d'abord un hub ne peut accueillir qu'un nombre limité de ports. N'oublions pas que le bus du hub est partagé entre toutes les machines connectées. Plus il y aura de machines, moins chaque machine aura en proportion de bande passante moyenne.
- Un hub constitue un domaine de collision et un domaine de broadcast. Ce qui signifie que :
  - ➔ Une seule machine peut émettre à un instant t dans un domaine de collision. Donc une seule machine peut émettre pour un hub donné.
  - ➔ Si une machine émet un broadcast, toutes les machines appartenant à son domaine de broadcast le recevront. C'est à dire, toutes les machines connectées à un hub.
- Si on utilise plusieurs hubs reliés entre eux, cela résout le problème de la limite du nombre de ports, mais cela ne résout pas le problème des domaines. En effet, relier des hubs entre eux ne fait qu'étendre le domaine de collision et le domaine de broadcast. Donc :
  - ➔ Une seule machine peut émettre à un instant t dans un domaine de collision. Donc une seule machine peut émettre pour l'ensemble des hubs connectés entre eux.
  - ➔ Si une machine émet un broadcast, toutes les machines appartenant à son domaine de broadcast le recevront. C'est-à-dire, toutes les machines dans un ensemble de hubs connectés entre eux.

SOLUTION

La solution consiste à réduire la taille des domaines de collision et de broadcast. C'est-à-dire la segmentation du réseau. Il existe pour cela trois méthodes :

- Le pontage, qui permet de réduire la taille des domaines de collisions. En effet, sur un pont, chaque port définit un domaine de collision. Autrement dit, une machine par port peut émettre. La bande passante est donc mieux utilisée, puisque plusieurs flux de données peuvent être gérés simultanément.
  Mais, un pont ne réduit pas la taille du domaine de broadcast. Un pont, ou un ensemble de ponts reliés entre eux, constitue un domaine de broadcast.
- La commutation. Elle est plus performante que le pontage et en reprend les principales fonctionnalités. Mais, les commutateurs permettent de créer des VLANs, des LANs virtuels. Un VLAN est défini comme un domaine de broadcast. On aura donc autant de domaines de broadcasts que de VLANs sur un commutateur. Mais un commutateur ne peut pas relier, interconnecter, les VLANs entre eux.
- Le routage. Chaque port d'un routeur constitue un domaine de collision et un domaine de broadcast. C'est le meilleur niveau de segmentation. De plus un routeur opère au niveau logique, au niveau 3. Ce qui fournit une souplesse incomparable : on pourra définir autant de domaines de broadcasts que de sous-réseaux IP.
  En revanche, les routeurs induisent des temps de réponse importants, comparativement aux commutateurs, et des variations de délais de traitement.
  La solution adaptée existe : c'est la commutation de niveau 3. Le principe est d'utiliser des routeurs très performants et dédiés au routage inter-VLAN.

Exemples



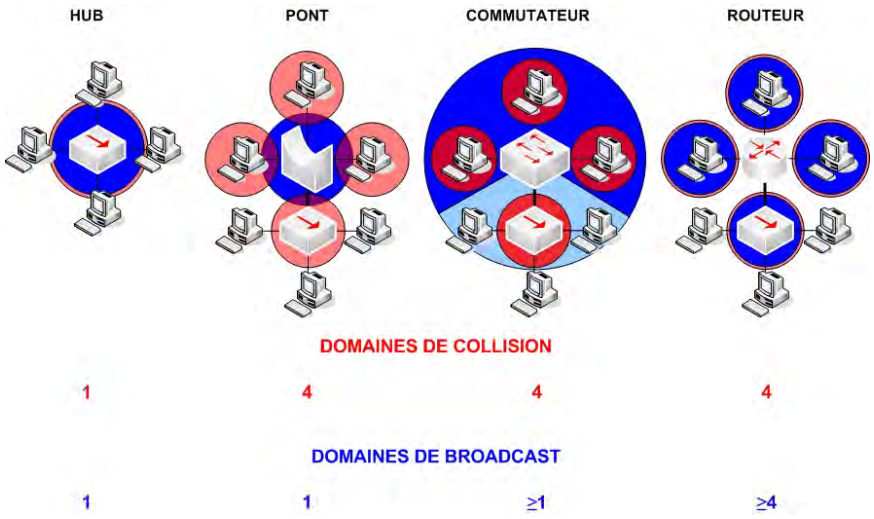
- Deux hubs connectés entre eux constituent :
  - Un seul domaine de collision
  - Un seul domaine de broadcast
- Cela revient à étendre le bus Ethernet

- Quatre hubs connectés entre eux de manière centralisée constituent :
  - Un seul domaine de collision
  - Un seul domaine de broadcast
- Cela revient à étendre le bus Ethernet

Nous avons ici deux exemples :

- Deux hubs reliés entre eux par un lien trunk, ce qui revient à étendre le bus Ethernet. En effet, ces deux hubs constituent :
  - ➔ Un seul domaine de collision
  - ➔ Un seul domaine de broadcast
- Quatre hubs connectés entre eux de manière centralisée. Un hub central est dédié à l'interconnexion des autres hubs. Cela revient, ici encore, à étendre le bus Ethernet. En effet, ces cinq hubs constituent :
  - ➔ Un seul domaine de collision
  - ➔ Un seul domaine de broadcast

Domaines réseaux



Ce tableau synthétise les domaines de collision et de broadcast selon les éléments réseaux utilisés. Nous avons pris comme exemple des machines à 4 interfaces afin d'avoir une approche comparative :

HUB

- Un hub constitue un seul domaine de collision. Une seule des quatre machines connectées peut accéder au réseau à un instant t. Les autres machines seront en écoute.
- De la même façon, un hub constitue un seul domaine de broadcast. Si une des quatre machines émet un broadcast, les trois autres le recevront.

PONT

- Chaque port d'un pont constitue un domaine de collision. Ce qui signifie que plusieurs machines peuvent émettre simultanément.
  Plus exactement dans notre exemple, chaque machine connectée directement au pont constitue un domaine de collision. Le hub et les trois machines qui y sont connectées constituent un autre domaine de collision.
- Un pont constitue un domaine de broadcast. L'ensemble des six machines connectées au réseau constituent donc un seul domaine de broadcast.

COMMUTATEUR

- Comme les ponts, chaque interface d'un commutateur constitue un domaine de collision.

- En revanche il y a une différence importante au niveau des domaines de broadcast. Il y aura autant de domaines de broadcast que de VLANs.
  Dans notre exemple :
  - ➔ Trois ports, ceux auxquels sont directement connectés des PCs, sont rattachés à un VLAN
  - ➔ Un autre port, celui connecté au hub, est définit dans un autre VLAN

ROUTEUR

- Chaque interface d'un routeur constitue un domaine de collision. Aucune différence, de ce point de vue, par rapport à un pont ou un commutateur.
- Chaque interface d'un routeur constitue également au moins un domaine de broadcast. En effet, il est possible de définir plusieurs sous-réseaux IP sur une même interface physique.

Le pontage

- Principe : connecter des réseaux physiques entre eux aux niveaux 1 et 2 en segmentant les domaines de collision
- Utilisation des adresses physiques MAC
- Étendue limitée
- Plusieurs type de pontage (bridging)
  - Transparent : connexion de réseaux de même topologie
  - Source route : réservé à Token Ring (champ RIF activé)
  - Translationnal : connexion de réseaux de topologie différentes

Le pontage consiste à interconnecter entre eux des réseaux physiques au niveau 1 et au niveau 2. Un pont travaille donc au niveau de la couche physique, mais également au niveau de la couche liaison de données.

PRINCIPES

Le rôle essentiel du pont est d'accroître l'étendue totale du réseau physique, tout en permettant à celui-ci de garder un fonctionnement cohérent.

On peut augmenter le nombre de hubs interconnectés. En faisant cela, on crée un réseau « à plat » constituant un seul domaine de collision et un seul domaine de broadcast. En effet, tous les ports d'un hub constituent un seul domaine de collision et un seul domaine de broadcast.

Chaque port d'un pont constitue un domaine de collision. L'ensemble de ses ports constitue un domaine de broadcast. Plusieurs machines pourront donc émettre simultanément si elles sont connectées sur des ports différents d'un même pont.
Le pont permet donc la segmentation du réseau. On ne créera pas de la bande passante, mais elle sera mieux utilisée. Le réseau fonctionnera de façon plus efficace.

De plus, les ponts prennent en compte les adresses MAC. Ce que ne font pas les hubs. Un pont va utiliser une table de correspondance MAC afin de déterminer la localisation de chaque adresse MAC. En clair, à quel port correspond telle adresse MAC.

Les ponts ont néanmoins de nombreuses limitations :

- Un débit, un fond de panier, limité. Un pont fonctionne essentiellement au niveau logiciel, ce qui en limite fatalement les performances.
- Le débit nominal est garanti globalement, et non par ports, ce que permet un commutateur de niveau 2.

- Une étendue limitée. L'étendue est le nombre maximum de ponts qu'il faut traverser pour relier les points les plus éloignés d'un réseau ponté. On considère que l'étendue maximale d'un réseau ponté est de 7.

TYPES DE PONTAGE

Il existe trois types de pontage, de bridging :

- Le transparent bridging. On connecte entre eux des réseaux de même topologie : Ethernet/Ethernet, Token Ring/Token Ring, FDDI/FDDI…
- Le source route bridging. Utilisé exclusivement par Token Ring et FDDI, il permet de gérer le routage à la source. C'est-à-dire l'utilisation du champ RIF dans les trames Token Ring et FDDI.
- Le translationnal bridging. Il permet des interconnexions de réseaux hétérogènes. Notamment, l'interconnexion d'un réseau Ethernet et d'un réseau Token Ring avec usage du champ RIF.

Avec la quasi disparition de Token Ring et de FDDI, le transparent bridging est le seul type de pontage que nous aborderons.

Les trois fonctions d'un pont

- Découverte des adresses MAC
- Transmission / filtrage des trames
- Détection et suppression des boucles

Un pont a essentiellement trois fonctions :

DECOUVERTE DES ADRESSES MAC

Un pont localise les adresses MAC et les enregistre dans une table en mémoire vive. Cette table contient la correspondance entre les adresses MAC et les ports du pont. Le principe est simple : le pont lit les adresses MAC sources des trames émises et les associe avec le numéro du port d'émission. La durée de présence d'un enregistrement dans la table MAC est configurable. Généralement, la valeur par défaut est de 300s, 5 minutes.

TRANSMISSION ET FILTRAGE DES TRAMES

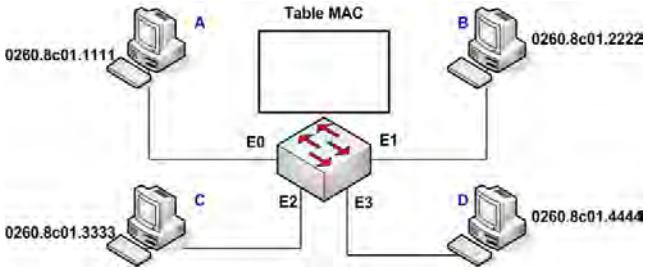
Un pont est en charge de transmettre et de filtrer les trames qu'il reçoit sur chacun de ses ports. A chaque trame reçue :

- Le pont lit l'adresse MAC source et vérifie sa présence dans sa table MAC. Si elle n'y est pas présente, il enregistre la correspondance avec le port d'émission.
- Le pont lit ensuite l'adresse MAC de destination et détermine le port de destination si l'adresse est présente dans sa table MAC. Dans le cas contraire, il transmet la trame sur tous ses ports.

DETECTION ET SUPPRESSION DES BOUCLES

Enfin, les ponts ont pour rôle crucial de détecter et de supprimer les boucles, ou orages de broadcasts. Pour cela, les ponts utilisent le protocole Spanning Tree.

Découverte des adresses MAC (1)



- État initial : la table MAC est vide

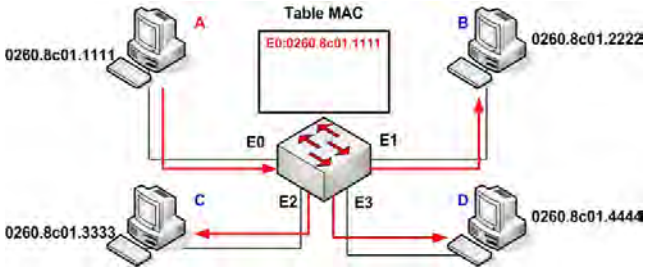
Prenons le cas suivant :

- Un pont disposant de quatre ports auxquels sont connectés respectivement quatre machines A, B, C et D.
- Les machines possèdent les adresses MAC 0260.8c01.xxxx. x=1 pour A, 2 pour B, 3 pour C et 4 pour D.
- A est connecté au port 0, B au port 1, C au port 2 et D au port 4.

ETAT INITIAL

Dans l'état initial, la table MAC est encore vide. Aucune machine n'a encore émis de trame.
Cet état est purement formel et de courte durée. En effet, les machines actuelles, essentiellement sous Windows, signalent rapidement leur présence au démarrage. Pour localiser les maîtres explorateurs, les serveurs WINS, les contrôleurs de domaines…

Découverte des adresses MAC (2)

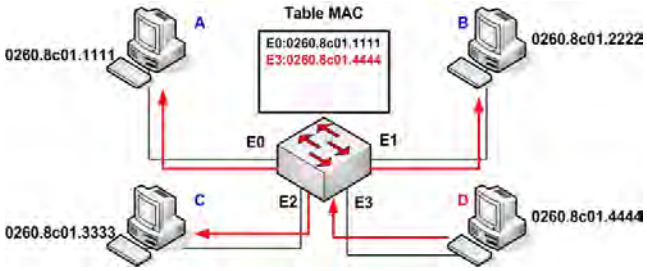


- A envoie une trame à C
- Le pont enregistre dans le cache la correspondance entre l'adresse MAC de A et le port E0
- La trame est diffusée sur tous les ports sauf E0

PREMIERE EMISSION

- A émet une trame à destination de C. C'est-à-dire que la machine possédant l'adresse 0260.8c01.1111 envoie une trame Ethernet à destination de 0260.8c01.3333.
- Le pont vérifie la présence de l'adresse MAC de A dans sa table MAC. Elle n'y figure pas, donc le pont ajoute une entrée avec la correspondance entre l'adresse MAC de A, 0260.8c01.1111 et le port E0. Port sur lequel A a émis sa trame.
- Le pont vérifie ensuite la présence de l'adresse MAC de C dans sa table MAC. Elle n'y figure par non plus. Le pont duplique donc la trame sur tous les ports, sauf le port d'origine E0.

Découverte des adresses MAC (3)

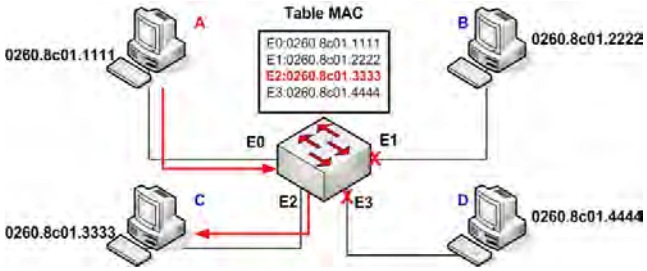


- D envoie une trame à C
- Le pont enregistre dans le cache la correspondance entre l'adresse MAC de D et le port E3
- La trame est diffusée sur tous les ports sauf E3

DEUXIEME EMISSION

- D émet une trame à destination de C. C'est-à-dire que la machine possédant l'adresse 0260.8c01.4444 envoie une trame Ethernet à destination de 0260.8c01.3333.
- Le pont vérifie la présence de l'adresse MAC de D dans sa table MAC. Elle n'y figure pas, donc le pont ajoute une entrée avec la correspondance entre l'adresse MAC de D, 0260.8c01.4444 et le port E3. Port sur lequel D a émis sa trame.
- Le pont vérifie ensuite la présence de l'adresse MAC de C dans sa table MAC. Elle n'y figure par non plus. Le pont duplique donc la trame sur tous les ports, sauf le port d'origine E3.

Filtrage des trames

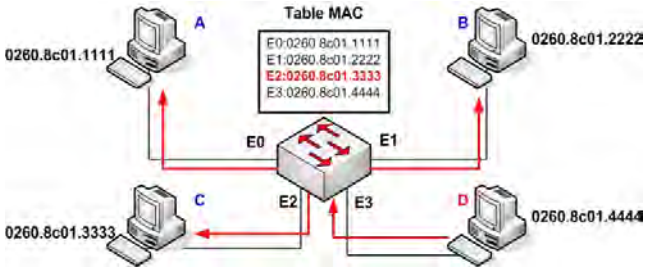


- TABLE COMPLETE :
  - A envoie une trame à C
  - La trame est uniquement envoyée sur le port E2 car l'adresse MAC de C est connue dans le cache MAC

TABLE MAC COMPLETE

- A émet une trame à destination de C. C'est-à-dire que la machine possédant l'adresse 0260.8c01.1111 envoie une trame Ethernet à destination de 0260.8c01.3333.
- Le pont vérifie la présence de l'adresse MAC de A dans sa table MAC. Elle y figure déjà, aucune action n'est donc nécessaire.
- Le pont vérifie ensuite la présence de l'adresse MAC de C dans sa table MAC. Elle y figure également. L'adresse MAC de C, 0260.8c01.3333 y est associée avec le port E3.
- La trame ne sera donc transmise que sur le port E2, port auquel C est connecté. Cette action est qualifiée de micro-segmentation.

Broadcast et multicast



- D envoie une trame broadcast ou multicast
- La trame est diffusée sur tous les ports excepté le port d'origine

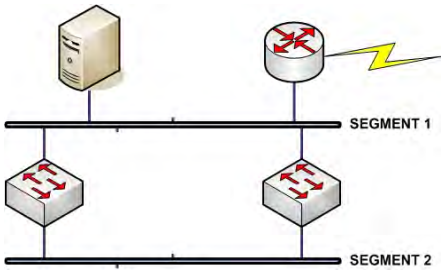
TRAITEMENT DES DIFFUSIONS

Un pont ne fait aucune différence entre un broadcast et un multicast.
Quand une machine émet un broadcast ou un multicast, le pont consulte sa table MAC et n'y trouve aucune correspondance. Il transmet donc la trame sur tous les ports, sauf le port émetteur.

Un pont ne pourra jamais enregistrer une adresse de diffusion dans sa table MAC pour la bonne raison qu'une adresse de diffusion n'est jamais une adresse source mais toujours une adresse de destination. Or, un pont alimente sa table MAC en lisant les adresses MAC source des trames.

Il est à remarquer qu'un pont se comporte de la même façon pour une adresse de diffusion ou une adresse MAC inconnue. Pour un pont, une adresse de diffusion EST une adresse inconnue.

Topologie redondante



- Une topologie redondante élimine les points de défaillance
- Une topologie redondante est la cause d'orages de broadcasts, de duplication de trames et de tables MAC instables

PRINCIPE

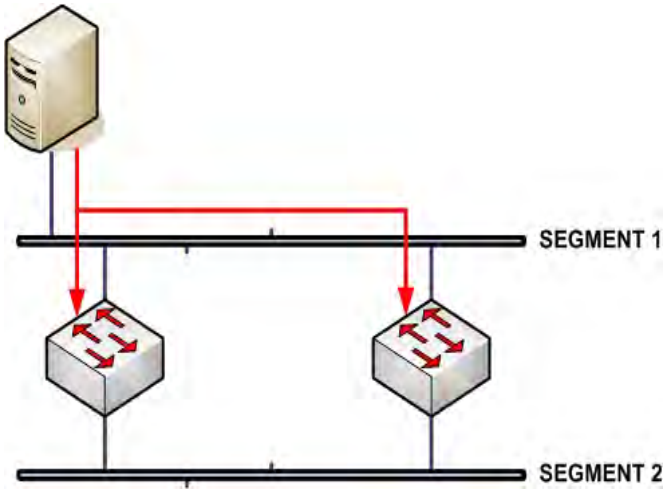
Les ponts ont des avantages déterminants pour étendre un réseau Ethernet. Mais il constitue un point central qu'il est nécessaire de rendre disponible en permanence. La solution est triviale : il suffit de mettre les ponts en redondance pour l'interconnexion des segments Ethernet. Les segments Ethernet symbolisent un ou plusieurs hubs reliés entre eux.

PROBLEMES

Mais une topologie redondante n'est pas sans poser quelques problèmes :

- Orages de broadcasts : une trame tourne indéfiniment sur le réseau Ethernet.
- Instabilité de la table MAC : les tables MAC des ponts en redondance deviennent instables.
- Duplication de trames. Une machine reçoit plusieurs copies de la même trame.

Orages de broadcasts (1)

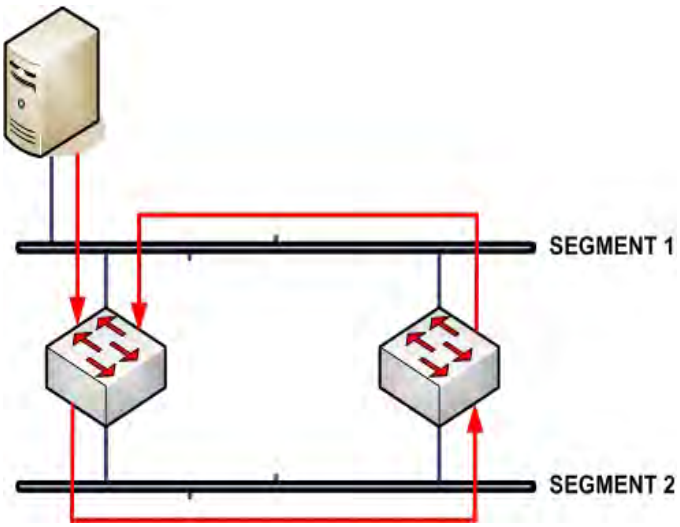


Étudions le cas suivant : un réseau constitué de deux segments connectés via deux ponts en redondance.

EMISSION D'UN BROADCAST

- Une machine émet un broadcast sur le segment 1
- Les deux ponts reçoivent la trame

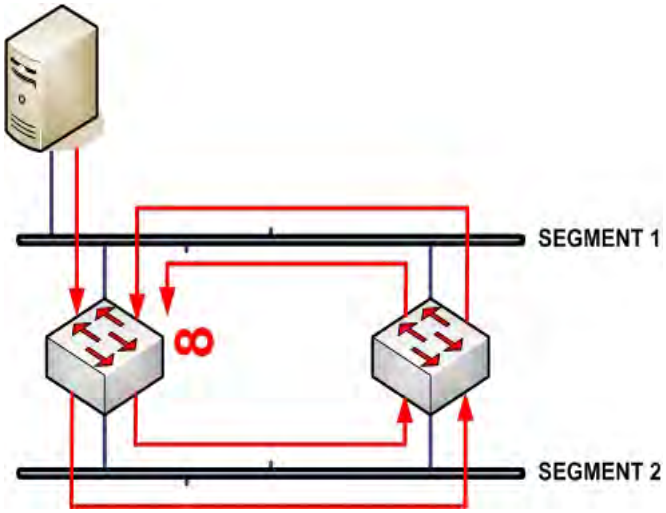
Orages de broadcasts (2)



TRAITEMENT DU BROADCAST

- Le pont de gauche analyse sa table MAC et ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet la trame sur le segment 2
- Le pont de droite reçoit cette trame
- Il analyse sa table MAC et ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet donc la trame sur le segment 1

Orages de broadcasts (3)

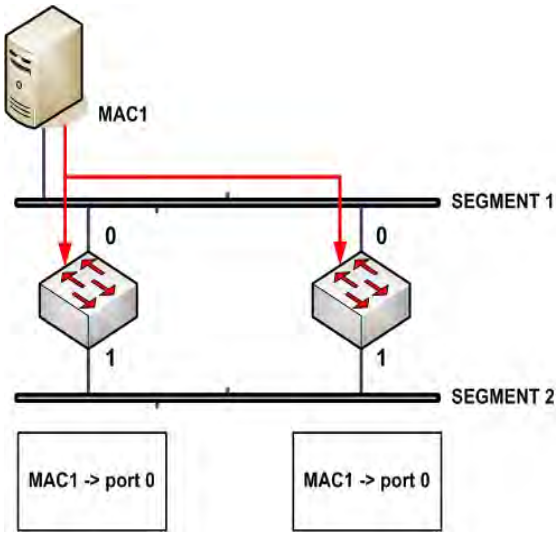


BOUCLE

- Le pont de gauche reçoit cette trame et analyse sa table MAC. Il ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet la trame sur le segment 2
- Le pont de droite reçoit cette trame
- Il analyse sa table MAC et ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet donc la trame sur le segment 1… et ainsi de suite indéfiniment puisqu'une trame Ethernet n'a pas de durée de vie ou de limite de sauts.

Il y a bien orages de broadcast puisque, initialement, le pont de droite reçoit lui aussi le broadcast originel de la machine. Il y a donc deux orages : un dextrogyre (vers la droite) et un lévogyre (vers la gauche).

Instabilité de la table MAC (1)

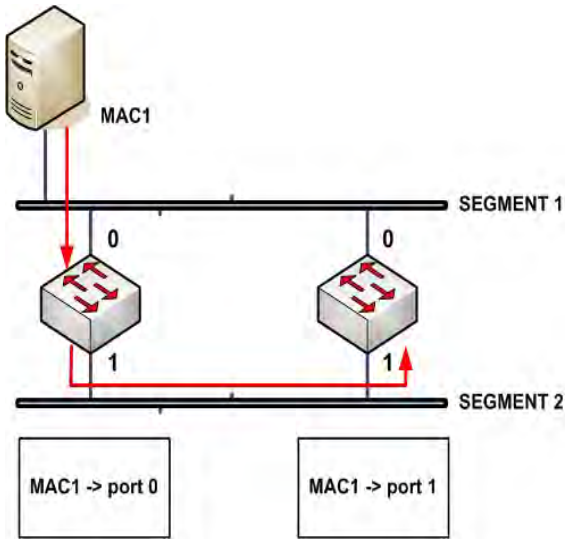


Autre problème, l'instabilité de la table MAC. Il est moins critique car, généralement, il précède les orages de broadcasts.

EMISSION D'UN BROADCAST

- Une machine, ayant l'adresse MAC1, émet un broadcast sur le segment 1
- Les deux ponts reçoivent la trame
- Ils enregistrent dans leur table MAC la correspondance entre MAC1 et le port de réception, le 0

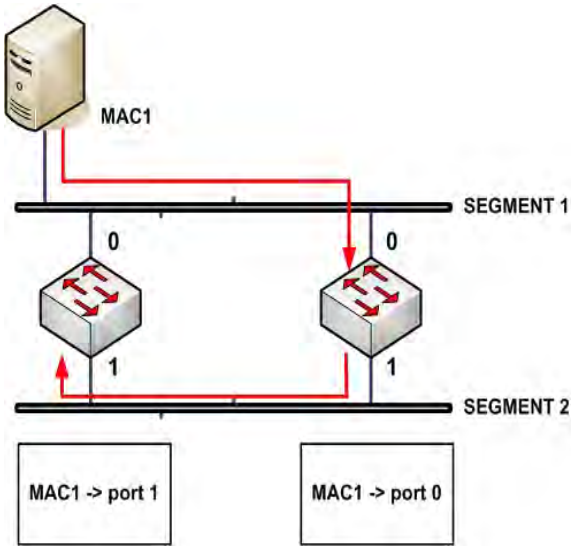
Instabilité de la table MAC (2)



TRAITEMENT DU BROADCAST

- Le pont de gauche analyse sa table MAC et ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet la trame sur le segment 2
- Le pont de droite reçoit cette trame
- L'adresse source de cette trame reste inchangée : MAC1. Or le pont de droite la reçoit sur le port 1
- Le pont de droite met à jour sa table MAC et enregistre la correspondance entre MAC1 et le port 1
- Il analyse sa table MAC et ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet donc la trame sur le segment 1… et c'est de début d'une boucle

Instabilité de la table MAC (3)



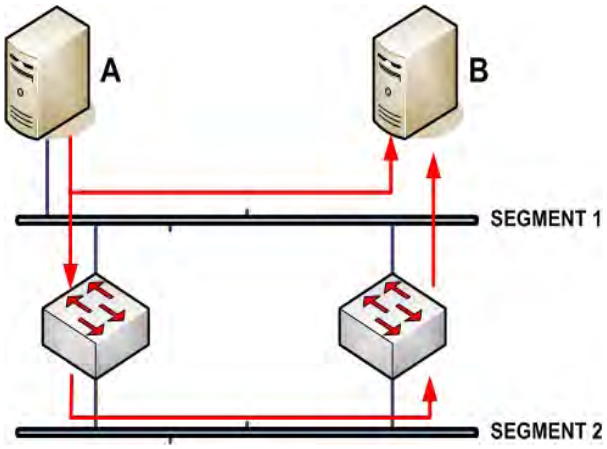
Mais le mécanisme a aussi lieu dans l'autre sens :

TRAITEMENT DU BROADCAST

- Le pont de droite reçoit également une copie de la trame initiale
- Il enregistre dans sa table MAC la correspondance entre MAC1 et le port 0
- Il analyse ensuite sa table MAC et ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet la trame sur le segment 2
- Le pont de gauche reçoit cette trame
- L'adresse source de cette trame reste inchangée : MAC1. Or le pont de gauche la reçoit sur le port 1
- Le pont de gauche met à jour sa table MAC et enregistre la correspondance entre MAC1 et le port 1
- Il analyse sa table MAC et ne trouve pas de correspondance pour l'adresse FF.FF.FF.FF.FF.FF
- Il transmet donc la trame sur le segment 1… et c'est de début de la seconde boucle.

A chaque révolution d'une trame, la table MAC sera mise à jour par les routeurs. Autrement dit, elle ne sera jamais exacte simultanément sur les deux routeurs.

Duplication de trames



Enfin, dernier problème posé par la redondance : la duplication de trames.

Supposons que A émette une trame à destination de B et que l'adresse MAC de B n'est pas encore, ou n'est plus, connue des ponts.

Les étapes suivantes ont lieu :

- B reçoit la trame directement puisqu'il est sur le même segment que A
- Quant le pont de gauche reçoit la trame, l'adresse MAC de B n'étant pas dans sa table MAC, il la transmet sur le segment 2
- Le pont de droite reçoit la trame sur le segment 2. Comme l'adresse MAC de B n'est pas non plus dans sa table MAC, il la transmet sur le segment 1
- B reçoit donc une deuxième copie de la même trame.

Pour la plupart des applications, cela ne pose pas de problème. Il vaut mieux avoir deux copies d'une même trame qu'aucune. Mais, pour d'autres, notamment les applicatifs de sécurité, cela pose problème : elles préfèrent détruire les deux trames en cas de doute que de prendre le moindre risque.

Spanning-Tree Protocol

- Algorithme permettant de résoudre les problèmes liés à une topologie redondante
- Défini par la norme IEEE 802.1d
- Principe : convertir une topologie redondante en topologie arborescente (théorie des graphes) en désactivant certains liens
- Le but est d'obtenir l'unicité du chemin reliant un nœud quelconque de la topologie à tous les autres
- Les nœuds bloqués sont mis en réserve jusqu'à ce qu'une panne survienne
- Dans le cas d'une panne, le protocole STP tente de reconstruire une nouvelle arborescence en utilisant un ou plusieurs des nœuds bloqués
- L'élément central, unique, est le Root Bridge, la racine

Le protocole Spanning Tree (arbre recouvrant) a été développé par Radia Perlman dans les laboratoires de DEC. Il est défini et normalisé par l'IEEE sous la norme 802.1d, ou STP (Spanning Tree Protocol). Son but est d'obtenir l'unicité du chemin reliant un nœud quelconque de la topologie à tous les autres nœuds. Autrement dit, un chemin pour relier des points quelconques du réseau ne devra pas passer deux fois par la même entité, pont ou segment.

PRINCIPE

- Le principe est d'obtenir un arbre recouvrant l'ensemble des segments interconnectés. Pour cela, l'algorithme Spanning Tree convertit une topologie en boucle, redondante, en topologie arborescente (théorie des graphes) en désactivant certains liens. En fait, sur chaque segment, un seul port sera autorisé à émettre, les autres ports seront en mode « blocking », bloqué.
- Les nœuds bloqués sont mis en réserve jusqu'à ce qu'une panne survienne.
- Dans le cas d'une panne, le protocole STP tente de reconstruire une nouvelle arborescence en utilisant un ou plusieurs des nœuds bloqués. Le but restant toujours le même : pouvoir atteindre tous les segments du réseau sans provoquer de boucle.
- L'élément central (la racine) est le Root Bridge. Toute l'arborescence calculée par STP partira de ce point central. Son élection est donc très importante.

Terminologie

Débit (Mbps)	Coût Recommandé
4	250
10	100
16	62
100	19
1.000	4
10.000	2

- Les élections et les déterminations se basent sur deux paramètres : le BridgeID et le Path Cost.
- Chaque pont possède un identifiant unique, le BridgeID, codé sur huit octets et composé de 2 éléments :
  - Numéro de priorité (paramétrable) sur 2 octets
  - Adresse MAC sur 6 octets
- Path Cost : coût total vers la racine
- Le coût pour traverser un segment est inversement proportionnel à sa bande passante
- Les ponts communiquent entre eux en utilisant des BPDUs (Bridge Protocol Data Unit) envoyées à un intervalle compris entre 1 et 10 secondes en MAC multi-diffusion 01-80-C2-00-00-00

STP a son propre jargon et ses termes spécifiques. Étudions les plus importants :

- Les élections et les déterminations se basent sur deux paramètres :
  - ➔ Le Bridge ID qui identifie de manière univoque chaque pont sur le réseau
  - ➔ Le Path Cost qui représente le total entre un pont et la racine
- Chaque pont possède un identifiant unique codé sur deux octets et composé de 2 éléments :
  - ➔ Un numéro de priorité sur 2 octets. Les valeurs vont donc de 1 à 65535. Chaque pont possède une priorité. La valeur par défaut est de 32768. Il est bien évidement possible de modifier cette valeur.
    En STP, la priorité la plus forte est celle qui a la valeur numérique la plus faible. Autrement dit, la valeur la plus forte est 1, la plus faible est 65535.
  - ➔ L'adresse MAC du pont. Un pont possède une seule adresse MAC.
- Le Path Cost est défini comme le coût total à la racine d'un port. Autrement dit, quel est le coût total pour atteindre la racine à partir d'un port du pont ? Le coût total est égal à la somme des coûts des différents segments traversés.
- Le coût pour traverser un segment est inversement proportionnel à sa bande passante. Le tableau ci-dessus indique les coûts pour les interfaces réseaux courantes.
- Les ponts communiquent entre eux en utilisant de petites trames, les BPDUs (Bridge Protocol Data Unit). Elles sont envoyées à un intervalle compris entre 1 et 10 secondes. L'adresse de destination utilisée, 01-80-C2-00-00-00, est de type multi-diffusion.
  Seules les machines sur lesquelles tourne STP traiteront les trames BPDU.
  Une BPDU contient les informations essentielles suivantes :

- ➔ Le BridgeID de la racine
- ➔ Le meilleur coût à la racine que connait l'émetteur
- ➔ Le BridgeID de l'émetteur lui-même

Les BPDUs sont utilisées :

- ➔ Par la racine pour se signaler sur le réseau à intervalle régulier. Ces trames sont propagées à travers tout le réseau.
- ➔ Par les ponts en cas d'élection d'une nouvelle racine sur le réseau.
- ➔ Par les ponts en cas de détermination d'un nouveau DP (Designated Port) sur un segment.

Construction de l'arborescence

- Etapes de fonctionnement :
  - Election du Root Bridge : plus petit BridgeID
  - Sur chaque pont : détermination du Root Port (RP), plus court chemin à la racine
  - Sur chaque segment : détermination du Designated Port, seul port autorisé à transmettre
  - Les ports redondants sur un segment seront en Blocking State

Comment se construit l'arborescence de STP ? En voici les principales étapes :

ELECTION DE LA RACINE

Le pont qui sera élu racine est celui qui possède le BridgeID le plus petit. Celui-ci est structuré de la façon suivante PRIORITE.@MAC. Donc, le premier critère sera la priorité, ensuite seulement, en cas d'égalité de celle-ci, ce sera l'adresse MAC qui fera le départage.

On peut résumer cela de la façon suivante : c'est le routeur avec la meilleure priorité qui deviendra racine. En cas d'égalité, ce sera celui qui possède la plus petite adresse MAC. La racine est unique pour un arbre STP donné.

DETERMINATION DES RPs

Une fois la racine élue, chaque port doit déterminer son port racine, le Root Port (RP). Ce port est unique pour chaque pont. Sera désigné RP le port ayant le coût total à la racine le plus faible. En cas d'égalité, ce sera le port possédant le plus petit numéro qui l'emportera.

Un RP ne peut ni devenir Designated Port ni être en Blocking State.

CISCO utilise, en plus de ces mécanismes, une priorité de port, codée sur un octet. Ce qui permet de favoriser un port par rapport à un autre, indépendamment de son numéro. A égalité de Path Cost, c'est le port avec la meilleure priorité qui l'emportera. En cas de nouvelle égalité, le numéro affecté à chaque port permettra le départage.

DETERMINATION DES DPs

Cela fait, pour chaque segment, un Designated Port est élu. C'est le port connecté au segment du pont ayant le meilleur BridgeID qui l'emportera. Si le pont possède plusieurs ports connectés sur le même segment, c'est celui possédant le plus petit numéro qui l'emportera.

Le DP est unique pour chaque segment, ce sera le seul port autorisé à transmettre les trames. Il existe toutefois une exception : les ports racine. Ils ne participent pas à l'élection du DP, mais peuvent néanmoins transmettre les trames.

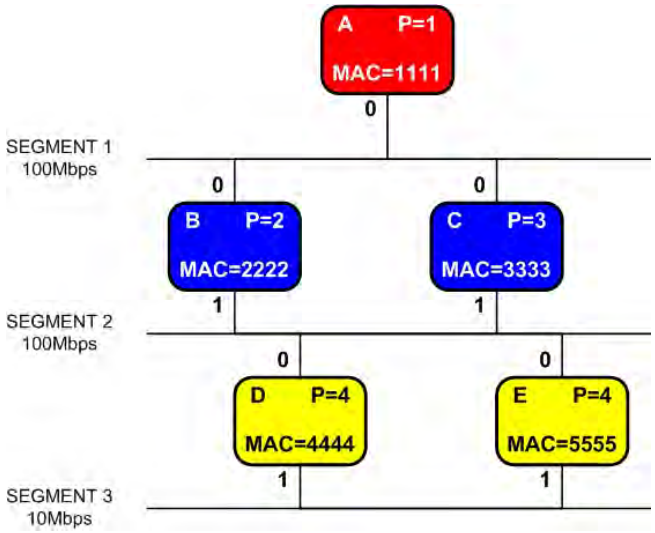
Le Root Bridge a tous ses ports en DP.

La même remarque s'applique concernant CISCO : la priorité de port permettra le départage indépendamment du numéro de port.

PORTS EN BLOCKING STATE

Les autres ports d'un segment, ceux qui ne sont ni Root Port ni Designated Port, se mettent en en Blocking State. Un port en Blocking State est en veille : il ne peut transmettre aucune trame, il traite uniquement les BPDUs qu'il reçoit. Ce qui lui permettra de détecter les défaillances de la racine et du DP de son segment.

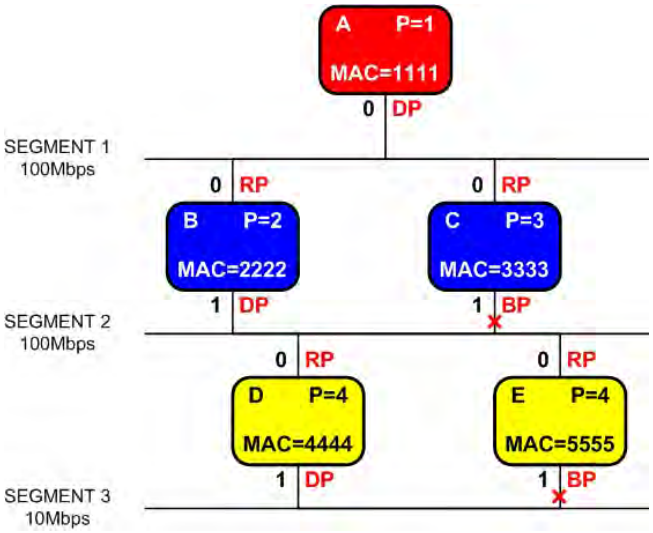
Exemple (1)



Prenons comme exemple un réseau fortement redondant composé de :

- 5 ponts :
  - ➔ A avec une priorité de 1 et l'adresse MAC 1111
  - ➔ B avec une priorité de 2 et l'adresse MAC 2222
  - ➔ C avec une priorité de 3 et l'adresse MAC 3333
  - ➔ D avec une priorité de 4 et l'adresse MAC 4444
  - ➔ E avec une priorité de 4 et l'adresse MAC 5555
- 3 segments :
  - ➔ 1 de 100Mbps sur lequel sont connectées les interfaces 0 de A, B et C
  - ➔ 2 de 100Mbps sur lequel sont connectées les interfaces 1 de B et de C, et les interfaces 0 de D et de E
  - ➔ 3 de 10Mbps sur lequel sont connectées les interfaces 0 de D et de E

Exemple (2)



La première étape est l'élection de la racine. La première machine qui s'initialise sur un réseau devient la racine. Ensuite, au fur et à mesure du démarrage des autres ponts, une racine permanente sera élue.
Autrement dit, si une machine s'initialise sur un segment et que les BPDUs qu'elle reçoit contiennent un BridgeID inférieur au sien, cette machine s'annoncera comme la nouvelle racine. Sinon, elle valide cette information et calcule son arbre Spanning Tree en conséquence.

ORDRE DE PREFERENCE

Ce sont les BPDUs échangées entre les ports qui permettront l'élection de la racine et la détermination des RP et des DP. Le format, simplifié, de ces trames est le suivant :
[BridgeID].[COUT].[EMETTEUR]

L'ordre de préférence général de STP est défini comme suit :

- BridgeID de la racine
- Coût à la racine de l'émetteur de la BPDU
- Bridge ID de l'émetteur
- Numéro de port par lequel la BPDU a été reçue

ELECTION DE LA RACINE

La racine est la machine possédant le meilleur, numériquement le plus petit, BridgeID. Dans notre exemple, il n'y a pas d'ambiguïté, c'est A qui possède la meilleure priorité. A deviendra donc la racine, le Root Bridge. Et ce, tant qu'une machine possédant la même priorité mais avec une adresse MAC plus petite n'est pas connectée sur le réseau.

DETERMINATION DES RPs

Le Root Port est ensuite désigné sur chaque pont :

- A est la racine, aucun de ses ports n'est RP par conséquent.
- B possède deux chemins pour atteindre la racine :
  - ➔ Par son interface 0 avec un coût de 19 (100Mbps). Sur cette interface, B reçoit les BPDUs suivantes : [1.1111].[0].[1.1111] de A. Remarquez que la racine s'annonce toujours avec un coût de 0.
  - ➔ Par son interface 1 avec un coût de 38. En effet, C annonce sur le segment 2 les BPDUs suivantes : [1.1111].[19].[3.3333]. B en déduit que pour atteindre la racine en passant par C, le coût total sera de 19, annoncé par C, plus le coût de l'interface par laquelle la BPDU a été reçue, 19 également.

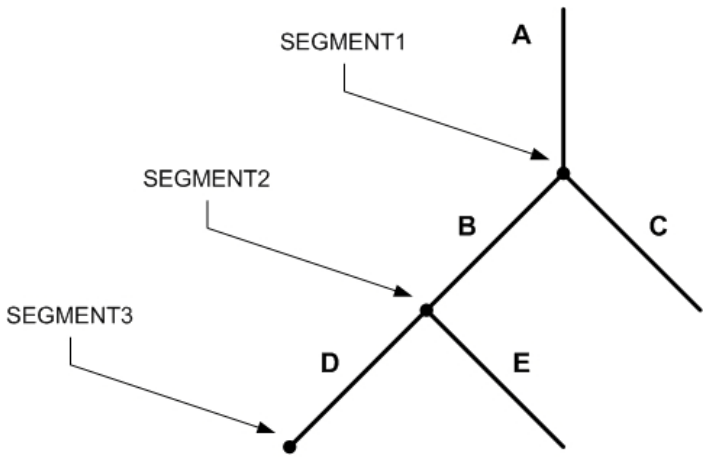
    B en déduit donc que son meilleur coût à la racine passe par son interface 0, avec un coût total de 19. Le RP de B est donc son interface 0.
- C est dans le même cas que B. Son RP sera son interface 0.
- Pour D, deux chemins sont possibles pour atteindre la racine :
  - ➔ Par son interface 0 avec un coût de 38. Sur cette interface, D reçoit les BPDUs suivantes : [1.1111].[19].[x.xxxx]. x est égal à 2 si c'est B qui devient DP sur le segment 2 et égal à 3 si c'est C qui le devient. Le coût total à la racine de cette interface sera donc de 38.
  - ➔ Par son interface 1 avec un coût de 138. En effet, E annonce sur le segment 3 les BPDUs suivantes : [1.1111].[38].[4.5555]. D en déduit que pour atteindre la racine en passant par E, le coût total sera de 38, annoncé par E, plus le coût de l'interface par laquelle la BPDU a été reçue, 100.
    D en déduit donc que son meilleur coût à la racine passe par son interface 0, avec un coût total de 38. Le RP de D est donc son interface 0.
- E est dans le même cas de figure que D. Son RP sera son interface 0.

DETERMINATION DES DPs

Pour chaque segment, il y aura un seul DP, Designated Port. C'est le port du pont ayant le meilleur BridgeID qui l'emportera, à l'exclusion toutefois des RP qui ne peuvent devenir DP.

- Pour le segment 1, le port du Root Bridge est forcément DP, comme tous les ports de la racine.
- Pour le segment 2, B possède une priorité, et donc un BridgeID, meilleure que celle de C. Le port 1 de B devient donc le DP du segment 2.
- Pour le segment 3, D et E ont la même priorité. Ce sera donc l'interface du pont ayant la plus petite adresse MAC qui l'emportera. Le port 1 de D devient donc le DP pour le segment 3.

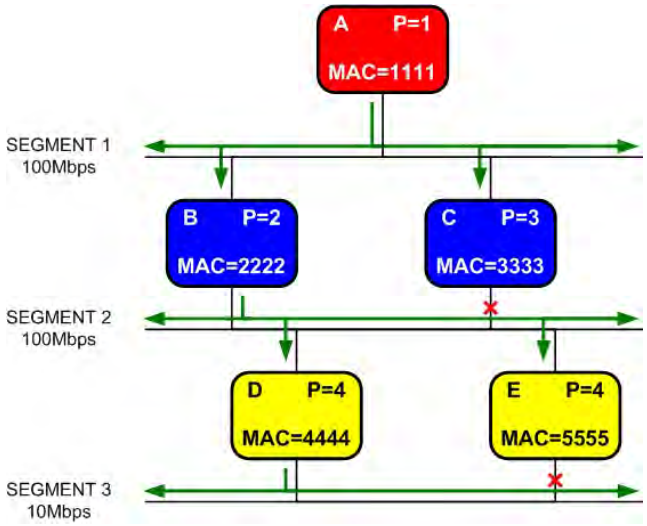
Exemple (3)



REPRESENTATION ARBORESCENTE DU RESEAU

- Le réseau est donc représenté par STP sous forme d'une arborescence. Dans la représentation schématique, en conformité avec la norme 802.1d, les ponts sont représentés par des traits et les segments par des points.
- Le point de départ est la racine, A.
- La racine est reliée, via le segment 1, à B et C. C joue uniquement un rôle redondant, puisqu'il ne permet de relier aucun segment à partir de A.
- B est relié à D et E via le segment 2. C'est donc B seul qui assure le lien entre les segments 1 et 2.
- Enfin, E est relié au segment 3. Même remarque que pour C : E joue le rôle de pont redondant pour le segment 3.

Exemple (4)



VERIFICATION

Supposons qu'une machine connectée à A émette un broadcast :

- A le transmet sur le segment 1 par son interface 0
- B et C reçoivent cette trame
- C ne peut la transmettre sur le segment 2 car son port 1 est en Blocking State
- Pour B, en revanche, son port 1 est DP sur ce segment, il peut donc transmettre cette trame sur le segment 2
- D et E reçoivent cette trame
- E ne peut la transmettre sur le segment 3 car son port 1 est en Blocking State
- Pour E, en revanche, son port 1 est DP sur ce segment. Il peut donc transmettre cette trame sur le segment 3.

Le broadcast transmis par A a bien atteint tous les segments du réseau sans provoquer aucune boucle, duplication de trame ou instabilité de la table MAC.

Timers STP

- Hello Timer
  - Intervalle d'émission des BPDUs
  - Par défaut : 2 secondes chez la plupart de constructeurs
- MaxAge
  - Délai maximum d'attente entre deux BPDUs
  - Passé ce délai, un paquet TCN (Topology Change Notification) est envoyé
  - Par défaut : 20 secondes chez la plupart de constructeurs
- Forward Delay
  - Délai de transition entre deux états des ports
  - Par défaut : 15 secondes chez la plupart de constructeurs

Les mécanismes liés aux BPDUs, pour fonctionner, s'appuient sur 3 valeurs de timers :

HELLO TIMER

Le Hello Timer définit l'intervalle entre deux émissions de BPDUs. Chez la plupart des constructeurs, la valeur par défaut est de 2 secondes. En fonctionnement normal, seule la racine émet des BPDUs, qui sont ensuite relayées par les ponts à travers le réseau. Le Hello Timer est annoncé dans les trames BPDUs. Sa valeur est imposée par la racine.

MAXAGE

Ce timer définit le délai d'attente maximum entre deux BPDUs par les ponts. Le timer MaxAge est généralement égal à dix fois la valeur du Hello Timer. Par défaut, il est donc égal à 20 secondes.

Si au bout de 20 secondes un pont n'a toujours par reçu la BPDU escomptée, il émet un paquet TCN (Topology Change Notification). Ce paquet provoquera les mécanismes de recouvrement de STP qui permettront de calculer une nouvelle arborescence.

Par exemple, si la racine n'est plus opérationnelle, une nouvelle sera élue.
Si un pont dont un des ports était DP n'est plus accessible, un autre port sur un autre pont sur le même segment sera désigné nouveau DP.

FORWARD DELAY

Le Forward Delay représente le délai de transition entre deux états des ports. Par défaut, chez la plupart des constructeurs, sa valeur est fixée à 15 secondes.

Etat de ports

- Disabled
  - Pas de transmission de trames
  - Pas de table de transmission
- Blocking
  - Pas de transmission de trames
  - Ecoute des BPDUs reçues
- Listening
  - Ne traite que les trames qui lui sont adressées
  - Ecoute les BPDUs reçues
- Learning
  - Le pont construit passivement sa table de transmission
  - Traitement des BPDUs
- Forwarding
  - Transmission des trames
  - Participation complète

En STP, les ports d'un pont peuvent être dans différents états :

DISABLED

Le port est désactivé. Aucune trame traitée, aucune trame transmise. La table MAC est vide. Pas d'émission ni de réception de BPDUs.

BLOCKING

Dans cet état, un port ne transmet aucune trame. En revanche, il écoute les BPDUs émises ou transmises par le DP. Si l'intervalle entre deux BPDUs dépasse le MaxAge, il bascule en état Listening.

Il y a deux cas où un port est en mode Blocking :

- Au démarrage d'un pont
- En fonctionnement normal pour un port qui n'est ni DP sur un segment, ni RP pour le pont

LISTENING

Cet état correspond à un état transitoire. Après le MaxAge, un pont émet un TCN. C'est durant cet état Listening que l'arborescence est recalculée par STP. La durée de cet état est égale à la valeur du Forward Delay, 15 secondes par défaut.

Dans cet état, le port écoute les BPDUs et traite uniquement les trames qui lui sont adressées.

Seuls les ports ayant gagné une élection passeront à l'état suivant. Par exemple, si sur un segment le DP est indisponible, un nouveau est désigné. Tous les autres ports, sauf les RP, rebasculent en mode Blocking.

LEARNING

L'état Learning est atteint uniquement par les ports qui vont jouer un rôle actif dans le réseau en STP. C'est-à-dire un DP ou un RP.

Le pont construit alors passivement sa table MAC. C'est-à-dire qu'il ne transmet toujours pas de trames, mais alimente sa table via l'analyse des trames qu'il reçoit. La durée de cet état est égale à la valeur du Forward Delay, 15 secondes par défaut.

Dans cet état, le port traite également les BPDUs qu'il reçoit.

FORWARDING

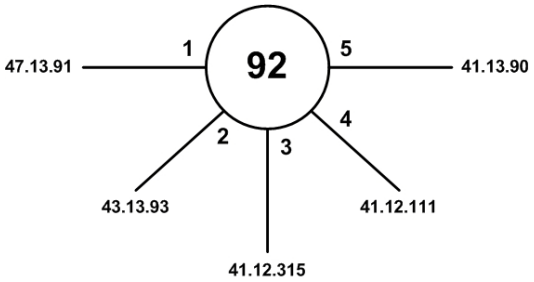
C'est l'état opérationnel d'un port. Il peut transmettre les trames qu'il reçoit et continue à alimenter activement sa table MAC. Enfin, il relaye également les BPDUs reçues.

Deux types de ports peuvent prétendre être en état Forwarding : les RPs et les DPs.

Au mieux donc, il faudra 20+15+15=50 secondes pour que le réseau converge, qu'il soit de nouveau opérationnel après un changement de topologie.

A tout moment, un port peut revenir à l'état Blocking. Par exemple si le DP ou la racine redeviennent disponibles, ils émettent des BPDUs qui permettront de recouvrer l'état antérieur quasi instantanément.

Exemple 2



- Racine : 41
- Meilleur coût à la racine : 13 (12+1)
- Port racine : 4 (ID du voisin : 111, pour le port 3 : 315)
- Ports désignés : 1 et 2
- Ports bloqués : 3 et 5

Prenons un autre exemple : un pont démarre sur le réseau.

CARACTERISTIQUES

Ce pont a les caractéristiques suivantes :

- Son BridgeID est égal à 92. Nous prenons cette valeur afin de simplifier la démarche.
- Il possède 5 ports, numérotés de 1 à 5.

Sur le schéma sont représentées sur chaque segment auquel le pont est connecté, les BPDUs qu'il reçoit de ses voisins. Nous supposerons, arbitrairement, que les coûts des interfaces sont tous égaux à 1.
Rappelons que les BPDUs ont pour format : RACINE.COUT.EMETTEUR.
Enfin, rappelons l'ordre de préférence : BridgeID de la racine, Coût à la racine, BridgeID de l'émetteur et enfin numéro de port.

DETERMINATION DE LA RACINE

La racine est le pont ayant le plus petit BridgeID :

- Sur son interface 1, 92 reçoit une BPDU indiquant que, pour le pont 91, la racine est 47. Ce BridgeID est meilleur que celui de 92 et 91.
- Sur son interface 2, 92 reçoit une BPDU indiquant que, pour le pont 93, la racine est 43. Ce BridgeID est meilleur que celui de 47.
- Sur son interface 3, 92 reçoit une BPDU indiquant que, pour le pont 315, la racine est 41. Ce BridgeID est meilleur que celui de 43.
- Sur son interface 4, 92 reçoit une BPDU indiquant que, pour le pont 111, la racine est également 41.

- Sur son interface 5, 92 reçoit une BPDU indiquant que, pour le pont 90, la racine est également 41.

La racine est donc 41 pour le pont 92.

DETERMINATION DU RP

Le Root Port est le meilleur coût à la racine :

- 315 annonce un coût de 12, son meilleur coût à la racine. Pour atteindre la racine via 315, le coût serait donc de 13 pour 92.
- 111 annonce un coût de 12. Le coût total à la racine serait donc de 13 pour 92.
- 90 annonce un coût de 13. Le coût total à la racine serait donc de 14 pour 92.

Le meilleur coût pour atteindre la racine est donc de 13. 92 a deux ports ayant le même coût : le 3 et le 4.
Le RP sera le port 4, car l'émetteur sur ce port a un meilleur BridgeID (111) que celui du port 3 (315).

DETERMINATION DES DP

- Sur le port 1, 91 ne voyait pas le pont 41, la nouvelle racine, avant le démarrage de 92. C'est donc le seul chemin pour l'atteindre, autrement il aurait annoncé 41 comme racine à 92 au lieu de 47. Si c'est son seul chemin, c'est forcément son RP. Donc, en face, le port 1 de 92 sera forcément DP.
- Même logique sur le port 2 avec 93 et 43. Le port 2 de 92 sera également DP.
- Sur le port 3, 315 a un meilleur coût à la racine que 92. Il sera donc DP sur ce segment. Le port 3 de 92 sera donc en mode Blocking.
- Sur le port 5, 90 a un coût à la racine identique à celui de 92. Mais, comme le BridgeID de 90 est meilleur que celui de 92, son port sera DP sur leur segment commun. Le port 5 de 92 sera donc en mode Blocking.

802.1s / PVST

- Per Vlan Spanning Tree (PVST)
- Permet de déclarer un domaine Spanning Tree par VLAN
- Avantages :
  - Répartition statique de la charge par VLAN
  - Meilleure utilisation des ressources réseau
- Utilisation conjointe avec des commutateurs qui ne supportent pas 802.1s possible
- Règles :
  - Par défaut, tous les VLANs font partie du domaine ST par défaut
  - Un VLAN ne peut appartenir qu'à un seul domaine ST
  - Les BPDUs de PVST utilisent l'adresse 01-00-1D-00-00-05

Une évolution importante de STP a été le Per Vlan Spanning Tree, PVST. Développé initialement par CISCO, il est aujourd'hui standardisé sous la norme IEEE 802.1s.

PRINCIPE

Le principe consiste à n'avoir qu'une seule instance de Spanning-Tree par VLAN. Un VLAN est un réseau virtuel permettant une segmentation très modulable du réseau. Nous y reviendrons.

Avec le STP d'origine, une seule instance fonctionne sur le réseau. Une seule racine existe pour l'ensemble du réseau. Autrement dit, plus le réseau devient grand, plus l'arborescence va devenir importante, avec tous les inconvénients intrinsèques liés à cette taille :

- Mémoire vive nécessaire sur les commutateurs
- Temps de convergence longs
- Réactivité faible
- Trafic réseau induit

L'idée du PVST est d'avoir une arborescence, un domaine, pour chaque VLAN. On a ainsi des arborescences plus petites, mais plus réactives, avec des temps de convergence plus courts et globalement moins de mémoire vive utilisée.

Enfin, il est possible de faire de la répartition de charge statique par VLAN afin de mieux utiliser les ressources du réseau. De fait, un port pourra être en DP pour un VLAN, mais en Blocking pour un autre VLAN. Ce qui fait que le chemin emprunté par les trames dépendra du VLAN d'origine.

Le PVST est rétro-compatible avec STP. Il est donc possible d'avoir sur un même réseau des commutateurs fonctionnant en STP et d'autres en PVST.

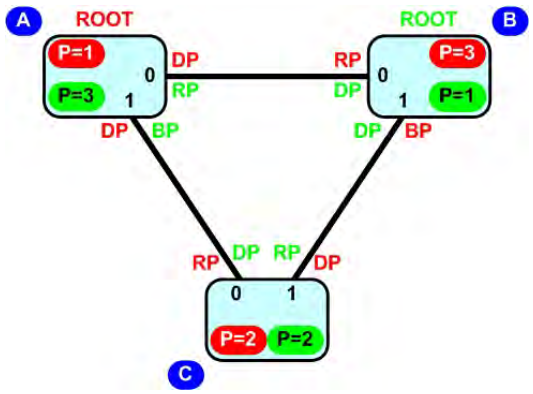
Le PVST ne fonctionne que sur les commutateurs, pas sur les ponts. En effet, ceux-ci ne gèrent pas les VLANs.

Les BPDUs de PVST utilisent l'adresse de multicast réservée 01-00-1D-00-00-05. Elles intègrent notamment, en plus des informations standards, l'identifiant du VLAN.

REGLES DE FONCTIONNEMENT

- Par défaut, tous les VLANs appartiennent au domaine ST par défaut. Autrement dit, ils sont tous dans la même instance.
- Un VLAN ne peut appartenir qu'à un seul domaine de ST.
- Un port peut être associé à autant de domaines de ST que nécessaire.

Exemple



- Deux VLANs : ROUGE et VERT
- A :
  - Priorité =1 pour ROUGE
  - Priorité =3 pour VERT
- B :
  - Priorité =3 pour ROUGE
  - Priorité =1 pour VERT
- C :
  - Priorité =2 pour ROUGE
  - Priorité =2 pour VERT

TOPOLOGIE

Supposons que nous ayons deux VLANs : ROUGE et VERT. Ces deux VLANs sont définis sur chacun des trois commutateurs.

Nous avons ici 3 commutateurs A, B et C.

- A a les caractéristiques suivantes :
  - ➔ Il a la priorité 1 dans le VLAN ROUGE
  - ➔ Il a la priorité 3 dans le VLAN VERT
- B a les caractéristiques suivantes :
  - ➔ Il a la priorité 3 dans le VLAN ROUGE
  - ➔ Il a la priorité 1 dans le VLAN VERT
- C a les caractéristiques suivantes :
  - ➔ Il a la priorité 2 dans le VLAN ROUGE
  - ➔ Il a la priorité 2 dans le VLAN VERT

ELECTIONS

Pour le VLAN ROUGE :

- La racine est A puisque c'est lui qui a la meilleure priorité dans ce VLAN
- Tous les ports de A sont en DP (c'est la racine)
- Le RP de B est le port 0

- Le RP de C est le port 0
- Sur le segment entre B et C, c'est le port 1 de B qui est BP et le port 1 de C qui est DP

Pour le VLAN VERT :

- La racine est B puisque c'est lui qui a la meilleure priorité dans ce VLAN
- Tous les ports de B sont en DP (c'est la racine)
- Le RP de A est le port 0
- Le RP de C est le port 1
- Sur le segment entre A et C, c'est le port 1 de A qui est BP et le port 0 de C qui est DP

802.1w / Rapid Spanning Tree

- Version 2 de STP définie par la norme IEEE 802.1w
- BPDU version 2 également
- Compatibilité avec STP v1
- Améliorations par rapport à 802.1d :
  - Etats des ports
  - Rôles des ports
  - Types de liens
- Convergence plus rapide
- Basculement des ports plus rapide

Une évolution essentielle de STP a été le Rapid Spanning Tree, ou STP v2.

RSTP (Rapid Spanning-Tree Protocol) utilise des BPDUs en version 2 également. Néanmoins, il y a rétrocompatibilité avec STP. Simplement, quand un commutateur faisant tourner RSTP reçoit une BPDU version 1, il répond dans le même format.

Les améliorations par rapport au STP standard (802.1d) sont les suivantes :

- Distinction entre le rôle d'un port et son état
- Simplification des états des ports :
  - ➔ Discarding. Equivalent à Blocking.
  - ➔ Learning. Identique à STP.
  - ➔ Forwarding. Identique à STP.

  L'état Learning disparait car il n'est plus nécessaire.
- Rôle des ports :
  - ➔ Edge Port. C'est un port sur lequel on connecte un PC, un serveur ou un téléphone IP. Bref, tout ce qui ne fait pas de Spanning-Tree.
    Un Edge port bascule donc quasi instantanément de l'état Discarding à l'état Forwarding, car il n'y pas nécessité d'élection pour savoir si le port basculera ou non en Forwarding.
  - ➔ Root Port. Identique à STP.
  - ➔ Designated Port. Identique à STP.
  - ➔ Alternative Port. En cas d'indisponibilité du DP sur un segment, l'AP bascule en Forwarding.

- ➔ Backup Port. Si un pont possède deux interfaces sur un même segment, et que l'un est DP, l'autre sera Backup. En cas de défaillance du DP, le Backup basculera en Forwarding.

- Prise en compte des types de liens :
  - ➔ Point-to-point (p2p). C'est le cas des liens entre les commutateurs et entre les ponts.
  - ➔ Shared. C'est le cas d'un hub connecté sur le port d'un pont ou d'un commutateur.

802.1s / Multiple Spanning Tree

- MSTP, Multiple Spanning-Tree Protocol
- Défini dans la norme IEEE 802.1s
- Le principe est d'associer un ou plusieurs VLANs à une instance de STP
- Il peut y avoir multiplicité des instances STP
- Les BPDUs incluent le numéro d'instance
- Plus souple que PVST, qui associe chaque VLAN à une instance

---

Une autre évolution de STP est le Multiple Spanning Tree, ou MSTP. Cette évolution est définie dans la norme IEEE 802.1s.
Le principe est simple : on associe un ou plusieurs VLANs à une instance de STP. On peut avoir plusieurs instances STP dans un même réseau. Le numéro d'instance est codé dans les BPDUs.

Le MSTP est beaucoup plus souple que le PVST (Per Vlan Spanning-Tree), qui associe chaque VLAN à une instance de STP.
Avec MSTP, il est possible de moduler l'appartenance des VLANs aux instances de STP afin d'équilibrer la charge sur les liens ou d'alléger la charge sur certains commutateurs.

Per VLAN Rapid Spanning Tree

- PVRST, Per Vlan Rapid Spanning-Tree
- Implémentation de Rapid Spanning Tree par VLAN
- Développé par CISCO
- En cours de normalisation

Enfin, CISCO a développé une version « Rapid » de PVST.
Le principe est identique à celui-ci, mais c'est la version 2 de STP, RSTP, qui est utilisée.

Cette version est en cours de normalisation par l'IEEE.

Commutation de niveau 2

- Pontage :
  - Basé sur du logiciel
  - Une instance de STP par bridge
  - Jusqu'à 16 ports par bridge
  - Débit du fond de panier faible
- Commutation de niveau 2 :
  - Basée sur des composants matériels (ASIC)
  - Plusieurs instances de STP par commutateur
  - Nombre de ports limité uniquement par les capacités de la machine
  - Débit du fond de panier élevé
  - Débit nominal d'un port garanti
  - Possibilité de créer des VLANs
  - Différents modes de transmission
  - Connexion en half ou full duplex pour chaque port
  - Coût conséquent

La commutation de niveau 2 est une évolution du pontage. Un commutateur, ou switch, est donc un super pont. Comme lui, il travaille exclusivement au niveau de la couche PHYSIQUE et de la couche LIAISON DE DONNEES. Il inclut toutes les fonctionnalités d'un pont en les améliorant, et en ajoute d'autres.
Comparons les deux technologies :

PONTAGE

- Le pontage est basé sur du logiciel. Ce qui en limite fatalement les performances.
- Un pont ne peut exécuter qu'une seule instance de STP.
- Un pont supporte au maximum 16 ports.
- Le débit du fond de panier est faible comparativement à celui d'un commutateur. Généralement, les ponts ont des débits de 10 ou de 100 Mbps en Ethernet.

COMMUTATION DE NIVEAU 2

- Un maximum de fonctionnalités est « câblé », c'est-à-dire réalisée par des composants matériels dédiés, les ASICs.
- Un commutateur peut faire tourner plusieurs instances de STP, dans la limite de ses capacité RAM et CPU.
- Le nombre de ports qu'un commutateur peut supporter n'est limité que par ses capacités propres.
- Le débit du fond de panier est beaucoup plus élevé que celui d'un pont. Actuellement, des débits de plusieurs centaines de Gbps sont courants.

- Le débit nominal d'un port est garanti. Un commutateur 100Mbps garantit 100Mbps sur tous ses ports.
- Les commutateurs disposent de la fonctionnalité de pouvoir créer et gérer des VLANs, des LAN virtuels.
- Il existe différents modes de transmission adaptés à l'usage et la fonction d'un commutateur.
- Chaque port peut fonctionner en half ou en full duplex.
- Enfin, le coût d'un commutateur est en proportion de ses prestations.

Transmission des trames

- Trois types de transmissions généralement supportés :
  - Store and Forward : lecture et stockage complets de trame avant transmission
  - Cut-through : lecture de l'adresse de destination et début de transmission immédiat
  - Fragment Free : lecture des 64 premiers octets et début de transmission immédiat

Il existe trois modes de transmission des trames pour un commutateur : Cut-through, Fragment Free et Store & Forward. Certains commutateurs supportent les trois, d'autres n'en supportent qu'un ou deux.

STORE & FORWARD

C'est le mode originel de transmission des trames par les ponts et les commutateurs. La trame est stockée et vérifiée dans son intégralité : longueur, valeur des champs, FCS. Si tout est correct, la trame est transmise en concordance avec la table MAC.

C'est le mode le plus fiable, mais, fatalement, le plus lent. Il est généralement utilisé dans les commutateurs d'accès.

CUT THROUGH

C'est le mode le plus rapide : le commutateur lit uniquement les adresses MAC destination et source. Il vérifie ensuite la présence ou l'absence des adresses dans la table MAC, et commence la transmission.

C'est le mode le plus performant, mais le moins fiable. En effet, rien ne garantit que la trame transmise soit de la bonne longueur, que les champs aient des valeurs correctes, que le FCS est bon… Il est souvent utilisé sur les commutateurs Backbone, au cœur des réseaux.

Il est à remarquer que c'est également ce mode qui garantit la variation du délai de transmission des trames le plus faible. Ce qui n'est pas anodin pour le transport de la voix sur IP.

FRAGMENT FREE

C'est un mode intermédiaire entre le Cut Through et le Store & Forward. Le commutateur ne lit que les 64 premiers octets d'une trame. Ce qui lui permet de vérifier que la trame n'est pas une trame « collisionnée ». Ce mode est donc plus rapide que le Store & Forward, mais plus fiable que le Cut Through. Il est généralement utilisé dans les commutateurs de niveau distribution.

Duplex

- Half duplex
  - Flux de données unidirectionnel
  - Risque potentiel de collisions plus élevé
  - Utilisation en connexion hub
- Full duplex
  - Point à point uniquement
  - Connecté à un port dédié
  - Nécessite une comptabilité full-duplex aux deux extrémités
  - Aucune collision possible, circuit de détection désactivé
  - Flux de données bidirectionnel
  - Utilisé pour connecter les serveurs et les routeurs

Le mode duplex définit la méthode utilisée pour accéder au réseau.

Il existe deux modes duplex :

HALF DUPLEX

Le flux de données est unidirectionnel. Une seule machine peut émettre à un instant t. Le risque potentiel de collisions est donc plus élevé. Ce mode est quasi-exclusivement utilisé pour les connexions à des hubs.

FULL DUPLEX

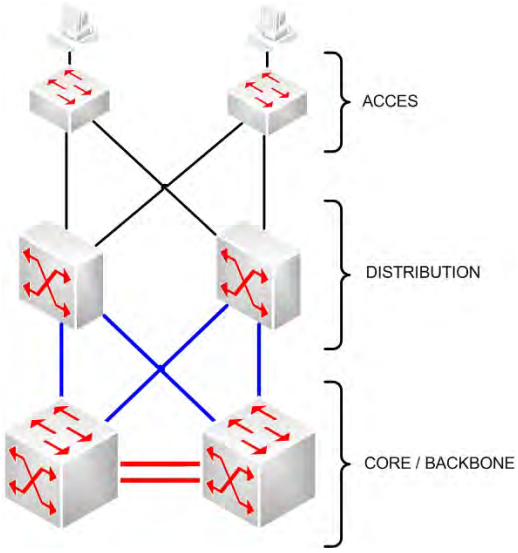
Le flux de données est bidirectionnel. Une machine peut simultanément émettre et recevoir. La détection de collision est, par conséquence, désactivée.

Ce mode ne fonctionne qu'en point à point. C'est le cas des connexions :

- Entre un PC et un pont ou un commutateur
- Entre deux ponts
- Entre deux commutateurs
- Entre deux PCs
- Entre un routeur et un commutateur ou un pont

Il faut que les machines aux deux extrémités soient compatibles full-duplex. Dans les réseaux modernes, la majorité des connexions Ethernet est en full-duplex.

Topologie commutée



- Trois niveaux sont définis en topologie commutée :
  - Le niveau ACCES permet la connexion des PCs, des serveurs et des téléphones IP
  - Le niveau DISTRIBUTION est chargé du routage IP, du filtrage, de la QoS et de la sécurité
  - Le niveau CORE est chargé de transmettre le plus rapidement possible les données d'un point à un autre

Afin d'avoir une vision plus claire du réseau, mais aussi de faciliter le dépannage et l'évolutivité, on utilise un modèle topologique à trois niveaux :

NIVEAU ACCES

Le rôle de ce niveau est de fournir, aux machines utilisatrices, les différentes méthodes d'accès au réseau. Le niveau accès est constitué par tout ce qui permet à une machine d'accéder au réseau. Les hubs, les ponts, les points d'accès WiFi, les antennes radio et, dans certains cas, les routeurs constituent un point d'entrée sur le réseau.

NIVEAU DISTRIBUTION

Le niveau distribution est constitué de commutateurs de niveau 2 et 3, c'est-à-dire de commutateur possédant également des fonctionnalités spécifiques de routage.
Ils sont chargés des tâches suivantes :

- Le routage IP. C'est à ce niveau qu'est réalisé le routage inter-vlans, qui permet au VLANs de communiquer entre eux grâce à l'adressage et au routage logique.
- Le filtrage. Les commutateurs de niveau 3 peuvent également filtrer les paquets provenant des commutateurs de niveau ACCES.
  Les filtres sont constitués de règles testées séquentiellement. Une règle est elle-même constituée de deux éléments : une ou plusieurs conditions et une action. L'action n'est accomplie qu'en cas de correspondance des conditions avec les caractéristiques de la trame Ethernet ou du datagramme IP.
  Les actions sont :
  - ➔ Permit, la trame ou le datagramme est autorisé
  - ➔ Deny, la trame ou le datagramme est rejeté

Les conditions Ethernet peuvent porter sur :

➔ L'adresse MAC source

➔ L'adresse MAC destination

➔ Le type de protocole

➔ La longueur de la trame

➔ L'interface de réception

Les conditions sur IP peuvent porter sur :

➔ L'adresse IP source

➔ L'adresse IP destination

➔ Le protocole

➔ Le port source

➔ Le port destination

➔ La fragmentation

➔ La valeur des bits de contrôle (SYN, ACK, PSH, RST…)

- La QoS, Quality of Service. Elle consiste à :

  ➔ Identifier et classifier les applications. L'identification se fait le plus souvent par reconnaissance des ports de destination et du protocole de niveau 4 utilisé. La classification permet de définir la classe à laquelle appartient une application et les paramètres associés. Les classes définissent les types d'applications courantes : DATA, DATA sensible, VoIP…
  Les paramètres associés sont :
  ✓ Le délai de transit sur le réseau
  ✓ La variation de ce délai
  ✓ Le débit garanti
  ✓Le taux de pertes acceptable

  ➔ Définir leur niveau de priorité

  ➔ Gérer la congestion en tenant compte des caractéristiques des applications

  ➔ Anticiper la congestion

- Assurer la sécurité du réseau. Cela concerne tout ce qui est firewalling, détection d'intrusion, analyse réseau…

NIVEAU CORE / BACKBONE

Ce niveau a le rôle le plus simple, mais le plus exigeant : commuter le plus rapidement possible les trames reçues. Le CORE n'est pas un réseau de destination, mais un réseau de transit. Il faut manipuler le moins possible les données à ce niveau. Le but est la performance, la vitesse. L'idéal est d'obtenir en plus un délai de transit constant quelque soit la source et la destination.

Longtemps, ce niveau était exclusivement constitué de gros commutateur de niveau 2. Actuellement il est également possible d'utiliser des commutateurs de niveau 3. Ces derniers sont devenus à la fois très performants et abordables, comparativement à leurs performances bien sûr.

VLAN

- Virtual Lan : Lan virtuel
- On peut « découper » un commutateur en plusieurs commutateurs indépendants
- Un VLAN est identifié par un ID
- Le nombre de vlan dépend du matériel
- Un commutateur simple ne sait pas router entre les VLANs
- Souvent, le VLAN 1 est le vlan de maintenance
- Le « découpage » peut se faire :
  - Par adresse MAC
  - Par numéro de port

Un VLAN est un lan virtuel, un domaine de broadcast. Une machine ne peut communiquer directement qu'avec les machines rattachées au même VLAN qu'elle.

Il est possible de « découper » un commutateur en plusieurs commutateurs indépendants, en autant de VLANs.

Un VLAN est identifié par un ID sur 12 bits. Au maximum, on peut donc définir 2^12=4096 VLANs sur un commutateur donné. Le nombre réel de VLANs que peut gérer un commutateur dépend de ses caractéristiques matérielles.

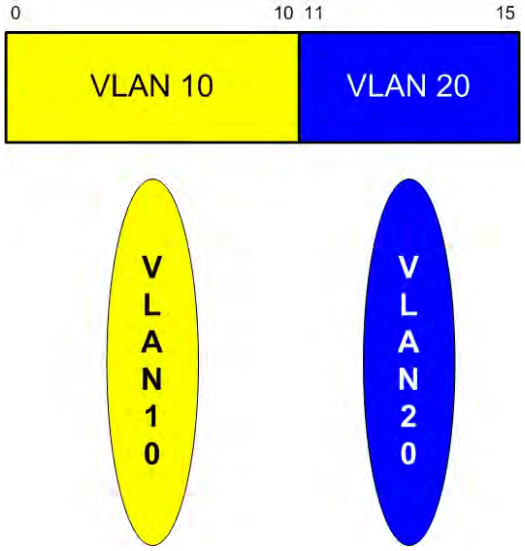
Insistons sur le fait qu'un commutateur de niveau 2 ne sait pas interconnecter des VLANs. Il faut pour cela disposer d'un routeur, autonome ou intégré au commutateur.

Souvent, chez la plupart des fabricants, le VLAN 1 est le VLAN de maintenance. C'est via ce VLAN que l'on peut administrer les machines d'infrastructure du réseau : commutateurs, routeurs, firewalls, sondes d'intrusion…

Un VLAN peut être défini par :

- Les adresses MAC des machines. C'est-à-dire qu'une machine sera toujours associée au même VLAN quelque soit son point de connexion sur le réseau. Ce type de VLAN est également appelé VLAN dynamique.
- Les numéros de ports des commutateurs. Dans ce cas, c'est le port qui est associé avec un VLAN. Autrement dit, quelque soit la machine connectée sur un port, elle sera associée au VLAN auquel est rattaché le port. Ce type de VLAN est également appelé VLAN statique. Un port ne peut appartenir qu'à un seul VLAN à un instant t, à l'exception des ports trunks qui appartiennent, par défaut, à tous les VLANs. Par défaut, les ports appartiennent tous au VLAN par défaut, souvent le VLAN 1.

Exemple 1

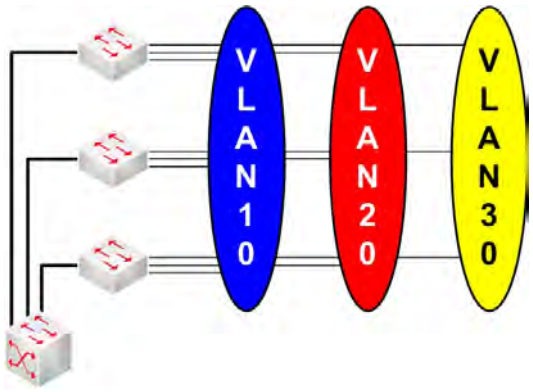


- Les ports 0 à 10 sont associés au VLAN 10
- Les ports 11 à 15 sont associés au VLAN 20
- Tout se passe comme si nous avions deux LAN physiquement séparés
- Pour communiquer directement entre elles, deux machines doivent être dans le même VLAN

Sur le commutateur, les ports 0 à 10 sont associés au VLAN 10, les ports 11 à 15 étant associés au VLAN 20.
En fait, tout se passe comme si nous avions physiquement deux LAN physiquement séparés. Comme si nous avions deux commutateurs indépendants.

La topologie est très souple, car il est très simple d'agrandir un VLAN et d'en réduire un autre. Par exemple supposons que le VLAN 10 soit trop petit de 2 ports et le VLAN 20 trop grand de 2 ports vis-à-vis des besoins du réseau. Il suffit de déclarer les ports 0 à 13 dans le VLAN 10 et les ports 14 et 15 dans le VLAN 20. Aucun recâblage n'est nécessaire, tout est fait logiquement, par configuration.

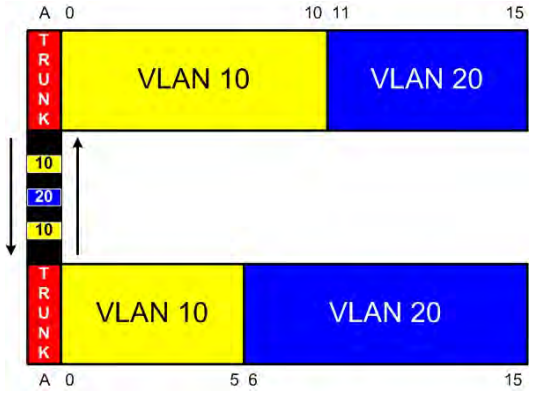
Exemple 2



- Les VLANs 10, 20 et 30 sont répartis sur plusieurs commutateurs
- Ils sont définis selon les entités administratives de l'entreprise
- Les VLANs sont créés indépendamment des localisations physiques des machines
- Ces VLANs sont dits « end to end »

- Mais, il est également possible de définir des VLANs répartis sur plusieurs commutateurs, en ne tenant compte que des entités administratives.
- Ces VLANs sont donc créés indépendamment des localisations physiques des machines. Sur un même commutateur, deux machines connectées à des VLANs différents ne pourront pas communiquer directement entre elles.
- Par exemple, le VLAN 10 est celui des comptables, le VLAN 20 celui des commerciaux et le VLAN 30 celui des informaticiens.
- Ces VLANs sont qualifiés de « end to end ».

Trunk



- Les trunks permettent l'échange de trames entre les commutateurs
- Problème : Quand un VLAN est réparti sur plusieurs commutateurs, comment identifier le VLAN ?
- Solution : Le VLAN ID est tagué dans les trames par les commutateurs sur les liens trunks
- Le standard IEEE 802.1q est la technique la plus répandue

PROBLEMATIQUE

Une problématique apparait quand un VLAN est réparti sur plusieurs commutateurs : comment vont s'échanger les données entre eux ? Comment un commutateur recevant une trame sur un trunk déterminera-t-il le VLAN de destination ? Dans notre exemple : est-ce que la trame sera à destination du VLAN 10 ou du VLAN 20 ?

802.1q

La solution est de taguer les trames qui transitent sur les liens trunks :

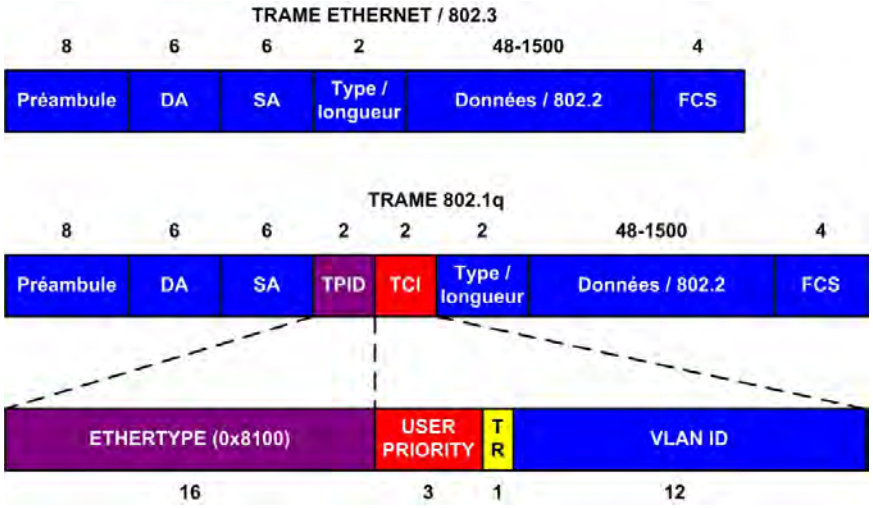
- Le commutateur transmetteur de la trame indiquera le VLAN ID en ajoutant un champ supplémentaire à la trame Ethernet.
- Le commutateur récepteur lira le tag et le supprimera avant de transmettre la trame dans le VLAN indiqué.

Cette méthode est normalisée dans le standard IEEE 802.1q.

Une trame reçue sur un trunk utilisant l'encapsulation 802.1q sans tag sera transmise dans le VLAN natif. Souvent, le VLAN natif est le VLAN 1.

Précision importante :
Le VLAN par défaut est celui auquel sera affecté par défaut tout port d'un commutateur.
Le VLAN natif sera celui dans lequel sera transmise une trame n'ayant pas de tag sur un trunk 802.1q.

802.1q



PRINCIPE

Le marquage des trames fonde l'appartenance à un réseau virtuel. Ce marquage est notamment nécessaire lorsque l'on utilise des trunks et des VLANs « end to end », répartis sur plusieurs commutateurs.

Deux types de marquage des trames existent :

- Implicite :
  - ➔ Port de réception
  - ➔ Contenu de la trame : adresse MAC, protocoles de niveau 3, adresse de sous-réseau, contenu de certains champs
- Explicite :
  - ➔ Chaque trame possède un identificateur caractérisant son appartenance à un réseau virtuel
  - ➔ Ajout d'un en-tête à chaque trame
  - ➔ Selon la norme 802.1q, cet en-tête est inséré immédiatement après les adresses MAC

    Deux champs sont utilisés :
  - ➔ TPID (Tag Protocol Identifier) : indicateur de protocole VLAN. Indique le type de protocole Ethernet
  - ➔ TCI (Tag Control Information) : identificateur de réseau virtuel

NOMENCLATURE D'UNE TRAME 802.1q

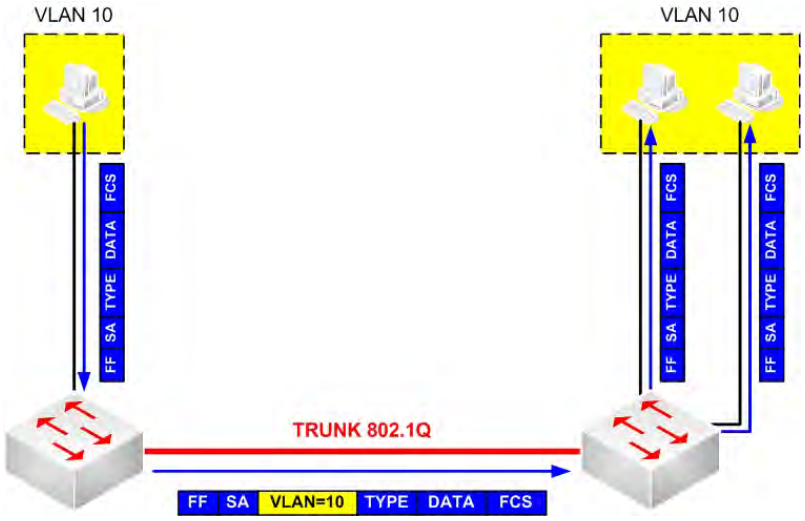
L'en-tête 802.1q, le tag, est inséré immédiatement après l'adresse MAC source. Sa longueur est de 4 octets. Une trame 802.1q aura donc une longueur maximale de 1522 octets (1518+4).

L'en-tête est composé de deux éléments :

- Le TPID (Tag Protocol Identifier). Il indique le type de protocole Ethernet utilisé. Actuellement la seule valeur utilisée est 0x8100 permettant d'identifier les trames Ethernet tagués. En effet, sur un trunk en 802.1q, peuvent circuler des trames taguées et des trames non taguées. Comment un commutateur fait la différence entre les deux ? Grâce à la valeur qu'il va lire juste après l'adresse MAC source : si c'est 0x8100, c'est une trame taguée, sinon c'est une trame Ethernet ou 802.3 « normale », non taguée.
- Le TCI (Tag Control Information). Cet élément est composé de trois champs :
  - ➔ Le VLAN ID codé sur 12 bits.
  - ➔ USER PRIORITY. Ce champ codé sur 3 bits permet d'indiquer le niveau de priorité de la trame. Cette valeur n'est utilisée qu'en cas de congestion du réseau. On peut d'ailleurs mapper les valeurs de ce champ avec celles du champ ToS / Precedence de IP. Ou mieux encore avec la classe définie dans le champ ToS / DSCP.
- Enfin, le bit TR permet d'indiquer le caractère canonique d'une trame transmise de Ethernet vers Token Ring. Sur un commutateur Ethernet, cette valeur est toujours à zéro.

Il existe une alternative à 802.1q : ISL de CISCO. Cette encapsulation est propriétaire. Le principe est de réencapsuler les trames Ethernet dans des trames ISL. Les performances et les fonctionnalités sont proches. 802.1q a tendance à s'imposer, même chez CISCO.

Exemple



Supposons que la machine sur le commutateur de gauche, dans le VLAN 10, émette un broadcast. Un broadcast doit atteindre toutes les machines dans le VLAN10. :

- Le commutateur de gauche reçoit le broadcast et émet une copie sur chaque port appartenant au VLAN 10… sans oublier le port trunk.
- Avant de l'émettre sur le port trunk, le commutateur ajoute les 4 octets d'en-tête 802.1q. Ce qui inclut l'identifiant 10 pour le VLAN ID.
- Le commutateur de droite reçoit la trame 802.1q.
- Il lit le champ VLANID et transmet le broadcast sur tous les ports associés au VLAN 10. Le commutateur prend soin, avant cette transmission, de supprimer l'en-tête 802.1q.

Types de ports

- Access :
  - Généralement, port d'extrémité relié à des stations, des serveurs ou des téléphones IP
  - Les trames ne sont pas « taguées »
  - Un seul VLAN associé à ce type de port
- Trunk :
  - Accepte des trames taguées et des trames non taguées
  - Plusieurs VLANs peuvent être associés à ce type de port
- Hybrid :
  - Supporte les deux modes
  - C'est la connexion et la configuration qui détermineront le mode de fonctionnement

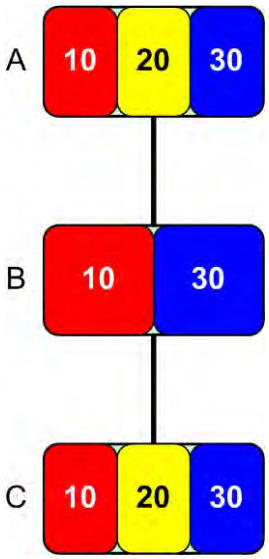
Les ports d'un commutateur peuvent être de trois types :

- Access. Ce qui signifie que c'est un port d'extrémité de l'infrastructure. Sur ces ports, seuls des stations, des serveurs et des téléphones IP seront connectés.
  Les trames reçues sur ces ports seront forcément non taguées. On ne peut associer qu'un seul VLAN à ce type de port.
- Trunk. Dans ce cas, le port accepte des trames taguées et des trames non taguées qui seront transmises dans le VLAN natif.
  Par défaut, les ports trunk sont associés à tous les VLANs définis sur un commutateur. Il est possible de restreindre, pour des questions d'efficacité ou de sécurité, la liste des VLANs associés à un port trunk.
- Hybrid. Ce sont les ports qui supportent les deux modes. Il y a deux cas de figure :

  ➔ Définition du mode par configuration, manuellement.

  ➔ Définition du mode dynamiquement, par détection du commutateur.

Problématique des VLANs « end to end »



- Sur le commutateur B, il n'y a pas de VLAN 20
- Si le commutateur A envoie une trame avec le VLAN ID 20, le commutateur détruira la trame
- Deux possibilités :
  - Créer le VLAN 20 sur le commutateur B, sans affectation de ports
  - Utiliser le protocole GVRP qui permet l'échange standardisé d'information sur les VLANs entre commutateurs

PROBLEMATIQUE

La problématique des VLANs « end to end » est l'obligation pour chaque commutateur intermédiaire sur le réseau d'avoir tous les VLANs déclarés, même si aucune assignation de port n'est faite.

EXEMPLE

Prenons comme exemple significatif de ce problème le réseau représenté sur le schéma. Sur le commutateur B, le VLAN 20 n'existe pas. Si B reçoit de A une trame taguée avec le VLAN ID 20, que va faire B ? Il détruit la trame, car le VLAN n'existe pas dans sa table de VLAN. Cette table va référencer tous les VLANs créés sur le commutateur. On l'appelle aussi parfois la VLAN Database.

Que faire pour que B transmette la trame à C via leur trunk commun ?
Il existe deux solutions, deux possibilités :

- Créer le VLAN 20 sur B. Aucune affectation de port n'est nécessaire. De fait, quand B recevra une trame taguée avec le VLAN 20, il la transmettra sur le trunk commun avec C. N'oublions pas que les trunks appartiennent, par défaut, à tous les VLANs. Cela fonctionne, mais l'opération peut être automatisée et dynamisée.
- Utiliser le protocole GVRP. Il permet l'échange standardisé d'information sur les VLANs entre les commutateurs.

GVRP

GVRP : GARP VLAN Registration Protocol. GARP : Generic Attribute Registration Protocol.

Autrement dit, cela ne veut pas dire grand-chose mit bout à bout.

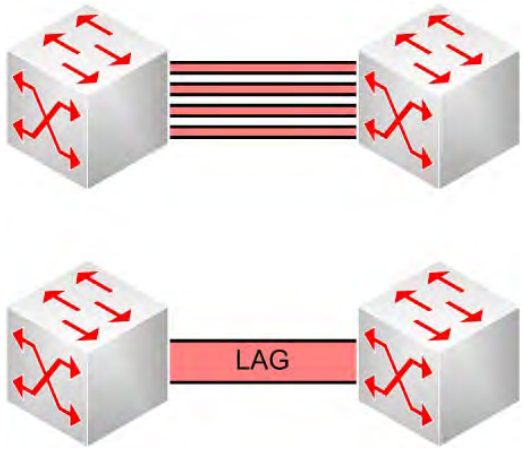
GVRP permet l'échange STANDARDISE d'informations sur les VLANs via 802.1q entre les commutateurs. GVRP est défini dans les spécifications IEEE 802.1p. Il est utilisé uniquement sur les ports trunks et sur le VLAN par défaut, généralement le VLAN 1.

Dans notre exemple, il n'y aurait pas eu besoin de déclarer le VLAN 20 sur B pour que C reçoive les trames de A. Via GVRP, B aurait apprit que le VLAN existait sur le réseau et aurait donc dynamiquement créé le VLAN 20 en local.

Une fonction de prunning (élagage) est également activable optionnellement afin d'éviter les doublons.

Il existe une alternative à GVRP : VTP de CISCO.

802.3ad



- Permet l'agrégation standardisée de liens entre les commutateurs via le protocole LACP (Link Aggregation Control Protocol) qui fonctionne aux niveaux 2 et 3
- LACP :
  - Permet la répartition de charge par Round-robin ou par charge de lien
  - Redistribution rapide de la charge en cas de défaillance d'un lien
- LAG (Link Aggregation Group) : ensemble de liens agrégés

PROBLEMATIQUE

Quand on veut relier des commutateurs entre eux, on utilise des liens trunks. Le problème est que le débit standard Ethernet le plus rapide est de 10Gbps, à comparer aux centaines de Gbps de fonctionnement d'un fond de panier d'un commutateur backbone.
Alors, que faire ? Relier les commutateurs avec plusieurs liens trunks ? Techniquement, cela ne pose aucun problème. En revanche, cela en pose un à Spanning-Tree. En effet, un seul des liens trunks sera réellement actif, les autres seront simplement des liens de secours en cas de défaillance. Le chemin entre deux points quelconques du réseau doit être unique. Une des solutions est d'utiliser le protocole LACP.

LACP

Le protocole LACP (Link Aggregation Control Protocol) permet l'agrégation standardisée de liens entre les commutateurs. Il fonctionne aux niveaux 2 et 3.

- Au niveau 2, LACP permet de créer une interface virtuelle, un LAG (Link Aggregation Group). Spanning-Tree ne verra plus les liens individuellement, mais uniquement cette interface. Plus de problèmes donc, on peut utiliser au mieux la bande passante disponible. Dans notre exemple, au lieu de voir 4 interfaces Gigabit, Spanning-Tree n'en verra qu'une, le LAG, en 4 Gbps. Le nombre d'interfaces que l'on peut agréger et le nombre de LAG dépend du constructeur et du modèle.
  On peut effectuer la répartition de charge de deux façons :
  - ➔ Par Round Robin. Les données seront reparties cycliquement sur chaque interface physique. C'est de loin la méthode la plus utilisée. En cas de défaillance d'une interface, la répartition se contractera sur celles qui sont toujours actives.

➔ Par charge de lien. Quand un lien atteint une certaine charge, le commutateur active l'interface suivante. En obsolescence.

- Au niveau 3. Le LAG possèdera une adresse IP commune à l'ensemble des interfaces physiques le composant. Cela permet de simplifier les chemins redondants utilisés en routage IP. Cette fonctionnalité n'est évidement disponible que sur les routeurs et les commutateurs de niveau 3.

Port mirroring / SPAN

- Le principe du port mirroring ou SPAN, est de répliquer le trafic d'un port vers un autre port
- Le port « répliqué » continue à fonctionner normalement, mais pour toute émission ou réception, une copie est envoyée au port SPAN
- Le port SPAN fonctionne uniquement en réception
- Il est également possible d'écouter un port situé sur un autre commutateur : c'est la technique du remote SPAN
- Usages :
  - Détection de problème de configuration ou de fonctionnement
  - Détection de trafic anormal, généralement opéré par les sondes d'intrusion

PRINCIPE

Le principe du port mirroring ou SPAN, est de répliquer le trafic d'un port vers un autre port sur un commutateur. Il est possible d'y associer un filtre afin de ne capturer que le trafic intéressant pour l'analyse.
Le port « répliqué » continue à fonctionner normalement, mais pour toute émission ou réception, une copie est envoyée au port SPAN. Le port SPAN fonctionne uniquement en réception. Selon le matériel, le port SPAN est fixe ou peut être assigné à n'importe quel port du commutateur.
Il est possible, sur certains matériels, d'écouter tous les ports du commutateur simultanément. Néanmoins, cela induit une charge très importante sur le fonctionnement du commutateur.

REMOTE SPAN

Il est également possible d'écouter un port situé sur un autre commutateur : c'est la techniques dite du Remote SPAN ou RSPAN. Le principe consiste à créer un Virtual VLAN (sic) que l'on associera aux ports écouté et au port écoutant. Il est ainsi facile de pouvoir filtrer et de gérer le trafic dans ce VVLAN. Attention cependant, le port écouté est toujours associé à son VLAN propre, le VVLAN constitue simplement une astuce et une affectation purement formelle.

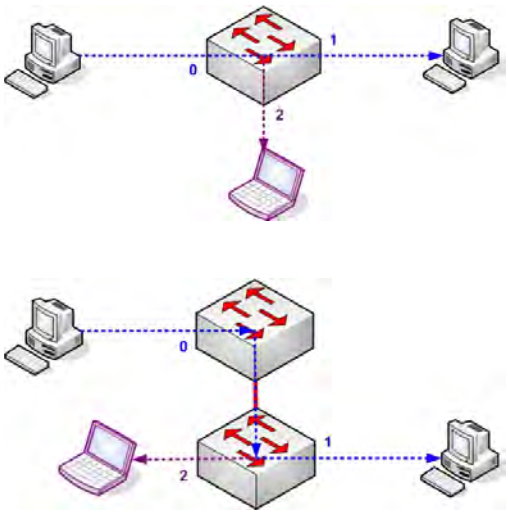
USAGE

Quand utilise-t-on le SPAN ou le RSPAN ?

- Afin de détecter des problèmes de configuration ou de fonctionnement du réseau, d'une application, d'un protocole.

- Afin de détecter du trafic anormal, suspicieux. Cette opération est notamment opérée par les sondes d'intrusion réseau.
- Enfin, afin de mieux comprendre certains mécanismes réseau ou applicatifs.

Exemples



- SPAN
  - Deux machines échangent des données via les ports 0 et 1
  - Le port 2 est mis en SPAN avec réplication du trafic du port 0
- Remote SPAN
  - Deux machines, connectées sur des commutateurs différents, échangent des données via les ports 0 et 1
  - Le port 2 d'un des deux commutateurs est mis en port SPAN avec réplication du trafic du port 0 de l'autre commutateur

Nous avons ici deux exemples, un de SPAN et un de RSPAN :

- SPAN. On désire analyser ce qui se passe entre les ports 0 et 1 d'un commutateur. On place le port 2 en SPAN en indiquant les ports concernés par l'analyse. Sur le port 2, on connecte généralement un portable avec un outil d'analyse réseau adapté.
- RSPAN. On désire analyser ce qui se passe entre les ports 0 d'un commutateur et le port 1 d'un autre commutateur. On place le port 2 d'un des commutateurs en SPAN en indiquant le VVLAN concerné par l'analyse. Sur le port 2, on connecte généralement un portable avec un outil d'analyse réseau adapté.

Routage inter-VLAN

- Un commutateur simple travaille purement au niveau 2, il ne sait donc pas interconnecter des VLANs
- Plusieurs solutions possibles pour interconnecter les VLANs :
  - Le routeur possède une interface physique dans chaque VLAN
  - Le routeur est relié au commutateur par un lien trunk, en 802.1q, et l'interface sera subdivisée en sous interfaces, chacune appartenant à un VLAN
  - Le routeur est directement connecté au fond de panier du commutateur :
    - •Par ajout d'une carte de routage sur les commutateurs modulaires
    - •En natif sur le commutateur

PROBLEMATIQUE

Pour interconnecter des VLANs, il faut du routage logique, IP la plupart du temps.

Un commutateur simple travaille uniquement au niveau 2. Il ne fait donc pas de routage logique. Il faut donc disposer d'un routeur. Il existe trois solutions pour disposer du routage logique permettant d'interconnecter les VLANs :

ROUTEUR AUTONOME SIMPLE

La solution la plus simple est le routeur autonome disposant d'une interface physique par VLAN. Autrement dit, s'il existe 10 VLANs dans le réseau, le routeur devra posséder 10 interfaces physiques, chacune connectée à un port associé à chaque VLAN.

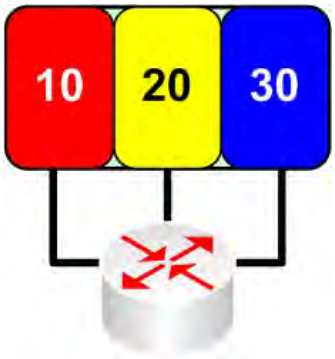
Avantages :

- Simple à mettre en place
- Peu coûteux

Inconvénients :

- Evolutivité limitée. Le nombre d'interface dont dispose un routeur n'est pas extensible à l'infini.
- Débit limité. Le débit est limité par l'usage d'interfaces standard reliant le routeur au commutateur.
- Performances minimales. Plus le routeur devra interconnecter de VLANs, plus les performances vont se dégrader. De plus, un routeur réalise l'essentiel de ses

fonctions logiciellement, ce qui induira des variations dans les délais de traitement des datagrammes IP.



ROUTEUR AUTONOME EN 802.1q

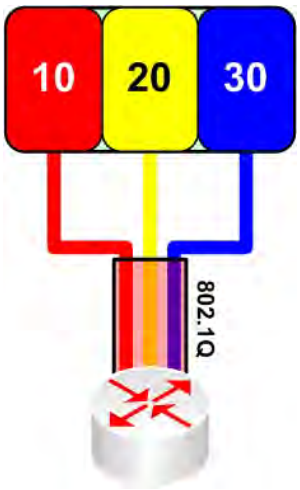
Solution plus évoluée et plus souple. Le principe consiste à connecter le routeur au commutateur via un lien 802.1q. Ensuite, l'interface trunk sera découpée logiquement en autant de sous-interfaces qu'il y a de VLANs, chaque sous-interface étant affectée à un VLAN.

Avantages :

- Simple à mettre en place
- Peu coûteux
- Evolutivité plus grande que le routeur autonome simple. A chaque ajout d'un nouveau VLAN, il suffira de créer une nouvelle sous-interface.
- On peut utiliser des LAGs grâce à l'encapsulation 802.1q, et ainsi augmenter le débit d'interconnexion

Inconvénients :

- Les performances intrinsèques du routeur présentent toujours les mêmes limitations : traitement massivement logiciel, variation des délais de traitements.
- Pour les réseaux très chargés ou très performants, le LAG reste tout de même une limitation.



COMMUTATEUR DE NIVEAU 3

Un commutateur de niveau 3 est un commutateur qui en plus des fonctionnalités de niveau 2 afférentes à son rôle, dispose également du routage logique. Autrement dit, qui intègre à la fois un commutateur et un routeur. Les routeurs utilisés en commutation de niveau 3 sont légèrement différents des routeurs autonomes habituels :

- Ils intègrent un maximum de composants ASICs dédiés à des fonctions particulières. On élimine au maximum le traitement logiciel des tâches de routage.
- Ils sont beaucoup plus puissants en capacité de traitement.
- Ils sont directement connectés au fond de panier du commutateur. Ce qui permet d'éliminer les limitations physiques des interfaces standard.

Les commutateurs de niveau 3 existent sous deux formes :

- Des cartes (des blades) d'extension que l'on ajoute sur les commutateurs modulaires
- Intégrés directement dans le châssis du commutateur

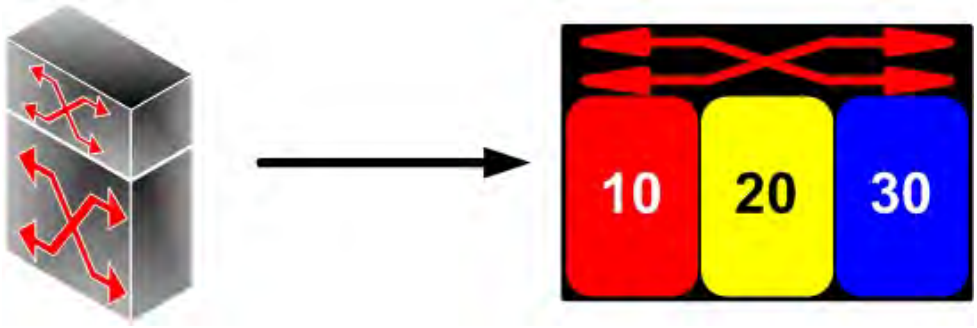
Avantages :

- Routage inter-vlan plus performant et plus simple à réaliser
- Débit de connexion
- Puissance de traitement
- Variation des délais de traitement faible

Inconvénients :

- Fonctionnalités plus restreintes que les routeurs autonomes
- Evolutivité moindre
- Usage spécifique
- Prix en conséquence

Actuellement, les commutateurs de niveau 3 atteignent de telles performances qu'ils sont utilisés même dans les cœurs de réseaux des opérateurs. C'est le cas, par exemple, du CRS-1 de CISCO.



Commutation de niveau 4

- En général, module inséré ou intégré dans un commutateur
- Le fonctionnement des protocoles de transport est optimisé via l'utilisation de composants dédiés (ASICs) : TCP, UDP, OSPF…
- Avantages
  - Transport des données plus performant
  - Utilisation du fond de panier du commutateur
- Inconvénients
  - Coût
  - Matériel dédié
  - Évolutivité limitée

PRINCIPE

Enfin, la dernière innovation dans ce domaine concerne la commutation de niveau 4. Le principe est identique à la commutation de niveau 3 :

- On « câble » au maximum les fonctionnalités
- On optimise le fonctionnement afin de pouvoir fournir des variations de délais de transmission les plus constants possibles

USAGE

L'usage de la commutation de niveau 4 concerne les deux domaines suivants :

- Renforcer la QoS et garantir ou faciliter son application, voir fournir de nouvelles possibilités
- Améliorer le fonctionnement de certains applicatifs particuliers. Ce qui peut être le cas de certains gros serveurs http, de grandes bases de données…

CARACTERISTIQUES

La commutation de niveau 4 existe sous deux formes :

- Un module additionnel inséré dans un commutateur modulaire
- Intégré directement sur des commutateurs dédiés à la QoS et à l'optimisation du transport de certains applicatifs

Avantages :

- Transport des données plus performant

- Variations des délais de transmission faibles
- Directement connecté sur le fond de panier

Inconvénients :

- Évolutivité limitée
- Matériel dédié, donc usage limité et spécifique
- Coût conséquent

- *WLAN*
- *802.11*
- *802.11a/b/g/n*
- *Sécurité*
- *WEP*
- *WPA*
- *EAP*

4

WiFi

Objectifs

Ce module traite des réseaux WLAN et plus particulièrement des normes 802.11 ou WiFi.

Connaissances

- Les WLAN
- Les normes 802.11
- Les topologies sans fils
- Les extensions de WLAN
- Les fréquences utilisées
- Maillages des canaux
- Les méthodes de communication
- La sécurité WiFi

Progression

Présentation	802.11b
Réseaux informatiques sans fils	802.11g
WLAN	802.11n
Topologies	Sécurité
SSID	WEP
Extensions des WLAN	WPA
Méthodes de communication	EAP
802.11	RADIUS
802.11a	

Présentation

- Le principe est de transporter de la voix ou des données via des ondes radios
- Les réseaux sans fils offrent une souplesse d'utilisation (accès) et de déploiement (couverture) plus grandes que celles des réseaux filaires
- Cette souplesse d'utilisation implique également des contraintes différentes
  - Connexion : couverture, chemins multiples, interférences, bruit
  - Confidentialité
- Les topologies d'accès sont par conséquent spécifiques
- Les technologies les plus répandues sont :
  - 802.11
  - Bluetooth

PRINCIPES

- Le principe des réseaux sans fils est de transporter des données ou de la voix via des ondes radio. Le média est donc l'air.
- Les réseaux sans fils offrent une souplesse d'utilisation au niveau de l'accès au réseau, et une facilité de déploiement au niveau de la couverture, supérieures aux réseaux filaires.
- Cette souplesse d'utilisation implique, et s'accompagne, de contraintes différentes :
  - ➔ Au niveau de la connexion. Il faut tenir compte :
    - ✓ Des problèmes de zone de couverture des émetteurs
    - ✓ Des chemins multiples
    - ✓ Des interférences
    - ✓ Du bruit
    - ✓ Des obstacles absorbants ou au contraire réfléchissants
  - ➔ Au niveau de la confidentialité. Le média étant l'air, il est on ne peut plus indiscret.
- Les topologies et les méthodes d'accès sont, par conséquent, spécifiques.

- Les technologies actuellement les plus utilisées sont :
  - ➔ Les normes 802.11 (a, b, g et n). Utilisé aussi bien en entreprise, sur des lieux publics que chez les particuliers.
  - ➔ Bluetooth. Usage beaucoup plus restreint. Le rayon d'action, les débits disponibles et les fonctionnalités restreintes en limitent l'usage à des connexions brèves, à faible débit et occasionnelles. On rencontre le Bluetooth essentiellement pour la connexion de petits appareils à faible puissance informatique.

Sans fils vs filaire

- Avantages des réseaux sans fils :
  - Accès plus simple et moins contraignant (mobilité)
  - Déploiement
  - Couverture des sites et mutualisation
- Inconvénients :
  - Débits actuellement moins importants
  - Sécurité
  - Technologies moins mûres

Analysons les avantages des réseaux sans fils vis-à-vis des réseaux filaires.

AVANTAGES

- Accès plus simple au média. Le média étant l'air, le contact physique est élémentaire.
- Moins de contraintes. Il est possible de se déplacer physiquement, dans la limite de couverture d'un point d'accès (AP, Access Point) ou WLAN (maillage d'AP). Une mobilité native minimale est donc disponible.
- La couverture d'un site est plus simple à réaliser. Dans les lieux de grandes surfaces accueillants de fortes densités de population, il est facile de rendre disponible l'accès au réseau. C'est le cas des hôpitaux, des aéroports, des centres de conférences, des hôtels, des universités, des écoles, des centres de formation, des usines, des gares, des Open Space…
- Enfin, la mutualisation est également plus simple à réaliser. On peut beaucoup plus facilement partager un accès radio que n'importe quel autre média. D'ailleurs, la technologie WiMax permet de partager sa propre borne avec d'autres utilisateurs.

INCONVENIENTS

- Les méthodes d'accès, la spécificité du média et la maturité encore limitée des technologies limitent les débits disponibles. Toutefois, les technologies progressent très rapidement, et le 802.11n permet, théoriquement, de disposer de 320 Mbps.
- Le fait que le média soit l'air, n'est pas toujours une bonne chose d'un point de vue de la sécurité, car la protection au niveau physique est plus délicate qu'avec les réseaux filaires.

- De plus, certaines « légèretés » de conception initiales et l'usage de certaines techniques de sécurité peu performantes ont induit des failles importantes de sécurité dans les technologies d'accès sans fil.

Réseaux informatiques sans fils

- Les réseaux informatiques offrent les avantages suivants :
  - Débits devenus élevés
  - Coûts plus faibles en utilisation que les réseaux cellulaires et filaires
  - Mutualisation des accès
  - Interconnexion avec les réseaux filaires
- Et les inconvénients suivants :
  - Distance entre l'émetteur et le récepteur faible, voire très faible
  - Certaines technologies ne sont pas encore mûres
  - Couverture encore faible

Les réseaux informatiques sans fils ont les caractéristiques suivantes :

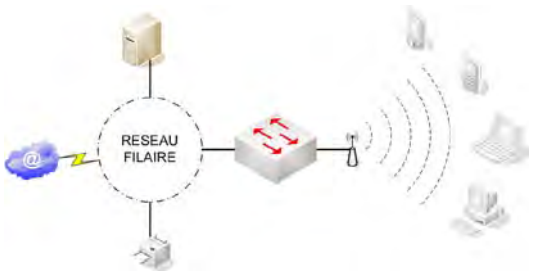
AVANTAGES

- Des débits de plus en plus élevés, qui permettent de disposer d'accès devenus confortables
- Les coûts sont relativement faibles par rapport au filaire et au cellulaire
- La mutualisation des accès est intrinsèque
- L'interconnexion avec les réseaux filaires est native

INCONVENIENTS

- Les distances entre les émetteurs et les récepteurs sont encore faibles. Et, surtout, le débit diminue très rapidement avec l'augmentation de cette distance.
- Par ailleurs, certaines technologies ne sont pas encore arrivées à un degré de maturation suffisant. Mais, cela se fait à grands pas…
- Enfin, la couverture reste encore limitée. Deux choses limitent la couverture :
  - ➔ Le rayon d'action des émetteurs, limité par les technologies utilisées et par la régulation limitant les puissances d'émission.
  - ➔ Le nombre limité d'utilisations connectées simultanément. Là encore, les AP (Access Point) ont fait des bonds spectaculaires en performances.

WLAN



- Un WLAN (Wireless LAN) est un réseau partagé
- Un point d'accès (AP, Access Point) permet l'accès au réseau
- Un AP fonctionne comme un hub Ethernet partagé
- Les accès se font en Half duplex
- On utilise la même fréquence pour l'émission et la réception
- La méthode d'accès utilisée est le CSMA/CA
- Un répéteur permet d'amplifier un signal radio affaibli afin d'accroitre la couverture d'un AP.

CARACTERISTIQUES

Un réseau WLAN a les caractéristiques suivantes :

- Un WLAN, Wireless LAN, est, littéralement, un réseau sans fil partagé.
- Les accès se font en half duplex. Une machine ne peut simultanément émettre et recevoir, car la même fréquence radio est utilisée pour l'émission et la réception des données.
- La méthode d'accès est du type CSMA/CA (Carrier Sense Mulitple Access / Collision Avoidance). Contrairement à l'Ethernet filaire, on ne peut détecter une collision. On va donc tenter de les empêcher autant que faire se peut.

COMPOSANTS

Un WLAN a les composants suivants :

- Le point d'accès ou AP, Access Point. C'est l'élément le plus commun, matérialisé par les bornes d'accès qui ont fleuri un peu partout ces dernières années. Un AP fonctionne comme un hub Ethernet partagé par ses clients. Son rôle principal consiste à permettre l'accès de ses clients aux ressources du réseau filaire auquel il est rattaché.
- Des clients. Ils disposent du matériel et du logiciel nécessaires pour se connecter au point d'accès.
- Des répéteurs. Un répéteur permet d'amplifier un signal radio afin d'accroitre la couverture d'un point d'accès.

Topologies (1)

- Connectivité mobile :
  - Permet aux utilisateurs d'accéder aux ressources des réseaux filaires
  - Utilisation la plus répandue
  - Utilise des antennes omnidirectionnelles
  - 802.11b, g et n
- Connectivité LAN-to-LAN
  - Utilisée pour connecter entre eux des réseaux éloignés
  - Utilise des antennes unidirectionnelles
  - 802.11a

Il existe principalement trois grandes topologies WLAN :

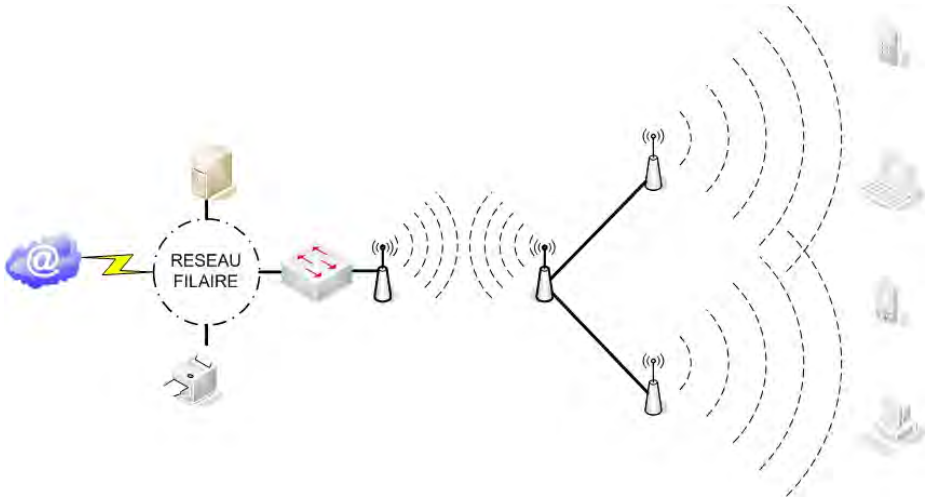
CONNECTIVITE MOBILE

- C'est la plus répandue, celle qui permet aux utilisateurs –portable, téléphone, PAD, PCs- d'accéder aux ressources des réseaux filaires auxquelles est relié le point d'accès.
- Les APs utilisent dans ce cas des antennes omnidirectionnelles, qui émettent et reçoivent sur 360°.
- Les technologies les plus utilisées sont IEEE 802.11b, 802.11g et 802.11n.

CONNECTIVITE LAN-TO-LAN

- Cette topologie a un usage plus restreint. Elle permet de relier des réseaux distants à moindre coût. Généralement les bornes sont dédiées à cette connectivité, elles n'acceptent donc pas des clients mobiles.
- Les deux bornes fonctionnent comme deux ponts Ethernet.
- Les APs utilisent pour cette topologie des antennes unidirectionnelles.
- La technologie la plus répandue est IEEE 802.11a

Topologies (2)



RESEAUX MAILLE

En fait, c'est une utilisation mixte des deux topologies précédentes. On utilise à la fois une connectivité cliente pour les utilisateurs mobiles, et le pontage afin d'étendre la couverture totale du réseau WLAN.

Dans notre exemple, les deux bornes de gauche permettent la connectivité cliente. Elles sont câblées à la borne centrale. Celle-ci permet, par radio, d'atteindre les ressources du réseau filaire.

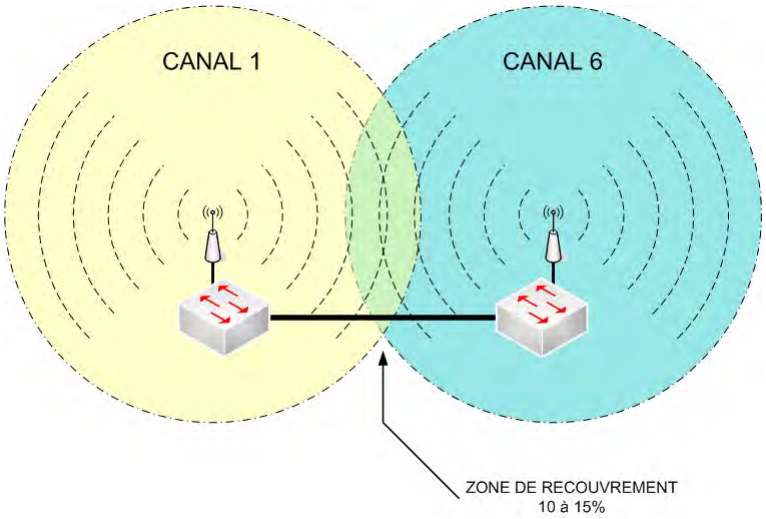
SSID

- Le Service Set Identifier permet de différentier les réseaux logiques WLAN
- Un client doit connaitre le SSID du réseau WLAN auquel il veut se connecter
- Souvent, ce sont les AP qui les annoncent eux-mêmes
- Pour accéder de manière univoque à une borne, il faut que le couple (SSID, canal) soit unique

---

- Le Service Set Identifier, SSID, est le nom donné à un réseau WLAN. Il permet de différentier les réseaux logiques.
  - ➔ Un client doit connaitre le SSID du réseau WLAN auquel il veut se connecter. Il y a deux possibilités :
    - ✓ Le client connait le SSID au préalable
    - ✓ Le client écoute les annonces émises par les AP, qui diffusent (beacon) à intervalles réguliers leur(s) SSID(s).
  - ➔ Un client ne peut être connecté qu'à un seul SSID à un instant t
- Un AP peut gérer plusieurs SSID simultanément
- L'accès doit être univoque :
  - ➔ Deux AP peuvent utiliser le même SSID, mais ils devront alors utiliser des canaux différents si elles sont à proximité l'une de l'autre.
  - ➔ Deux AP proches l'un de l'autre, c'est-à-dire avec un espace de recouvrement commun, utilisant des SSID différents peuvent utiliser les mêmes numéros de canaux.

Extension d'un WLAN par canaux



PROBLEMATIQUE

Une des contraintes des WLAN est la zone de couverture restreinte des émetteurs. Que se passe-t-il lorsqu'un utilisateur sort de la zone couverte ? Le débit devient très faible, les erreurs plus nombreuses, la détection du SSID plus difficile.

Afin d'étendre la zone de couverture d'un WLAN donné, identifié par son SSID, deux solutions principales s'offrent à nous :

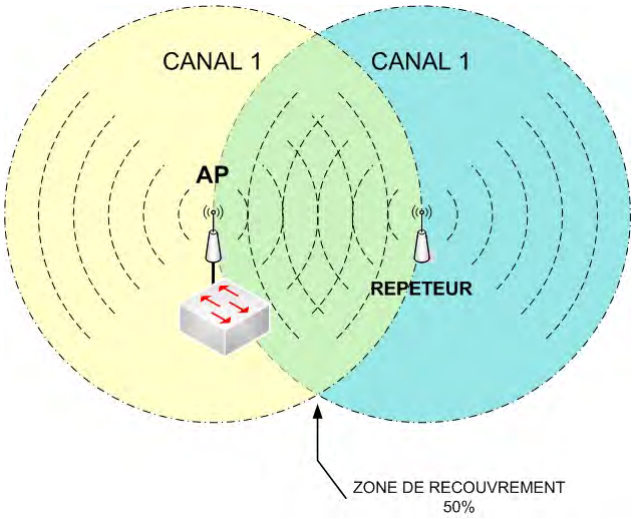
- L'extension par canaux
- L'extension par répétition

EXTENSION PAR CANAUX

Le principe est simple : plusieurs points d'accès possèdent le même SSID.
Ils permettent donc, en théorie, l'accès aux mêmes ressources. Mais, il faut que l'accès à une borne soit univoque. Il faut qu'elles puissent être différenciées sans ambiguïté. On va donc utiliser des canaux différents pour des bornes voisines.
Généralement, il est conseillé d'avoir une zone de recouvrement de 10 à 15% entre les bornes. Tous simplement pour éviter les coupures brutales du signal.

Cette solution est efficace, mais elle doit tenir compte des spécificités de chaque technologie. Par exemple, en 802.11b on utilise des canaux qui se chevauchent (méthode radio DSSS). Les seuls canaux qui ne se chevauchent pas sont les 1, 6 et 11. Ce seront donc ces trois canaux qui seront utilisés afin d'accroitre la portée d'un WLAN.

Extension d'un WLAN par répéteur

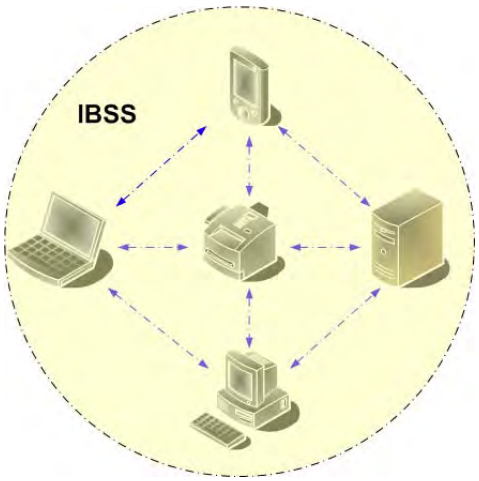


EXTENSION PAR REPETEUR

C'est une solution alternative à la précédente. Le principe est d'utiliser une borne en répéteur. C'est-à-dire qu'elle réamplifiera les signaux qu'elle reçoit du point d'accès principal.

- L'avantage de cette solution est la facilité de sa mise en place :
  - ➔ On utilise le même canal sur la source et le répéteur
  - ➔ Pour l'utilisateur, la transition est transparente
- Les inconvénients sont les suivants :
  - ➔ Une zone de recouvrement de 50% est nécessaire entre la source et le répéteur
  - ➔ La source est la seule en charge de l'accès au réseau

Méthode de communication Ad-hoc



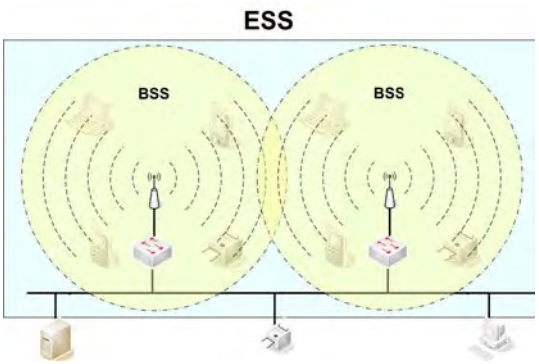
- Ad-hoc ou point-à-point : pas de différenciation entre les composants du réseau
- Relation directe entre homologues en point-à-point (Peer to Peer)
- Pas de possibilité d'interconnexion avec un réseau filaire
- Simple à mettre en place, mais limite, de facto, l'étendue des échanges
- On désigne par IBSS, Independent Basic Service Set, l'ensemble des stations à portée radio mutuelle
- Utilisée pour les communications directes entre deux machines : les homologues doivent être à portée radio

Il existe deux méthodes de communication pour les réseaux sans fils : Ad-hoc et infrastructure.

AD-DOC

- Que l'on désigne également par point-à-point.
- Il n'y a pas de différenciation entre les composants du réseau.
- Les communications se font directement entre homologues, en point-à-point (Peer to Peer). Chaque élément joue un rôle semblable et équivalent aux autres.
- Les homologues doivent être à portée radio, il ne peut y avoir de relais entre eux.
- Il n'y a pas de possibilité d'interconnexion avec un réseau filaire. Pour accéder à une ressource, il faut établir une communication directe avec la machine qui l'héberge.
- L'avantage de cette méthode de communication est sa facilité de mise en œuvre.
- L'inconvénient est la limitation de l'étendue des échanges et du nombre d'intervenants. Les performances chutent rapidement à mesure que le réseau se complexifie.
- On désigne par IBSS, Independent Basic Service Set, l'ensemble des stations à portée radio mutuelle.
- Cette méthode de communication est utilisée dans les cas suivants :
    - Pour des connexions ponctuelles et occasionnelles de faible débit
    - Avec des technologies orientées point-à-point avec des exigences en performances mesurées. Par exemple le Bluetooth.

Méthode de communication en infrastructure



- Centralisée ou à point d'accès : différenciation entre les composants du réseau
- Un pont permet aux machines munies d'un émetteur sans fil d'accéder aux réseaux filaires
- Plus complexe à mettre en place
- Etendue et couverture beaucoup plus importantes
- On désigne par BSS, Basic Service Set, l'ensemble constitué du point d'accès et des stations à portée radio
- On désinge par ESS, Extended Services Set, l'ensemble des BSS reliés entre eux

---

On désigne aussi cette méthode par centralisée, ou encore à point d'accès.

- Il y a une différenciation entre les composants du réseau.
- Les communications se font par le biais d'un point d'accès ou Access Point (AP).

Le point d'accès joue deux rôles :

- Celui d'un hub pour les communications entre les machines radio.
- Celui d'un pont pour les communications entre les machines radio et les machines filaires.

Cette méthode de communication est plus complexe à mettre en place que la méthode Ad-hoc.

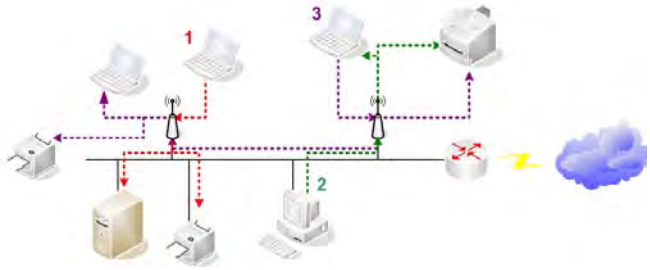
En revanche, elle permet une étendue et une couverture que ne peuvent offrir les méthodes point-à-point.

- On désigne par BSS, Basic Service Set, l'ensemble constitué du point d'accès et des stations à portée radio.
- On désigne par ESS, Extended Service Set, l'ensemble des BSS reliés entre eux par un réseau filaire et permettant l'accès aux mêmes ressources.

Cette méthode de communication est utilisée dans les cas suivants :

- Pour des connexions ponctuelles permanentes et de longue durée.
- Pour des connexions itinérantes.
- Pour une forte densité de machines connectées.
- Pour disposer de débits beaucoup plus élevés que ceux des réseaux Ad-hoc.

Mode infrastructure



- Composants d'un réseau en mode infrastructure :
  - Les stations radio émettrices
  - Les points d'accès, pont entre le réseau sans fil et le réseau filaire
- Un AP permet les échanges de données entre :
  - Les stations émettrices sans fil dépendantes ou non du même point d'accès
  - Entre une station émettrice sans fil et une machine sur le réseau filaire

COMPOSANTS

Une infrastructure WLAN est composée des éléments suivants :

- Les stations radio émettrices :
  - ➔ Des postes de travail
  - ➔ Des imprimantes
  - ➔ Des PAD
  - ➔ Des téléphones « intelligents »
- Les points d'accès. Ils permettent :
  - ➔ Le pontage entre le réseau sans fil et le réseau filaire. Ce qui permet aux machines présentes dans les deux types de réseaux de communiquer en toute transparence.
  - ➔ Les échanges entre les stations radio. Que celles-ci soient ou non dépendantes du même point d'accès.

Présentation de 802.11

- Appartient à la famille de WLAN, Wireless LAN
- 1992, début des travaux de l'IEEE sur les réseaux sans fils
- 1997, première norme : 802.11
- 1999, extensions :
  - 802.11a : 54 Mb/s, 5 GHz
  - 802.11b : 11 Mb/s, 2,4-2.5 GHz
- 2003 : 802.11g. 54 Mb/s, 2,4-2.5 GHz ou 5GHz
- WECA a défini la certification Wi-Fi. Cette certification a deux buts :
  - Promotion du 802.11 sous un nom moins technique
  - Assurer l'interopérabilité des constructeurs

Actuellement le WiFi est la norme WLAN la plus répandue et la plus utilisée à travers le monde.

QUELQUES DATES IMPORTANTES

- 1992. Début des travaux de l'IEEE sur les réseaux sans fils.
- 1997. Publication de la première norme, 802.11. Elle fonctionnait à 1 Mb/s.
- 1999. Publications des extensions :
  - 802.11a : 54 Mb/s à 5 GHz.
  - 802.11b : 11 Mb/s à 2,4-2,5 GHz
- 2003 : 802.11g. 54 Mb/s à 2,4-2,5 GHz ou 5 GHz

WECA

Wireless Ethernet Compatibility Alliance. Cet organisme est chargé de deux rôles essentiels :

- Assurer la promotion du 802.11
- Assurer l'interopérabilité des constructeurs, via la norme WiFi

Caractéristiques de 802.11

- 802.11 définit, à l'origine :
  - Une couche MAC unique
  - Trois couches physiques principales, incompatibles entre-elles
- Support des modes ad-hoc et infrastructure
- Sécurité : authentification et cryptage des données
- Fréquences utilisables :
  - 2.4 à 2.5 GHz
  - 5 GHz
- Deux modes de transmission radio :
  - DSSS et FHSS en étalement de spectre
  - Le multiplexage OFDM

La norme WiFi / 802.11 appartient à la famille des WLAN, Wireless LAN. Les caractéristiques et spécifications en sont établies par l'IEEE.

CARACTERISTIQUES

L'architecture 802.11 définit :

- Une couche MAC unique utilisant le même adressage MAC que celui d'Ethernet.
- Trois couches physiques principales incompatibles entre-elles : 802.11 en DSSS, 802.11 en FHSS et 802.11 en infrarouge.

802.11 supporte les modes ad-hoc et infrastructure. Mais ce dernier est de loin le plus utilisé.

802.11 fournit les fonctionnalités de sécurité suivantes :

- Authentification et intégrité des données échangées entre les éléments.
- Confidentialité des échanges par cryptage des données.

TRANSMISSION RADIO

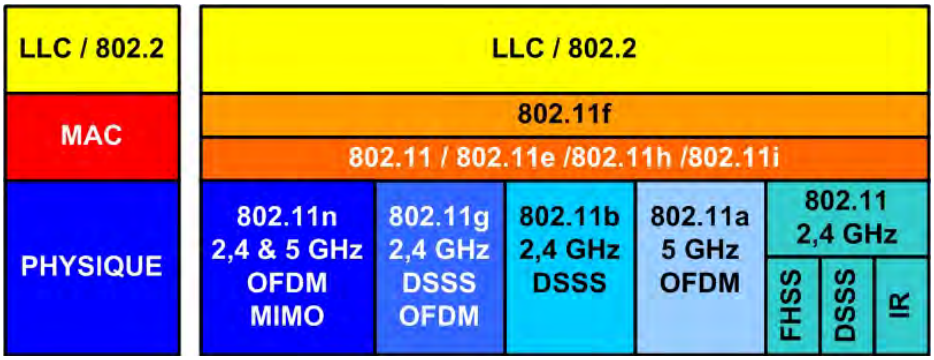
Les fréquences utilisées sont les suivantes :

- 2,4 à 2,5 GHz. C'est une ancienne technologie d'origine militaire. Les débits sont limités et les fréquences sont généralement celles d'anciens réseaux militaires ou médicaux. Les américains les qualifient de ISM : Industrial, Scientific & Medical.
- 5 GHz. Cette fréquence est beaucoup plus performante, mais plus coûteuse. Elle fournit également, à puissance égale, une zone de couverture plus restreinte.

Il y a deux modes de transmission radio :

- A étalement de spectre. Afin de renforcer la transmission radio, 802.11 utilise la méthode de transmission radio à étalement de spectre. Il existe deux techniques :
  - ➔ L'étalement de spectre par séquence directe. C'est la méthode DSSS (Direct Sequence Spread Spectrum). Utilisée par 802.11 natif, 802.11b et 802.11g.
  - ➔ L'étalement de spectre par saut de fréquence. C'est la méthode FHSS (Frequency-Hopping Spread Spectrum). C'était l'autre méthode utilisée par le 802.11 natif.
- A multiplexage. C'est la technique de multiplexage par fréquences orthogonales ou OFDM (Orthogonal Frequency Division Multiplexing), qui est utilisée en 802.11a et 802.11g.

Normes 802.11



A la norme originelle 802.11 proprement dite, d'autres normes, d'autres groupes de travail, sont venus améliorer au fur et à mesure les fonctionnalités, la sécurité, la fiabilité et le débit :

- 802.11f définit une surcouche logicielle entre la couche MAC 802.11 et les couches supérieures (LLC/ 802.2) afin de standardiser les points d'accès. Le protocole de niveau trois le plus utilisé est IP.
- 802.11e définit des améliorations de la couche MAC. Ces améliorations concernent essentiellement les services de QoS :
    - Définition des priorités de l'accès à la couche MAC
    - Mode d'accès sans contention
    - Réservation de créneaux de transmission
- Les services de QoS permettent le transport de la voix, notamment en VoIP.
- 802.11h définit la gestion améliorée du spectre pour la norme 802.11a.
- 802.11i définit l'amélioration des fonctionnalités de sécurité.
- Définition d'un standard 802.1x spécifique à la gestion de l'authentification et de l'échange des clés dans les réseaux 802.11 :
    - ➔ Serveurs d'authentification. C'est RADIUS qui a été choisi comme standard pour l'authentification en 802.11.
    - ➔ Authentifications EAP-MD5 et EAP-TLS. Ce sont les plus utilisées. D'autres méthodes sont définies.
    - ➔ Génération et gestion de clés dynamiques. Par opposition au 802.11 natif dont les clés étaient gérées en statique.

- ➔ Amélioration de WEP via le protocole TKIP, ne nécessitant qu'une mise à jour logicielle. Cette amélioration a été une étape importante vers le WPA, qui est l'évolution de WEP.
- ➔ Utilisation de AES, en lieu et place de RC4, pour le cryptage des données. Des faiblesses ont été découvertes dans l'algorithme de cryptage RC4.

- 802.11g définit les extensions pour le haut débit sur les fréquences 2.4-2.5 GHz. C'est grâce à ces extensions que la norme 802.11g atteint les 54 Mb/s.

Caractéristiques de 802.11b

- Extension de la norme 802.11
- Même plage de fréquence utilisable : 2.4-2.5 GHz
- Débits : 1 Mb/s, 5.5 Mb/s et 11 Mb/s
- Couche physique spécifique et incompatible avec celle d'origine
- Utilise la méthode DSSS (Direct Sequence Spread Spectrum) pour la transmission radio avec la modulation CCK (Complementary Code Keying)

- La norme 802.11b est une extension de 802.11.
- Elle utilise la plage de fréquence 2,4-2,5 GHz.
- Les débits supportés sont de 1 Mb/s, 5,5 Mb/s et 11 Mb/s.
- La couche physique est spécifique et incompatible avec celle d'origine. Cette dernière n'étant plus utilisée.
- La norme 802.11b utilise pour la transmission radio la méthode DSSS (Direct Sequence Spread Spectrum) avec la modulation CCK (Complementary Code Keying).

Fréquences radio 802.11b

NUMERO DE CANAL	FREQUENCE « CENTRALE » (MHz)	PLAGE DE FREQUENCES (MHz)	AMERIQUES	EUROPE MOYEN-ORIENT ASIE	JAPON
1	**2412**	**2401-2423**	**X**	**X**	**X**
2	2417	2406-2428	X	X	X
3	2422	2411-2433	X	X	X
4	2427	2416-2438	X	X	X
5	2432	2421-2443	X	X	X
6	**2437**	**2426-2448**	**X**	**X**	**X**
7	2442	2431-2453	X	X	X
8	2447	2436-2458	X	X	X
9	2452	2441-2463	X	X	X
10	2457	2446-2468	X	X	X
11	**2462**	**2451-2473**	**X**	**X**	**X**
12	2467	2466-2478		X	X
13	2472	2471-2483		X	X
14	2484	2473-2495			X

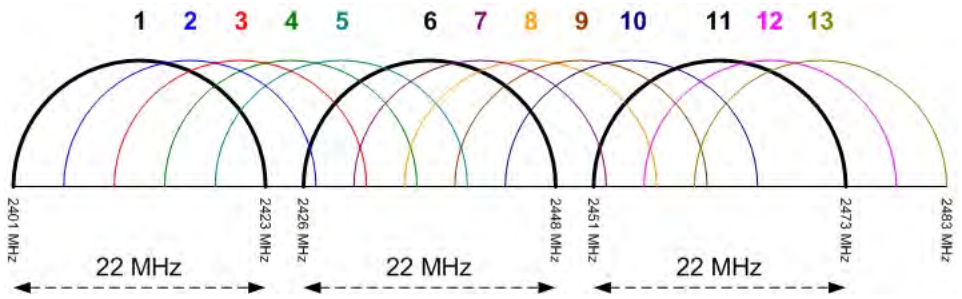
Ce tableau contient les plages de fréquences utilisées par la norme 802.11b dans les différentes zones du monde.

Chaque canal utilise une plage de fréquence de 22 MHz.

La zone Amériques compte 11 canaux disponibles. La zone Europe/M-O/Asie en compte 13. Enfin, le Japon en comporte 14.

Les normes 802.11b et 802.11g utilisent les mêmes canaux.

Canaux 802.11b/g



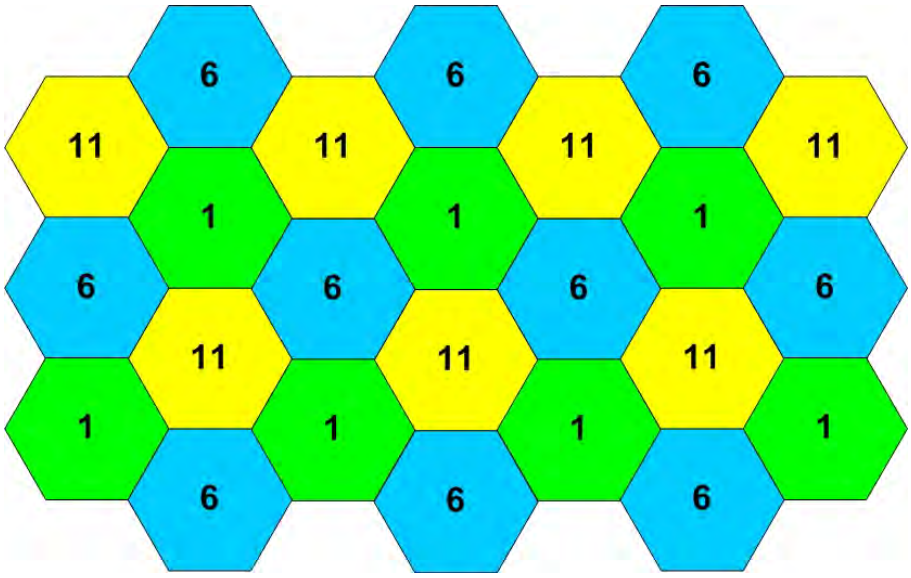
CANAUX DE FREQUENCES RADIO

Le schéma représente les canaux utilisés en 802.11b et 802.11g.
Il est à noter que les seuls canaux qui ne se recouvrent pas sont les 1, 6 et 11. Tous les autres utilisent des fréquences qui ne leur sont pas exclusives.

MAILLAGE

Pour étendre un WLAN on peut utiliser conjointement des points d'accès ayant le même SSID et utilisant un des canaux différents. La seule contrainte est que deux voisins directs n'utilisent pas le même canal. Ceci afin d'éviter toute interférence.

Maillage 802.11b/g



MAILLAGE 802.11b/g

Le maillage en 802.11b/g est plus délicat que celui en 802.11a. Comme les canaux peuvent avoir des fréquences communes, il ne faut pas utiliser sur deux points d'accès des canaux qui se recouvrent, même partiellement. Il est donc fortement conseillé dans ce cas les canaux 1, 6 et 11. Ce sont les seuls canaux dont les fréquences ne se recoupent pas.

Il est possible de « jouer » avec les différents canaux afin de savoir qui peut cohabiter avec qui. Mais cela devient très vite très complexe.

Par exemple si vous utilisez le canal 7, les voisins directs ne pourront être que 1, 2, 12 ou 13.
Mais, 1 et 2 d'une part et 12 et 13 d'autre part ont des fréquences qui se recoupent et ne peuvent donc être voisins. Et ainsi de suite… Il est donc plus simple de n'utiliser que le canal le plus à gauche, le canal central et le plus à droite… communs à toutes les législations.

Remarque sur les débits

DEBIT NOMINAL Mb/s	DEBIT REEL Mb/s	OVERHEAD %
1	0,93	7
2	1,72	14
5,5	4	27
11	6,38	42
54	26-30	52-44
540	?	?

- Il faut différencier le débit nominal du débit maximum réel
- Le débit nominal prend en compte le transfert total, l'intégralité de la trame
- Le débit maximal réel ne prend en compte que le transfert de la partie utile transportée

Il faut différencier le débit nominal du débit maximum réel.
Le débit nominal prend en compte le transfert total, l'intégralité de la trame. C'est-à-dire l'espace réellement utilisé pour l'acheminement des données.
Le débit maximal réel ne prend en compte que le transfert de la partie utile transportée. Autrement dit, le débit en charge utile réelle.

Dans le tableau ci-dessus sont indiqués les débits courants en 802.11, de 1 Mb/s à 540 Mb/s qui devrait être le débit maximal fourni par la norme 802.11n.
Généralement, plus le débit augmente, plus l'overhead, le ratio entre la taille totale des trames et la charge utile transportée, est grand. Une grande inconnue subsiste sur la norme 802.11n puisque diverses informations contradictoires annoncent un peu tout et n'importe quoi. Toutefois, la valeur de 540 Mb/s semble obtenir le consensus. Mais, pour le moment, aucune information précise n'est disponible sur le débit réel. Attendons…

Les deux valeurs pour 54 Mb/s correspondent respectivement à 802.11g et 802.11a.

Caractéristiques de 802.11a

- Extension de la norme 802.11
- Couche physique spécifique et incompatible avec les autres 802.11
- Fréquence utilisable : 5 GHz
- Débits : de 6, 9, 12, 18, 24, 36, 48 et 54 Mbit/s
- Utilise la méthode OFDM (Orthogonal Frequency-Division Multiplexing) pour la transmission radio
- USA (FCC) : 23 canaux sans chevauchement
- EUROPE (ETSI) : 19 canaux sans chevauchement

- La norme 802.11a est une extension de 802.11.
- Elle utilise la place de fréquence autour de 5 GHz.
- Les débits supportés sont de 6, 9, 12, 18, 24, 36, 48 et 54 Mb/s.
- La couche physique est spécifique et incompatible avec celle d'origine.
- La norme 802.11a utilise pour la transmission radio la méthode OFDM (Orthogonal Frequency-Division Multiplexing). Cette méthode utilise des canaux sans chevauchement.
- Aux Etats-Unis, le FCC a libéré 23 canaux sans chevauchement.
- En Europe, l'ESTI a mis à disposition 19 canaux sans chevauchement.

Caractéristiques de 802.11g

- Extension de juin 2003
- Utilise la plage de fréquence 2.4-2.5 GHz
- Trois canaux sans chevauchement : 1, 6 et 11
- Utilise DSSS/CCK et OFDM
- Débits
  - DSSS : 1, 2, 5.5 et 11 Mb/s
  - OFDM : 6, 9, 12, 18, 24, 36, 48 et 54 Mb/s
- Rétrocompatible avec 802.11b

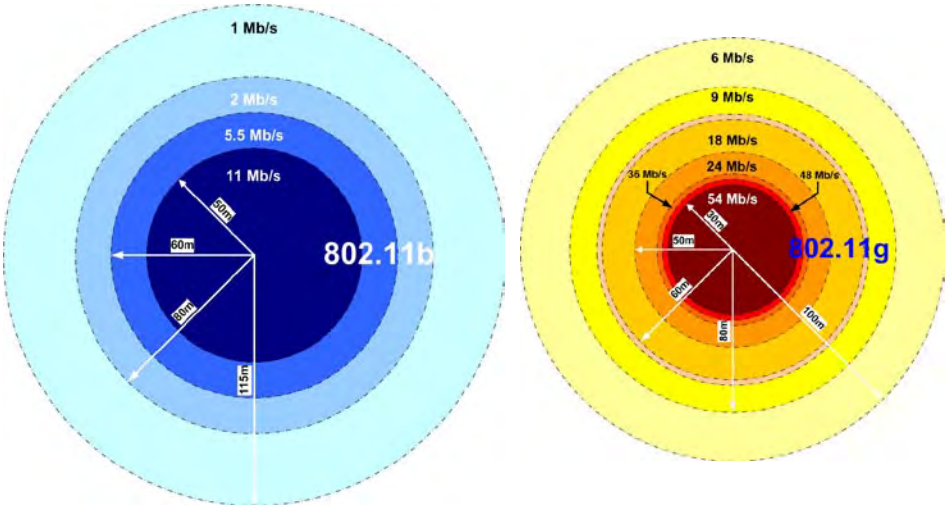
- La norme 802.11g est une extension de 802.11 qui date de 2003.
- Elle utilise la place de fréquence de 2.4-2.5 GHz.
- La couche physique est spécifique et incompatible avec celle d'origine.
- Les trois canaux sans chevauchement sont toujours 1, 6 et 11.
- La norme 802.11g utilise pour la transmission radio les deux méthodes DSSS/CCK et OFDM
- Les débits supportés sont :
  - ➔ En DSSS : 1, 2, 5.5 et 11 Mb/s
  - ➔ En OFDM : 6, 9, 12, 18, 24, 36, 48 et 54 Mb/s.
- 802.11g est rétrocompatible avec 802.11b. Un point d'accès en 802.11g peut donc accepter des clients radio en 802.11b.

Caractéristiques de 802.11n

- Extension prévue pour 2008
- Utilise MIMO (multiple in / multiple out)
- Probablement 540 Mb/s
- 8 canaux non superposés
- Fonctionne en OFDM
- Utilise Simultanément les plages 2.4-2.5 GHz et 5 GHz

- 802.11n est une extension de 802.11 prévue pour 2008. Pour le moment, c'est une pré-normalisation.
- 80.2.11 utilise la technologie MIMO (multiple in / multiple out), qui est déjà utilisée de façon propriétaire par certains constructeurs. Le principe consiste à utiliser plusieurs antennes simultanément.
- Le débit nominal maximal sera probablement de 540 Mb/s.
- 8 canaux non superposés seront utilisables.
- La transmission radio fonctionnera en OFDM.
- 802.11n utilisera simultanément les plages 2.4-2.5 GHz et 5 GHz.
- Certains constructeurs proposent déjà du matériel en pré-standard avec des débits de 200 à 320 Mb/S.

Distances et débits en 802.11b/g



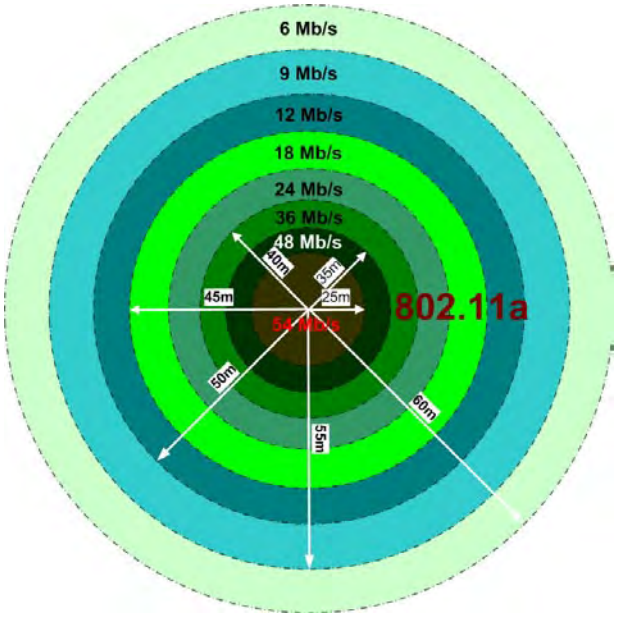
Les schémas ci-dessus représentent les débits atteignables en proportion de la distance séparant une machine cliente d'un point d'accès en 802.11b et 802.11g.

On peut voir que le maillage en 802.11g doit être plus dense que celui en 802.11b.

Autre remarque, la perte de débit très rapide entre 54 et 24 Mb/s sur quelques mètres seulement.

Les valeurs sont données à titre indicatif et dans des conditions idéales. Il faut toujours pondérer et procéder à des tests. Différents outils d'analyse logiciels ou matériels sont disponibles sur le marché dans ce but. De plus, l'utilisation d'antennes plus puissantes ou unidirectionnelles permettent d'obtenir des meilleurs résultats, mais avec des contraintes d'utilisation différentes.

Distances et débits en 802.11a



- Le schéma ci-dessus représente les débits atteignables en proportion de la distance séparant une machine cliente d'un point d'accès en 802.11a.
- On peut voir que le maillage en 802.11a doit être très dense par rapport aux autres normes 802.11.
- On remarque que l'atténuation est beaucoup plus progressive qu'en 802.11g. Ceci est dû à l'utilisation efficace de OFDM en transmission radio.
- Enfin, à distance égale, les débits sont meilleurs que ceux de 802.11g.

Documents de références

- Etats-Unis :
  - 2,400-2,483 GHz
  - FCC : documents CFR47 part 15 sec 15.205, 15.209 ,15.247 et 15.249
- Europe :
  - 2,400-2.483 GHz
  - ETSI : documents ETS 300 328, 300 339
  - France : ETSI SP/DGPT/ATAS/23
- Japon :
  - 2,471-2,497 GHz
  - ARIB : RCR STD-33A

ZONES WIFI

WiFi a défini trois grandes zones de fréquences radio utilisables dans le monde :

- La zone 1 pour les Amériques
- La zone 2 pour l'Europe, le Moyen-Orient et l'Asie
- La zone 3 pour le Japon

DOCUMENTS OFFICIELS

Plus précisément, les documents officiels concernant les fréquences utilisables librement et gratuitement sont les suivants :

- Pour les Etats-Unis : C'est la FCC (Federal Communications Commission) qui fournit les autorisations. Ce dont les documents CFR47 part 15 sections 15.205, 15.209, 15.247 et 15.249.
- Pour l'Europe : C'est l'ESTI (European Telecommunications Standards Institute) qui est en charge des attributions. Ce sont les documents ETS 300 328 et 300 339.
- Pour la France, ce sont les documents ETSI SP/DGPT/ATAS/23.
- Enfin pour le Japon : c'est l'ARIB (Association of Radio Industries and Businesses) avec le document RCR STD-33A.

En France

FREQUENCES (GHz)	PUISSANCE (mW)	
	INTERIEUR	EXTERIEUR
2.4-2.446	<10	<2.5
2.446-2.483	<100	Autorisation
5.150-5.250	<200	non
5.250-5.350	<200	non
5.470-5.725	A l'étude	A l'étude

- 2,400-2,483 GHz :
  - CEPT : CEPT/ERC/DEC/(01)07
  - ETSI : EN 300 328 et 300 339
  - France : ETSI SP/DGPT/ATAS/23
- 5 GHz :
  - CEPT : CEPT/DEC/(96)03 et (99)23
  - ETSI : EN 300 836

La France est un cas à part dans le monde des télécommunications, ce qui n'est pas démenti par les fréquences radio mises à disposition pour le WiFi.

FREQUENCES AUTORISEES

Les fréquences utilisables sont définies dans les documents suivants :

- Pour le 2,4-2,483 GHz :
  - ➔ CEPT (Conférence Européenne des Postes et Télécommunications) : CEPT/ERC/DEC/(01)07
  - ➔ ETSI : EN 300 328 et 300 339
  - ➔ France : ETSI SP/DGPT/ATAS/23
- Pour le 5 GHz :
  - ➔ CEPT : CEPT/DEC/(96)03 et (99)23
  - ➔ ETSI : EN 300 836

PUISSANCES AUTORISEES

Le tableau ci-dessus précise les puissances autorisées en France :

- En intérieur
- En extérieur
- Pour la plage 2.4-2.5 GHz
- Pour la plage 5 GHz

Sécurité WiFi

- Problématique
- Contrôle d'accès
- WEP
- WPA
- EAP
- 802.1x
- Radius

La sécurité en WLAN est un élément crucial de par la spécificité même du média : l'air. Nous allons en aborder la problématique ainsi que les aspects essentiels :

- Le contrôle d'accès. Ce qui permet de contrôler les machines et les utilisateurs tentant d'accéder au réseau.
- WEP. Cette technique de sécurisation peu fiable et peu sûre a participé à la mauvaise réputation sécuritaire du WiFi.
- WPA. C'est l'amélioration très sensible du WEP, qui permet d'obtenir un bon niveau de sécurité.
- EAP. Cette méthode d'authentification fait partie des spécifications WPA.
- 802.1x. Ce protocole d'authentification était utilisé à l'origine pour sécuriser les accès filaires, notamment en Ethernet. Son adaptation au sans fil (Wireless) a permis d'en renforcer le niveau de sécurité.
- RADIUS. Ce protocole sécurisé d'échange de données d'authentification est utilisé depuis longtemps dans les réseaux traditionnels. Il est très souvent associé à 802.1x.

Problématique

- Principe : fournir les trois fonctionnalités de bases de la sécurité réseau : Authentification, intégrité et confidentialité
- Trois types d'éléments à sécuriser :
  - La sécurité radio :

    Confidentialité, intégrité, signature des paquets

    WEP, TKIP, CCMP
  - Le filtrage des paquets : ACL et QoS
  - L'infrastructure d'authentification : 802.1x & RADIUS

PROBLEMATIQUE DE LA SECURITE WLAN

Le principe est de fournir les trois fonctionnalités essentielles de la sécurité réseau :

- Authentification. Les intervenants doivent s'assurer de leur identité mutuelle.
- Intégrité. Les données ne doivent pas avoir été modifiées durant leur transport. Souvent, la vérification d'intégrité est associée, liée, à l'authentification.
- Confidentialité. Les données ne doivent être lisibles en clair que par le ou les destinataires.

ELEMENTS A SECURISER

En WLAN, il y a trois types d'éléments à sécuriser :

- La transmission radio. Ce qui inclut l'accès et la protection des données échangées.
- Le filtrage des paquets. Ce qui consiste à n'autoriser que le trafic jugé intéressant.
- L'infrastructure d'authentification. Protéger les échanges d'informations entre le point d'accès et le serveur d'authentification.

Contrôle d'accès

- SSID
  - Service Set ID
  - Nom du réseau
  - Le SSID broadcast permet d'annoncer le nom du réseau, sa désactivation oblige à connaître préalablement le nom du réseau
  - Netstumbler et d'autres logiciels permettent de scanner le réseau et d'obtenir de nombreuses informations
- Authentification
- Filtrage
  - Access Control List
  - Filtrage sur les adresses MAC, les adresses IP, les applications...

Le contrôle d'accès permet de limiter l'accès des utilisateurs. Il y a plusieurs fonctionnalités disponibles :

SSID

- Le SSID, Service Set ID. Il désigne le nom du réseau WLAN. A intervalle régulier, les points d'accès émettent des broadcasts afin d'annoncer les réseaux qu'ils gèrent (beaconing).
- Sa désactivation oblige les utilisateurs à connaitre au préalable le nom du réseau auquel ils veulent accéder. Ce qui est un minimum si aucune autre méthode de sécurisation n'est utilisée. Ce qui n'apporte pas grand-chose si d'autres techniques, plus performantes, sont utilisées.
- Des logiciels et des appareils spécialisés permettent d'analyser les flux radios et d'obtenir de nombreuses informations, dont le SSID.

AUTHENTIFICATION

- Elle renforce la sécurité d'accès. Il faut au préalable identifier avant que le point d'accès ne donne un accès au réseau.
- Il est possible d'authentifier la machine cliente et/ou l'utilisateur.
- Les techniques ont beaucoup évolué depuis quelques années. Actuellement la plus efficace est le 802.1x.

FILTRAGE

Le filtrage consiste à contrôler les données acceptées par un point d'accès. Généralement on utilise des listes d'accès de contrôle (ACL, Access Control List).

Les ACLs sont constituées de règles lues séquentiellement. Une règle est constituée d'une ou de plusieurs conditions et d'une action. Si les conditions correspondent, l'action est accomplie.
Deux actions sont utilisées :

- PERMIT, qui autorise les données si les conditions sont remplies
- DENY, qui interdit l'accès aux données si les conditions sont remplies

Les conditions peuvent porter sur :

- Les adresses MAC, notamment l'adresse MAC source du client
- Sur les adresses IP, source et destination
- Sur les ports source et destination
- Sur certaines applications
- Sur les valeurs de certains champs IP et TCP la plupart du temps.

Il est donc possible de n'autoriser à accéder à un réseau que certaines adresses MAC ou certaines adresses IP et également possible de n'autoriser que certains flux applicatifs.

WEP

- Afin de sécuriser les échanges entre un point d'accès et une station, celles-ci doivent établir une association
- Une association est une relation de sécurité entre deux machines
- Protocole utilisé pour réaliser l'association en 802.11 : WEP (Wired Equivalent Pricacy)
- Le standard 802.11 définit
  - WEP comme méthode de cryptage pour la confidentialité et la vérification d'intégrité
  - Deux méthodes d'authentification :

    L'une sans authentification de fait

    L'autre permettant de vérifier la concordance de la clé secrète de cryptage

---

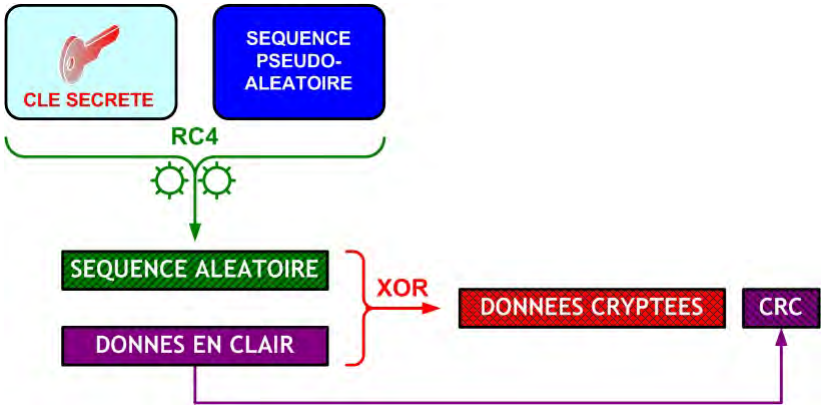
Afin de sécuriser les échanges entre un point d'accès et une station, ils doivent établir une association. Une association est une relation de sécurité entre deux machines.
Le protocole utilisé pour réaliser cette association en 802.11 est le WEP (Wired Equivalent Pricacy).

Le standard 802.11 définit :

- WEP comme méthode de cryptage pour la confidentialité et la vérification d'intégrité
- Deux méthodes d'authentification :
  - ➔ L'une sans authentification de fait. Utilisée pour les accès libre.
  - ➔ L'autre permettant de vérifier la concordance de la clé secrète de cryptage partagée entre le point d'accès et ses clients.

WEP est la technique d'origine du 802.11. Ses limitations et ses faiblesses sont nombreuses, raisons pour lesquelles il est de moins en moins utilisé.

Cryptage WEP



Comment est sécurisée une trame par WEP ?

CRYPTAGE WEP

PRINCIPE

Le cryptage s'effectue au niveau de la couche liaison de données (niveau 2), sur la trame. Ce qui signifie que tout ce qui est transporté dans les couches supérieures est également protégé.

Le cryptage est à clé symétrique secrète. On crypte et on décrypte avec la même clé secrète partagée par le point d'accès et les clients.

L'algorithme public utilisé est RC4.

La clé utilisée pour le cryptage est composée de deux éléments :

- Une clé statique sur 40 bits, c'est-à-dire sur 5 caractères. C'est la séquence qu'il faut configurer sur chaque station cliente.
- Une séquence pseudo-aléatoire (ou vecteur d'initialisation), sur 24 bits, qui change à chaque trame expédiée. Elle est générée par la station émettrice.

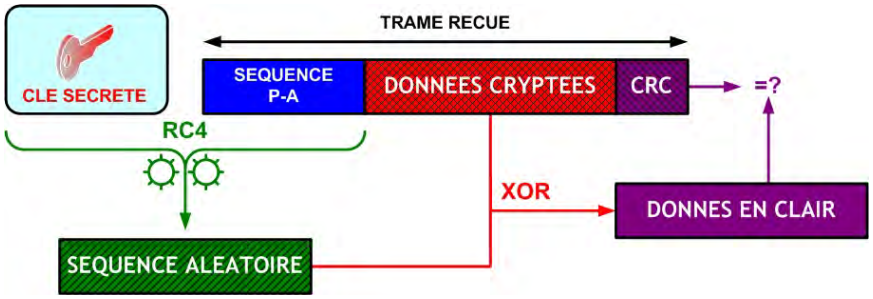
La trame envoyée contient les données cryptées, le CRC et la séquence pseudo-aléatoire.

MECANISMES

- L'émetteur génère une séquence pseudo-aléatoire sur 24 bits.
- La clé secrète, sur 40 bits, est cryptée avec cette séquence par l'émetteur en utilisant l'algorithme RC4.

- On obtient une séquence aléatoire.
- L'émetteur réalise alors un XOR (OU exclusif) avec cette séquence et les données en clair.
- On obtient les données cryptées.
- Enfin, un CRC est calculé à partir des données en clair.
- La trame composée des données cryptées, du CRC et de la séquence pseudo aléatoire est expédiée au destinataire.

Décryptage WEP



DECRYPTAGE WEP

Le décryptage WEP se déroule de la façon suivante :

- Le destinataire reçoit une trame composée des données cryptées, du CRC et de la séquence pseudo-aléatoire.
- Il crypte cette séquence avec la clé secrète en utilisant l'algorithme RC4.
- On obtient une séquence aléatoire.
- Le destinataire effectue ensuite un XOR entre cette séquence aléatoire et les données cryptées.
- On obtient les données en clair, la fonction XOR étant réversible.
- Il ne reste plus qu'à calculer le CRC des données en clair et à le comparer avec celui contenu dans la trame reçue.

Authentification WEP

- Deux méthodes existent :
  - A système ouvert ou sans vérification. Pour l'accès libre.
  - A clé partagée ou challenge. Une séquence aléatoire de 128 bits est utilisée afin de s'assurer que les deux stations possèdent bien la même clé secrète.

AUTHENTIFICATION WEP

Il existe deux méthodes :

- A système ouvert, ou sans authentification. Cette méthode, purement formelle, permet uniquement de vérifier que les stations clientes s'authentifiant supportent bien cette méthode. Cette méthode est plutôt réservée aux accès libres.
- A clé partagée. Une séquence aléatoire de 128 bits est utilisée afin de vérifier que les deux intervenants possèdent bien la même clé secrète. On nomme également cette méthode authentification par challenge.

SYNTHESE

- La longueur de la clé initiale est de 40 bits. Ce qui est faible au regard de la puissance des machines actuelles. Le cryptage est réalisé sur 64 bits (40+24), mais la séquence pseudo-aléatoire circule en clair sur le réseau.
- La puissance de l'algorithme de cryptage n'est plus adaptée aux conditions actuelles. Il existe actuellement des algorithmes plus puissants que RC4. De plus, en 2001, des failles ont été découvertes dans RC4.
- La méthode d'authentification est faible ou nulle. La vérification repose sur le partage d'une même clé secrète et non sur l'identité réelle de la machine. Toutes les machines clientes utilisent la même clé.
- La méthode d'échange ou de vérification des clés pose également des problèmes. Les clés utilisées sont statiquement définies, en cas de vol il faut reconfigurer toutes les machines. De plus, plus une clé est utilisée, plus le risque de découverte de cette clé augmente.

- WEP n'empêche pas le REPLAY. Il est très simple d'enregistrer, puis de rejouer la séquence initiale d'authentification.
- Une amélioration de WEP, WEP2 permettait d'utiliser une clé initiale de 104 bits (13 caractères). Ce qui est un petit peu mieux, mais n'assure toujours pas un niveau de sécurité satisfaisant.

802.11i / WPA

- 2003 :
  - WPA : WiFi Protected Access, sous ensemble de 802.11i
  - Amélioration de l'architecture de sécurité du WiFi
  - Nécessite uniquement une mise à jour du firmware
  - TKIP (Temporal Key Integrity Protocol) : amélioration de RC4, compatible avec le matériel existant
- 2005 :
  - WPA2 / RSN
  - Incompatible avec la version précédente
  - CCMP (Counter-mode / CBC-MAC Protocol) qui utilise l'algorithme AES pour le cryptage des paquets
  - Utilisation du 802.1x et RADIUS pour l'authentification des ports

Une amélioration notable de la sécurité WiFi est apparue en 2003 : WPA.
Comme certaines faiblesse n'étaient toujours par résolues, une autre amélioration, plus radicale celle là, a fait son apparition en 2005 : WPA2.

WPA

- WiFi Protected Access. Définie dans un sous ensemble de 802.11i.
- Cette évolution permettait une amélioration sensible de la sécurité WiFi.
- La migration de WEP à WPA était simple : une simple mise à jour du firmware du matériel était nécessaire.
- WPA utilise une amélioration de RC4, TKIP (Temporal Key Integrity Protocol). Ce protocole restait compatible avec le matériel existant. La différence essentielle est l'utilisation de clés de session provisoires.

WPA2 / RSN

- WPA2 est moins connu sous son nom officiel : RSN, Robust Security Network.
- La méthode et l'algorithme de cryptage ont été modifiés : CCMP (Counter-mode / CBC-MAC Protocol) qui utilise AES en mode OCB. AES est le successeur de DES, qui est l'algorithme de cryptage le plus utilisé. AES peut fonctionner en 128 et en 256 bits.
- Mise en place d'une méthode fiable et puissante d'authentification : EAP-TLS. EAP est le successeur de PAP et de CHAP pour l'authentification.
- Augmentation de la longueur des clés utilisées. On utilise maintenant du 128 bits.

- Individualisation des clés utilisées par session : une clé sera spécifique entre une station et un point d'accès donnés. Ce qui permet l'individualisation de l'accès.
- Les clés seront renouvelées à intervalles réguliers et échangées dynamiquement. Elles sont donc beaucoup plus difficiles à découvrir (à « casser » dans le langage courant).
- 801.x est utilisé pour l'authentification en EAP.
- Enfin, l'authentification centralisée s'appuie sur RADIUS. Ce qui permet la mobilité sécurisée des utilisateurs.

EAP

- Extensible Authentication Protocol
- RFC 3748
- Remplaçant de CHAP, utilisé par PPP
- Utilise différentes méthodes d'authentification :
  - MD5
  - SHA-1
  - PEAP
  - TLS
  - TTLS

PRESENTATION

EAP, Extensible Authentication Protocol est un protocole d'authentification standard et normalisé dans la RFC 3748.

Il est le remplaçant de CHAP, mais beaucoup plus puissant et, surtout, beaucoup plus évolutif. Il existe sous diverses formes et peut s'appuyer sur différentes méthodes d'authentification. En fait, EAP n'inclut pas les méthodes d'authentification, il s'appuie sur celles existantes. De même, il ne peut valider l'authentification, il s'appuie pour cela sur des serveurs d'authentification existants. De façon privilégiée, ce sont les serveurs RADIUS qui sont utilisés.

VERSIONS DE EAP

- LEAP, Lightweight EAP. Disponible sur les plates-formes Windows, dont il utilise la méthode d'authentification MS-CHAPv2. S'appuie sur Radius et MD5 pour la validation de l'authentification. Propriétaire CISCO.
- EAP-FAST. Evolution de LEAP, dont il corrige des failles et des faiblesses. Propriétaire CISCO.
- EAP-SIM. Version destinée à l'authentification des GSM, qui utilise la carte SIM. S'appuie également sur RADIUS.
- EAP-TLS (Transport Layer Security). Utilise TLS 1.0 (SSL 3.1 en fait) et RADIUS. C'est le protocole qui a été retenu pour WPA2. Le principe est d'établir un tunnel TLS par lequel transiteront les données d'authentification.
- PEAP (Protected EAP) / TTLS (Tunneled TLS) sont proches dans le principe de EAP-TLS. La différence notable est l'emploi de serveurs dédiés TTLS/AAA.

802.1x

- Normalisation de l'authentification réseau réalisée par les points d'accès au réseau
- La machine utilisatrice doit s'authentifier à la première utilisation du réseau
- Cette authentification est initiée par le point d'accès
- Une machine ne peut accéder au réseau qu'en cas d'authentification réussie
- Le point d'accès utilise RADIUS afin de transmettre la requête d'authentification
- Les informations d'authentification sont souvent stockées sur un serveur de type LDAP
- De nombreux paramètres associés à l'authentification peuvent être utilisés : adresse IP, protocoles autorisés, ACL…

CARACTERISTIQUES

- Les spécifications IEEE 802.1x définissent et normalisent l'authentification réseau réalisée par les points d'accès. Ces points d'accès peuvent être des commutateurs Ethernet ou des points d'accès WiFi.
- La machine utilisatrice doit s'authentifier à la première utilisation du réseau.
- Cette authentification est initiée par le point d'accès. Une machine ne pourra accéder au réseau qu'en cas d'authentification réussie. Autrement l'accès sera refusé ou autorisé mais avec des restrictions d'utilisation.
- Le point d'accès utilise le protocole RADIUS afin de transmettre la requête d'authentification.
- Les informations d'authentification sont souvent stockées sur un serveur de type LDAP. Il est néanmoins possible de les stocker dans toute base de données supportant le format de données RADIUS.
- De nombreux paramètres associés à l'authentification peuvent être utilisés : adresse IP, protocoles autorisés, ACL… Ces paramètres associés ne seront éventuellement utilisés qu'en cas d'authentification réussie.

802.1x

1. Le client lance une authentification 802.1x
2. L'AP envoie une requête d'authentification au serveur RADIUS
3. Le serveur RADIUS envoie une requête à l'annuaire LDAP
4. Le serveur LDAP répond
5. Le serveur RADIUS transmet la réponse à l'AP
6. L'AP autorise ou interdit en conséquence l'accès au réseau à la machine

---

Analysons les étapes d'une authentification s'appuyant sur 802.1x en WiFi :

1. Le client lance une authentification 802.1x. La plupart du temps, c'est l'AP qui requière, qui initie cette authentification.
2. L'AP envoie une requête d'authentification au serveur RADIUS. C'est ce serveur qui va valider ou non l'authentification.
3. Le serveur RADIUS envoie une requête à l'annuaire LDAP. Ceci afin d'obtenir les informations dont il a besoin pour réaliser l'authentification. Par exemple, à partir d'un nom d'utilisateur, il pourra récupérer son mot de passe ou son certificat numérique.
4. Le serveur LDAP répond à la requête du serveur RADIUS.
5. Le serveur RADIUS transmet la réponse à l'AP. Il valide ou invalide l'authentification. Si l'authentification est réussie, le serveur LDAP peut y associer un certain nombre de paramètres et d'autorisations ; adresse IP, ACL spécifique, applications autorisées…
6. L'AP autorise ou interdit en conséquence l'accès au réseau à la machine.

RADIUS

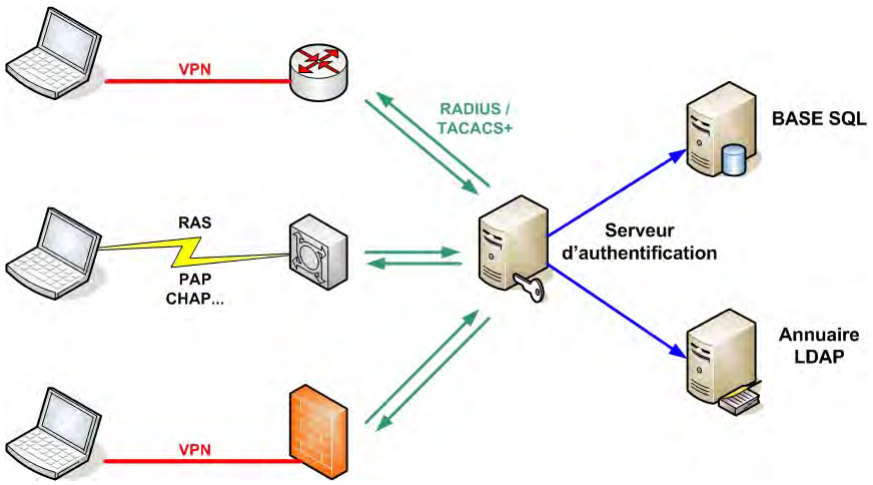
- *Remote Authentication Dial In User Service*, protocole sécurisé d'échange d'informations d'authentification et d'autorisation
- L'intérêt principal réside dans la centralisation de l'authentification
- Normalisé et libre.
- UDP 1646 & 1813
- Fonctionnalités :
  - Authentification des utilisateurs
  - Autorisations allouées aux utilisateurs
  - Services délivrés : PPP, Telnet, accès réseau…
  - Définition de nombreux attributs associés aux utilisateurs : standards, spécifiques, propriétaires
  - Interfaçage avec : LDAP, Unix/Linux, NDG, NDS, RDBMS, CVS, SAM, ODBC…

CARACTERISTIQUES

- RADIUS, *Remote Authentication Dial In User Service*, est un protocole sécurisé d'échange d'informations d'authentification et d'autorisation.
- Il est normalisé et libre.
- Les RFCs sont les suivantes : 2138, 2139, 2243, 2289, 2548, 2618-20, 2809, 2865-69, 2882 et 3162
- Les ports utilisés par RADIUS sont UDP 1646 & 1813.
- Largement répandu dans tous les environnements. Néanmoins, son domaine de prédilection reste l'authentification réseau.
- Fonctionnalités fournies par un serveur RADIUS :
  - ➔ Authentification des utilisateurs
  - ➔ Autorisations allouées aux utilisateurs
  - ➔ Services délivrés : PPP, Telnet, Accès réseau…
  - ➔ Définition de nombreux attributs associés aux utilisateurs : standards, spécifiques, propriétaires
  - ➔ Interfaçage avec les sources de données suivantes : LDAP, Unix/Linux, NDG, NDS, RDBMS, CVS, SAM, ODBC…
- L'intérêt essentiel de RADIUS est la centralisation de l'authentification. Ainsi, un utilisateur peut accéder au réseau et à ses services indépendamment de son point d'accès.
- Seul le mot de passe est crypté, les autres informations sont transmises en clair

- Protocoles supportés par RADIUS :
  - ➔ PAP
  - ➔ CHAP / MS-CHAP
  - ➔ EAP
- Quelques exemples :
  - ➔ Windows : Microsoft IAS
  - ➔ Unix / Linux : FreeRadius

Exemple



Dans cet exemple, un serveur Radius est utilisé :

- Par le routeur pour les accès VPN et WAN distants.
- Par le NAS pour les Remote Access Services (RAS), services d'accès distants.
- Par le firewall pour les accès VPN.

L'avantage est que l'authentification, par sa centralisation, permet une configuration unique et cohérente des propriétés d'authentification de chaque utilisateur.

Enfin, le serveur RADIUS s'appuie ici sur une base de données SQL et un annuaire LDAP. Ceci pour obtenir les données nécessaires à l'authentification et les paramètres associés à celle-ci.

- *Modèle ARPA*
- *ARP/RARP*
- *IP*
- *ICMP*
- *Adressage IP*
- *Sous-réseaux*
- *Sur-réseaux*

5

TCP/IP

Objectifs

Ce module traite du modèle de la pile TCP/IP et de la couche 3.

Connaissances

- Modèle ARPA/IP
- La couche internet
- L'adressage IP
- VLSM

Progression

Présentation de TCP/IP	Adressage IP
Le modèle ARPA	Sous-réseaux
ARP/RARP	Sur-réseaux
IP	VLSM
ICMP	

Présentation de TCP/IP

- Public / Open Source : gratuit et libre
- Normalisé : les RFCs, documents de référence, décrivent le fonctionnement des mécanismes liés à TCP/IP
- Universel : s'installe sur tout système d'exploitation, toute machine
- Routable : le routage logique permet une indépendance entre l'acheminement des datagrammes IP et les couches basses
- Accès Internet : seul protocole de niveau 3 utilisé pour l'accès à Internet

---

TCP/IP est aujourd'hui la pile de protocoles la plus utilisée sur les réseaux informatiques. En voici les principales caractéristiques :

PUBLIC / OPEN SOURCE

TCP/IP est dans le domaine public. Tout un chacun peut l'utiliser librement et gratuitement. Il est même possible d'écrire sa propre pile IP, il faut cependant respecter les règles de fonctionnement des protocoles qui la composent. Pour cela, des documents officiels permettent de définir ces règles : les RFCs.

REQUEST FOR COMMENT

Les RFCs sont des documents de référence, publiés par l'IETF (Internet Engineering Task Force), qui décrivent le fonctionnement :

- Des protocoles qui composent la pile TCP/IP, comme IP, TCP, UDP, ICMP, ARP…
- Des mécanismes réseaux associés. Comment ces protocoles communiquent entre eux sur le réseau et leur interaction avec les couches basses du réseau.
- Des applications libres. DNS, HTTP, FTP, SMTP, POP, IMAP…

Les préconisations des RFCs peuvent avoir un caractère :

- Obligatoire : les fonctions et les règles décrites doivent être respectées afin d'être pleinement compatibles.
- Conseillé : il est fortement conseillé de les respecter.
- Informatif : la plupart des implémentations les respectent, sans pour autant relever un caractère contraignant.

- Obsolète : une RFC est remplacée par une autre plus récente.
- Déconseillé : assez rare, généralement pour éviter qu'un éditeur ou un constructeur n'impose, de facto, un standard.

UNIVERSEL

TCP/IP peut être installé sur tout système d'exploitation, tout type de machine. La communication IP entre deux machines ne dépend ni de leurs systèmes d'exploitation ni de leurs topologie réseau. Un PAD en WiFi peut communiquer avec un mainframe IBM en Gigabit Ethernet, un téléphone IP en UMTS avec un serveur UNIX en ATM, un portable en Fast Ethernet avec un AS/400 en FDDI…

ROUTABLE

TCP/IP utilise des adresses logiques, de niveau 3, indépendantes de la technologie réseau sous-jacente. Deux machines connectées sur des réseaux de types différents peuvent communiquer de manière transparente, elles n'ont besoin que de connaitre leurs adresses IP respectives.

IP est un protocole réseau routable, ce qui permet d'interconnecter des réseaux hétérogènes en s'appuyant sur les adresses logiques. Les calculs et les techniques de routages ne dépendent pas des topologies et des technologies réseaux traversées entre la source et la destination.

Le routage IP consiste à interconnecter des réseaux logiques entre eux afin d'acheminer de bout en bout des datagrammes.

ACCES INTERNET

TCP/IP est le seul protocole de niveau 3 permettant l'accès à Internet. Avant que TCP/IP ne devienne le standard dans les entreprises, il existait des passerelles entre IP et les autres protocoles tels que IPX, NetBEUI, DECNet…

Organismes importants

- IAB : Internet Architecture/Activity Board, chapeaute tout ce qui a trait à Internet et TCP/IP
- IRTF : Internet Research Task Force, responsable de l'évolution de Internet et de TCP/IP
- IETF : Internet Engineering Task Force, édite les RFCs
- IANA / ICANN (Internet Corporation for Assigned Names and Numbers), assigne les adresses publiques, les noms de domaine, les numéros de protocoles IP, les numéros de ports et les numéros d'AS officiels
- IEEE (Institute of Electrical and Electronics Engineers), définit les normes sur les matériels électriques et électroniques

Quels sont les organismes qui font évoluer TCP/IP et Internet ? Les deux ont évolué de conserve puisque TCP/IP a été développé pour faire fonctionner Internet et son ancêtre, Arpanet.

IAB

L'Internet Activity Board chapeaute tout ce qui a trait au développement et à l'évolution de TCP/IP et d'Internet. Cet organisme est constitué d'experts et de représentants d'éditeurs, de constructeurs, de FAI/ISP (Fournisseur d'Accès Internet/Internet Service Provider), d'organismes gouvernementaux… Son financement est assuré par les droits que versent les FAI/ISP et les entreprises membres.

IRTF

L'Internet Research Task Force est responsable de l'évolution technique de TCP/IP et d'Internet. Cet organisme, qui depend de l'IAB, est constitué de chercheurs et d'experts techniques.

IETF

L'Internet Engineering Task Force est chargé de la rédaction, de l'édition et de la publication des RFCs. Il dépend également de l'IAB.

IANA/ICANN

L'Internet Corporation for Assigned Names and Numbers, ex-IANA, est en charge de l'assignation :

- Des adresses publiques, officielles
- Des noms de domaine
- Des numéros de protocoles IP

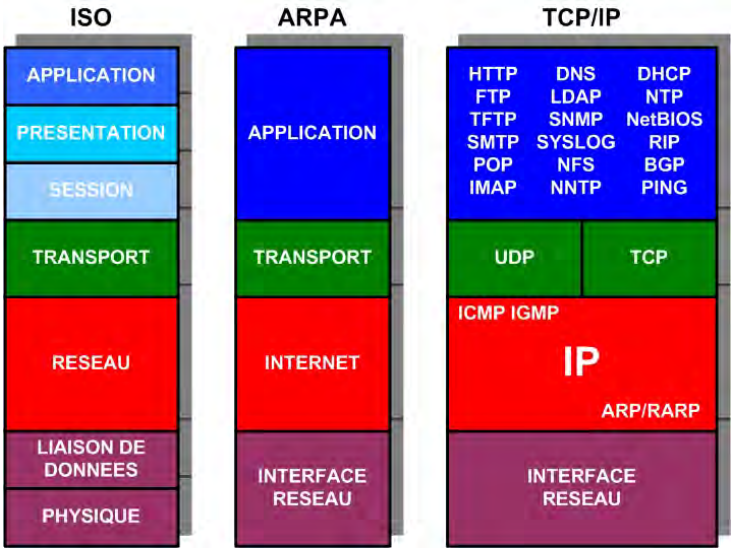
- Des numéros de ports de TCP et d'UDP
- Des numéros d'AS publics, officiels

L'ICANN dépend également de l'IAB. Des branches locales existent dans chaque pays. En France, c'est l'INRIA.

IEEE

L'Institute of Electrical and Electronics Engineers est un organisme américain qui préconise, valide, définit et publie les normes sur les matériels électriques et électroniques. Les normes 802 concernent les réseaux informatiques (802.2/802.3, 802.11, 802.1x, 802.1q…). L'IEEE ne dépend pas de l'IAB mais une grande synergie existe concernant TCP/IP.

Pile TCP/IP – Modèle ARPA



La pile TCP/IP se conforme au modèle ARPA, et non pas DOD comme on le lit souvent.

HISTORIQUE

Originellement, le Department Of Defense (DOD) des USA a créé en 1958 l'ARPA (Advanced Research and Projects Agency), dont le projet le plus connu est la création de l'ARPANET, (ARPA Network) qui est à la fois l'ancêtre d'Internet et de Milnet, le réseau militaire américain. Au départ, ARPANET désignait à la fois le réseau et la pile protocolaire.
Une des évolutions notables d'ARPANET a été XNS (Xerox Network Systems), qui par la suite a donné TCP/IP en Open Source et IPX/SPX, propriétaire de Novell.

MODELE ARPA

Le modèle ARPA a été crée pour normaliser le fonctionnement des protocoles réseaux. Ce modèle est antérieur au modèle ISO. En fait, le modèle ISO s'est inspiré de deux modèles précédents : le modèle ARPA et le modèle SNA d'IBM.

Le modèle ARPA définit uniquement 4 couches :

La couche Interface Réseau

Chargée de l'acheminement physique des données sur les réseaux. Elle est équivalente aux couches 1 (physique) et 2 (liaison de données) du modèle OSI. Cette couche définit les fonctions suivantes :

- Types de médias utilisés
- Caractéristiques des interfaces
- Codage des bits
- Adressage physique

- Modes d'échange supportés, connecté et non connecté
- Détection d'erreur
- Contrôle de flux éventuel

La couche Internet

Équivalente à la couche 3 (réseau) du modèle OSI, elle est chargée des fonctions suivantes :

- Adressage logique
- Routage entre les réseaux logiques
- Fragmentation/réassemblage des datagrammes
- Détection d'erreurs
- Modes d'échange des données

La couche Transport, ou Host-to-host

Équivalente à la couche 4 (transport) du modèle OSI, elle définit :

- Le mode de transport supporté entre applications
- L'identification des applications
- La détection d'erreur
- Le contrôle de flux, optionnellement

La couche Application

Équivalente aux couches 5 à 7 (session, présentation et application) du modèle OSI. Elle définit :

- Le mode de connexion au niveau des applications
- Le codage, la compression et le cryptage des données
- Les interfaces utilisateurs

LA PILE TCP/IP

TCP/IP est beaucoup moins précis et beaucoup moins contraignant dans la définition des couches basses et des couches hautes du modèle ARPA. En revanche, les couches internet et transport sont définies très précisément.

Couche Interface Réseau

Rien n'est définit intrinsèquement concernant le fonctionnement et les mécanismes de cette couche. TCP/IP a seulement deux exigences :

- La possibilité de disposer d'une identification claire du protocole IP dans les trames. Par exemple en Ethernet, IP est codé en type 0x800.
- La possibilité de pouvoir mapper les adresses physiques et les adresses logiques IP. C'est ARP qui se charge de cette fonctionnalité.

Couche internet

La couche réseau est constituée des protocoles ARP/RARP, IP, ICMP et IGMP. Cette couche fournit les fonctionnalités suivantes :

- L'adressage logique, via IP
- La signalisation entre entités IP, via ICMP
- La résolution des adresses logiques en adresses physiques, via ARP
- La gestion des groupes, via IGMP
- La segmentation et le réassemblage des datagrammes, via IP
- Le contrôle de parité permettant de vérifier l'intégrité des données acheminées

Couche Transport

Elle est constituée essentiellement des protocoles TCP et UDP pour le transport en mode fiable et non fiable. D'autres protocoles existent, comme OSPF, EIGRP… Cette couche fournit les fonctionnalités suivantes :

- Adressage de niveau 4 permettant la différentiation des applications
- Le mode d'échange des données, fiable ou non
- La détection d'erreur
- Le contrôle de flux, optionnellement

Couche Application

Elle définit la manière de se connecter avec TCP et UDP, et les règles de fonctionnement à respecter. Bref, c'est plus l'interfaçage qui est défini qu'une véritable couche applicative.

ARP/RARP

ARP / RARP

- ARP
  - Permet de résoudre le mappage entre les adresses logiques et les adresses physique
  - En TCP/IP sur Ethernet, ARP permet de connaitre l'adresse MAC correspondant à une adresse IP
- RARP
  - Permet d'attribuer dynamiquement une adresse IP à toute machine possédant une adresse MAC
  - Toutefois, RARP ne se substitue pas à DHCP ou BOOTP, plus riches en fonctionnalités

ARP et RARP utilisent le même format d'en-tête, seul le code opérationnel est différent.

ARP

Le protocole ARP, Address Resolution Protocole, est chargé de résoudre les adresses logiques IP en adresses physiques. Autrement dit, quelle adresse physique correspond à telle adresse IP ?
En Ethernet, ARP va résoudre des adresses de type MAC. ARP est identifié en Ethernet par le type 0x806.

Toute machine IP possède un cache ARP qui contient les mappages entre les adresses IP et les adresses physiques. Les entrées de ce cache ont une durée de vie prédéfinie, variable selon la pile IP. La durée de vie d'un mappage est généralement de quelques minutes. Par exemple, sous Windows, elle est de deux minutes. A chaque utilisation de ce mappage, le TTL est réinitialisé. Au maximum, un mappage sera présent dix minutes dans le cache.
Ce cache est consultable, sous Windows ou Linux, via la commande ARP –a ou ARP –g.

Il est possible de définir des mappages statiques (ARP –s), dans le cas de réseaux NBMA (Non Broadcast Multi-Access), ou pour des raisons de sécurité. Les réseaux NBMA sont des réseaux multi-accès, c'est-à-dire qu'il est possible de communiquer avec plusieurs machines directement via la même interface, mais sur lesquelles les diffusions ne sont pas supportées.

Une résolution ARP ne peut porter que sur une adresse IP locale. La source et la destination doivent être dans le même réseau IP. En effet, le broadcast MAC est utilisé initialement par la requête ARP. Or, les broadcast, physiques ou logiques, ne sont pas transmis par défaut par les routeurs.

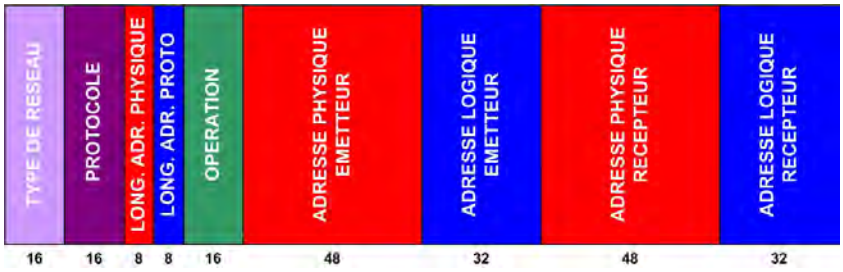
RARP

Le protocole RARP, Reverse ARP, permet d'attribuer dynamiquement une adresse IP à toute machine IP qui en fait la demande.

RARP est peu utilisé dans les réseaux locaux. On l'utilise encore dans des liaisons point-point, comme les réseaux radio ou satellite.

RARP ne se substitue pas à DHCP ou BOOTP, qui offrent des fonctionnalités beaucoup plus riches et une plus grande souplesse d'utilisation.

Format ARP/RARP

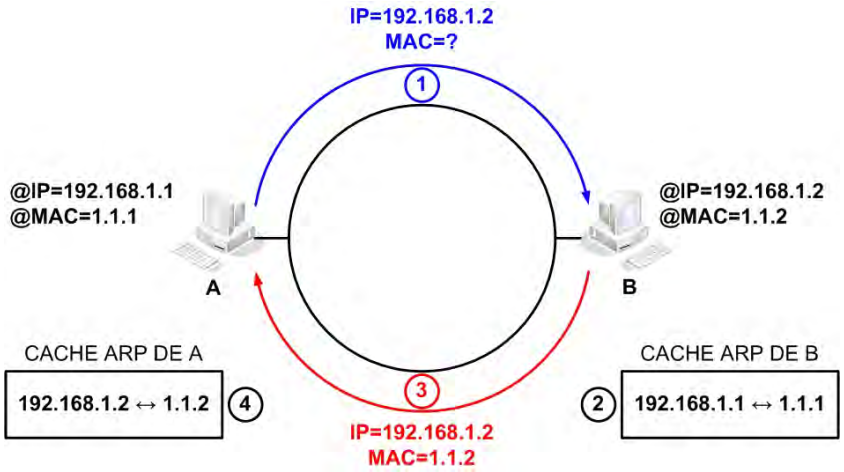


Un en-tête ARP/RARP est constitué des champs suivants :

- TYPE DE RESEAU. Sur 16 bits. Indique le type de réseau. Le plus utilisé est le 01 qui correspond à Ethernet.
- PROTOCOLE. Sur 16 bits. Indique le protocole de niveau 3 utilisé. Pour IPv4, cette valeur est égale à 0x800. Pour IPv6, elle est égale à 0x8DD.
- LONGUEUR D'ADRESSE PHYSIQUE. Sur 8 bits. Indique, en octets, la longueur de l'adresse physique. En Ethernet, cette valeur est égale à 6.
- LONGUEUR D'ADRESSE DE PROTOCOLE. Sur 8 bits. Indique, en octets, la longueur de l'adresse logique. En IPv4, cette valeur est égale à 4.
- OPERATION. Sur 16 bits. Contient le code opérationnel. 4 codes sont utilisés : ARP Request / ARP Reply / RARP Request / RARP Reply
- ADRESSE PHYSIQUE EMETTEUR. La longueur de ce champ dépend bien évidemment des adresses physiques utilisées. Dans le cas d'Ethernet, ce champ a une longueur de 48 bits et contient l'adresse MAC de l'émetteur.
- ADRESSE LOGIQUE DE L'EMETTEUR. La longueur de ce champ dépend des adresses logiques utilisées. Dans le cas de TCP/IP, ce champ a une longueur de 32 bits et contient l'adresse IP de l'émetteur.
- ADRESSE PHYSIQUE DU RECEPTEUR. La longueur de ce champ dépend des adresses physiques utilisées. Dans le cas d'Ethernet, ce champ a une longueur de 48 bits et contient l'adresse MAC du destinataire.
- ADRESSE LOGIQUE DU RECEPTEUR. La longueur de ce champ dépend des adresses logiques utilisées. Dans le cas de TCP/IP, ce champ a une longueur de 32 bits et contient l'adresse IP du destinataire.

Exemple ARP

Exemple ARP



EXEMPLE ARP

Prenons l'exemple le plus courant : deux machines IP sur un réseau Ethernet.

A, la machine émettrice, connait l'adresse IP du destinataire, B. Afin de pouvoir communiquer physiquement avec celle-ci, elle doit connaitre son adresse MAC. Pour cela, A émet une requête ARP (ARP REQUEST) sur le réseau.

Cette trame Ethernet a les caractéristiques suivantes :

- L'adresse MAC source est celle de A, 1.1.1 ;
- L'adresse MAC destination est FF:FF:FF:FF:FF:FF, soit l'adresse de diffusion MAC. Chaque machine sur le réseau doit traiter cette trame ;
- La requête ARP contient les informations suivantes :
  - ➔ L'adresse physique source est celle de A, 1.1.1 ;
  - ➔ L'adresse IP source est celle de A, 192.168.1.1 ;
  - ➔ L'adresse physique de destination est 00:00:00:00:00:00 ;
  - ➔ L'adresse IP de destination est celle de B, 192.168.1.2.

La machine destinatrice, B, reçoit cette requête et enregistre le mappage entre les adresses physique et IP de A dans son cache. Ensuite, B répond à la requête en émettant une réponse ARP (ARP REPLY).

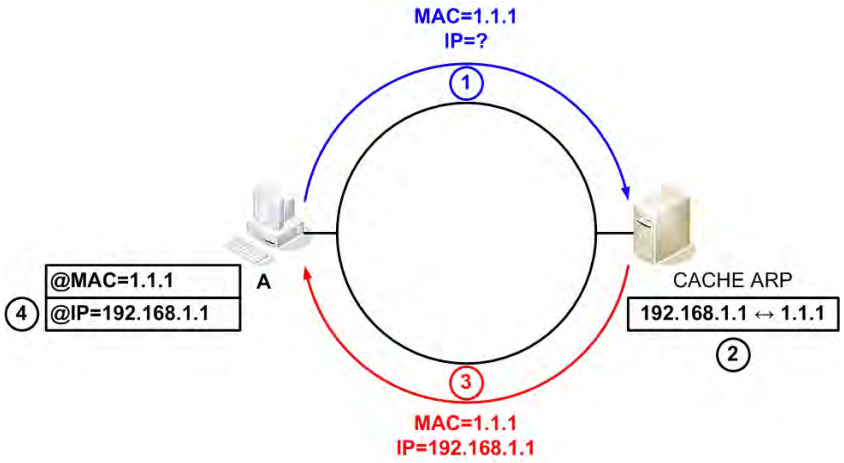
Cette trame Ethernet a les caractéristiques suivantes :

- L'adresse MAC source est celle de B, 1.1.2 ;
- L'adresse MAC destination est celle de A, 1.1.1 ;
- La réponse ARP contient les informations suivantes :
  - ➔ L'adresse physique source est celle de B, 1.1.2 ;

- ➔ L'adresse IP source est celle de B, 192.168.1.2 ;
- ➔ L'adresse physique de destination est celle de A, 1.1.1 ;
- ➔ L'adresse IP de destination est celle de A, 192.168.1.1.

A reçoit la réponse de B et met à jour son cache ARP en enregistrant le mappage entre les adresses MAC et IP de B.

Exemple RARP



EXEMPLE RARP

Dans cet exemple, A est une machine diskless, sans disque dur. Sur le même réseau, un serveur RARP, souvent un routeur ou un modem est chargé de fournir des adresses IP. Le mécanisme d'attribution des adresses IP est le suivant :

Au démarrage, A émet une requête RARP REQUEST. Cette trame Ethernet a les caractéristiques suivantes :

- L'adresse MAC source est celle de A, 1.1.1 ;
- L'adresse MAC destination est FF:FF:FF:FF:FF:FF, soit l'adresse de diffusion MAC. Chaque machine sur le réseau doit traiter cette trame ;
- La requête RARP contient les informations suivantes :
  - ➔ L'adresse physique source est celle de A, 1.1.1 ;
  - ➔ L'adresse IP source est 0.0.0.0 ;
  - ➔ L'adresse physique de destination est 00:00:00:00:00:00 ;
  - ➔ L'adresse IP de destination est 0.0.0.0.

Le serveur RARP reçoit cette requête. Il va :

- Sélectionner une adresse IP disponible, 192.168.1.1 dans notre exemple ;
- Enregistrer le mappage dans son cache ARP.

Le serveur RARP émet une réponse RARP (RARP REPLY). Cette trame Ethernet a les caractéristiques suivantes :

- L'adresse MAC source est celle du serveur ;
- L'adresse MAC destination est de A, 1.1.1 ;
- La requête RARP contient les informations suivantes :

- ➔ L'adresse physique source est celle du serveur ;
- ➔ L'adresse IP source est celle du serveur ;
- ➔ L'adresse physique de destination est celle A, 1.1.1 ;
- ➔ L'adresse IP de destination est 192.168.1.1.

A reçoit la réponse RARP et va utiliser l'adresse 192.168.1.1 pour communiquer avec les autres machines du réseau.

IP

IP

- Fonctionne en mode non-connecté ou « Best Effort »
- On parle de datagramme IP
- Rôles :
  - Adressage logique de niveau 3 (OSI)
  - Routage logique entre les réseaux IP
  - Fragmentation et ré-assemblage des paquets de niveau supérieur
  - Détection d'erreurs (checksum)

IP est le cœur de la pile TCP/IP. Il fonctionne au niveau de la couche internet, la couche trois, et possède les caractéristiques suivantes :

FONCTIONNEMENT

IP fonctionne en mode non connecté (connectionless) ou « Best Effort ». Ce qui signifie qu'il n'y a pas d'établissement préalable d'une session entre l'émetteur et le destinataire avant tout échange de données. On parle de datagramme IP.

Les données sont envoyées au fur et à mesure qu'elles sont reçues des couches supérieures, UDP ou TCP la plupart du temps.

Il n'y a aucune gestion du contrôle de flux. Cette fonctionnalité est laissée, si nécessaire, à la charge de TCP ou de l'application (si elle utilise UDP).

Aucune retransmission des datagrammes en cas de perte ou d'erreur de parité.

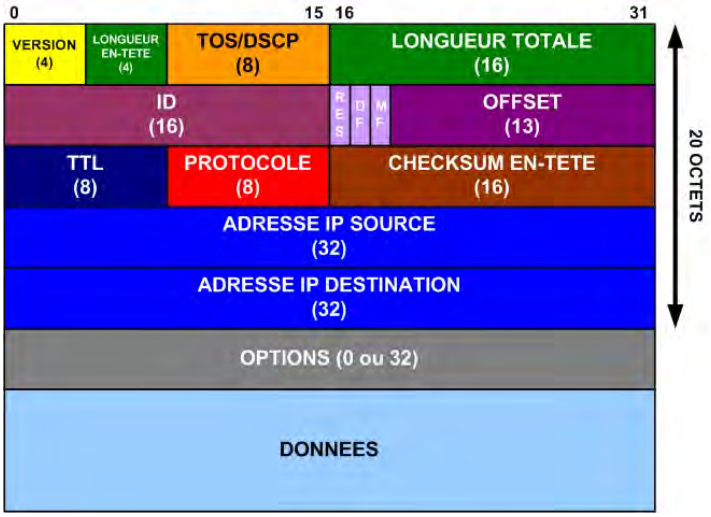
ROLES DE IP

- Adressage logique de niveau 3. L'adressage logique permet de faire abstraction de l'adressage physique du réseau.
- Routage logique entre les réseaux IP, une des fonctions essentielles de IP. IP nécessite souvent l'adjonction d'applications dédiées, les protocoles de routages afin d'étendre ses possibilités et son efficacité dans ce domaine.
- Fragmentation et réassemblage des datagrammes. IP utilise la fragmentation lorsqu'il reçoit des données trop volumineuses de la couche transport, quand la taille des données ajoutée à l'en-tête IP dépasse la MTU du réseau.
  TCP ne fragmente généralement pas, car il gère dynamiquement les échanges et tient compte de la MSS. La Maximum Segment Size est égale à la MTU moins les 20 octets correspondant à l'en-tête IP.

En revanche les applications utilisant UDP sont propices à ce genre de débordements car elles ne tiennent généralement pas compte de la MTU.

- Détection d'erreurs. IP intègre un calcul de parité permettant de détecter une altération éventuelle des données entre leur émission et leur réception. Aucune correction d'erreur ou de retransmission n'est utilisée.

En-tête IP



L'en-tête IP est constitué de deux parties :

- Une partie fixe obligatoire sur 20 octets ;
- Une partie optionnelle contenant des informations supplémentaires pour des fonctionnalités spécifiques.

Voyons quels sont les composants d'un en-tête IP :

VERSION

- Sur 4 bits ;
- Indique la version de IP utilisée ;
- Deux versions sont actuellement disponibles : 4 pour IPv4 et 6 pour IPv6.

LONGUEUR DE L'EN-TÊTE

- Sur 4 bits ;
- Indique en mots de 32 bits la taille totale de l'en-tête IP ;
- La valeur par défaut est de 5, soit 160 bits ou 20 octets ;
- Les options auront donc une taille multiple de 32 bits, quitte à utiliser du bourrage si nécessaire.

LONGUEUR TOTALE

- Sur 16 bits ;
- Indique, en octets, la longueur totale du datagramme IP.

TTL (TIME TO LIVE)

- Sur 8 bits ;
- Indique le nombre de sauts que peut effectuer le datagramme. Chaque routeur traversé incrémente cette valeur de 1 et recalcule le CHECKSUM. Lorsque la valeur du TTL est de 0, le datagramme est détruit ;
- Selon le système d'exploitation, la valeur initiale peut être de 32, 64, 128 ou de 255 ;
- A l'origine, ce champ indiquait la durée de vie du datagramme.

PROTOCOLE

- Sur 8 bits ;
- Désigne le protocole destinataire des données que transporte IP ;
- Le champ est renseigné par IP à la réception des données de la couche transport sur la machine émettrice et lu sur la machine destinatrice.

Quelques exemples de valeurs utilisées couramment :

- ➔ 0 : IP
- ➔ 1 : ICMP
- ➔ 6 : TCP
- ➔ 17 : UDP
- ➔ 27 : RDP
- ➔ 89 : OSPF

OPTIONS

- Sur x32 bits. Sinon, des bits de bourrages sont utilisés ;
- Contient des informations relatives à des fonctionnalités particulières.

Quelques exemples :

- ➔ Enregistrement de la source
- ➔ Routage à la source
- ➔ Horodatage
- ➔ Options de fragmentation

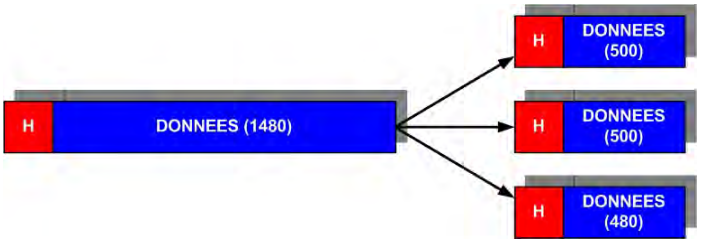
ID, RES, DF, MF et OFFSET

- Ces champs concernent la fragmentation ;
- ID, sur 16 bits, permet d'identifier un datagramme ;
- Le bit RES est réservé pour un usage futur ;
- Le bit DF (DON'T FRAGMENT) interdit la fragmentation s'il est positionné à 1 ;
- Le bit MF (MORE FRAGMENT ?) permet de préciser si un fragment est ou non le dernier de la série ;
- Offset, sur 13 bits, indique la position qu'occupe un fragment dans le datagramme original.

ToS/DSCP

- Sur 8 bits ;
- Type of Service / Differentiated Services Code Point ;
- Ce champ est utilisé pour la QoS (Quality of Service), la qualité de service.

Fragmentation



- La fragmentation est utilisée lorsque la taille des données initiale est trop grande pour traverser un réseau intermédiaire (qui possède une MTU inférieure au réseau d'origine)
- Le datagramme initial est alors scindé en autant de datagrammes que nécessaire
- Les datagrammes fragmentés seront réassemblés par la destination

PRINCIPE

La fragmentation est utilisée dans les cas suivants :

- IP doit transmettre un datagramme sur un réseau possédant une MTU inférieure au réseau d'origine de celui-ci. Ce cas de figure tend à se raréfier car les réseaux actuels supportent, ou émulent, une MTU de 1500 octets, correspondant à la valeur native d'Ethernet.
- Une application s'appuyant sur UDP ne tient pas compte de la MTU du réseau. UDP ne gère pas ce paramètre. C'est normalement à l'application de le prendre en charge.

Avec TCP, il est rare qu'IP doive fragmenter car TCP fractionne, séquence et réordonne ses segments.

Certaines piles IP et certaines applications utilisent le MTU PATH DISCOVERY. Cette technique consiste à positionner le bit DF (DON'T FRAGMENT) à 1, ce qui interdit la fragmentation, et à réaliser des tests afin de connaitre la plus grande valeur possible utilisable pour une destination donnée. En effet, si le datagramme doit être fragmenté et que le bit DF est positionné à 1, le datagramme est détruit et un message ICMP est envoyé à l'expéditeur.

FONCTIONNEMENT

Le datagramme original nécessitant d'être fragmenté, sera scindé en autant de datagrammes que nécessaire.

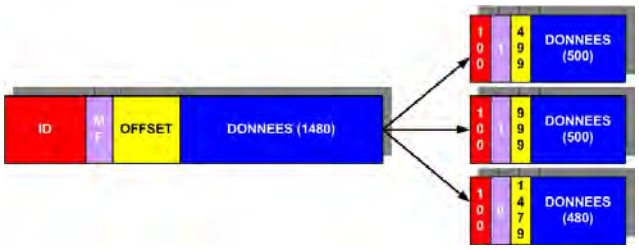
Ces datagrammes auront le même ID que l'original, afin pour pouvoir les identifier sans ambiguïté.

Seul le dernier aura le bit MF positionné à 0. Ce qui permet au destinataire de savoir combien de fragments il doit recevoir au total.

Le champ OFFSET précisera la position des données transportées dans le datagramme original, afin de pouvoir réassembler dans l'ordre les différents fragments. Rien ne nous garantit, en IP, que les datagrammes parviennent au destinataire dans l'ordre dans lequel ils ont été émis.

Seule le destinataire réassemblera le datagramme original à partir des fragments reçus.

Exemple de fragmentation



- L'ID utilisé pour tous les fragments est le même que celui d'origine
- Le bit MF (More Fragment ?) :
  - Positionné à 1 précise qu'il y a encore un ou plusieurs fragments
  - Positionné à 0 précise que ce fragment est le dernier
- Le numéro d'offset indique la position du dernier octet dans le datagramme d'origine transporté par ce fragment

Prenons pour exemple un datagramme ayant une taille totale de 1500 octets. Supposons, en pure théorie, qu'il faille lui faire traverser un réseau dont la MTU est égale à 520 octets.

FRAGMENTATION

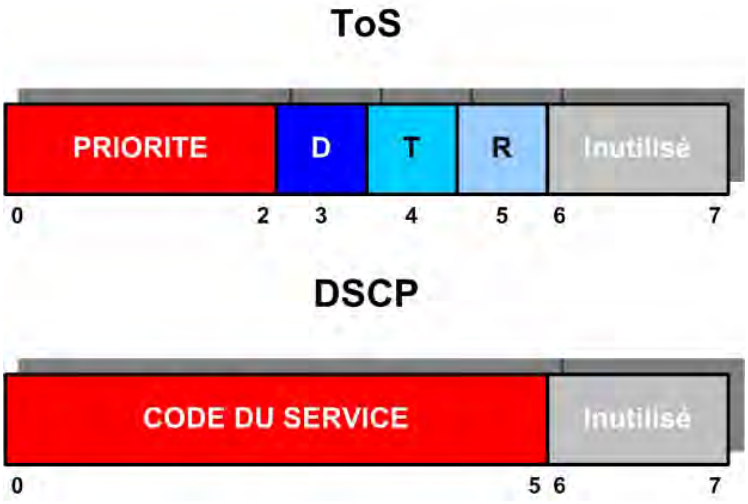
Les fragments générés à partir du datagramme original ont les caractéristiques suivantes :

- Ils ont tous le même ID, le même que le datagramme original. Ici, il est égal à 100 ;
- Les deux premiers fragments auront le bit MF positionné à 1 ;
- Le troisième et dernier fragment aura le bit MF positionné à 0 ;
- Le premier fragment contiendra les 500 premiers octets du datagramme d'origine. Les octets étant numérotés de 0 à 1499, le champ OFFSET a la valeur 499 ;
- Le second fragment contiendra les 500 octets suivants du datagramme d'origine. Le champ OFFSET aura donc la valeur 999 (499+500) ;
- Enfin, le troisième et dernier fragment contiendra les 480 octets restants. Le champ OFFSET aura la valeur 1479 (999+480).

REASSEMBLAGE

Une fois que tous les fragments ont été reçus par le destinataire du datagramme, celui-ci procède à son réassemblage.

ToS/DSCP



Le champ dit ToS/DSCP est utilisé pour la qualité de service (QoS, Quality of Service). Le principe de la QoS est de définir les niveaux de priorité des flux applicatifs. Le but est de gérer l'accès au réseau en cas de congestion en se basant sur ce critère. Il est possible d'utiliser deux techniques : ToS/IP Precedence ou DSCP.

ToS/IP Precedence

Permet de définir le niveau de priorité du datagramme IP, ainsi que ses exigences en termes de délais de transmission, de débit et de fiabilité.

La priorité est codée sur 3 bits, ce qui fournit 8 niveaux de priorité. Les niveaux de priorité vont de 0 (priorité normale) à 7 (supervision réseau).

Le bit D (Delay), s'il est positionné à 1, permet d'indiquer la sensibilité aux délais de transmission sur le réseau. Cela concerne essentiellement les flux de données de type VoIP (Voice over IP), les applications temps réel et les applications centralisées (de type CITRIX).

Le bit T (Throughput), s'il est positionné à 1, permet d'indiquer qu'un débit élevé est requis. Cela concerne les applications de transfert des données, les bases de données, etc. Bref toute application nécessitant de forts échanges de données.

Le bit R (Reliability), s'il est positionné à 1, permet d'indiquer que la fiabilité est requise. Cela concerne la plupart des applications client/serveur. En revanche la voix sur IP et la vidéo sur IP n'exigent pas une fiabilité absolue, leurs codecs acceptant un taux de perte faible, mais non nul.

Cette technique est aujourd'hui obsolète, pour les raisons suivantes :

- La granularité est insuffisante, huit niveaux de priorité définissable seulement.
- Elle ne fournit qu'un niveau de priorité, pas les caractéristiques associées à un type d'application donné.

- Une application ayant un niveau de priorité supérieur à une autre aura toujours un accès privilégié au réseau vis-à-vis de celle-ci. Certaines applications peuvent ne jamais avoir accès au réseau durant la congestion, alors qu'il est parfois possible de retarder la transmission de certaines données très prioritaires afin de permettre l'accès à certaines données moins prioritaires sans altérer leur fonctionnement.
- Les bits D, T et R ne sont qu'informatifs et non quantitatifs. Une application en temps réel et une application VoIP n'ont pas les mêmes exigences en délais de transmission, en débit et en fiabilité. Pourtant, elles seront gérées de la même manière.

DSCP

On utilise 6 bits pour DSCP

DSCP permet de définir des classes de services, et non pas une simple priorité. Ce n'est plus une priorité que l'on va fournir à l'application, mais un service.

Chaque classe peut être associée à des caractéristiques de :

- Sensibilité aux délais de transmission
- Exigence en débit minimal
- Taux de pertes acceptable
- Variation des délais de transmissions (la gigue)

Certaines classes sont prédéfinies et normalisées (IETF), d'autres sont libres d'utilisation et de définition (LOCAL).

Structure :

- Si les 3 derniers bits sont à 0 : compatibilité avec les anciennes valeurs de ToS (xxx000) ;
- Il existe 3 groupes :
  - ➔ Groupe 1 : xxxxx0, IETF ;
  - ➔ Groupe 2 : xxxx11, local ou expérimental ;
  - ➔ Groupe 3 : xxxx01, local ou expérimental IETF.

Les flux applicatifs sont mieux caractérisés et définis qu'ils ne l'étaient avec IP Precedence.

Types de datagrammes IP

- Unicast : un à un
  - Une adresse source représentant une source unique
  - Une adresse destination unique représentant une destination unique
  - Routable
- Broadcast (diffusion) : un à tous, indistinctement
  - Une adresse source unique représentant une source unique
  - Une adresse destination spéciale, destinée à atteindre l'ensemble des machines IP
  - Non routable
- Multicast : un à plusieurs, sélectivement
  - Une adresse source unique
  - Une adresse de destination représentant un groupe de machines spécifique
  - Routable

Il existe trois type de datagramme en IP : Unicast, Broadcast et Multicast.

UNICAST

Appelé également un à un : une source unique, une destination unique

Les adresses source et destination identifient chacune une machine unique

Les unicasts sont routables

BROADCAST

Ou aussi diffusion, un à tous

Une adresse source unique

Un broadcast utilise des adresses de destination spéciales réservées

Un broadcast permet d'atteindre toute machine IP d'un réseau ou d'un VLAN sans en connaitre les adresses

Utilisé pour les mécanismes applicatifs ou réseau nécessitant un caractère dynamique

Les broadcasts ne sont pas routables par défaut

Ils peuvent générer une pollution importante sur le réseau

Une adresse de broadcast ne peut pas être une adresse source

TCP ne peut utiliser les mécanismes de diffusion

MULTICAST

Ou aussi multi-diffusion, un à plusieurs de manière sélective

Une adresse source unique

Les multicasts utilisent des adresses de destination spéciales réservées

Les adresses de broadcast représentent des groupes de machines

Pour recevoir une copie d'un datagramme destiné à un groupe, une machine doit d'abord adhérer à ce groupe

Les multicast permettent de garder un fonctionnement dynamique du réseau, sans générer autant de pollution que les broadcasts

Les multicasts sont routables, car contrôlables

Une adresse multicast n'est jamais utilisée en adresse source

TCP ne peut utiliser les mécanismes de multicast

ICMP

ICMP

- Internet Control Message Protocol
- Signalisation IP sur le réseau
- Numéro de protocole 1
- Utilisé pour transporter les messages de TCP/IP :
  - Informations
  - Erreurs
  - Tests
- Composé de 4 champs :
  - Type
  - Code
  - Checksum
  - Données (variable)

ICMP (Internet Control Message Protocol) est le protocole de signalisation de IP sur le réseau. ICMP a les caractéristiques suivantes :

- Il est identifié par le numéro de protocole n°1 en IP ;
- Il est permet de transporter les messages de TCP/IP ;
- Il est décrit dans le RFC 792 ;
- Il existe trois types de messages :
  - ➔ Informations
  - ➔ Erreurs
  - ➔ Tests
- Un message ICMP est composé de 4 champs :
  - ➔ Type, sur 8 bits, qui identifie le type de message ;
  - ➔ Code, sur 8 bits, qui indique le code opérationnel ;
  - ➔ Checksum, sur 16 bits ;
  - ➔ Données (variable), contient les données éventuellement associées au message.

EXEMPLES

- Destination Unreachable. Type 3, code 0 à 11. Impossible de joindre la destination. Le code indique pourquoi.
- Echo request. Type 8, code 0. Utilisé par PING et TRACEROUTE.
- Echo reply.
- Type 0, code 0. Utilisé par PING et TRACEROUTE.
- Redirect. Type 5, code 0 à 3. Permet de rediriger des données vers un autre routeur.

- Source Quench. Type 4, code 0. Indique que l'émetteur demande au destinataire une suspension momentanée de l'envoi de datagrammes IP.
- Expiration Time. Type 1, code 0 ou 1.TTL expiré ou temps alloué au réassemblage des fragments d'un datagramme dépassé.

Adresses IP

Adresses IP

- En IPv4, une adresse est codée sur 32 bits ou 4 octets W.X.Y.Z
- Elle est composée de 2 parties :
  - Une adresse réseau, ou ID réseau, qui identifie le réseau IP
  - Une adresse hôte, ou ID hôte, qui identifie une interface d'une machine sur le réseau IP
- Les parties réseau et hôte ne sont pas fixes, elles dépendent de la classe à laquelle appartient l'adresse
- Il y a unicité globale de l'adresse
- Notation sous forme décimale ou binaire

Les adresses IPv4 sont codées sur 32 bits, ou 4 octets. On les note sous la forme W.X.Y.Z. Une adresse IP identifie une interface réseau d'une machine. Une interface peut posséder plusieurs adresses IP. En revanche, une adresse IP ne peut nativement être partagée entre plusieurs interfaces. Il existe des cas particuliers, pour les clusters notamment.

Une adresse IP est composée de deux parties :

- Une adresse réseau, ou ID réseau, qui identifie de manière unique un réseau logique IP. Un réseau physique, ou un VLAN, peut accueillir plusieurs réseaux logiques IP. En revanche, un réseau logique IP doit être inclus dans un réseau physique ou un VLAN.
- Une adresse hôte, ou ID hôte, qui identifie de manière unique une interface IP sur le réseau logique. Une adresse hôte doit être unique dans le sous réseau IP, dans le cas contraire il y a duplication d'adresse.

Les parties réseau et hôte ne sont pas fixes, comme c'est le cas pour d'autres protocoles. La nomenclature dépend de la classe à laquelle appartient d'adresse.

Les adresses IP doivent être globalement uniques, c'est-à-dire qu'elles doivent permettre d'identifier clairement l'interface d'une machine. Cette unicité peut être à l'échelle de l'entreprise, pour les adresses dites privées, ou à l'échelle de la planète, pour les adresses dites publiques.

Il est possible de noter une adresse IP sous forme décimale, binaire, voir hexadécimale.

Classes d'adresses IP

Les classes d'adresses

- Les adresses sont segmentées en classes
- Il existe 5 classes d'adresses :
  - Trois classes d'adressage : A, B et C
  - Une classe de fonction, de multicast : la classe D
  - Une classe réservée, de recherche : la classe E

Les adresses sont segmentées en classes. Le but original était d'adapter la structure d'adressage à la taille des réseaux physiques. Comme nous allons le voir, cela a donné des réseaux gigantesques inexploitables en l'état, des réseaux énormes et enfin des réseaux raisonnables. Heureusement, les classes d'adresses sont utilisées comme des référentiels plus que comme des normes.

Il existe cinq classes d'adresses :

- Trois classes d'adressages : les classes A, B et C. Elles sont utilisées pour l'adressage des machines et des réseaux.
- Une classe de fonction, la classe D. Elle est utilisée pour la gestion des groupes de multicast. Chaque adresse identifie un groupe, il n'y a pas de référence aux réseaux et aux adresses hôtes.
- Enfin, une classe réservée, la classe E. Elle servait initialement pour la recherche. Elle ne sert plus à grand chose aujourd'hui.

Règles d'adressage

- Un ID hôte ne peut avoir tous ses bits ni à 1 ni à 0
  - Tout à 1 signifie : « tout hôte de ce réseau », c'est l'adresse de diffusion de réseau logique IP
  - Tout à 0 signifie : « ce réseau »
- Le réseau 127.0.0.0 est réservé pour les adresses de bouclage, de loopback
- Le réseau 0.0.0.0 est réservé :
  - En adresse source pour les machines clientes DHCP/BOOTP
  - En adresse de destination pour désigner la route par défaut dans les tables de routage
- 255.255.255.255 est une adresse de diffusion locale, qui n'est pas routable, qui signifie « toute machine IP »

La nomenclature d'adressage IP est soumise à quelques règles, dont certaines sont d'ailleurs discutables :

Identifiant hôte

- L'identifiant d'hôte ne peut avoir l'ensemble de ses bits à 1. Cette adresse est réservée et signifie « tout hôte de ce réseau ». Autrement dit, c'est une adresse de diffusion de réseau logique IP.
- L'identifiant d'hôte ne peut avoir l'ensemble de ses bits à 0. Cette adresse est réservée et signifie « ce réseau ».

Le réseau 127.0.0.0

Le réseau 127.0.0.0 est réservé pour les adresses de bouclage. Toute machine IP possède une interface virtuelle de bouclage, indépendante des interfaces réelles physiques, à laquelle on affecte l'adresse 127.0.0.1. Cette interface permet de réaliser un test de la pile IP. Si le PING 127.0.0.1 ne fonctionne pas, il faut réinstaller TCP/IP.

Le réseau 0.0.0.0

Le réseau 0.0.0.0 est réservé pour deux fonctions :

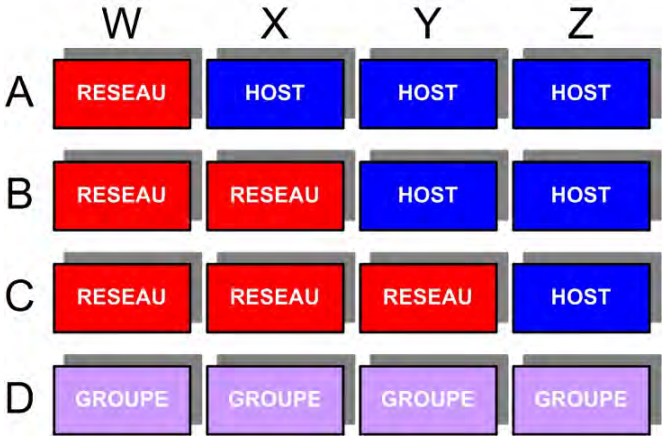
- En source, l'adresse est utilisée par les clients DHCP/BOOTP qui n'ont pas encore obtenu d'adresse IP d'un serveur.
- En destination, elle désigne la route par défaut dans la table de routage.

L'adresse 255.255.255.255

L'adresse 255.255.255.255 qui est dite de diffusion locale, signifie « toute machine IP de ce réseau ». Elle n'est ni routable ni transmise par les routeurs.

Classes d'adresses

Les classes d'adresses



Etudions maintenant la nomenclature des quatre classes d'adresses exploitables :

CLASSE A

La classe A a la structure suivante : W.X.Y.Z. W représente l'adresse réseau, X, Y et Z l'adresse hôte. L'adresse réseau est codée sur 8 bits et l'adresse hôte sur 24 bits.

Le premier bit du premier octet est toujours égal à 0.

W est donc compris entre 1 et 126, puisque 127 est réservé pour les interfaces de loopback. Il y a donc 126 réseaux de classe A disponibles.

La plage des réseaux de classe A est: 1.0.0.0 – 126.0.0.0.

Pour chaque réseau de classe A, on peut avoir 2^24-2=16777214 hosts. En effet, il faut retrancher l'adresse du réseau lui-même (W.0.0.0) et l'adresse de broadcast du réseau (W.255.255.255).

Exemple : la machine possédant l'adresse 10.1.1.1 est dans le réseau 10.0.0.0 et a l'adresse hôte 0.1.1.1.

CLASSE B

La classe B a la structure suivante : W.X.Y.Z. W et X représentent l'adresse réseau, et Y et Z l'adresse hôte. L'adresse réseau est codée sur 16 bits et l'adresse hôte sur 16 bits également.

Les deux premiers bits du premier octet sont toujours 10.

W est donc compris entre 128 et 191, et X entre 0 et 255. Il y a donc 64*256=16384 réseaux de classe B disponibles.

La plage de réseaux de classe B est: 128.0.0.0 – 191.255.0.0.

Pour chaque réseau de classe B, on peut avoir 2^16-2=65534 hosts.

Exemple : la machine possédant l'adresse 172.16.0.7 est dans le réseau 172.16.0.0 avec l'adresse hôte 0.0.0.7.

CLASSE C

La classe C a la structure suivante : W.X.Y.Z. W, X et Y représentent l'adresse réseau, et Z l'adresse hôte. L'adresse réseau est donc codée sur 24 bits et l'adresse hôte sur 8.

Les trois premiers bits du premier octet sont toujours 110.

W est donc compris entre 192 et 223, X et Y entre 0 et 255. Il y a donc environ 2 millions (32*256*256) d'adresses de classe C disponibles.

La plage de réseaux de classe C est : 192.0.0.0 – 223.255.255.0.

Pour chaque réseau de classe C, on peut avoir 2^8-2=254 hosts.

Exemple : la machine possédant l'adresse 192.168.1.100 est le réseau 192.168.1.0 avec l'adresse hôte 0.0.0.100.

CLASSE D

La classe D a la structure suivante W.X.Y.Z. Il n'y a pas d'identification du réseau ou de l'hôte puisque la classe D est utilisée pour identifier des groupes.

Les quatre premiers bits sont toujours 1110.

W est donc compris entre 224 et 239.

La plage utilisable est 224.0.0.0 – 239.255.255.255, soit 256 millions d'adresses de groupes disponibles (16*256*256*256).

Adresses publiques et privées

- Il existe deux catégories d'adresses
  - Publiques : adresses officielles ou « naturelles »
    - Utilisées sur Internet
    - Attribuées par l'IANA/ICANN (INRIA en France)
  - Privées :
    - Utilisées en interne uniquement
    - Non-routables sur Internet
    - Utilisation libre et gratuite
    - Plages : 10.0.0.0; 172.16.0.0-172.31.0.0; 192.168.0.0-192.168.255.0

Afin, entre autres, de contourner la pénurie d'adresses disponibles, deux catégories d'adresses existent : les adresses privées et les adresses publiques.

ADRESSES PUBLIQUES

Les adresses de réseaux publiques, ou officielles, sont toutes celles qui ne sont pas privées. On parle également d'adresses « naturelles ».

Leur attribution est à la charge de l'ICANN (ex IANA) et de ses agences, l'INRIA pour la France.

Elles sont en pénurie depuis 1995.

ADRESSES PRIVEES

Les adresses privées sont utilisables uniquement en interne, pas sur Internet.

Leur utilisation est libre de droit et gratuite.

En revanche, les adresses privées ne sont pas routables sur Internet. Elles devraient même être normalement filtrées par les FAI/ISP, ce qui est rarement fait.

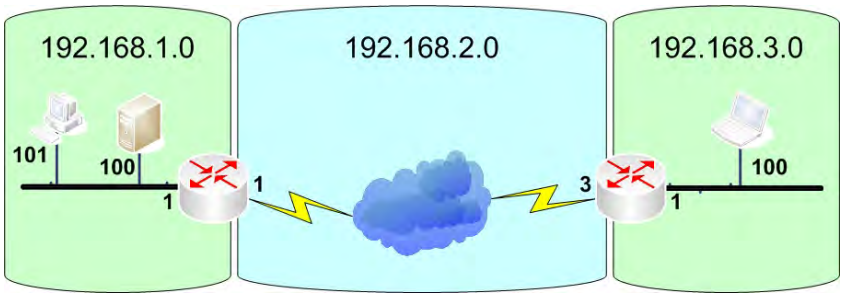
Les plages des réseaux privés sont les suivantes :

- Pour la classe A, un seul réseau le 10.0.0.0
- Pour la classe B, 16 réseaux : 172.16.0.0 à 172.31.0.0
- Pour la classe C, 256 réseaux : 192.168.0.0 à 192.168.255.0

La définition des adresses privées est disponible dans la RFC 1918.

Exemple

Exemple



Dans cet exemple, nous avons deux réseaux distants :

- Le 192.168.1.0. Sur ce réseau, deux machines sont représentées : 192.168.1.100 et 192.168.1.101. Le routeur possède l'adresse 192.168.1.1.
- Le 192.168.3.0. Sur ce réseau, une machine est représentée, la 192.168.3.100. Le routeur possède l'adresse 192.168.3.1.

Pour connecter ces deux réseaux distants, un lien WAN (Wide Area Network) est mis en place entre les deux routeurs. Il est nécessaire que les deux routeurs mis en relation soient dans le même réseau IP. Pour que deux machines IP puissent communiquer directement entre elles, elles doivent être dans le même réseau IP. Autrement, un routeur est nécessaire. Le réseau 192.168.2.0 est commun à nos deux routeurs, l'un possédant l'adresse 192.168.2.1, l'autre l'adresse 192.168.3.1.

Masque de sous-réseau

- Une adresse IP est associée à un masque de sous-réseau
- Le format, sur 32 bits, est noté A.B.C.D en décimale
- Les bits à 1 du masque identifient la partie réseau de l'adresse, les bits à 0 la partie hôte
- Le masque de sous-réseau a 2 rôles :
  - Différencier l'adresse réseau de l'adresse hôte. Par défaut, c'est le masque de sous-réseau de la classe d'adresse qui s'applique
  - Déterminer si l'adresse IP de destination est locale ou distante, donc si l'envoi sera direct ou transitera par un routeur

---

Il y a deux paramètres obligatoires pour configurer une machine en IP : l'adresse IP et le masque de sous-réseau.

FORMAT

Le masque de sous réseau est codé sur 32 bits

Sa notation décimale est la suivante : A.B.C.D.

Le rôle premier du masque est de différentier l'adresse réseau de l'adresse hôte. Pour cela, on positionne à 1 tous les bits utilisés pour coder l'adresse réseau et à 0 tous les bits utilisés pour coder l'adresse hôte.

ROLES

Le masque de sous-réseau a deux rôles :

- Différencier l'adresse réseau de l'adresse hôte. Pour cela, un AND logique est opéré entre l'adresse IP et le masque de sous-réseau, le résultat constitue l'adresse réseau.

```
EXEMPLE

Prenons l'adresse et le masque suivants :

192.168.3.77 255.255.255.0

Si l'on procède à un AND logique entre l'adresse et le masque, on
obtient le réseau 192.168.3.0. Le restant, 77, est l'adresse hôte.
```

- Déterminer si l'adresse IP de destination, que l'on veut joindre, est locale ou distante. Pour cela, une machine émettrice applique son masque de sous-réseau à l'adresse de destination et en extrait le pseudo réseau de destination. Elle le compare ensuite à sa propre adresse réseau :

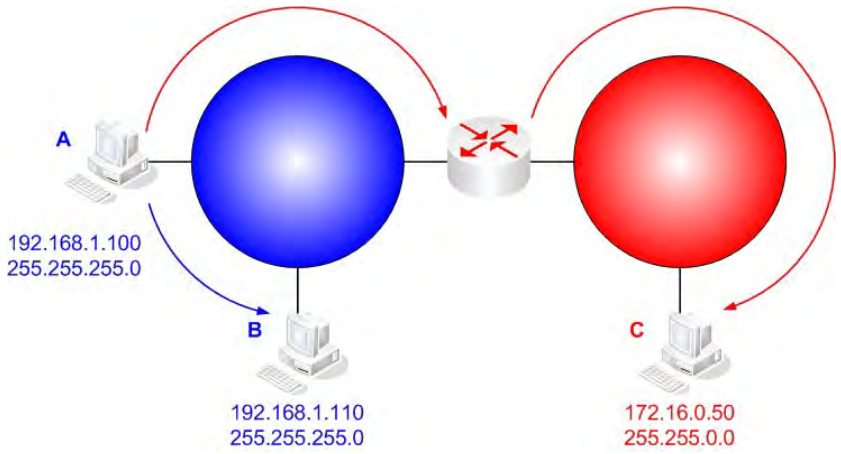
  ➔ Si les valeurs correspondent, l'adresse de destination est locale. L'envoi sera direct, après résolution de l'adresse physique du destinataire.

➔ Si les valeurs diffèrent, l'adresse de destination est distante. Le datagramme sera envoyé au routeur local, aussi identifié comme passerelle par défaut.

Rappelons que le masque de sous-réseau n'est pas indiqué dans un en-tête IP.

Exemple

Exemple



TOPOLOGIE

Le réseau est constitué de deux réseaux IP, 192.168.1.0 et 172.16.0.0.
Un routeur permet de les interconnecter. Ce routeur possède une interface dans chacun de ces deux réseaux.

Trois machines sont présentes sur le réseau :

- A avec l'adressage 192.168.1.100 255.255.255.0, sur le réseau 192.168.1.0
- B avec l'adressage 192.168.1.110 255.255.255.0, sur le réseau 192.168.1.0
- C avec l'adressage 172.16.0.50 255.255.0.0, sur le réseau 172.16.0.0

COMMUNICATION ENTRE A & B

Supposons que A veuille entrer en communication avec B. Les étapes suivantes ont lieu :

- A applique son masque de sous-réseau à l'adresse de B, la destination, soit 192.168.1.110. Le résultat est 192.168.1.0.
- L'adresse réseau de A et le résultat obtenu correspondent. L'adresse de B est donc locale avec celle de A.
- A émet une résolution ARP afin d'obtenir l'adresse physique de B.
- A émet ses datagrammes à destination directe de B. Ces datagrammes ont les caractéristiques suivantes :
  - ➔ L'adresse physique source et l'adresse IP source sont celles de A
  - ➔ L'adresse physique destination et l'adresse IP destination sont celles de B
- B répond en procédant exactement de la même façon.

COMMUNICATION ENTRE A & C

Supposons que A veuille maintenant entrer en communication avec C. Les étapes suivantes ont lieu :

- A applique son masque de sous-réseau à l'adresse de C, la destination, soit 172.16.0.50. Le résultat est 172.16.0.0.
- L'adresse réseau de A et le résultat obtenu ne correspondent pas. L'adresse de C est donc sur un réseau distinct de celui de A.
- A émet une résolution ARP afin d'obtenir l'adresse physique du routeur.
- A émet ses datagrammes à destination de C. Ces datagrammes ont les caractéristiques suivantes :
  - ➔ L'adresse physique source et l'adresse IP source sont celles de A
  - ➔ L'adresse physique destination est celle du routeur et l'adresse IP destination est celle de C
- C répond en procédant exactement de la même façon.

Formats d'adressage

Formats d'adressage

- Sans sous-réseaux
  - On utilise une adresse IP de classe par réseau physique
  - On utilise le masque de sous-réseau par défaut de la classe d'adresse
- Avec sous-réseaux
  - On segmente l'adresse IP de classe en sous-réseaux plus petits en utilisant une partie des bits d'hosts inutilisés
  - On utilise un masque de sous-réseau plus grand que celui par défaut de la classe d'adresse
  - On utilise une adresse de sous-réseau par réseau physique

Deux formats d'adressage sont possibles en IP :

SANS SOUS-RÉSEAUX

Dans ce cas, on utilise les adresses de classe telle quelles. Le masque de sous-réseau utilisé est alors celui de la classe d'adresse, ou masque par défaut :

- Pour la classe A, il est égal à 255.0.0.0
- Pour la classe B, 255.255.0.0
- Pour la classe C, 255.255.255.0

Ce format n'est plus utilisé que dans le cas d'adresses de classe C, pour les classes A et B, on segmente en sous-réseaux.

AVEC SOUS-RÉSEAUX

Comment faire lorsque, par exemple, on dispose de 400 VLANs ou réseaux physiques ? Chaque VLAN ou réseau physique doit avoir une adresse IP assignée. Or, il n'existe que 273 adresses de réseaux privées. Les adresses publiques, elles, sont saturées depuis 1995.

La solution est l'utilisation des sous-réseaux. Autrement dit, on a la possibilité de découper une adresse majeure, l'adresse de classe, en sous-réseaux plus petits. On pourra alors assigner ces adresses de sous-réseaux aux VLANs et aux réseaux physiques.

Pour procéder, on va utiliser un masque de sous-réseau plus grand que le masque par défaut de la classe d'adresse.

On utilise une partie des bits d'hôte, en commençant par les plus à gauche (les bits de poids fort). On prend autant de bits que nécessaire. Ces bits serviront à identifier chacun des sous-réseaux.

Principes des sous-réseaux

Principes des sous-réseaux

- Une partie des bits de l'adresse hôte est utilisée pour coder les sous-réseaux
- Plus on prend de bits pour les sous-réseaux, plus ils seront nombreux et petits
- Pour une même adresse IP majeure, il faut trouver le compromis entre le nombre de sous-réseaux et le nombre d'hôtes par sous-réseau
- Une adresse réseau a deux composants :
  - Un ID de réseau défini par la classe d'adresse
  - Un ID de sous-réseau défini par le masque de sous-réseau

PRINCIPES

Le principe d'adressage des sous-réseaux est d'utiliser une partie des bits de l'adresse hôte pour coder les sous-réseaux. Plus on prend de bits, plus on aura de sous-réseaux. En revanche, les sous-réseaux seront d'autant plus petits. Il faudra donc faire un choix entre le nombre de sous réseaux et leur taille.

L'adresse réseau sera alors composée de :

- L'adresse majeure, ou ID de réseau, sur 1, 2 ou 3 octets selon la classe d'adresse ;
- L'adresse de sous-réseau, ou ID de sous-réseau.

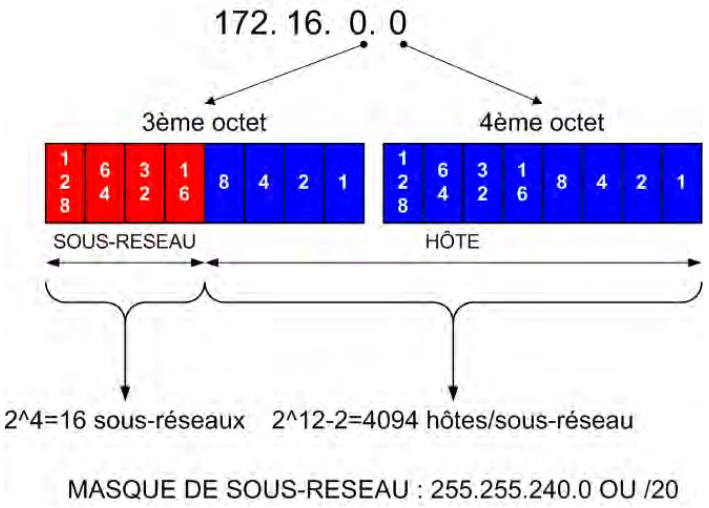
Le nombre de sous-réseaux disponibles sera égal à 2^n où n est le nombre de bits utilisé pour leur codage.

Le nombre d'hôtes par sous-réseau sera égal à 2^m-2.Où m+n=24 pour la classe A, m+n=16 pour la classe B et m+n=8 pour la classe C.

Enfin, le masque de sous-réseau coïncidera avec la plus grande adresse de sous-réseau.

Exemple 1

Exemple 1



POINT DE DEPART

Dans notre exemple, supposons que nous disposions de l'adresse de classe B 172.16.0.0/16. Les 3ème et 4ème octets sont utilisés pour l'adressage des hôtes, ce qui permet d'avoir un seul réseau pouvant contenir 65534 adresses (2^16-2). Supposons encore que nous ayons besoin de découper ce réseau en 12 sous-réseaux.

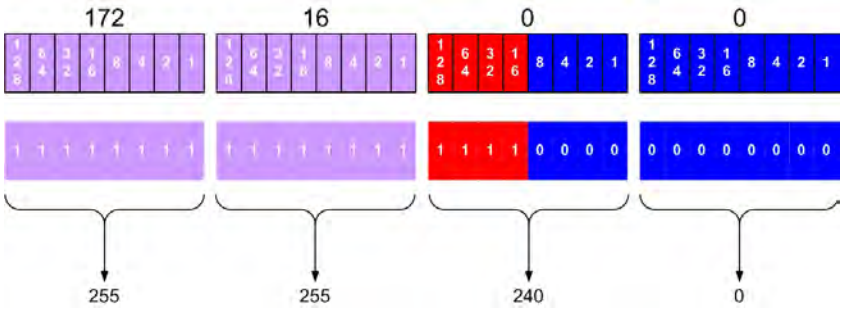
CALCULS

Combiens de bits permettent de coder 12 valeurs ? Réponse 4 bits. Nous disposerons donc de 2^4=16 sous-réseaux, ce qui nous donnera une marge de 4 sous-réseaux.

Il restera 12 bits disponibles pour les adresses hôtes. Nous aurons donc la possibilité d'avoir 2^12-2=4094 hôtes pour chaque sous-réseau.

Exemple 1 : calcul du masque de sous-réseau

Exemple 1 : calcul du masque de sous-réseau



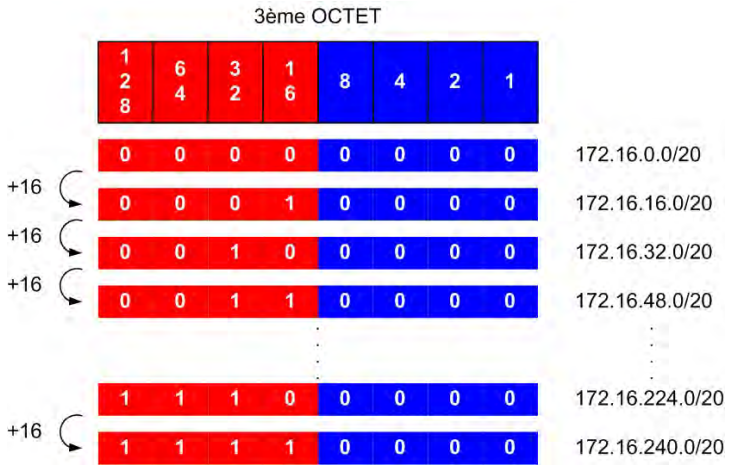
Le masque de sous réseau est simple à calculer, en mettant à 1 tous les bits utilisés pour le codage de l'adresse réseau :

- Les deux premiers octets correspondent à la classe d'adresse ;
- Les 4 premiers bits du troisième octet sont utilisés pour coder les sous-réseaux.

Au final nous obtenons 255.255.240.0 ou, en notation CIDR /20. La notation CIDR est très simple, on écrit l'adresse IP suivie d'un « / » et du nombre de bits utilisés au total pour coder l'adresse réseau. Ici nous avons 8+8+4=20 octets.

Exemple 1 : calcul des sous-réseaux

Exemple 1 : calcul des sous-réseaux



Le calcul des sous-réseaux est effectué de la manière suivante :

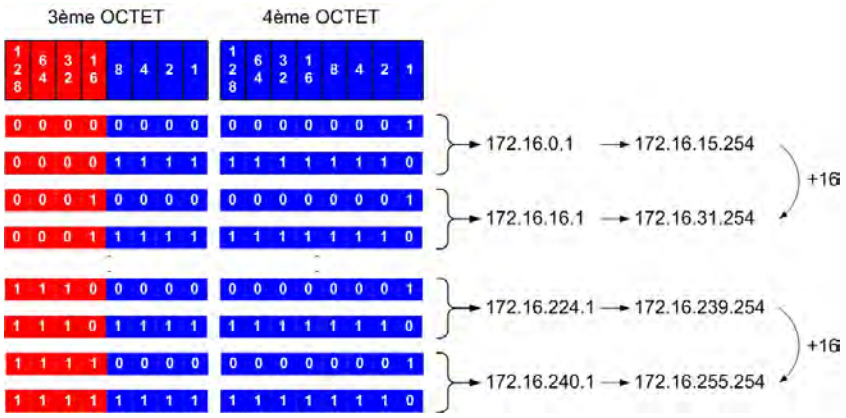
- On fait varier les quatre bits utilisés pour le codage des sous-réseaux ;
- Le premier sous-réseau est toujours 0 ;
- Le dernier sous-réseau est toujours égal au masque de sous-réseau ;
- Les sous-réseaux s'incrémentent de la valeur du bit de poids faible. On appelle « PAS » cet incrément. Dans notre exemple, les sous-réseaux s'incrémentent de 16 en 16.

En additionnant le dernier octet du masque de sous-réseau et le pas, on obtient toujours 256. Ici, nous avons 240 pour le masque de sous-réseau et 16 pour le pas. Connaitre l'un permet de déduire l'autre.

Le premier sous-réseau (tous les bits à 0) est un sous-réseau comme les autres, tout comme le dernier sous-réseau (tous les bits à 1). On peut choisir ou non de les utiliser. Malheureusement, un grand éditeur américain de logiciels a choisit de ne pas les utiliser. C'est son choix, mais il est souvent prit, à tort, comme référence. Le but était d'éviter toute confusion entre le réseau majeur et le premier sous-réseau. Par exemple entre 172.16.0.0 et 172.16.0.0/20. Or, il n'y a pas d'ambiguïté : une adresse réseau sans masque signifie « le réseau majeur », avec un masque supérieur à son masque de classe il indique clairement un sous-réseau.

Exemple 1 : calcul des étendues

Calcul des étendues

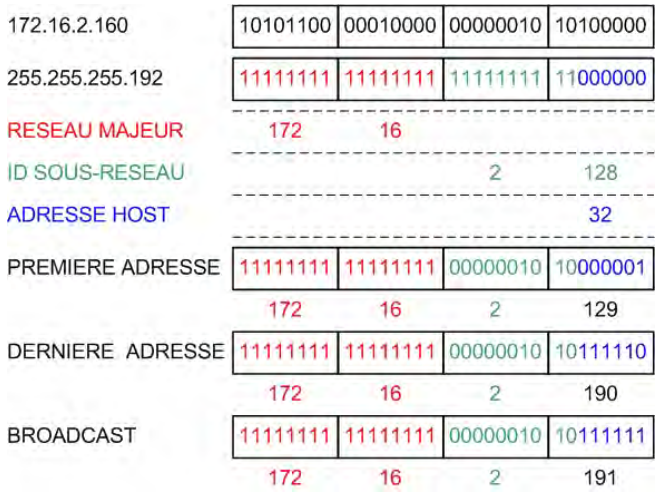


Le calcul des étendues consiste à déterminer les plages d'adresses disponibles pour chaque sous-réseau. On fait varier, pour un sous-réseau donné, l'ensemble des bits utilisés pour le codage de l'adresse hôte :

- La plus petite adresse est toujours 1 ;
- La plus grande adresse est toujours égale à l'adresse du sous-réseau suivant -2, car il faut ôter l'adresse de diffusion du sous-réseau dont les bits d'adresse hôte sont tous à un ;
- On retrouve bien évidemment l'incrément du pas entre les étendues ;
- Pour les classes A et B, les plus souvent segmentées, la dernière adresse d'une étendue se termine toujours par 254.

Exemple 2

Exemple 2



Prenons cette fois ci le problème à l'envers. Partons d'une adresse existante, 172.16.2.160 255.255.255.192 et calculons :

- L'adresse réseau
- L'adresse hôte
- La plage des sous-réseaux
- Les étendues d'adresses

CALCUL DES ADRESSES

En appliquant le masque de sous-réseau 255.255.255.192 à l'adresse 172.16.2.160, on obtient l'adresse réseau 172.16.2.128. Cette adresse est constituée de deux parties :

- L'adresse de réseau majeur, qui dépend de la classe d'adresse, 172.16.0.0
- L'adresse de sous-réseau 2.128 ou 0.0.2.128
- L'adresse hôte est le complément entre l'adresse complète et l'adresse réseau : 32 ou 0.0.0.32.

PLAGE DE SOUS-RESEAUX

Le masque 255.255.255.192 ou /26 est appliqué à une adresse de classe B.

Par conséquent, les deux premiers octets sont réservés à l'adresse majeure, ou adresse de classe, 172.16.0.0.

Les bits restants sont donc utilisés pour coder les sous-réseaux. Il y en a 10. Il reste 6 bits pour l'adressage des hôtes.

Il est possible de coder 1024 sous-réseaux dans le réseau majeur 172.16.0.0 avec le masque 255.255.192.0.

Le bit de poids faible est 64, le pas aura donc la même valeur :

- Le premier sous-réseau sera 172.16.0.0/26, le second sera 172.16.0.64/26, le troisième 172.16.0.128…
- Les deux derniers sous-réseaux seront 172.16.255.128/26 et 172.16.255.192/26.

PLAGES D'ADRESSES

Pour chaque sous-réseau, il est possible de coder 2^6-2=62 hôtes.

Pour les deux premiers sous-réseaux :

172.16.0.0/26 172.16.0.1 – 172.16.0.62

172.16.0.64/26 172.16.0.65 – 172.16.0.126

Pour les deux derniers :

172.16.255.128/26 172.16.255.129 – 172.16.255.190

172.16.255.192/26 172.16.255.193 – 172.16.255.254

Pour notre sous-réseau, 172.16.2.128 en particulier :

172.16.2.129 – 172.16.2.190

L'adresse de broadcast de sous-réseau est donc : 172.16.2.191 (tous les bits de l'adresse hôte à 1).

Adresses de diffusion (broadcast)

Adresses de diffusion (broadcast)

- Flooding ou locale : 255.255.255.255; n'est pas transmis par les routeurs. Signifie : toute machine IP
- Directed ou de sous-réseau. Toutes les machines appartenant à ce sous-réseau. N'est pas transmis par les routeurs.
  - Exemple : 172.16.3.255
- All subnets ou de classe. Tous les sous-réseaux de cette adresse de classe. Peut être transmis par les routeurs.
  - Exemple : 172.16.255.255

Il existe trois types d'adresses de diffusion en IP :

Flooding ou locale : 255.255.255.255

Signifie : toute machine IP du réseau

Ce datagramme n'est pas transmis par les routeurs

Directed ou de sous-réseau :

Signifie : toutes les machines de ce sous-réseau

Ce datagramme n'est pas transmis par les routeurs

Exemple 172.16.3.255/24

All subnets ou de classe :

Signifie : toute machine dans un des sous-réseaux de cette adresse majeure

Ce datagramme peut, optionnellement, être transmis par les routeurs

Exemple 172.16.255.255/16

Masques de sur-réseau ou supernet

Masques de sur-réseau ou supernet

- Utilisé pour simplifier les tables de routages
- Le but est de résumer plusieurs adresses de réseaux
- Ne fonctionne qu'avec les protocoles de routage classless
- Le principe est de prendre les bits en commun d'une plage d'adresses
- On ne peut résumer les réseaux que par puissances de deux : 2, 4, 8, 16…

On parle de sur-réseau quand le masque de sous-réseau est plus petit que le masque de classe, ou plus petit que le masque de sous-réseau utilisé dans l'adressage de cette adresse.

On utilise les masques de sur-réseau uniquement dans les routeurs dans les tables de routage, ce n'est pas un masque d'adressage. Ils permettent de simplifier la table de routage, de la rendre plus concise, plus lisible, plus facile à diagnostiquer et surtout plus efficace pour le routeur.

Le but est de résumer plusieurs adresses de réseaux en une seule, quand c'est possible.

Cette technique n'est pérenne qu'avec des protocoles de routage CLASSLESS, qui annoncent les masques de sous-réseau.

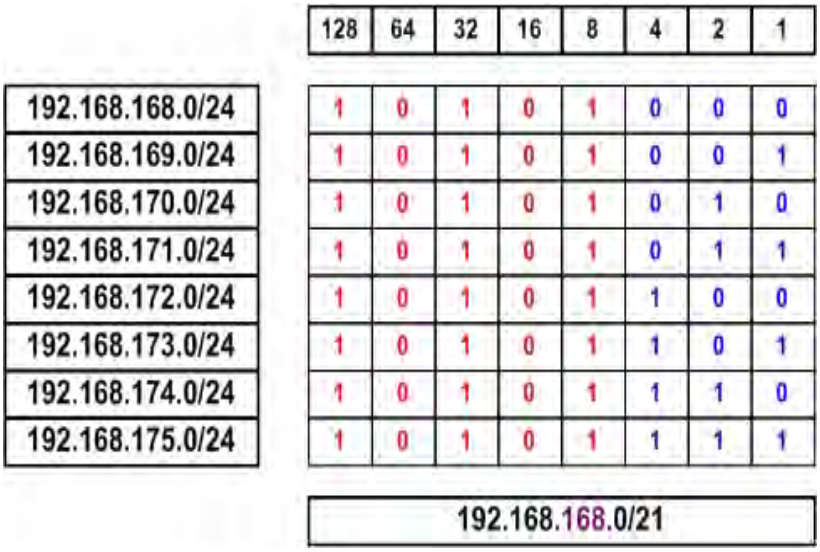
Le principe est le suivant :

- On prend tout les bits en commun aux adresses que l'on veut résumer pour calculer l'adresse résumée résultante ;
- Le masque de sous-réseau correspondra aux nombres de bits en commun.

On ne peut résumer les réseaux que par puissances de deux : 2, 4, 8, 16… De plus, ils doivent être contigus.

Exemple

Exemple



	128	64	32	16	8	4	2	1
192.168.168.0/24	1	0	1	0	1	0	0	0
192.168.169.0/24	1	0	1	0	1	0	0	1
192.168.170.0/24	1	0	1	0	1	0	1	0
192.168.171.0/24	1	0	1	0	1	0	1	1
192.168.172.0/24	1	0	1	0	1	1	0	0
192.168.173.0/24	1	0	1	0	1	1	0	1
192.168.174.0/24	1	0	1	0	1	1	1	0
192.168.175.0/24	1	0	1	0	1	1	1	1
	192.168.168.0/21							

Supposons que nous ayons les réseaux de classe C 192.168.168.0/24 à 192.168.175.0/24. Il est évident que les deux premiers octets sont communs aux huit réseaux.

Si nous représentons sous forme binaire le troisième octet, nous nous apercevons que les cinq premières colonnes sont communes, soit les colonnes binaires 128 à 8. Le masque du sur-réseau sera donc de /21 (8+8+5) ou 255.255.255.248 en notation décimale.

La lecture des cinq colonnes communes fournit la valeur du sur-réseau : 192.168.168.0 /21

Il nous reste à vérifier que ce résumé de routes ne fonctionne qu'avec la plage 192.168.168.0/24 à 192.168.175.0/24 :

Si nous appliquons le masque /21 à cette plage, nous obtenons toujours 192.168.168.0/21, ce qui est fort logique.

Si nous appliquons le masque /21 à 192.168.167.0, nous obtenons 192.168.160.0. Donc ce résumé ne fonctionne pas pour ce réseau.

Si nous appliquons le masque /21 à 192.168.176.0, nous obtenons 192.168.176.0. Donc ce résumé ne fonctionne pas pour ce réseau.

VLSM

- Variable-Lenght Subnet Masking
- Par défaut, on utilise le même masque de sous-réseau pour un adresse majeure donnée (FLSM, Fixe)
- Le masque de sous-réseau peut-être variable pour s'adapter à des sous-réseaux de tailles différentes
- Le principe est la généralisation de la segmentation :
  - Un « redécoupe » un des sous-réseau en réseaux plus petits
  - Le découpage se fera selon les besoins : VLAN, WAN, point-à-point…
- Les protocoles de routage utilisés sur le réseau devront être classless

Les réseaux constituant un réseau d'entreprise sont rarement tous de la même taille. Pourtant, par défaut, on utilise en IP un masque de sous-réseau unique, fixe, pour un réseau majeur donné.

Le principe de VLSM (Variable-Lenght Subnet Masking) est d'adapter la longueur du masque de sous-réseau à la taille des réseaux physiques ou des VLANs.
Pour une liaison point-à-point, par exemple, il suffit de disposer de deux adresses IP. Or, si le réseau majeur utilise le masque de sous-réseau /26, on disposera de 62 adresses, dont 60 ne serviront jamais.

Techniquement, le principe est le suivant :

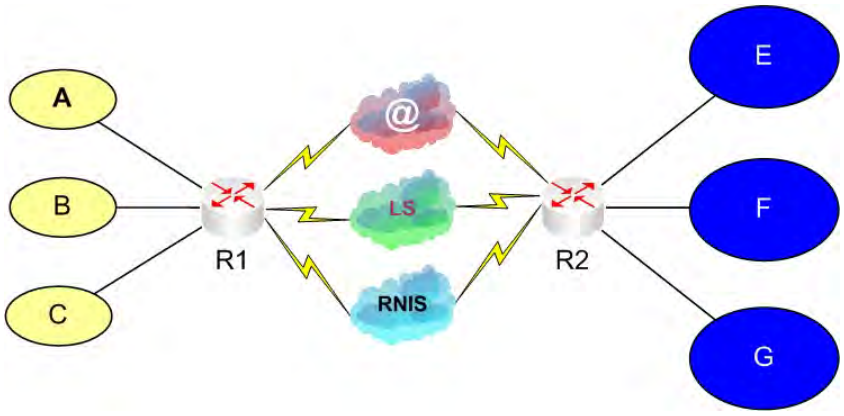
- On référence les différents besoins en taille de réseaux et les contraintes d'adressage.
- On procède à une première segmentation, le découpage du réseau majeur en sous-réseaux.
- Ensuite, on choisit un de ces sous-réseaux, que l'on ne va pas utiliser tel quel, mais découper à son tour en réseaux plus petits.

On pourra continuer ainsi selon la granularité désirée et le nombre de bits disponibles au total.

Les protocoles de routage utilisés dans un réseau VLSM devront impérativement être de type classless. Ce qui est le cas de tous les protocoles actuels : RIPv2, OSPF, EIGRP, BGP, ISIS.

Exemple : topologie et problématique

Exemple : topologie et problématique



TOPOLOGIE

Prenons la topologie réseau suivante :

- Deux sites distincts comportant chacun trois réseaux
- 3 réseaux de taille moyenne, E, F et G, qui recevront au maximum 60 machines
- 3 réseaux de petite taille, A, B et C, dont le nombre de machines ne dépassera pas 10
- 2 routeurs R1 et R2 permettant l'interconnexion des deux sites. Ces routeurs disposent chacun de trois liaisons WAN :
  - ➔ Une liaison spécialisée (LS) entre R1 et R2, point-à-point
  - ➔ Une liaison RNIS utilisée en cas de défaillance de la LS
  - ➔ Un accès Internet

PROBLEMATIQUE

Pour adresser cette topologie, nous avons besoin de :

- 10 adresses réseau :
- 3 réseaux en /26
- 3 réseaux en /28
- 4 réseaux en /30
- 216 adresses d'hôte :
  - ➔ 60 pour E, F et G, nécessitant 6 bits pour l'adresse hôte
  - ➔ 10 pour A, B et C, nécessitant 4 bites pour l'adresse hôte
  - ➔ 6 pour les routeurs, nécessitant 2 bits pour l'adresse hôte

Supposons que nous disposions uniquement de l'adresse 192.168.1.0/24.
Nous ne pouvons, avec un masque de sous-réseau fixe, répondre à nos besoins. Soit nous n'aurons pas assez de réseaux, soit ils seront trop petits pour certains usages :

- Si nous utilisons /26, nous aurons 4 sous-réseaux uniquement, mais de bonne taille pour tous les usages (62 hôtes) ;
- Si nous utilisons /28, nous aurons 16 sous-réseaux, mais de taille insuffisante pour E, F et G, car on ne pourrait coder que 16 adresses hôtes ;
- Si nous utilisons /30, nous aurons 64 sous-réseaux, mais de taille insuffisante pour A, B, C, D, E, F et G, car on ne pourrait coder que 2 adresses hôtes.

Exemple : topologie et problématique

Exemple : solution

SOLUTION

La solution consiste à découper le réseau de la manière suivante :

- Un premier découpage de sous-réseau en /26, ce qui nous permettra de disposer de 4 sous-réseaux principaux. Il reste 6 bits pour la partie hôte. Il sera possible, en conséquence, d'adresser 62 machines dans chaque sous-réseau. Ce qui convient parfaitement aux réseaux moyens E, F et G.
  Nous avons 4 sous-réseaux :
  - ➔ 192.168.1.0/26, que nous attribuerons arbitrairement à E
  - ➔ 192.168.1.64/26, que nous attribuerons arbitrairement à F
  - ➔ 192.168.1.128/26, 26 que nous attribuerons arbitrairement à G
  - ➔ 192.168.1.192 que nous n'attribuerons pas tel quel
- Le dernier sous-réseau, 192.168.1.192, ne sera pas utilisé tel quel en /26, mais segmenté en réseaux plus petits. On appelle ces réseaux VLSM1, plutôt que sous-sous-réseaux. Comme nous avons besoin de 3 réseaux de petite taille, nous allons « découper » 192.168.1.192 en /28.
  Nous avons 4 réseaux VLSM1 :
  - ➔ 192.168.1.192/28 que nous attribuerons à A
  - ➔ 192.168.1.208/28 que nous attribuerons à B
  - ➔ 192.168.1.224/28 que nous attribuerons à C
  - ➔ 192.168.1.240 que nous n'attribuerons pas tel quel.

Dans chacun de ces réseaux, il est possible d'adresser 14 machines.

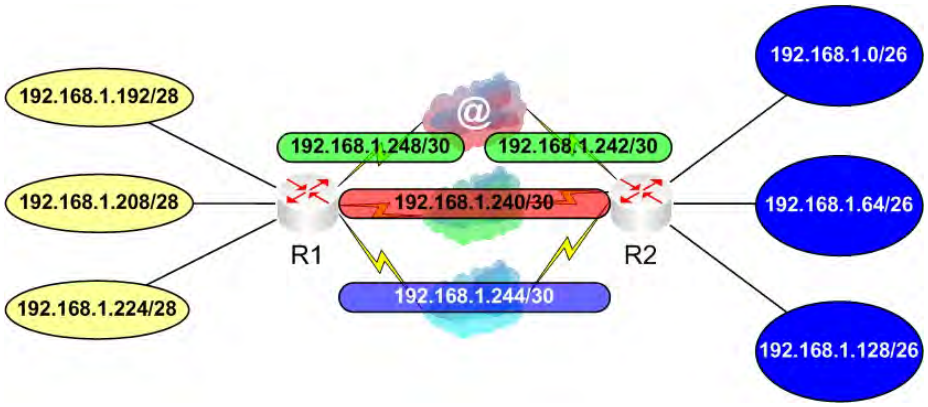
Le dernier réseau VLSM1, 192.168.1.240 sera à son tour segmenté en réseaux plus petits, en /30. Les réseaux en /30 sont communément nommées WAN, car ils ne disposent que de deux adresses hôte.

Nous avons 4 réseaux WAN :

- ➔ 192.168.1.240/30, que nous attribuerons à la LS
- ➔ 192.168.1.244/30, que nous attribuerons à la ligne RNIS
- ➔ 192.168.1.248/30, que nous attribuerons à l'accès Internet de R1
- ➔ 192.168.1.252/30, que nous attribuerons à l'accès Internet de R2

Exemple : Solution

Exemple : solution



- *La couche Transport*
- *UDP*
- *TCP*
- *Adressage de niveau 4*

6

La couche Transport

Objectifs

Ce module traite de la couche transport de TCP/IP.

Connaissance

- Présentation des protocoles de la couche transport
- Adressage de niveau 4
- UDP
- TCP

Progression

La couche Transport	UDP
Adressage de niveau 4	TCP

La couche Transport

Présentation

- La couche transport permet de définir le mode d'échange de données entre des applications
- Il existe deux modes principaux en TCP/IP : connecté et non-connecté
- Il existe deux protocoles principaux en TCP/IP : UDP et TCP

La couche transport dans le modèle OSI définit le mode d'échange entre des applications.
Dans le modèle ARPA, celui de TCP/IP, la couche Transport est aussi appelée parfois Host-to-Host.

Elle définit les mêmes rôles que celle du modèle OSI :

- Adressage de niveau 4 permettant de différencier les applications.
- Définition des modes d'échange entre les machines : connecté ou non-connecté.
- Prise en charge du séquencement et de la retransmission des données.
- Gestion du contrôle de flux.
- Vérification de l'intégrité des données et des en-têtes.

Une application s'appuyant sur TCP/IP peut utiliser l'un ou l'autre des deux modes. Certaines applications, minoritaires, peuvent même utiliser les deux modes.

TCP/IP utilise deux modes principaux : le mode fiable, TCP, et le mode non fiable UDP.

Adressage de niveau 4

Adressage de niveau 4

- Les numéros de ports UDP et TCP permettent la différenciation des applications
- Il existe 65536 ports pour chacun des deux protocoles de niveau 4, TCP et UDP
- L'association entre une adresse IP, un protocole de niveau 4 et un numéro de port se nomme un ou une socket

L'adressage de niveau 4 en TCP/IP se fait via les numéros de ports, qui permettent par leur unicité de différencier les applications.

L'adresse IP identifie la machine sur le réseau, le port identifie l'application sur la machine.
Chaque application utilise un ou plusieurs ports de communication avec le protocole de transport qu'elle utilise.

Chacun des deux protocoles UDP et TCP dispose de 65536 ports.

Un socket est l'association entre une adresse IP, un protocole de niveau 4 et un numéro de port. Ce paramètre identifie de façon unique le point d'accès de l'application sur le réseau IP. Par exemple, une connexion en TCP sur le port 80 sur l'adresse 192.168.1.100 permet d'accéder à un serveur web.

Le fichier SERVICES

Le fichier SERVICES contient la définition de l'association entre les protocoles, les ports et les applications. Ce fichier est présent sur toute machine IP.

Dans Windows, ce fichier est dans le répertoire :
\WINDOWS\SYSTEM32\DRIVERS\ETC
Dans Linux, il est dans le répertoire /ETC.

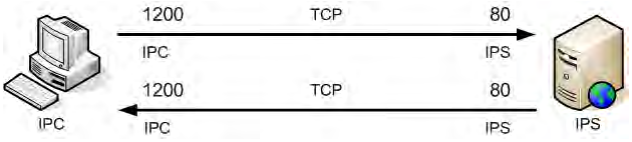
Exemples

TCP :	***UDP***
21 : FTP	53 : DNS
23 : Telnet	69 : TFTP
25 : SMTP	161 : SNMP
53 : DNS	520 : RIP
80 : http	

Ports

Numéros de port

- Plages réservées :
  - 0-1023 serveurs
  - 1024-65535 clients
- Port source indifférent, port client identique à la destination ou dynamique, plus rarement fixe
- Port destination spécifique à l'application, au serveur



Plages réservées

Les plages réservées sont réparties de la façon suivante :

- Les ports 0 à 1023, les Well Known Ports, sont réservés aux serveurs. Normalement, les ports 0 à 511 sont réservés pour les applications standards, et les ports 512 à 1023 pour les applications propriétaires.
  Ce sous-découpage n'est factuellement pas respecté. Par exemple, RIP utilise le port 520 en UDP et SunRPC utilise les ports 111 en TCP et UDP. Ou encore le client BOOTP/DHCP utilise le port 68.
- Les ports 1024 à 49151 sont dits enregistrés, Registred Ports. Souvent on les utilise comme ports clients.
- Enfin, les ports 49152 à 65535 sont dits dynamiques ou privés (Dynamic/Private Ports). Ils sont souvent utilisés pour des applications particulières ou des ports serveurs dynamiques.

Bref, la seule chose dont on soit sûr, c'est qu'entre 0 et 1023, on n'utilise pas de clients propriétaires.

Ports clients

Seul le port serveur doit être clairement connu et identifié.
En effet, c'est le client qui contacte le serveur. Or, dans chaque en-tête de niveau 4 sont renseignés les ports source et destination. Le serveur peut donc facilement répondre au client.

Ports fixes ou ports dynamiques ?

Pourquoi certains ports clients sont-ils fixes et d'autres dynamiques ? La réponse est liée au fonctionnement de l'application elle-même.

Par exemple, quand vous surfez sur Internet, vous pouvez parfaitement être connecté simultanément à plusieurs pages différentes d'un même site web sur un même serveur. Comment différentier les connexions utilisées entre le client et le serveur ? Les adresses sources et destinations sont les mêmes. La solution est simple : en utilisant un port client différent pour chaque page à laquelle vous êtes connecté. Ainsi il y aura unicité d'identification des connexions par le doublet port source / port destination.

Autre exemple, quand une machine cliente DHCP envoie une demande de bail, elle émet une demande en broadcast, une seule. Inutile d'en émettre plusieurs, puisque tous les serveurs DHCP concernés recevront la requête. Le port client DHCP est donc fixe. De façon générale, lorsqu'il n'y aucune nécessité ou aucune possibilité pour qu'il y ait de multiples connexions de la même application entre un client et un serveur, on utilise un port fixe. Si, a contrario, c'est le cas, on utilise plutôt des ports clients dynamiques. Bien évidement, il existe toujours des exceptions.

UDP

UDP

- User Datagramm Protocol (UDP)
  - Orienté sans connexion
  - Ni séquencement, ni ACK, ni contrôle de flux
- Usage :
  - Débit important
  - Fiabilité moindre
  - Séquencement, contrôle de flux et acquittement assurés éventuellement par l'application

UDP

UDP, User Datagramm Protocol, est le protocole de transport en mode non connecté de TCP/IP. Voici ses principales caractéristiques :

- Fonctionnement sans connexion (connectionless) : les données sont envoyées sans aucun contrôle préalable :
  - ➔ Pas de vérification de la validité de la destination : est-ce que le port destinataire est actif ?
  - ➔ Pas de négociations initiales sur le débit entre l'émetteur et le récepteur.
  - ➔ Pas de vérification de la fiabilité des échanges.
- Pas de séquencement des datagrammes UDP. Les données doivent arriver dans l'ordre, ou c'est l'application qui doit implémenter ce mécanisme.
- Pas d'accusé de réception. L'émetteur ne sait pas si ses données ont été bien acheminées ou pas. En cas de perte, c'est l'application qui est chargée de le détecter et de retransmettre les données manquantes via UDP.
- Pas de contrôle de flux. UDP utilise systématiquement toute la bande passante disponible ou allouée par le routeur. Autrement dit, quand l'émetteur et le récepteur ont des différences de capacités réseaux importantes, UDP n'en tient pas compte. Une fois de plus, c'est l'application qui devra s'en charger.

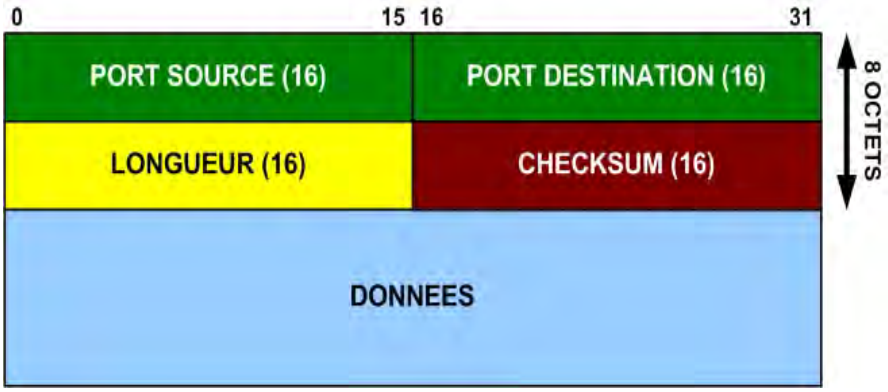
Usage

UDP est adapté pour :

- Les applications privilégiant les débits importants. UDP est beaucoup plus performant en transfert de données sur les réseaux fiables que TCP, car il y a moins de contrôle, donc moins de temps de traitement et moins de overhead (surcharge supplémentaire apportée par les en-têtes protocolaires).
- Les applications nécessitant ou acceptant une fiabilité moindre, un taux de perte qui n'est pas nul.
  Par exemple les applications de voix sur IP utilisent UDP car TCP n'accepte pas un taux de pertes différent de 0. UDP lui, ne gère même pas le taux de pertes. De plus, UDP assure un acheminement beaucoup plus continu que TCP, ce qui favorise le caractère isochrone du transport de la voix.
- Les applications qui intègrent déjà les mécanismes de séquencement, d'accusé de réception et de contrôle de flux et qui seraient en redondance ou en concurrence avec TCP.

Format d'un datagramme UDP

Format d'un datagramme UDP



Le format d'en-tête d'UDP est des plus simples, il a une longueur fixe de 8 octets. Voici le détail de chaque champ :

- Ports source & destination : chaque champ est codé sur 16 bits, d'où les 65536 ports possibles.
- Longueur : longueur totale en octets du datagramme UDP, qui, en théorie, peut atteindre 65535 octets.
  En Ethernet, par exemple, avec une MTU de 1500, le datagramme de IP fera au maximum 1480 octets et celui de UDP 1472.
- Checksum : optionnel. Calculé sur l'ensemble du datagramme, par somme des compléments à 1 de mots de 16 bits.
- Données : données applicatives. Noter que si l'application ne tient pas compte de la taille maximale du datagramme UDP, c'est IP qui devra fragmenter les données. En effet, UDP ne sait pas segmenter les données, il retransmettra donc les données en bloc, en y ajoutant son propre en-tête. TCP, lui, est capable de segmenter les données.

TCP

TCP

- Transport Control Protocol (TCP)
  - Orienté connexion
  - Séquencement des segments
  - Accusé de réception
  - Contrôle de flux
- Usage :
  - Fiabilité
  - Débit moindre
  - Séquencement, contrôle de flux et acquittement assurés

TCP

TCP, Transport Control Protocol, est le protocole de transport en mode connecté de TCP/IP. C'est le plus utilisé par les applications standard Internet. Pour deux raisons essentielles : la fiabilité et le contrôle de flux.
Voici ses principales caractéristiques :

- Fonctionnement en mode connexion : les données ne sont envoyées qu'après des contrôles préalables :
  - ➔ Vérification de la validité de la destination : est-ce que le port destinataire est actif ?
  - ➔ Négociations initiales sur le débit entre l'émetteur et le récepteur.
  - ➔ Vérification de la fiabilité des échanges.
- Séquencement des segments TCP. Les données peuvent arriver dans le désordre, TCP les réordonnera.
- Mécanisme d'accusé de réception. L'émetteur sait si ses données ont été bien reçues ou non. En cas de perte, TCP retransmettra les données manquantes.
- Contrôle de flux. Dans chaque segment TCP expédié, l'émetteur indique la taille de sa fenêtre en réception. Ce mécanisme permet d'adapter le débit dans les deux sens de la transmission. Un échange de données peut être asymétrique, ce qui permet de mettre en relation une machine ayant des capacités réseau faibles (un PAD, un téléphone…) avec des machines beaucoup plus puissantes (Serveur, Mainframe, AS/400…).

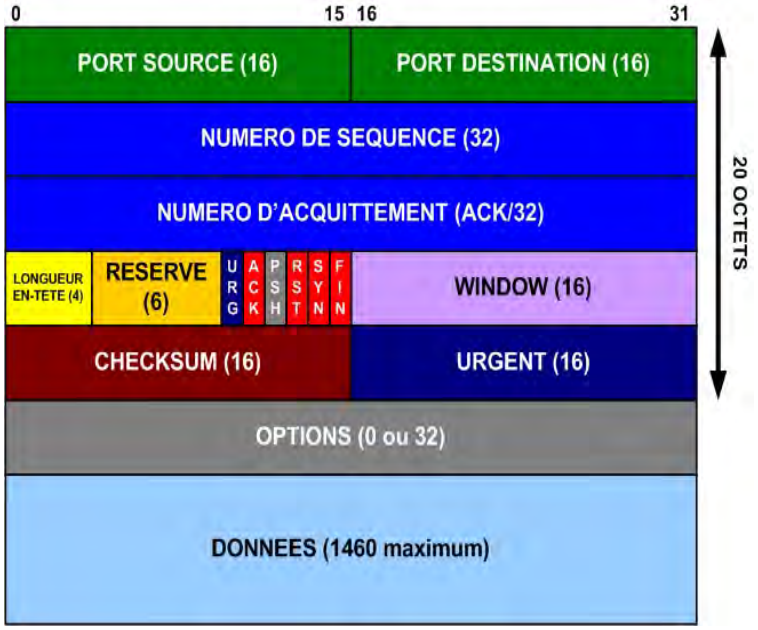
Usage

TCP est adapté pour :

- Les applications n'implémentant pas de mécanismes de contrôle. Il est plus simple d'écrire des applications utilisant les mécanismes de séquencement, d'accusé de réception et de contrôle de flux de TCP, que d'en développer des spécifiques.
- Les applications nécessitant une fiabilité absolue, un taux de perte nul.

Format de segment TCP

Format d'un segment TCP

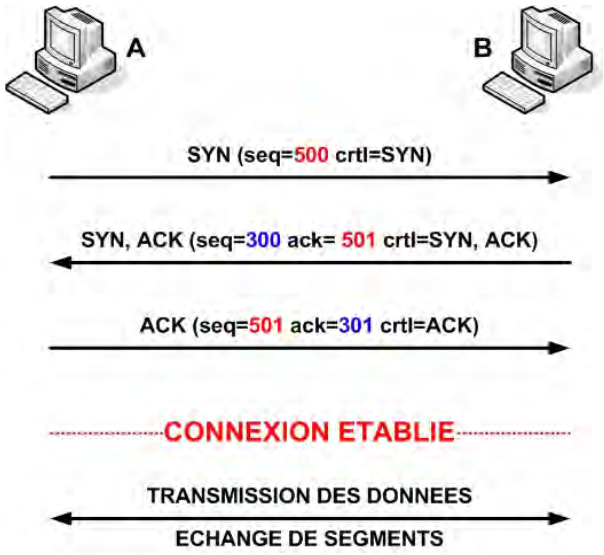


- Le format d'en-tête d'un segment TCP est constitué d'une partie fixe sur 20 octets et d'une partie optionnelle sur 32 octets.
- PORT SOURCE et PORT DESTINATION sur 16 bits.
- NUMERO DE SEQUENCE : permet, en cas de fragmentation des données, de numéroter les segments à l'émission et de les réassembler dans le bon ordre à la réception. Le numéro de séquence initial est déterminé à l'établissement de chaque nouvelle connexion TCP.
- NUMERO D'ACQUITTEMENT : permet d'accuser réception des segments reçus. C'est après avoir reçu cet acquittement que la machine émettrice expédiera les segments suivants.
- LONGUEUR D'EN-TETE : en « mots » de 32 bits.
- RESERVE : réservé pour un usage futur.
- WINDOW : annonce la taille de la fenêtre en réception de la machine émettrice du segment. Plus cette valeur est grande, plus la capacité de la machine est grande. La valeur de ce champ sera également utilisée pour les mécanismes d'acquittement.
- CHECKSUM : obligatoire. Calculé avec la même technique que celui d'UDP.
- URGENT : contient les données relatives à la priorité. Ce champ est utilisé si le champ de contrôle URG est positionné à 1.
- CHAMPS DITS DE CONTROLE :
  - ➔ URG : Pointeur urgent, indique la présence de données urgentes, utilisé avec le champ URGENT.
  - ➔ ACK : Numéro d'acquittement valide.

- ➔ PSH : Push, demande au récepteur de transmettre cette donnée le plus rapidement possible à l'application, sans mise en cache.
- ➔ RST : Reset, réinitialise une connexion. Souvent utilisé par la machine contactée pour réinitialiser la connexion établie par la machine contactante.
- ➔ SYN : Synchronisation des numéros de séquence lors de l'initialisation d'une connexion.
- ➔ FIN : L'émetteur a fini sa transmission de données. Soit la machine contactée émet à son tour, soit la connexion est terminée.

Etablissement d'une connexion TCP

THREE WAY HANDSHAKE



Etablissement d'une connexion TCP

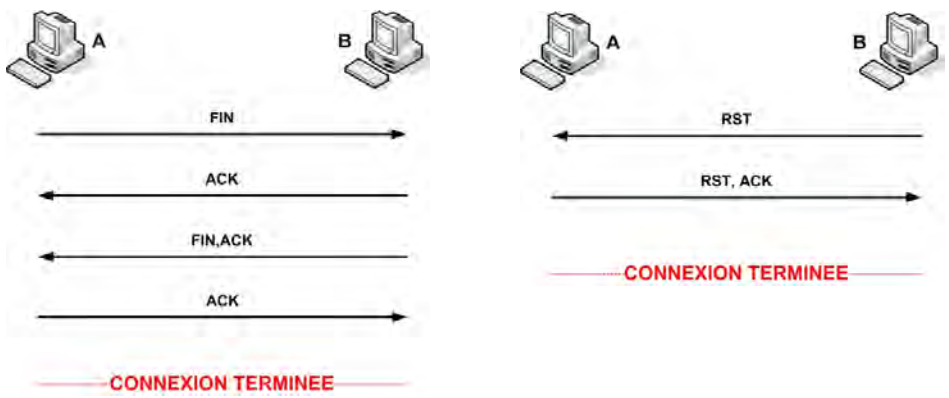
Cette technique est appelée Three Way Handshake :

- La machine veut établir une connexion TCP avec la machine B.
- A envoie à B un segment TCP avec le bit SYN positionné (c'est-à-dire égal à 1). Dans cette trame est également indiqué le numéro de séquence initial des segments émis par A, ici 500.
- B répond, si elle accepte cette connexion entrante, par un segment dont le bit SYN est lui aussi positionné ainsi que le numéro de séquence initial à 300. De plus, le bit ACK est positionné et le champ Numéro d'acquittement contient le numéro de séquence reçu précédemment de A incrémenté de 1.
- Enfin, dernière étape, A envoie un segment ayant le numéro de séquence 501 et accuse réception du segment 300. A partir de là, la connexion est établie.

Toute machine IP possède une table de connexions TCP qui enregistre l'adresse IP de l'interlocuteur. Cette table a une taille limite qui dépend généralement de la configuration du système d'exploitation.

Fin de connexion

FIN D'UNE CONNEXION



Pour terminer une connexion TCP, deux méthodes sont possibles :

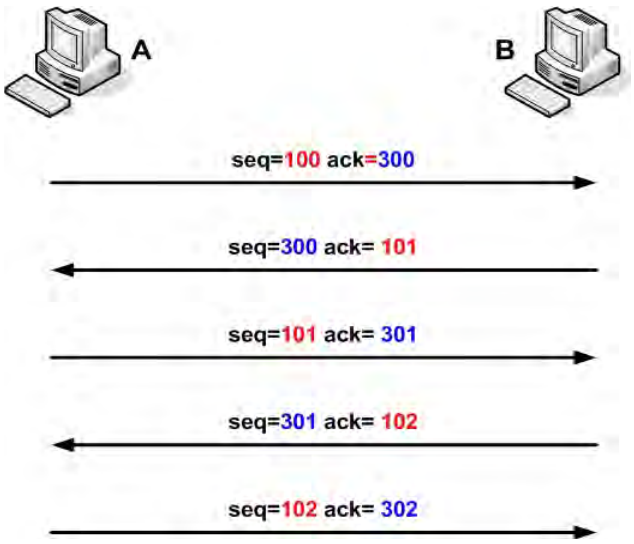
FIN

- C'est le contactant qui termine la session TCP. Dans notre exemple, A envoie à B un segment TCP avec le bit de contrôle FIN positionné.
- B renvoie un ACK à A. Ici, B va à son tour « prendre la main » et émettre à son tour.
- Si B n'a rien à émettre, il envoie ensuite un segment à A dans lequel les bits ACK et FIN sont positionnés.
- Enfin, A envoie un ACK à B afin de mettre fin à la connexion TCP.

RESET

- C'est le contacté dans ce cas qui termine la session TCP. Dans notre exemple, B envoie un segment TCP avec le bit de contrôle RST positionné.
- A répond en envoyant un segment TCP dans lequel les bits RST et ACK sont positionnés.

Window



Le champ Windows, inclus dans chaque segment TCP, permet de préciser la taille du tampon en réception de la machine émettrice. Ce paramètre permet deux choses : fiabiliser les échanges et faire du contrôle de flux.

Fiabiliser les échanges

- Les segments reçus ne seront acquittés par une machine que lorsque la quantité de données définie dans le champ window est atteinte.
- En cas d'erreurs fréquentes d'acquittement, les machines réduisent leur taille de fenêtre. De la même façon, elle sera augmentée dynamiquement lorsque l'échange redevient fiable.
- La taille de fenêtre initiale, ainsi que les seuils sont paramétrables sur la plupart des piles IP.

Faire du contrôle de flux

- Chaque machine peut adapter la valeur du paramètre window selon ses capacités, ce qui permet de faire de l'échange de données asymétriques entre des machines de puissances différentes.
- Selon le taux de remplissage du cache, par anticipation, certaines piles IP réduisent la valeur du paramètre window. De la même façon, elles l'augmentent lorsque le taux descend en dessous d'une certaine valeur.

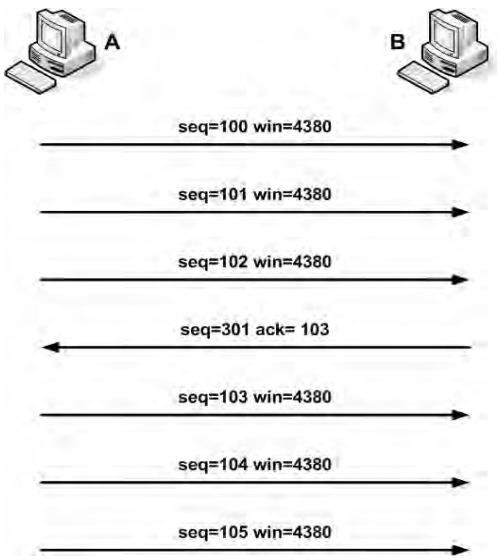
Exemple

Dans cet exemple, la taille de fenêtre est de 1460 octets. A chaque envoi d'un segment, la machine A attend que B lui envoie un accusé de réception avant d'expédier le suivant.

Cette taille de fenêtre minimale assure une grande fiabilité, par contre elle consomme de la bande passante et, surtout, ralentit considérablement les transferts volumineux.

Généralement, les piles IP actuelles tentent d'utiliser la taille de fenêtre la plus importante possible. La fiabilité des réseaux actuels permet de le faire avec des risques réduits.

Exemple : window=4380

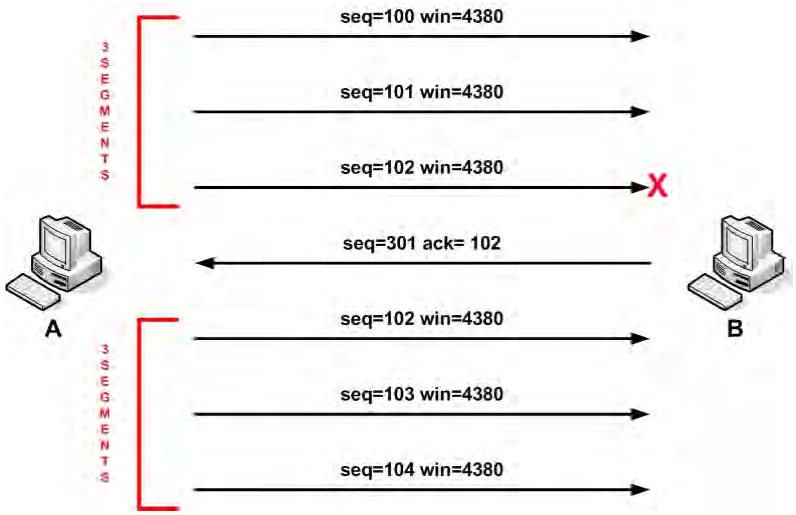


En TCP, il existe deux caches : un cache en réception et l'autre en expédition.
Le cache en réception est lié à la valeur que la machine indique dans le champ window.
Le cache en envoi, ou expédition, correspond et est ajusté à la valeur window lue sur les segments reçus de son interlocutrice.

Dans cet exemple, la taille de fenêtre du récepteur, B, est fixée à 4380 (3x1460) :

- A envoie successivement 3 segments TCP, 100 à 102, et attend l'accusé de B.
- B, dès qu'il a reçu les trois segments, envoie un accusé de réception à A. L'accusé envoyé indique que les trois segments ont bien été réceptionnés. Dans cet exemple B accuse réception de 103.
- A reçoit l'accusé et envoie trois nouveaux segments.

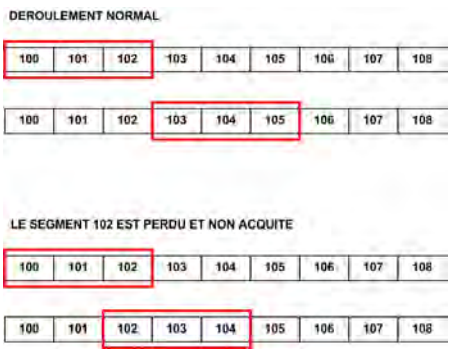
Fenêtre glissante



Étudions maintenant les mécanismes dits de fenêtre glissante. Que se passe-t-il lorsqu'un segment est perdu ?
Prenons un exemple avec une taille de fenêtre à 4380, soit 3 segments de 1460 octets :

- A envoie trois segments TCP à B, 100 à 102.
- B reçoit les segments 100 et 101, mais pas le 102.
- B, après expiration du délai d'attente maximum entre deux segments, émet un accusé de réception avec la valeur 102.
- A déplace sa fenêtre en expédition, de taille trois, de 100-101-102 à 102-103-104 et envoie les segments correspondants.

Si tout s'était bien passé, A, après réception du ACK 103, aurait déplacé la fenêtre glissante sur les segments 103-104-105.



- *DNS*
- *Noms de domaine*
- *Enregistrements*
- *Nslookup*
- *DHCP*
- *Agent de relais*
- *Tolérance de panne*

7

DNS & DHCP

Objectifs

Ce module traite des applications standard DNS et DHCP.

Connaissance

- Les applications Internet standard DNS et DHCP
- Structure d'adressage des noms de domaine
- Le rôle des serveurs DNS
- Les enregistrements standards DNS
- Les relais DHCP

Progression

Présentation de DNS	Principes de DHCP
Structure des noms de domaine	Fonctionnement
Rôle des serveurs	Relais DHCP
Résolution de noms	Tolérance de panne
Enregistrements standards	

DNS

Objectifs

- Présentation
- Structure DNS
- Zones
- Rôles des serveurs DNS
- Enregistrements standards
- Résolution de noms
- Nslookup

Dans cette section, nous allons étudier différents aspects de DNS qui, avec http, smtp et BGP, est un des piliers d'Internet.

- Dans un premier temps, nous verrons un aperçu global de DNS, les principes généraux, l'historique, les limitations.
- Nous aborderons ensuite la structure de DNS qui conditionne celle d'Internet.
- Les zones ont un rôle primordial pour DNS et Interner : la segmentation en domaines.
- Nous verrons les rôles que peut tenir un serveur DNS et les avantages apportés par ceux-ci.
- Les enregistrements permettent de localiser des ressources de différents types. Nous en verrons les principaux.
- Comment se déroule une résolution de noms entre un client et un serveur ? Entre serveurs ?
- Enfin, nous utiliserons NSLOOKUP, qui est un outil standard permettant d'interroger les serveurs DNS.

Présentation de DNS

Présentation de DNS

- ARPANET : utilisation de fichiers HOSTS pour résoudre des noms d'hôte en adresse IP
- Limitations : espace de noms et localisation
- DNS, Domain Name System : RFCs 2035, 3007, 3008
- TCP & UDP 53
- DNS est une base de données hiérarchique client/serveur distribuée
- Resolver : machine émettrice de la requête, inclus dans la plupart des piles TCP/IP
- Serveur de noms : serveur DNS

Il est plus facile de mémoriser un nom qu'une adresse logique, une adresse IP. Comment DNS est-il devenu ce que nous connaissons aujourd'hui ?

Historique

Au temps d'ARPANET, l'ancêtre d'Internet, ce problème est vite apparu. La première solution a été d'utiliser des alias, des noms d'hôtes, pour désigner des machines. Un nom correspond à une adresse IP. Pour que la machine fasse les correspondances entre les noms et les adresses, on utilisait un fichier, HOSTS. Ce fichier contient, sous forme de table, les noms utilisés localement comme alias des adresses IP.

HOSTS

Ce fichier est localisé dans le répertoire ETC, sous Windows ou Unix/Linux.
Son utilisation est très simple, chaque ligne contient un enregistrement, un mappage entre un nom et une adresse IP :

NOM1 [TAB] W.X.Y.Z

NOM2 [TAB] A.B.C.D

```
Par exemple, avec le mappage suivant :

TOTO      192.168.100.1
on peut utiliser la commande ping de deux façons :

PING 192.168.100.1

ou

PING TOTO
le résultat sera strictement le même. En finalité, c'est bien la
machine ayant l'adresse 192.168.100.1 qui sera pinguée. Notez bien
qu'il n'est pas nécessaire de connaitre le nom d'hôte réel de la
```

```
machine de destination. Un alias a une valeur purement locale, même si
sur Internet le FQDN doit être unique.
```

Il est possible d'associer plusieurs adresses à un même nom (pour un routeur par exemple). En revanche, il est déconseillé d'associer une adresse IP à plusieurs noms. Il est toutefois possible de le faire indirectement avec les mappages de types CNAME que nous verrons un peu plus loin.

La localisation de ce fichier pose évidement le problème de la mise à jour : à chaque nouvelle machine ou à chaque changement d'adresse ou de nom, il faut mettre à jour chaque fichier présent dans chaque machine. La solution a été simple : au démarrage, la machine charge le fichier sur un serveur centralisé, puis à intervalles réguliers va vérifier que le fichier n'a pas été modifié. C'est facilement réalisable par l'exécution programmée de scripts.

Attention, ce fichier HOSTS est toujours lu AVANT d'interroger un serveur DNS, ce qui peut provoquer des interférences. Si un mappage existe dans le fichier HOST, la machine ne fera pas de requête DNS. En cas de doute, vous pouvez le supprimer sans aucun risque, s'il ne vous est d'aucune utilité par ailleurs.

Limitations

Il existait deux limitations essentielles à cette technique :

- La limitation de l'espace de noms. Que se passe-t-il lorsque le nombre de machines devient tel qu'il dépasse la taille du vocabulaire actif ? En effet, n'oublions pas qu'Internet a une origine militaire, avec des règles et des contraintes militaires. Une de ces contraintes est la mémorisation aisée du nom des machines. On choisissait donc le nom des machines dans le vocabulaire actif moyen.
- L'identification de l'entité possédant la machine. Les premiers noms utilisés étaient des noms de couleurs : RED, BLUE, GREEN… faciles à identifier au début, toutes les machines étant militaires. Mais, peu à peu, des chercheurs civils sont venus se greffer aux militaires, les grandes universités ont apporté leur contribution, d'autres organismes étatiques, et… même des étudiants.
  Que signifie la machine RED ? A qui appartient-elle ? Aux militaires ? A un centre de recherche ? Au gouvernement ? A une université ?
- Enfin, un fichier est gérable avec quelques dizaines, quelques centaines d'entrées. Au delà, cela devient difficile à exploiter et à maintenir, on préfèrera utiliser une base de données hiérarchisée pour permettre une évolution importante.

Noms de domaine

- La réponse à ces deux grandes limitations a été la création et la structuration des noms de domaines.
- Le nom complet d'une machine, ou FQDN (Full Qualified Domain Name) se présente sous la forme ALIAS.DOMAINE, il est constitué de deux parties :
  - ➔ L'alias, le nom d'hôte, qui identifie une machine localement et doit être unique pour un domaine donné.
  - ➔ Le nom de domaine complet, constitué de l'ensemble des noms de domaine et de sous-domaine. Le nom de domaine identifie une entité, une entreprise, une

organisation, une agence gouvernementale, etc. On ajoute le nom de domaine comme suffixe au nom d'hôte.

- Les domaines principaux identifient :
  - ➔ En trois lettres le type de l'entité :
    - GOV : gouvernement
    - MIL : militaire
    - EDU : éducation
    - COM : commercial
    - NET : Internet
    - ORG : Organisation non gouvernementale…
  - ➔ En deux lettres l'origine de l'entité :
    - US : Etats-Unis
    - FR : France
    - UK : Royaume-Uni…
- Le nom complet d'une machine doit être unique à l'échelle de la planète, ce qui permet de la localiser sans équivoque.

```
Par exemple, une machine dans le domaine MIL (militaire) ayant pour
nom RED, aura pour nom complet RED.MIL. Une autre machine dans le
domaine GOV peut avoir le même nom d'hôte, RED, mais son nom complet
sera RED.GOV.
```

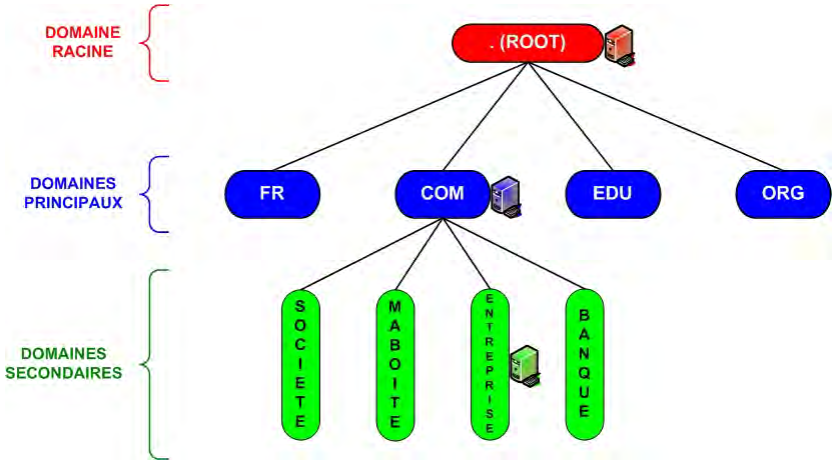
DNS

DNS, Domain Name System, définit la structure des noms de domaines et la gestion de ceux-ci par les serveurs DNS. DNS est une base de données hiérarchique client/serveur distribuée.

Le fonctionnement de DNS s'appuie sur :

- Une partie cliente, ou resolver, incluse dans toute pile IP moderne. Les échanges entre le client et les serveurs, requêtes et réponses, utilisent le port UDP 53.
- Une partie serveur, le serveur DNS ou serveur de noms. Le serveur utilise le port UDP 53 pour répondre aux clients et interroger les autres serveurs DNS, et le port TCP 53 pour les transferts de zone avec les autres serveurs d'un même domaine qui permettent de synchroniser la base de données.

Structure DNS



Les serveurs DNS constituent l'infrastructure même de DNS, ils gèrent chacun des domaines qui la constituent.

Le principe est de fragmenter, de hiérarchiser, les données. Un serveur DNS n'a besoin de connaitre qu'une partie relativement faible des données afin de résoudre les FQDN. Autrement, à l'échelle d'Internet, les serveurs DNS seraient devenus des géants ingérables contenant des millions d'entrées.

C'est cette segmentation de l'information qui a permis à cette architecture de perdurer et de continuer à croître malgré le fantastique accroissement de l'espace de noms d'Internet.

STRUCTURE

La structure des domaines est la suivante :

- Le domaine principal est le domaine ROOT, noté « . ». Ce domaine est géré directement par l'IAB (Internet Architecture Board).
- Les domaines de premier niveau, ou domaines principaux, sont directement rattachés au domaine racine : com, edu, org, net, fr, us… Tous ces domaines sont gérés par l'IAB et ne sont pas vendables.
- Les domaines de second niveau, ou sous-domaines, sont rattachés aux domaines principaux. Ce sont ces domaines que l'on peut acheter auprès de l'ICANN (Internet Corporation for Assigned Names and Numbers, nouveau nom de l'IANA, Internet Assigned Numbers Authority). Ils sont gérés par leurs propriétaires ou leur FAI/ISP.
- Tous les domaines issus des domaines de second niveau sont gérés par leurs propriétaires et n'ont d'autre contrainte que les noms commerciaux (si vous appelez un de vos domaines MICROSOFT, ce dernier peut vous demander des comptes car

c'est un nom déposé). Il est, par exemple, possible de créer un sous-domaine de ENTREPRISE se nommant PARIS, un autre LYON, etc.

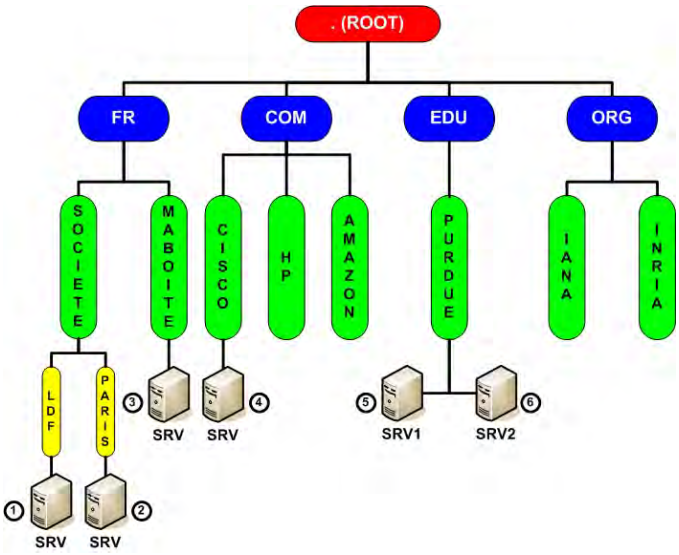
SERVEURS DNS

Les serveurs DNS de chaque domaine contiennent les enregistrements des serveurs DNS (NS, Name Serveur) des domaines sous-jacents :

- Les serveurs DNS du domaine racine contiennent les enregistrements des serveurs DNS des domaines COM, FR, EDU, MIL…
- Les serveurs DNS du domaine COM, par exemple, contiennent les enregistrements des serveurs DNS des domaines secondaires directement rattachés à celui-ci.
- Les domaines secondaires contiennent les mappages nécessaires au fonctionnement de l'entreprise.
- Chaque serveur DNS, autre que ceux gérant le domaine ROOT, possède une liste des serveurs DNS racine sous la forme du fichier CACHE.
- Les enregistrements se font manuellement pour les serveurs « classiques » ou statiques. Il existe néanmoins une version dynamique appelée DDNS (Dynamic DNS). DDNS est surtout utilisé en interne dans les entreprises, car il permet aux postes de travail de s'enregistrer dynamiquement.
  Sur Internet, seuls les serveurs statiques sont utilisés.

Exemples

EXEMPLE



EXEMPLES

1) La machine SRV appartient au sous-domaine LDF, lui-même étant un sous-domaine de SOCIETE rattaché au domaine principal FR. Le FQDN de cette machine est donc « SRV.LDF.SOCIETE.COM. ». Notez que, normalement, on ajoute un point à la fin ; ce n'est généralement pas nécessaire car la plupart des clients IP le font automatiquement.
2) La machine SRV appartient au sous-domaine PARIS, lui-même étant un sous-domaine de SOCIETE rattaché au domaine principal FR. Le FQDN de cette machine est donc « SRV.PARIS.SOCIETE.COM. ». Plusieurs machines peuvent avoir le même nom d'hôte, seul leur FQDN doit être unique à l'échelle de l'entreprise ou d'Internet.
3) Cette machine possède le FQDN « SRV.MABOITE.FR. ».
4) Le FQDN est ici : « SRV.CISCO.COM. ».
5) Le FQDN est « SRV1.PURDUE.EDU. ».
6) Enfin, le FQDN est « SRV2.PURDUE.EDU. ». Les machines 5 et 6 ne peuvent avoir un nom d'hôte identique car elles sont dans le même domaine.

Zones

Zones

- Une zone est un fichier contenant les enregistrements de ressources d'un domaine
- Une zone peut contenir plusieurs domaines, à condition que ces domaines soient contigus
- Un domaine ne peut appartenir qu'à une seule zone
- Un serveur DNS peut gérer plusieurs zones
- Transfert de zone : copie du fichier de zone entre serveurs DNS
- Zone spéciale : in-addr.arpa, permet la résolution inverse adresse_ip-noms_d'hôte

---

La gestion des domaines s'effectue par zones. Une zone est un fichier contenant les enregistrements de ressources d'un ou de plusieurs domaines.

ZONE

Une zone peut contenir plusieurs domaines, à condition toutefois que ces domaines soient contigus. Généralement, pour les domaines importants, une zone est limitée à un domaine. Les petits domaines peuvent être regroupés dans une seule zone. Tout dépend de la taille des domaines et de la puissance du ou des serveurs DNS.

Un domaine ne peut lui appartenir qu'à une seule zone. Autrement, il y aurait à la fois risque de conflit d'information et incohérence de l'architecture.

SERVEUR DNS

Un serveur DNS peut gérer plusieurs fichiers de zone. Comme nous l'avons dit, le choix du « découpage » dépendra de la taille des domaines, du nombre de ressources enregistrées, de la puissance du serveur DNS, et des contraintes réseau. Il faut compter sur le nombre de clients susceptibles d'interroger un serveur, de la bande passante allouée, etc.
Un transfert de zone consiste à effectuer une copie, ou une synchronisation, d'un fichier de zone entre deux serveurs DNS, pour des raisons de tolérance de panne et de répartition de charge. Un transfert de zone utilise le port TCP 53.

IN-ADDR.ARPA

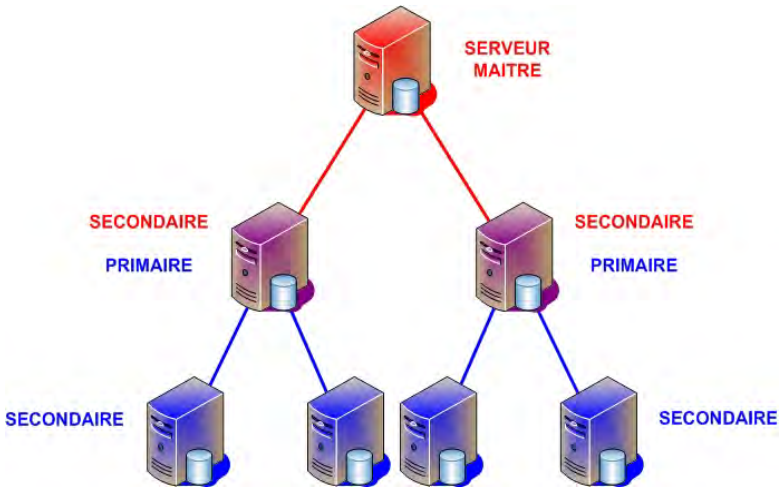
Il existe une zone spéciale, in-addr.arpa. Cette zone permet de faire des résolutions inverses : il est possible de connaitre le domaine auquel appartient une adresse IP donnée. Le nom de domaine IN-ADDR.ARPA est structuré en sous-domaines

numériques correspondant aux adresses publiques.
Par exemple, si l'adresse 195.196.197.198 appartient au domaine MONDOMAINE.COM, elle sera enregistrée en « 198.197.196.195.IN-ADDR.ARPA. ».
En fait, le domaine est structuré de la façon suivante :

- Le domaine principal, IN-ADDR, subdivisé en 224 sous domaines, de 1 à 223.
- Chacun de ces sous-domaines est lui-même divisé en 256 sous domaines, 0 à 255.
- Ces domaines sont eux-mêmes repartis en 256 sous domaines, de 0 à 255.
- Le dernier niveau de domaine contient directement les enregistrements.

Rôles des serveurs DNS

Rôles des serveurs DNS



Les serveurs DNS peuvent jouer plusieurs rôles dans une zone ou un domaine :

SERVEUR MAITRE

Il existe un serveur maître unique pour une zone donnée. C'est celui qui possède la base de données originale. Pour une zone donnée, le serveur maître est également serveur primaire. Tous les autres serveurs de la zone sont dits esclaves.

SERVEUR PRIMAIRE

On dit d'un serveur DNS qu'il est primaire s'il fournit une copie du fichier de zone à un ou plusieurs serveurs secondaires. Le serveur maître d'une zone est également primaire.

SERVEUR SECONDAIRE

Un serveur secondaire reçoit une copie du fichier de zone d'un serveur primaire. Un serveur peut être à la fois secondaire vis-à-vis d'un serveur et primaire vis-à-vis d'un autre.

Un serveur peut avoir des rôles différents dans différentes zones. Etre primaire dans une zone et secondaire dans une autre, par exemple.

SERVEUR CACHE

Un serveur cache ne possède pas de fichier de zone, mais contient les mappages les plus souvent demandés ou les plus utilisés. Ce genre de serveur est très commun chez les FAI. D'ailleurs très souvent les serveurs DNS interrogeables sur Internet sont des serveurs cache.
Et ce, pour deux raisons :

- Des raisons de performances. Ces serveurs ont en cache les mappages les plus demandés par les utilisateurs du FAI, ce qui permet d'avoir des temps de réponses faibles et une surcharge réseau moindre pour les sites les plus visités. De plus, ces serveurs rafraichissent leurs données par anticipation aux périodes de moindre charge.
- Des raisons de sécurité. Il serait bien évidemment très dangereux, ou très téméraire, de permettre un accès direct via Internet à un serveur maître ou primaire. Un pirate prenant le contrôle d'un tel serveur pourrait créer de vrais faux enregistrements afin de réaliser très simplement des attaques par « phishing » ou de détournement de données.

Enregistrements standard

- Classe d'enregistrement : elles sont quasiment toutes de type IN : Internet
- Enregistrements de ressources :
  - SOA, Start Of Authority : indique que le serveur est la meilleure source d'information pour la zone
  - A, Alias : mappage noms-adresse
  - NS, Name Server : serveur DNS de la zone
  - MX, serveur de messagerie d'un domaine donné
  - SRV, service
  - PTR, pointer : mappage adresse-noms. Utilisé avec le domaine in-addr.arpa
  - CNAME, noms canoniques ou alias d'alias

Il existe une seule classe réellement utilisée d'enregistrement DNS : IN, pour Internet. A l'origine, d'autres étaient prévues, mais elles n'ont jamais été réellement développées. Parmi ces enregistrements IN, il existe divers types d'enregistrements de ressources, adaptés aux besoins des mécanismes permettant le bon fonctionnement d'Internet ou d'un réseau d'entreprise.

SOA

Start Of Authority. Indique quel serveur est la meilleure source d'information pour la zone.

```
Exemple pour HOTMAIL.COM
hotmail.com
        primary name server = ns1.msft.net
        responsible mail addr = msnhst.microsoft.com
        serial  = 2007030603
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 2419200 (28 days)
        default TTL = 3600 (1 hour)

ns1.msft.net    internet address = 207.68.160.190

Commentaires :
ns1.msft.net est le serveur maître pour le domaine
```

```
msnhst@microsoft.com est l'adresse mail de l'administrateur du domaine

Le numéro de série (serial) est 2007030603. Ce numéro est incrémenté à
cette nouvelle modification. Il permet la synchronisation des
informations entre le serveur maître et les esclaves.

L'intervalle de rafraichissement (refresh) est de 30 minutes. Cette
valeur indique la périodicité de test de validité des données d'un
serveur esclave.

L'intervalle de nouvel essai (retry) est de 15 minutes. Si le serveur
esclave ne parvient pas à contacter le serveur maître, il réessayera
toutes les 15 minutes. Généralement cette valeur est inférieure à
celle du refresh.

L'intervalle d'obsolescence (expire) est de 28 jours. Si un serveur ne
parvient pas à localiser son serveur maître au bout de 28 jours, il
cesse de répondre aux requêtes des clients.

Le TTL (Time To Live) par défaut est de 1 heure. Le TTL est la durée
de vie des données. Cette valeur est indiquée dans les réponses qu'un
serveur DNS renvoie aux clients. Passé ce délai, un client devra
renouveler sa requête au serveur DNS. Les proxies et certains clients
DNS TCP/IP ont la possibilité de modifier cette valeur.
```

A, ALIAS

C'est l'enregistrement le plus simple : c'est un mappage entre un nom, un alias et une adresse IP. Un alias peut être associé à plusieurs adresses IP.

```
Exemple pour WWW.YAHOO.FR

Address:  69.147.114.210

Aliases:  www.yahoo.com
```

Les mappages IPv6 utilisent le type d'enregistrement AAAA sous le format :
Nom IN AAAA xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

NS, Name Server

Permet de connaitre les serveurs DNS gérant une zone, quelque soit leur rôle. L'enregistrement ne fournit que les noms, les alias ; mais souvent le serveur DNS dans sa réponse inclut également les enregistrements A des noms des serveurs DNS, ce qui permet de récupérer les adresses IP correspondantes.

```
Exemple pour le domaine AMAZON.COM :

amazon.com      nameserver = pdns5.ultradns.info

amazon.com      nameserver = pdns6.ultradns.co.uk

amazon.com      nameserver = udns1.ultradns.net

amazon.com      nameserver = udns2.ultradns.net

amazon.com      nameserver = pdns1.ultradns.net

amazon.com      nameserver = pdns2.ultradns.net

amazon.com      nameserver = pdns3.ultradns.org

amazon.com      nameserver = pdns4.ultradns.org


pdns1.ultradns.net      internet address = 204.74.108.1

pdns2.ultradns.net      internet address = 204.74.109.1

pdns3.ultradns.org      internet address = 199.7.68.1
```

```
pdns4.ultradns.org      internet address = 199.7.69.1
pdns5.ultradns.info     internet address = 204.74.114.1
pdns6.ultradns.co.uk    internet address = 204.74.115.1
udns1.ultradns.net      internet address = 204.69.234.1
udns2.ultradns.net      internet address = 204.74.101.1
```

MX, MailBox

Cet enregistrement permet de connaitre le ou les noms des serveurs de messagerie gérant un domaine donné. C'est grâce à cet enregistrement de ressources que fonctionne l'acheminement des mails sur Internet.

Il existe une spécificité pour cette ressource : il est possible de définir un niveau de préférence pour chaque enregistrement. Plus cette valeur est faible, meilleur est l'indice de préférence. La valeur 0 est la plus petite utilisable.
Concrètement, si un client reçoit plusieurs réponses à une requête MX, il utilisera d'abord l'enregistrement ayant la plus petite valeur. Si le serveur correspondant ne répond pas, le client utilisera le mappage suivant, celui ayant la valeur de préférence juste supérieure.

```
EXEMPLE POUR LE DOMAINE HOTMAIL.COM :
hotmail.com     MX preference = 5, mail exchanger = mx4.hotmail.co
hotmail.com     MX preference = 5, mail exchanger = mx1.hotmail.co
hotmail.com     MX preference = 5, mail exchanger = mx2.hotmail.co
hotmail.com     MX preference = 5, mail exchanger = mx3.hotmail.co

mx1.hotmail.com internet address = 65.54.245.8
mx1.hotmail.com internet address = 65.54.244.8
mx1.hotmail.com internet address = 65.54.244.136
mx2.hotmail.com internet address = 65.54.245.40
mx2.hotmail.com internet address = 65.54.244.40
mx2.hotmail.com internet address = 65.54.244.168
mx3.hotmail.com internet address = 65.54.245.72
mx3.hotmail.com internet address = 65.54.244.72
mx3.hotmail.com internet address = 65.54.244.200
mx4.hotmail.com internet address = 65.54.245.104
mx4.hotmail.com internet address = 65.54.244.104
mx4.hotmail.com internet address = 65.54.244.232

SECONDE REQUETE POUR HOTMAIL.COM :
hotmail.com     MX preference = 5, mail exchanger = mx1.hotmail.com
hotmail.com     MX preference = 5, mail exchanger = mx2.hotmail.com
hotmail.com     MX preference = 5, mail exchanger = mx3.hotmail.com
hotmail.com     MX preference = 5, mail exchanger = mx4.hotmail.com

mx1.hotmail.com internet address = 65.54.245.8
```

```
mx1.hotmail.com internet address = 65.54.244.8
mx1.hotmail.com internet address = 65.54.244.136
mx2.hotmail.com internet address = 65.54.244.40
mx2.hotmail.com internet address = 65.54.244.168
mx2.hotmail.com internet address = 65.54.245.40
mx3.hotmail.com internet address = 65.54.245.72
mx3.hotmail.com internet address = 65.54.244.72
mx3.hotmail.com internet address = 65.54.244.200
mx4.hotmail.com internet address = 65.54.244.104
mx4.hotmail.com internet address = 65.54.244.232
mx4.hotmail.com internet address = 65.54.245.104


COMMENTAIRE : Dans cet exemple, il existe plusieurs mappages ayant le
même niveau de préférence. Dans ce cas, le client utilise le premier
de la liste envoyée par le serveur.
Afin de répartir la charge et de disposer d'une tolérance de panne,
les serveurs DNS envoient les listes ordonnancées différemment à
chaque requête.
Nous voyons ici que le serveur a répondu à la première interrogation
mx4 mx1 mx2 mx3, et mx1 mx2 mx3 mx4 à la seconde. Cette fonctionnalité
se nomme Round Robin. Le principe est de faire « tourner » les
mappages de même valeur. Le Round Robin est utilisé pour tous les
enregistrements, sauf PTR.
```

SRV, SERVICE

Les enregistrements SRV permettent de déclarer des services. Ce type est plutôt utilisé en interne dans les entreprises.

Le format de cette ressource est le suivant :
service.protocole in srv *priorité* *poids* *port* *cible*

- Service, définit le type de service recherché : ftp, http…
- Protocole, le protocole de transport utilisé : UDP ou TCP.
- Priorité, s'il existe plusieurs serveurs, c'est celui qui a la priorité la plus faible qui est utilisé en premier.
- Poids, permet la répartition de charge entre des serveurs ayant la même priorité. Les clients utiliseront les serveurs au prorata de cette valeur.
- Port, définit le port associé à cette application.

Microsoft, par exemple, l'utilise massivement dans son architecture d'annuaire ADS pour enregistrer les différents services des serveurs Windows disponibles dans le domaine.

PTR, Pointer

Ce type d'enregistrement fonctionne de façon inverse des enregistrements alias : le client envoie une demande en précisant l'adresse IP de la machine, le serveur répondra en envoyant le nom de domaine auquel appartient cette adresse IP. Ce type d'enregistrement de ressources s'appuie sur le domaine spécial in-addr.arpa.

```
Exemple pour l'adresse 65.64.245.104 :
```

```
104.245.54.65.in-addr.arpa      name = bay0-mc12-f.bay0.hotmail.com
104.245.54.65.in-addr.arpa      name = mx4.hotmail.com
```

CNAME

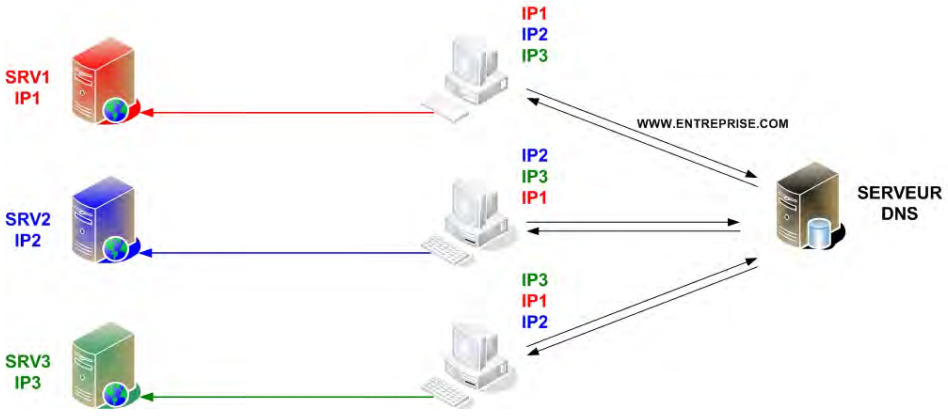
Un CNAME est un alias d'alias ou nom canonique. Quel intérêt ? Ne pas être obligé de connaître systématiquement les noms d'hôtes réels des machines. Le principe est d'associer un alias significatif ou générique aux noms réels des serveurs. Par exemple, FTP, SMTP ou MAIL, POP, IMAP…

Le plus utilisé, le plus connu, est le CNAME « WWW ». Comme les internautes ne sont pas sensés connaitre les noms d'hôtes réels des serveurs web, le nom canonique permet de définir un alias générique connu par tous.

```
Prenons un exemple : un serveur web, SERVEUR1 possède l'adresse IP1.
Afin de le rendre facilement accessible sur Internet, il suffira de
connaître uniquement le nom du domaine. L'enregistrement sera le
suivant :

www        CNAME       SERVEUR1
SERVEUR1         A           IP1

L'accès au serveur se fera via WWW.NOMDUDOMAINE.COM.
```

```
Exemple réel pour WWW.ORANGE.FR

CNAME :

www.orange.fr   canonical name = www.orange.fr.multis.x-echo.com


ALIAS :

www.orange.fr.multis.x-echo.com

Nom :    www.orange.fr.multis.x-echo.com

Addresses:  193.252.149.30, 193.252.122.103


ALIAS :

www.orange.fr

Nom :    www.orange.fr.multis.x-echo.com

Addresses:  193.252.149.30, 193.252.122.103

Aliases:  www.orange.fr
```

Round Robin



La fonctionnalité dite du « Round Robin » permet d'effectuer du partage de charge et de la tolérance de panne lorsqu'il existe plusieurs adresses IP pour un même enregistrement. Elle est activée par défaut sur la plupart des serveurs DNS récents.

FONCTIONNEMENT

Le principe est le suivant : quand un enregistrement est lié à plusieurs adresses, le serveur fait « tourner » les réponses. A chaque nouvelle requête, la liste n'est pas ordonnancée de la même manière.

Prenons un exemple simple d'enregistrement :

SERVEUR	A	IP1
SERVEUR	A	IP2
SERVEUR	A	IP3

Le premier client recevra comme réponse à sa requête sur SERVEUR une réponse dans l'ordre suivant : IP1 IP2 IP3 et se connectera à IP1. Si IP1 n'est pas disponible, il tentera de se connecter à IP2, et ainsi de suite.
Un second client ou une seconde requête aura comme réponse IP2 IP3 IP1.
Une troisième requête recevra IP3 IP1 IP2.
Une quatrième requête recevra IP1 IP2 IP3.

Noter que le Round Robin permet la répartition de charge et non l'équilibrage de charge. En effet, la répartition se fait de manière inconditionnelle sur tous les enregistrements d'une même ressource.
Sur Internet, on compte sur l'énorme quantité de requêtes pour avoir une répartition statistiquement équilibrée de la charge.
Pour l'équilibrage de charge statique, on utilise plutôt l'enregistrement SRV en jouant

sur le facteur de poids, permettant une répartition de charge statique.
Pour une répartition de charge dynamique, il faudra avoir recourt à des applications spécifiques ou à des boîtiers dédiés.

EXEMPLE AVEC CNAME

Dans cet exemple, supposons qu'une entreprise possède le nom de domaine ENTREPRISE.COM.

Elle dispose de trois serveurs WEB : SRV1, SRV2 et SRV3. Ces trois serveurs sont des miroirs, ils ont tous le même contenu. Afin de permettre un accès standard aux serveurs WEB, il a été décidé d'utiliser le CNAME WWW.

A cet effet, le serveur DNS gérant le domaine ENTREPRISE.COM dispose des enregistrements suivants :

WWW	CNAME	SRV1
WWW	CNAME	SRV2
WWW	CNAME	SRV3

SRV1	A	IP1
SRV2	A	IP2
SRV3	A	IP3

Le premier client recevra comme réponse à la requête sur www.entreprise.com. IP1 IP2 IP3 et se connectera à IP1.

Le premier client recevra comme réponse à la requête sur www.entreprise.com. IP2 IP3 IP1 et se connectera à IP2.

Le premier client recevra comme réponse à la requête sur www.entreprise.com. IP3 IP1 IP2 et se connectera à IP3.

Mécanismes de résolution

- Les différents types de requêtes :
  - Requêtes récursives : entre client et serveur ou entre serveurs. La réponse doit être exclusive, ne doit pas renvoyer à un autre serveur
  - Requêtes itératives : entre serveurs. La réponse peut renvoyer à un autre serveur.
- Le fichier CACHE contient les alias et les adresses des serveurs DNS du domaine ROOT

Pour résoudre un FQDN ou obtenir un enregistrement de ressources, on utilise :

- Des requêtes DNS entre clients et serveurs et entre serveurs ;
- Le fichier CACHE, qui contient les enregistrements des serveurs DNS du domaine ROOT.

Il existe deux types de requêtes DNS :

- Les requêtes récursives ;
- Les requêtes itératives.

REQUETES RECURSIVES

La réponse à une requête récursive peut uniquement contenir :

- La réponse à la requête. Le serveur DNS interrogé connait l'enregistrement demandé.
- Une réponse négative. Le serveur DNS interrogé ne connait pas l'enregistrement demandé.

Les requêtes récursives peuvent être utilisées :

- Entre client et serveur. C'est le type de requête utilisé par défaut entre le resolver et le serveur DNS.
  Le serveur, dans ce cas, ne peut répondre que par :
  - ➔ La positive. Il connait l'enregistrement intrinsèquement ou a obtenu l'information en interrogeant d'autres serveurs DNS. Le serveur DNS n'a pas obligation de répondre immédiatement, il peut le faire une fois qu'il a obtenu lui-même une réponse d'un autre serveur DNS.
- ➔ La négative. Le serveur n'a pu résoudre l'enregistrement.

Par contre, un serveur ne peut répondre en redirigeant le resolver vers un autre serveur DNS, comme dans le cas d'une requête itérative.

- Entre serveurs. Un serveur peut interroger un autre serveur de deux façons : via une requête récursive ou via une requête itérative.
  S'il utilise une requête récursive, le serveur DNS interrogé la considéra comme n'importe quelle autre requête cliente. Ce type de requête est utilisé généralement entre un serveur DNS d'entreprise et un serveur DNS cache appartenant à son FAI. L'option REDIRECTEUR ou REDIRECTION, disponible sur la quasi-totalité des serveurs DNS du commerce, vous permet d'indiquer l'adresse IP du serveur cache de votre FAI.

REQUETES ITERATIVES

Les requêtes itératives sont essentiellement utilisées entre serveurs DNS.
La réponse à une requête itérative peut contenir :

- L'enregistrement demandé. Le serveur DNS sollicité connait ou a obtenu l'information.
- L'enregistrement d'un autre serveur DNS. Dans ce cas, le serveur DNS renvoie le solliciteur vers cet autre serveur DNS. En général, le renvoi est effectué vers un serveur plus « bas » dans la hiérarchie DNS.

```
Par exemple en faisant une requête sur un enregistrement appartenant
au domaine EXEMPLE.COM à un serveur racine, celui-ci renverra la liste
des serveurs gérant le domaine .COM.
De même en interrogeant un serveur .COM sur un enregistrement de
EXEMPLE.COM, celui-ci renverra la liste des serveurs DNS gérant le
domaine EXEMPLE.
```

L'information est segmentée, répartie entre les serveurs DNS, chacun ne connaissant que les enregistrements concernant directement le domaine qu'il gère, pas les domaines supérieurs ni les sous-domaines.

RESULTATS

Les résultats des requêtes sont enregistrés dans un cache, en ram ou sur disque dur. Chaque enregistrement transmis possède une durée de vie : le TTL (Time To Live), ce TTL peut être modifié en cours de route (DNS cache, proxy…).

LE FICHIER CACHE

Ce fichier est présent sur chaque serveur DNS, il contient les enregistrements des serveurs racine, ceux qui gèrent le domaine ROOT. Il peut être mis à jour aisément en téléchargeant la mise à jour sur le site de l'ICANN. Rien ne presse, il y a au maximum un serveur DNS rajouté à la liste par an. Un serveur DNS interroge un de ces serveurs lorsqu'il doit résoudre un nom en dehors des domaines qu'il gère, à moins qu'il n'utilise la fonction redirection et qu'il interroge dans ce cas le serveur cache de son FAI.

Contenu du fichier CACHE :

.	3600000	NS	A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.	3600000	A	198.41.0.4
.	3600000	NS	B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.	3600000	A	128.9.0.107

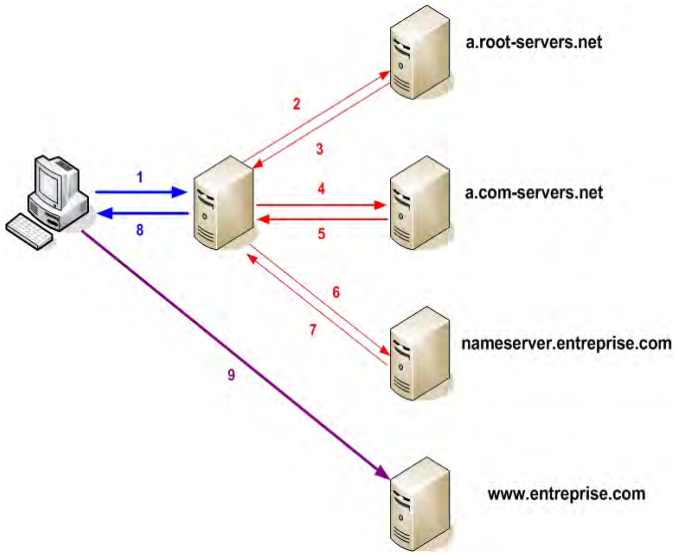
…

Actuellement, le dernier serveur est le M. Pour chaque serveur, il y a deux entrées :

- Un enregistrement NS pour le domaine « . »
- Un enregistrement A pour le nom du serveur

Exemple 1

EXEMPLE 1



EXEMPLE 1 : RESOLUTION DIRECTE

Prenons le cas d'un poste de travail voulant se connecter au serveur web www.entreprise.com :

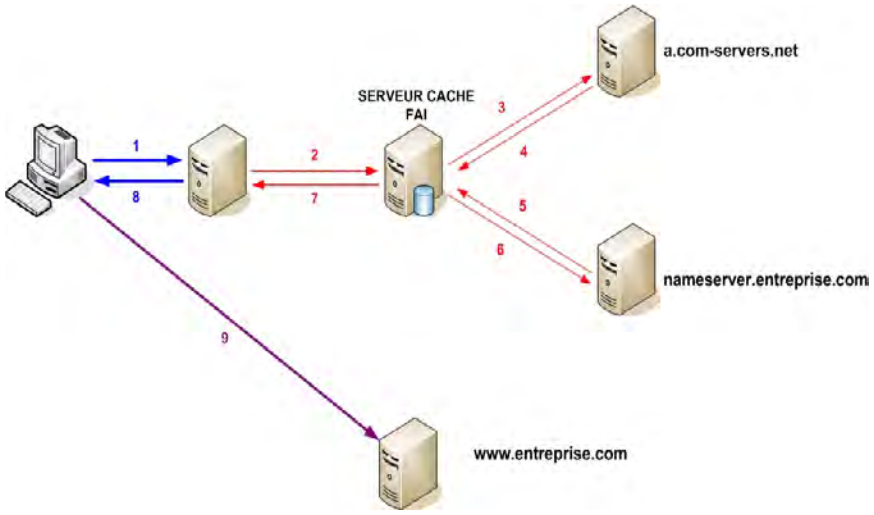
1) Le client émet une requête récursive vers son serveur DNS local, ou le serveur DNS de son opérateur, afin d'obtenir l'adresse IP de www.entreprise.com.
2) Celui-ci, ne connaissant pas le nom de domaine entreprise.com, lance une requête récursive vers le serveur racine afin d'obtenir la liste des serveurs DNS (NS) gérant le domaine .COM. Normalement, si on devait respecter scrupuleusement les procédures, le serveur devrait faire une requête itérative sur le nom complet www.entreprise.com. Le fait de demander directement les enregistrements des serveurs de niveau inférieur simplifie les requêtes et allège la charge des serveurs racine.
3) Le serveur racine répond en envoyant la liste des serveurs DNS (NS) gérant le domaine .COM.
4) Le serveur DNS local sélectionne un des serveurs DNS du domaine .COM et envoie une requête NS sur le domaine entreprise.com.
5) Le serveur DNS du domaine .COM répond en envoyant l'adresse IP du serveur DNS gérant le domaine entreprise.com.
6) Le serveur DNS local envoie une requête A sur le nom d'hôte www au serveur DNS de entreprise.com.
7) Le serveur DNS de entreprise.com répond en envoyant l'adresse IP du serveur www (en fait un enregistrement CNAME).

8) Le serveur DNS local répond au client en lui fournissant l'adresse IP du serveur www.entreprise.com.

9) Le client se connecte au serveur www.entreprise.com.

Exemple 2

EXEMPLE 2



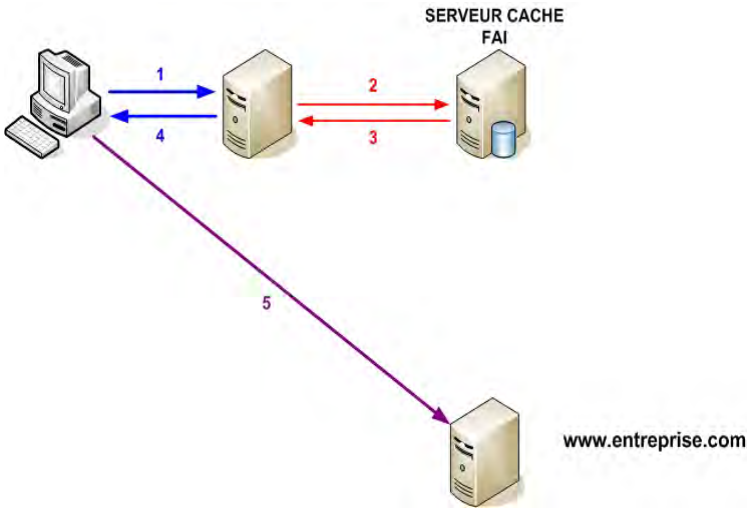
EXEMPLE 2 : SERVEUR CACHE DU FAI

Prenons le cas d'un poste de travail voulant se connecter au serveur web www.entreprise.com :

1) Le client émet une requête récursive vers son serveur DNS local, ou le serveur DNS de son opérateur, afin d'obtenir l'adresse IP de www.entreprise.com.
2) Celui-ci, ne connaissant pas le nom de domaine entreprise.com, lance une requête itérative vers le serveur cache du fournisseur d'accès, qui possède en cache la plupart des serveurs DNS des domaines de premier niveau (.com, .fr), ainsi que les requêtes les plus populaires. Nous supposerons ici qu'il n'a pas en cache l'enregistrement demandé.
3) Le serveur cache DNS sélectionne un des serveurs DNS du domaine .COM et envoie une requête sur le domaine entreprise.com.
4) Le serveur DNS du domaine .com répond en envoyant l'adresse IP du serveur DNS gérant le domaine entreprise.com.
5) Le serveur cache DNS envoie une requête sur le nom d'hôte www au serveur DNS de entreprise.com.
6) Le serveur DNS de entreprise.com répond en envoyant l'adresse IP du serveur www (en fait un enregistrement CNAME).
7) Le serveur cache DNS répond au DNS local.
8) Le serveur DNS local répond au client.
9) Le client se connecte au serveur www.entreprise.com.

Exemple 3

EXEMPLE 3



EXEMPLE 3 : SERVEUR CACHE DU FAI

Prenons le cas d'un poste de travail voulant se connecter au serveur web www.entreprise.com :

1) Le client émet une requête récursive vers son serveur DNS local, ou le serveur DNS de son opérateur, afin d'obtenir l'adresse IP de www.entreprise.com.
2) Celui-ci, ne connaissant pas le nom de domaine entreprise.com, lance une requête itérative vers le serveur cache du fournisseur d'accès, qui possède en cache la plupart des serveurs DNS des domaines de premier niveau (.com, .fr). Nous supposerons que cette fois l'enregistrement est déjà présent en cache sur le serveur.
3) Le serveur cache DNS répond au DNS local.
4) Le serveur DNS local répond au client.
5) Le client se connecte au serveur www.entreprise.com.

NSLOOKUP

NSlookup

- Outil permettant d'interroger les serveurs DNS
- Nslookup peut faire tous types de requêtes
- Utilisé pour la maintenance et le dépannage des serveurs DNS
- Il existe deux modes :
  - Direct : c:\nslookup www.entreprise.com qui résout des alias
  - Ligne de commandes, pour les autres requêtes

NSLOOKUP est un outil installé avec le client DNS et disponible sur toutes les plates-formes. Il permet d'interroger les serveurs DNS en interactif, de visualiser concrètement les résultats. Il est ainsi possible de l'utiliser pour la maintenance et le dépannage des serveurs DNS.
Il existe deux modes d'utilisation de NSLOOKUP : direct et ligne de commandes.

MODE DIRECT

Dans ce mode on ne résout que les alias, dans un sens (A) ou dans l'autre (PTR).

```
EXEMPLE 1 : A
C:\nslookup www.google.fr
Nom :    www.l.google.com
Addresses : 209.85.129.147, 209.85.129.99, 209.85.129.104
Aliases : www.google.fr, www.google.com

EXEMPLE 2 : PTR
C:\>nslookup 209.85.129.104
Nom :    fk-in-f104.google.com
Address:  209.85.129.104
```

Pour le NSLOOKUP de Microsoft, aucun serveur DNS qui n'est pas dans un domaine intégré ADS ne fait autorité. Le message indiquant « Réponse ne faisant pas autorité » est purement formel et ne doit pas vous inquiéter outre mesure. Je les ai d'ailleurs systématiquement supprimés des copies d'écran. En cas de doute, vous pouvez utiliser un autre serveur DNS afin de vérifier si les enregistrements sont les mêmes. Par

exemple ceux de FranceTélécom/Orange, 194.2.0.20 et 194.2.0.50, sont accessibles de partout. Sauf si votre opérateur ne joue pas le jeu et filtre les requêtes DNS autres que celle de ses propres serveurs.

MODE LIGNE DE COMMANDES

Dans ce mode, on peut faire des requêtes sur tous les types d'enregistrements. Il faut d'abord entrer en mode de commande en tapant NSLOOKUP sans argument, et ensuite saisir les commandes adéquates. Attention, certaines commandes sont sensibles à la casse.

Quelques commandes utiles :

- ? ou help : vous permet d'avoir la liste de toutes les commandes disponibles ainsi que leurs arguments.
- SET TYPE= permet de préciser le type d'enregistrement souhaité : A, PTR, NS, MX, SRV, CNAME et ANY

```
EXEMPLE 1 : A
D:\>nslookup
Serveur par défaut : dns1.noos.fr
Address : 212.198.0.91

> www.hotmail.com
Nom :    www.hotmail.aate.nsatc.net
Addresses : 166.63.208.158, 216.219.72.36
Aliases : www.hotmail.com, www.hotmail.com.nsatc.net

> www.google.fr
Nom :    www.l.google.com
Addresses : 209.85.135.99, 209.85.135.103, 209.85.135.104,
209.85.135.147
Aliases : www.google.fr, www.google.com
```

```
EXEMPLE 2 : NS ROOT
> set type=ns
> .
(root)  nameserver = J.ROOT-SERVERS.NET
(root)  nameserver = K.ROOT-SERVERS.NET
(root)  nameserver = L.ROOT-SERVERS.NET
(root)  nameserver = M.ROOT-SERVERS.NET
(root)  nameserver = A.ROOT-SERVERS.NET
(root)  nameserver = B.ROOT-SERVERS.NET
(root)  nameserver = C.ROOT-SERVERS.NET
(root)  nameserver = D.ROOT-SERVERS.NET
(root)  nameserver = E.ROOT-SERVERS.NET
```

```
(root)  nameserver = F.ROOT-SERVERS.NET
(root)  nameserver = G.ROOT-SERVERS.NET
(root)  nameserver = H.ROOT-SERVERS.NET
(root)  nameserver = I.ROOT-SERVERS.NET

A.ROOT-SERVERS.NET      internet address = 198.41.0.4
B.ROOT-SERVERS.NET      internet address = 192.228.79.201
C.ROOT-SERVERS.NET      internet address = 192.33.4.12
D.ROOT-SERVERS.NET      internet address = 128.8.10.90
E.ROOT-SERVERS.NET      internet address = 192.203.230.10
F.ROOT-SERVERS.NET      internet address = 192.5.5.241
G.ROOT-SERVERS.NET      internet address = 192.112.36.4
H.ROOT-SERVERS.NET      internet address = 128.63.2.53
I.ROOT-SERVERS.NET      internet address = 192.36.148.17
J.ROOT-SERVERS.NET      internet address = 192.58.128.30
K.ROOT-SERVERS.NET      internet address = 193.0.14.129
L.ROOT-SERVERS.NET      internet address = 198.32.64.12
M.ROOT-SERVERS.NET      internet address = 202.12.27.33
```

```
EXEMPLE 3 : NS COM.
> com.
com     nameserver = e.gtld-servers.net
com     nameserver = f.gtld-servers.net
com     nameserver = g.gtld-servers.net
com     nameserver = h.gtld-servers.net
com     nameserver = i.gtld-servers.net
com     nameserver = j.gtld-servers.net
com     nameserver = k.gtld-servers.net
com     nameserver = l.gtld-servers.net
com     nameserver = m.gtld-servers.net
com     nameserver = a.gtld-servers.net
com     nameserver = b.gtld-servers.net
com     nameserver = c.gtld-servers.net
com     nameserver = d.gtld-servers.net

a.gtld-servers.net      internet address = 192.5.6.30
a.gtld-servers.net      AAAA IPv6 address = 2001:503:a83e::2:30
b.gtld-servers.net      internet address = 192.33.14.30
b.gtld-servers.net      AAAA IPv6 address = 2001:503:231d::2:30
c.gtld-servers.net      internet address = 192.26.92.30
d.gtld-servers.net      internet address = 192.31.80.30
```

```
e.gtld-servers.net      internet address = 192.12.94.30
f.gtld-servers.net      internet address = 192.35.51.30
g.gtld-servers.net      internet address = 192.42.93.30
h.gtld-servers.net      internet address = 192.54.112.30
i.gtld-servers.net      internet address = 192.43.172.30
j.gtld-servers.net      internet address = 192.48.79.30
k.gtld-servers.net      internet address = 192.52.178.30
l.gtld-servers.net      internet address = 192.41.162.30
m.gtld-servers.net      internet address = 192.55.83.30
```

```
EXEMPLE 4 : MX ORANGE.FR
> set type=mx
> orange.fr
orange.fr       MX preference = 10, mail exchanger = smtp-in.orange.fr

orange.fr       nameserver = ns2.wanadoo.fr
orange.fr       nameserver = ns.wanadoo.fr
smtp-in.orange.fr       internet address = 193.252.23.67
smtp-in.orange.fr       internet address = 193.252.23.107
smtp-in.orange.fr       internet address = 193.252.23.110
smtp-in.orange.fr       internet address = 80.12.242.3
smtp-in.orange.fr       internet address = 80.12.242.6
smtp-in.orange.fr       internet address = 80.12.242.9
smtp-in.orange.fr       internet address = 80.12.242.12
smtp-in.orange.fr       internet address = 80.12.242.15
smtp-in.orange.fr       internet address = 80.12.242.53
smtp-in.orange.fr       internet address = 193.252.22.56
smtp-in.orange.fr       internet address = 193.252.22.65
smtp-in.orange.fr       internet address = 193.252.22.78
smtp-in.orange.fr       internet address = 193.252.22.79
smtp-in.orange.fr       internet address = 193.252.22.80
smtp-in.orange.fr       internet address = 193.252.22.81
smtp-in.orange.fr       internet address = 193.252.22.82
smtp-in.orange.fr       internet address = 193.252.22.83
smtp-in.orange.fr       internet address = 193.252.22.89
smtp-in.orange.fr       internet address = 193.252.22.92
smtp-in.orange.fr       internet address = 193.252.22.107
smtp-in.orange.fr       internet address = 193.252.22.116
smtp-in.orange.fr       internet address = 193.252.22.123
ns.wanadoo.fr     internet address = 80.12.255.24
ns2.wanadoo.fr    internet address = 80.12.255.159
```

DHCP

Objectifs

- Principes
- Fonctionnement
- Relais DHCP
- Redondance et tolérance de panne

DHCP est un serveur standard normalisé permettant de gérer dynamiquement l'adressage IP.

Nous allons voir dans cette partie :

- Les principes de DHCP ainsi que ses composants.
- Le fonctionnement de DHCP dans un réseau Ethernet.
- Ce qu'est un relais DHCP et comment il fonctionne.
- Enfin nous verrons comment obtenir une redondance de service afin de fournir une tolérance de panne en DHCP.

Principes de DHCP

- DHCP (Dynamic Host Configuration Protocol) est un protocole client/serveur permettant une configuration dynamique de TCP/IP
- Un serveur DHCP alloue un bail à un client qui lui en fait la demande, ce bail contient :
  - Une adresse IP et un masque de sous-réseau
  - Des options : adresses DNS, WINS, type de résolution NetBIOS, adresse de passerelle…
- Des adresses IP peuvent être réservées pour certaines adresses MAC
- Une étendue est la plage d'adresses que peut distribuer un serveur DHCP
- Un serveur DHCP peut gérer plusieurs étendues

DHCP (Dynamic Host Configuration Protocol) est un protocole client/serveur permettant une configuration dynamique de TCP/IP des machines utilisateurs.

DHCP est le successeur de BOOTP.

Le client DHCP est inclus dans la pile IP de la plupart des systèmes d'exploitation clients.

PRINCIPES DE DHCP

Le principe de base de DHCP est le suivant : les machines clientes sur lesquelles est activé le client DHCP démarrent sans configuration TCP/IP statique, en « dur », elles obtiendront les paramètres nécessaires à leur fonctionnent d'un serveur DHCP. Celui-ci leur fournira une adresse IP, un masque de sous-réseau, le nom de domaine, les adresses des serveurs DNS…

Pouvoir ainsi changer facilement et dynamiquement la configuration TCP/IP d'une machine représente un gain de temps important et réduit considérablement les erreurs inhérentes à ce genre de manipulation.

CLIENT DHCP

Sur quelles machines peut-on activer le client DHCP ?

- Les ordinateurs portables et autres PADs, ce qui permet de récupérer une configuration TCP/IP automatiquement, quelque soit le réseau auquel on se connecte, à condition que celui-ci dispose d'un serveur DHCP, ce qui est majoritairement le cas dans les entreprises actuelles.
- Les machines utilisateurs, ce qui permettra en cas de changement d'un paramètre TCP/IP de le faire de manière centralisée, sur les serveurs DHCP.

- Les imprimantes, pour les mêmes raisons que les machines utilisateurs. Dans ce cas, on fait des réservations d'adresse IP afin que les imprimantes se voient toujours allouer la même adresse.

Sur quelles machines ne doit-on pas activer le client DHCP ?

- Les serveurs DHCP eux-mêmes.
- Les serveurs en général, leur adresse doit toujours être la même et ne pas dépendre de la disponibilité d'autres serveurs ou d'une partie du réseau.
- Les éléments constitutifs de l'infrastructure réseau :
  - ➔ Les routeurs
  - ➔ Les firewalls
  - ➔ Les commutateurs
  - ➔ Les points d'accès WiFi

CARACTERISTIQUES DE DHCP

- Le serveur DHCP alloue un bail à chaque client qui lui en fait la demande.
- Ce bail a une durée déterminée et configurable.
- Le bail contient :
  - ➔ Une adresse IP et un masque de sous-réseau pour le moins ;
  - ➔ Des options : passerelle par défaut, serveurs DNS, nom de domaine, type de résolution NetBIOS, serveurs WINS…
- La réservation d'adresse se fait via le mappage entre une adresse IP et l'adresse MAC du client. Le client possédant cette adresse MAC se verra toujours attribuer la même adresse IP, qui lui est réservée.
- On appelle étendue la plage d'adresses distribuable dont dispose un serveur DHCP. Un serveur DHCP peut gérer plusieurs étendues.
- Le client utilise le port UDP 68.
- Le serveur utilise le port UDP 67.

Fonctionnement de DHCP

Fonctionnement de DHCP

- Le client émet une requête à destination de tous les serveurs DHCP
- Les serveurs répondent avec une proposition d'adresse IP et un masque de sous réseau
- Le client sélectionne la première proposition qu'il reçoit
- Le serveur confirme le bail et ajoute les options supplémentaires, ou refuse la réservation

---

Comment un client DHCP obtient-il sa configuration TCP/IP dynamique ? Quelle est la procédure de négociation et d'attribution ?

Il y a quatre étapes :

DHCP DISCOVER

Le client émet une requête à destination de tous les serveurs DHCP.
Cette requête a les caractéristiques suivantes :

- ➔ Adresse MAC source : celle du client
- ➔ Adresse IP source : 0.0.0.0
- ➔ Port source : UDP 68
- ➔ Adresse MAC destination : FF-FF-FF-FF-FF-FF
- ➔ Adresse IP destination : 255.255.255.255
- ➔ Port destination : UDP 67

DHCP OFFER

Tous les serveurs reçoivent cette requête et y répondent en faisant une offre de bail.
Cette offre contient uniquement une adresse IP et un masque de sous-réseau.
Cette offre a les caractéristiques suivantes :

- ➔ Adresse MAC source : celle du serveur
- ➔ Adresse IP source : celle du serveur
- ➔ Port source : UDP 67
- ➔ Adresse MAC destination : FF-FF-FF-FF-FF-FF

- ➔ Adresse IP destination : 255.255.255.255
- ➔ Port destination : UDP 68

Il est à noter que les serveurs ne répondent pas à l'adresse MAC du client mais en broadcast. En réalité, plusieurs machines clientes peuvent faire une demande quasi-simultanément sur le réseau, les serveurs envoient donc leurs propositions à tout le monde, le tri se fera par la promptitude de réponse des clients. Tous les clients reçoivent donc toutes les propositions de bail.

DHCP REQUEST

Le client sélectionne la première proposition qu'il reçoit et émet une requête à destination des serveurs.

Cette requête a les caractéristiques suivantes :

- ➔ Adresse MAC source : celle du client
- ➔ Adresse IP source : 0.0.0.0
- ➔ Port source : UDP 68
- ➔ Adresse MAC destination : FF-FF-FF-FF-FF-FF
- ➔ Adresse IP destination : 255.255.255.255
- ➔ Port destination : UDP 67

Il est à noter ici que le client envoie sa requête à tous les serveurs. C'est une différence par rapport à BOOTP, où le client ne répondait qu'au serveur dont il avait sélectionné l'offre. Les serveurs dont l'offre n'était pas retenue la proposaient à une autre machine après expiration d'un délai d'attente. En DHCP, les serveurs sont tous informés en même temps, grâce au broadcast MAC. Ils peuvent donc libérer plus rapidement une offre qui n'a pas été retenue.

DHCP ACK / DHCP NACK

Enfin, le serveur dont l'offre a été retenue par le client répond :

- Par un DHCP ACK si la requête émise par le client est la première à avoir été reçue par le serveur. Ce datagramme confirme au client que le serveur lui attribue le bail de cette adresse IP. Il contient également les options de configuration supplémentaires. Le serveur enregistre l'adresse MAC du client à qui il a attribué l'adresse IP.
- Par un DHCP NACK, si la requête émise par le client n'est pas la première à avoir été reçue par le serveur. Cela signifie que le serveur a déjà réservé cette adresse IP à une autre machine. Dans ce cas, le client recommencera la procédure.

Cette réponse a les caractéristiques suivantes :

- ➔ Adresse MAC source : celle du serveur
- ➔ Adresse IP source : celle du serveur
- ➔ Port source : UDP 67
- ➔ Adresse MAC destination : celle du client
- ➔ Adresse IP destination : 255.255.255.255
- ➔ Port destination : UDP 68

Vie des baux

- La durée du bail est configurable
- Lors de l'arrêt, une machine cliente DHCP libère le bail de son adresse IP
- Le client tente de renouveler le bail à la moitié de la durée de celui-ci
- En cas d'échec du renouvellement, une nouvelle tentative a lieu aux 7/8^{ième} de la durée du bail

---

La durée des baux est configurable, elle peut être différente pour chaque étendue, voire pour des adresses particulières.

En fonctionnement normal, il y a 3 étapes concernant la vie d'un bail :

ARRET D'UNE MACHINE CLIENTE

Lors de l'arrêt « propre » d'une machine, le bail est libéré par le client DHCP qui envoie au serveur un datagramme, unicast, de libération (DHCP RELEASE). Le serveur qui en est propriétaire peut alors proposer cette adresse IP à une autre machine. Néanmoins, la plupart du temps, les serveurs ne le font que lorsqu'ils ne disposent plus de suffisamment d'adresses IP dans une étendue. Généralement, un client a de fortes chances de toujours se voir attribuer la même adresse IP, car le serveur garde en mémoire le mappage entre l'adresse IP et l'adresse MAC du client qui en disposait.

RENOUVELLEMENT : LE BAIL ATTEINT 50% DE SA DUREE DE VIE

Le client émet un DHCP REQUEST, mais en unicast à destination du serveur DHCP propriétaire de l'adresse IP.

Il y a alors trois cas possibles :

- Le serveur répond par un DHCP ACK, en unicast également. Dans ce cas, le bail est renouvelé et le compteur de durée est remis à zéro.
- Le serveur répond par un DHCP NACK, toujours en unicast. Dans ce cas, le bail n'est pas renouvelé. Le fait de ne pas renouveler le bail peut être dû à plusieurs causes : le serveur a été réinitialisé et n'a plus d'informations sur les baux ou l'administrateur du serveur veut libérer cette adresse IP pour la réserver ou l'attribuer à une autre machine. Le client retentera sa chance au 7/8^{ième} du bail.

- Le serveur ne répond pas. Le cas est identique à celui de la réception d'un DHCP NACK. Le serveur peut avoir changé d'adresse IP, être momentanément indisponible, ou un problème réseau ne permet pas de le joindre.

RELIAISON : LE BAIL ATTEINT 87.5% DE SA DUREE DE VIE

Le client envoie un DHCP REQUEST, mais en broadcast IP (255.255.255.255), donc à tous les serveurs DHCP.

Si un serveur répond et renouvelle le bail, le compteur de durée est remis à zéro. Sinon, le client recommencera toute la procédure au début lorsque la durée de vie du bail aura atteint 100%.

Options DHCP

- CODE 1 : Masque de sous-réseau
- CODE 3 : Routeur
- CODE 6 : Serveurs DNS
- CODE 15 : Nom de domaine DNS
- CODE 44 : Serveurs WINS
- CODE 46 : Type de nœud NetBIOS
- CODE 47 : Etendue NetBIOS
- CODE 51 : Durée du bail
- CODE 58 : Durée de renouvellement (T1)
- CODE 59 : Délai de reliaison (T2)

Les options DHCP permettent de fournir au client des paramètres supplémentaires autres que la simple adresse IP. Les options sont définies par des codes. En voici les principales :

- CODE 1. Spécifie le masque de sous-réseau associé à l'adresse IP louée. Si cette option n'est pas indiquée, le client utilisera le masque de sous-réseau par défaut de la classe d'adresse.
- CODE 3. Fournit l'adresse IP du routeur, de la passerelle par défaut. Si rien n'est spécifié, le client ne pourra contacter que des machines locales, présentes dans le même sous-réseau IP. L'adresse fournie doit obligatoirement être dans le même sous-réseau IP que l'adresse louée.
- CODE 6. Spécifie la liste des adresses IP des serveurs DNS.
- CODE 15. Indique le nom de domaine DNS que doit utiliser le client. Associé au nom d'hôte de la machine, il permettra d'obtenir le FQDN (Full Qualified Domain Name).
- CODE 44. Fournit les adresses IP des serveurs WINS primaire et secondaire.
- CODE 46. Cette option permet d'indiquer au client la méthode de résolution de noms NetBIOS qu'elle utilisera. La résolution de noms NetBIOS consiste à faire correspondre un nom avec une adresse IP. Deux méthodes sont utilisées : le broadcast et le serveur de noms NetBIOS (WINS). Il existe quatre variantes, représentées par quatre valeurs :
  - ➔ 0x1 pour B-Node. Le client utilisera uniquement la diffusion, le broadcast, afin de résoudre les noms NetBIOS.
  - ➔ 0x2 pour P-Node. Le client utilisera uniquement WINS pour la résolution de noms.

- ➔ 0x4 pour M-Node. Le client utilisera d'abord la diffusion pour résoudre les noms. Si celle-ci échoue, le client tente trois fois, il utilisera WINS.
- ➔ 0x8 pour H-Node. Le client utilisera d'abord WINS pour résoudre les noms. Si cela échoue, il utilisera la diffusion.

Cette option s'applique à l'ensemble des adresses louées à une même machine. Elle ne peut s'appliquer individuellement pour chaque adresse.

- CODE 47. Fournit l'identifiant d'étendue NetBIOS. L'étendue NetBIOS permet de segmenter un réseau NetBIOS. Seules les machines ayant le même ID pourront communiquer entre-elles. La valeur par défaut est 0.
- CODE 51. Précise, en secondes, la durée totale du bail de l'adresse louée.
- CODE 58. Délai de renouvellement. Précise, en seconde, l'intervalle entre l'affectation d'une adresse et le renouvellement de celle-ci par le client. Par défaut cette valeur est égale à 50% de celle de la durée totale du bail.
- CODE 59. Délai de reliaison. Précise, en seconde, l'intervalle entre l'affectation d'une adresse et la tentative de reliaison de celle-ci par le client. Par défaut cette valeur est égale à 87,5 % de celle de la durée totale du bail.

Relais DHCP

Relais DHCP

- Relais DHCP : machine mandataire entre les clients et les serveurs (proxy DHCP)
- Principe :
  - Le client envoie une requête DHCP
  - Le proxy l'intercepte et la relaye au(x) serveur(s) DHCP configuré(s)
  - La réponse du serveur est transmise au client, etc.

Les mécanismes d'attribution des baux de DHCP s'appuient essentiellement sur la diffusion.
Or, les routeurs ne transmettent pas les diffusions. Cela revient à dire qu'il faudrait un serveur DHCP par réseau physique ou par VLAN, ce qui est bien évidement difficilement envisageable. L'alternative existe : l'utilisation de relais DHCP.

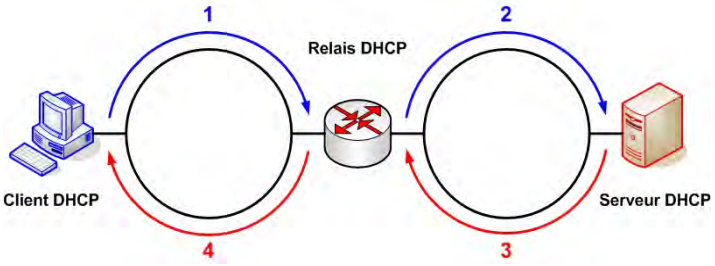
RELAIS DHCP

Un relais DHCP est une machine, un routeur la plupart du temps, qui va servir de mandataire entre les clients d'un réseau et le ou les serveurs DHCP.
Le principe est simple : le relais est configuré avec les adresses IP des serveurs, il intercepte les demandes des clients et les transforme en unicast à destination des serveurs. De la même façon, il relaye la réponse des serveurs aux clients. Cette fonctionnalité exploite l'option 82 de DHCP.

Souvent, dans les réseaux modernes, ce sont les commutateurs de niveau 3, de distribution, qui assurent ce rôle. En effet, ils sont en contact direct avec tous les VLANs définis localement, ce qui permet une simplification de configuration et du dépannage.

Relais DHCP

Relais DHCP



1. Le client émet une requête cliente DHCP
2. Le relais DHCP l'intercepte et la transmet au serveur DHCP
3. Celui-ci répond au relais DHCP
4. Le relais DHCP transmet la réponse au client initial

Prenons un schéma simple afin d'analyser les étapes de fonctionnement d'un relais DHCP. Le routeur est ici le relais DHCP :

1) Le client émet une requête cliente DHCP DISCOVER en broadcast IP (255.255.255.255).
2) Le routeur intercepte la requête DHCP, qui est facile à reconnaitre car le port source est UDP 68 (réservé à l'usage des clients DHCP) et le port destination est UDP 67 (réservé aux serveurs DHCP). De plus, l'adresse IP source est 0.0.0.0 (réservée aux clients DHCP qui n'ont pas encore obtenu d'adresse IP) et la destination 255.255.255.255, ce qui est caractéristique d'une demande cliente DHCP (DHCP DISCOVER).
   Ensuite, le routeur modifie la requête en ajoutant son adresse IP en tant que mandataire et le réseau source sur lequel il a reçu la requête. Ces informations sont importantes car cela permet aux serveurs de connaitre l'existence du mandataire, et, surtout, de savoir quelle étendue devra être utilisée pour le bail. Les serveurs, dans le cas d'utilisation de mandataires, gèrent autant d'étendues qu'il y a de réseaux physiques ou de VLANs.
3) Les serveurs répondent au mandataire, en unicast.
4) Celui-ci relaye la réponse au client, et ainsi de suite pour les opérations suivantes.

Redondance DHCP : règle des 80/20

- Le principe est de disposer d'une redondance d'adresses
- Chaque serveur dispose de plusieurs étendues, une par réseau IP
- Les étendues des serveurs sont complémentaires pour chaque réseau IP
- Chaque serveur sera principal ou secondaire pour chaque étendue
- Généralement on affecte 80% des adresses au serveur principal pour une étendue et 20% au secondaire

Les serveurs DHCP ne communiquent pas entre eux. Ce qui pose le problème de la redondance. Si le serveur gérant une étendue de réseau n'est plus disponible, les clients concernés ne pourront plus obtenir d'adresse dynamiquement.

Pour palier cette faiblesse, il existe deux techniques : les clusters et la règle du 80/20. Ces deux techniques peuvent d'ailleurs être utilisées en concordance.
Commençons par la règle des 80/20.

PRINCIPE DE LA REGLE DES 80/20

Le principe de cette règle consiste à créer deux étendues d'un même sous-réseau IP sur deux serveurs différents. Ces deux étendues ne doivent pas se chevaucher pour des raisons de duplication d'adresses. Les deux étendues seront actives simultanément.

MISE EN APPLICATION

Pour chaque sous-réseau IP on désigne :

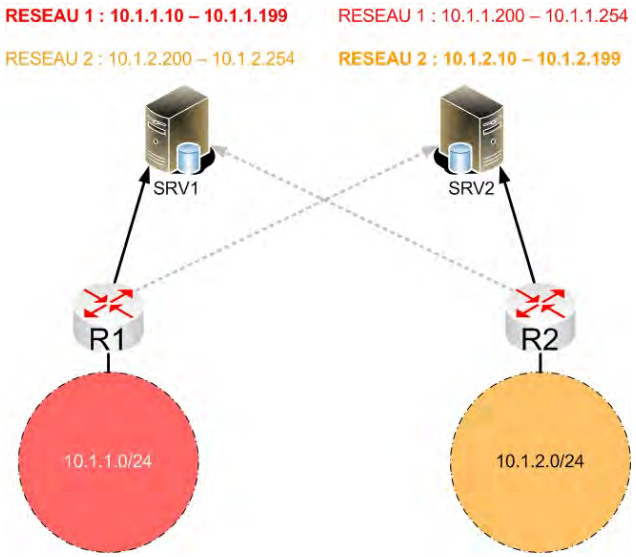
- Un serveur principal. Son étendue contiendra 80% des adresses IP distribuables pour le sous-réseau IP.
- Un serveur secondaire. Son étendue contiendra 20% des adresses IP distribuables pour le sous-réseau IP.

Afin de garantir, en plus de la redondance, de la répartition de charge statique, on répartit les rôles de principal et secondaire entre les deux serveurs. Il est à noter le rôle principal ou secondaire n'est pas une fonctionnalité explicite de DHCP. C'est la configuration des serveurs et des relais qui allouera, de facto, ces rôles.

Cette règle est surtout intéressante lorsqu'il y a utilisation de relais DHCP, comme nous allons le voir dans l'exemple suivant.

Exemple

Exemple



Prenons l'exemple suivant : nous disposons de deux serveurs DHCP centralisés, de deux routeurs faisant office de relais DHCP, et de deux sous-réseaux IP 10.1.1.0/24 et 10.1.2.0/24.
R1 est connecté au réseau 10.1.1.0/24 et R2 au réseau 10.1.2.0/24.

CONFIGURATION DES SERVEURS

SRV1 possède deux étendues :

- Une pour le réseau 10.1.1.0/24 : les adresses 10.1.1.10 à 10.1.1.199. SRV1 sera le serveur DHCP principal pour ce réseau.
- Une pour le réseau 10.1.2.0/24 : les adresses 10.1.1.200 à 10.1.1.254. SRV1 sera le serveur DHCP secondaire pour ce réseau.

SRV2 possède deux étendues :

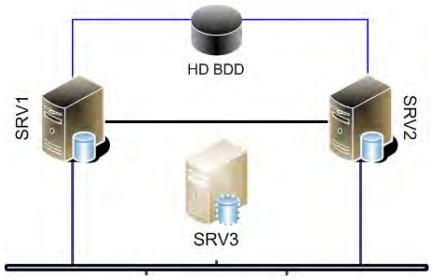
- Une pour le réseau 10.1.1.0/24 : les adresses 10.1.1.200 à 10.1.1.254. SRV2 sera le serveur DHCP secondaire pour ce réseau.
- Une pour le réseau 10.1.2.0/24 : les adresses 10.1.1.10 à 10.1.1.199. SRV2 sera le serveur DHCP principal pour ce réseau.

CONFIGURATION DES ROUTEURS

R1 est configuré avec, comme serveur principal, SRV1 et comme serveur secondaire SRV2. Il n'interrogera ce dernier qu'en cas d'absence de réponse de SRV1.

R2 est configuré avec, comme serveur principal, SRV2 et comme serveur secondaire SRV1. Il n'interrogera ce dernier qu'en cas d'absence de réponse de SRV2.

Cluster DHCP



- Le principe consiste à simuler un serveur virtuel supporté par deux serveurs physiques
- Chaque serveur, y compris le virtuel, possède son propre nom et sa propre adresse IP
- Une seule et même étendue est configurée sur les deux serveurs physiques
- Un seul serveur est actif, l'autre est en passif
- La règle des 80/20 est applicable aux clusters

L'autre solution de tolérance de panne est le cluster DHCP.

PRINCIPE DU CLUSTER

Le principe consiste à simuler un serveur virtuel supporté concrètement par deux serveurs physiques. Il faut pour cela disposer d'un applicatif spécifique fournissant cette fonctionnalité. Il en existe une multitude pour Windows et Linux/Unix.

Pour une application donnée, un des deux serveurs sera actif et l'autre sera passif. Le passif basculera en actif uniquement en cas de défaillance de l'autre serveur.

Les deux serveurs disposent de la même étendue, identique. Comme un seul serveur est actif, il n'y a pas de risques de duplication d'adresses.

Les clients accèderont uniquement à ce serveur virtuel. Les relais DHCP seront également configurés pour utiliser uniquement l'adresse IP virtuelle. Dans notre exemple, les clients « verront » uniquement le serveur SRV3.

MISE EN PRATIQUE

Chaque serveur dispose de deux cartes réseaux :

- Une carte est connectée à un réseau dédié à la signalisation entre les serveurs. Cette signalisation qui permet la détection des défaillances et le basculement des serveurs.
- Une carte est connectée au réseau de production par lequel les clients contactent les serveurs.

Les serveurs utilisent un disque dur externe partagé, mais auquel accède uniquement le serveur qui est actif. Ce disque contient la base de données DHCP ainsi que les logs d'audit du service. Lors du basculement, le serveur devenu actif prend la main sur le disque.

- *VoIP*
- *Codec*
- *RTP*
- *RTCP*
- *H323*
- *SIP*
- *MGCP*

8

VoIP

Objectifs

Ce module traite de la voix sur IP, la VoIP.

Connaissances

- VoIP
- Codecs
- RTP
- RTCP
- H323
- SIP
- MGCP

Progression

Présentation	Gigue
Principes	RTP
Numérisation de la voix	RTCP
Codecs	H323
Contraintes de la VoIP	SIP
	MGCP

Présentation

Présentation

- La Voix sur IP (Voice over IP, VoIP) consiste à transporter des flux audio sur IP
- IP n'est pas prévu, à l'origine, pour le transport de la voix et de la vidéo
- Les réseaux informatiques ne sont pas prévus non plus pour le transport du temps réel
- Il faut des protocoles spécifiquement adaptés pour palier les insuffisances de IP
- Il faut utiliser des techniques de QoS permettre au réseau de supporter les contraintes de la VoIP

PRINCIPES

- Le principe de la VoIP, Voice over IP, ou encore de la voix sur IP, est de transporter des flux audio sur IP.
- Les flux voix et vidéo requièrent des délais de propagation garantis, des délais peu variables, et des débits garantis.
- Or, IP n'est pas prévu à l'origine pour le transport des données en temps réel, en particulier de l'audio et de la vidéo. IP ne peut garantir en natif des délais de transmission, des variations de délais et un débit.
- Les réseaux locaux informatiques ne sont pas non plus prévus pour le transport du temps réel. Tout comme les réseaux télécom n'étaient pas adaptés à l'origine pour le transport des données informatiques. Ethernet, qui est la topologie très largement dominante, ne peut garantir que des données ont bien été transmises… quand aux conditions, elles sont inexistantes.

SOLUTIONS

- Pour qu'un réseau informatique puisse garantir un débit, un délai d'acheminement et une variation de la transmission (la gigue) minimale, il faut mettre en place des mécanismes de qualité de service ou QoS (Quality of Service).
- Pour que IP puisse transporter dans de bonnes conditions de la voix et de la vidéo, il faut utiliser des protocoles adaptés, spécifiques à cette tâche. Ces protocoles existent : RTP et RTCP.

Numérisation de la voix

Numérisation de la voix

- Pour numériser de la voix, on utilise un codec (codeur/décodeur)
- Le codec convertit un signal analogique en signal numérique et vice-versa
- Les codecs utilisés en VoIP sont à échantillonnage
- Pour le codage, l'amplitude du signal est mesurée à intervalles réguliers et convertit en échantillons numériques
- Pour le décodage, on procède en sens inverse : les échantillons permettent de reconstituer le signal original
- Il existe différents codecs, fournissant différents compromis entre la qualité de numérisation et le volume des échantillons

PRINCIPES

- On ne peut pas transporter de la voix telle quelle sur un réseau, il faut la numériser au préalable, utiliser un codec.
- Un codec, codeur/décodeur, est un algorithme qui convertit un signal analogique en signal numérique et vice-versa.
- Les codecs utilisés en VoIP sont à échantillonnage : l'amplitude du signal est mesurée à intervalles réguliers et convertie en données, en échantillons numériques.
- La qualité de la numérisation dépend :
  - ➔ De la fréquence d'échantillonnage
  - ➔ Du spectre pris en compte
  - ➔ De la précision de l'échantillonnage
- Pour le décodage, on procède en sens inverse : les échantillons reçus permettent de reconstituer le signal original.
- De nombreux codecs existent, nous nous intéresserons uniquement à ceux utilisés en VoIP actuellement. Un codec est toujours un compromis entre la qualité de numérisation et le volume des échantillons générés.
- On utilise un indice, le MOS, afin d'évaluer la qualité d'un codec. Le score va de 1 à 5, avec l'échelle suivante :
  - ➔ 4 à 5 : Haute Qualité
  - ➔ 3,5 à 4 : Qualité commerciale
  - ➔ 3 à 3.5 : Qualité acceptable
  - ➔ 2,5 à 3 : Qualité militaire
  - ➔ <2,5 Qualité synthétique

CODEC PCM

- Le codec PCM, Pulse Code Modulation, est le premier à avoir été normalisé pour les télécoms pour le système téléphonique.
- Il utilise un échantillonnage sur 8 bits à une fréquence de 8000Hz, soit une fois toutes les 128µs.
- Pour une seconde de voix, nous avons donc : 8*8000=64.000=64kbits. Il faut disposer d'une bande passante garantie de 64kbits/s pour acheminer correctement un flux voix codé en PCM.
- Deux variantes existent de cet algorithme :
  - ➔ Loi A pour l'Europe et l'international
  - ➔ Loi µ pour les USA et le Japon
- Le but des codecs en VoIP est de réduire la bande passante nécessaire avec une perte de qualité acceptable. Il existe pour cela trois techniques :
  - ➔ La réduction de la fréquence d'échantillonnage, ce qui engendrera fatalement une perte en qualité restituée.
  - ➔ Utiliser moins de bits pour chaque échantillon, donc réduire la précision de l'échantillonnage. Cela entrainera également une baisse de la qualité audible.
  - ➔ Compresser les données. Le prix à payer est l'apparition d'un délai variable supplémentaire.

CODECS VoIP

Ci-dessous figurent les codecs les plus utilisés en VoIP. Sont précisés :

- La norme du codec ;
- Le score MOS. Ces valeurs peuvent légèrement varier selon les sources ;
- Les débits supportés. Certains codecs peuvent fournir des qualités, et donc des débits, différents ;
- Le temps de conversation représenté par un paquet ;
- Le codec G711 utilise directement le codage PCM.

CODEC	SCORE MOS	DEBIT kbit/s	TEMPS/ PAQUET ms
G.711	4,2	64	10
G.722	3,6	48 56 64	1,5
G722.1	3,6	24 32 16	20
G723.1	3,7 3,9	6,4 5,3	30
G.729	4	8	10

Contraintes de la VoIP

Contraintes de la VoIP

- Garanties temporelles :
  - Délai de transmission
  - Décalage de transmission (gigue ou jitter)
- Garantie de fiabilité moindre que pour les données standard
- Garantie de bande passante disponible
- Un réseau informatique n'est pas isochrone par défaut, contrairement au réseaux téléphoniques traditionnels
- Solutions pour IP :
  - Horodatage : a quel moment « présenter » le paquet
  - Numéros de séquence : éviter les doublons, traiter les paquets dans l'ordre d'émission

GARANTIES

Le transport de la VoIP nécessite un certain nombre de garanties pour fonctionner correctement en IP sur un réseau informatique :

- Des garanties temporelles :
  - ➔ Un délai de transmission garanti, autrement une conversation sera difficile à maintenir, à cause des décalages perceptibles.
  - ➔ Un décalage de transmission, la gigue ou le jitter, le plus faible possible, ou du moins le plus constant possible. Une gigue trop importante provoquera une dégradation dans la qualité de la voix.
- Une garantie de fiabilité moindre que celle des données informatiques standards. Les codecs supportent tous, à différents niveaux, un taux de perte faible mais pas nul. Il est parfois plus adapté de détruire un faible pourcentage de données, mais garantir une gigue acceptable.
- Une garantie en bande passante faible mais impérieuse, eu égard aux performances des réseaux actuels. Autrement dit, une congestion réseau aura un impact quasi-immédiat sur la qualité de la transmission.

ISOCHRONISME

- Les réseaux téléphoniques traditionnels possédaient une architecture isochrone : tous les éléments du réseau pouvaient garantir une transmission des données au même débit que celui de l'émission.
- Les réseaux locaux informatiques ne sont pas isochrones nativement, il faut donc suppléer à cette faiblesse en adoptant des solutions spécifiques à IP :
  - ➔ L'horodatage. Basé sur NTP, il permet d'avoir un marqueur temporel lors de l'acheminement des paquets voix à travers le réseau.

- ➔ Le séquencement des données. Les buts sont les suivants : éviter les doublons et garantir un traitement en réception dans l'ordre correspondant à celui de l'émission.

Ces deux fonctions sont fournies par le protocole RTP.

Gigue

Gigue

- Solution : Playback Buffer ou Jitter Buffer, tampon permettant de compenser la gigue
- Principe :
  - Le récepteur stocke les données dans le buffer jusqu'à un certains seuil (playback point)
  - Quant le seuil est atteint, le récepteur commence à émettre
  - Permet de « lisser » les effets de la gigue

Une des solutions simples pour limiter l'effet de la gigue est l'utilisation de la technique dite du Playback Buffer ou Jitter Buffer. C'est un tampon permettant de compenser les effets de la gigue.

Le principe est le suivant :

- Le récepteur stocke les données reçues dans le buffer jusqu'à atteindre un certain seuil. Ce seuil peut être fixe ou dynamique selon les techniques de QoS et les protocoles utilisés.
- Quant le seuil est atteint, le récepteur commence à émettre.
- Cette technique permet le lissage des effets dus à la variation des délais, la gigue.

RTP

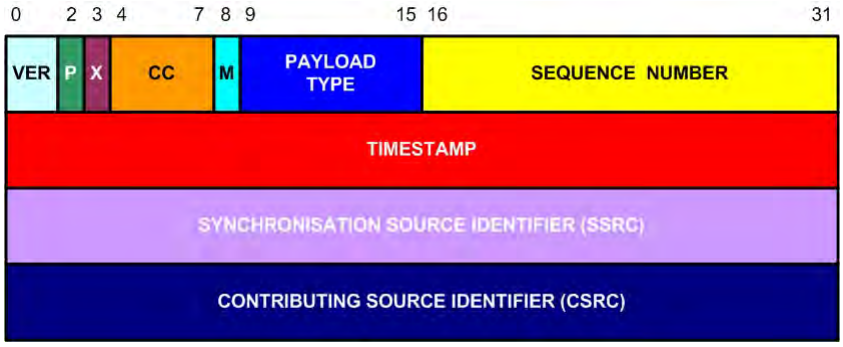
RTP

- Real-Time Transport Protocol
- Protocole utilisé pour transporter des données audio et vidéo sur IP
- Deux fonctions essentielles fournies par RTP : Séquencement des données et Horodatage
- RTP permet le mixage, la combinaison en un seul de plusieurs flux de données de différentes sources
- Attention, RTP ne fournit aucune garantie temporelle
- RFC 1889

- RTP, Real-Time Transport Protocol, est utilisé pour transporter des données audio et vidéo sur IP.
- RTP fournit deux fonctions essentielles :
  - ➔ Le séquencement des données, afin de permettre la détection des pertes de paquets et des erreurs de séquence par le récepteur ;
  - ➔ L'horodatage, afin de pouvoir limiter les problèmes de gigue et de délais.
- RTP permet le mixage, la combinaison en un seul de plusieurs flux de données de différentes sources. On peut utiliser des concentrateurs, des mixeurs. Il faudra pour cela être capable d'identifier l'émetteur et les sources des flux.
- Attention, RTP ne fournit aucune garantie temporelle, c'est le réseau qui doit s'en charger. Autrement dit, sur les réseaux locaux, ce sera le rôle de la politique de QoS.
- RTP utilise UDP, le port 5004 lui ayant été assigné. Néanmoins, il est possible d'utiliser n'importe quel port dynamique. En général, on utilise un numéro de port pair pour RTP et un numéro de port impair pour RTCP.
- RTP est défini dans la RFC 1889.

RTP

En-tête RTP



- VERSION. La version actuelle est la 2.
- SEQUENCE NUMBER. Numéro de séquence du paquet. Le premier numéro est aléatoire.
- X : indique, s'il est positionné, qu'il y a une extension entre l'en-tête et la charge utile.
- PAYLOAD TYPE. Type de charge utile (codes assignés par l'IANA/ICANN) :
  - ➔ AUDIO
    - ✓ 0 PCM loi µ
    - ✓ 8 PCM loi A
    - ✓ 9 G.722
    - ✓ 4 G.723
    - ✓ 15 G.728
    - ✓ 18 G.729
  - ➔ VIDEO
    - ✓ 34 H.263
    - ✓ 31 H261
- P : padding, utilisation de bit de bourrage si à 1. Dans ce cas, le dernier octet de RTP indique le nombre d'octets de bourrage utilisés. Par exemple en cas de cryptage, les opérations se font sur des blocs de taille fixe.
- M : mark. Permet de marquer, de repérer, un endroit particulier dans un flux de données. Par exemple, en début de chaque trame vidéo.
- TIMESTAMP : marqueur temporel ou horodatage. Utilise NTP.
- CC : CSRC Count indique le nombre d'identifiants de CSRC dans l'en-tête. Il est possible d'en avoir un maximum de 15.

- SSRC : indicateur de source de synchronisation. L'émetteur réel ou le mixeur.
- CSRC : indicateur de source contributive. Utilisé en cas de mixage de flux afin d'identifier les émetteurs originaux. Ce champ n'est pas utilisé par SIP et H323.

RTCP

RTCP

- RTP Control Protocol
- Permet de surveiller la qualité de la distribution des données :
  - Qualité de transmission
  - Statistiques
  - Participants de la session
  - Contrôle des information
- L'émetteur envoie des sender reports (SR)
- Le récepteurs envoie receive reports (RR)
- RTCP fournit une signalisation de contrôle out-of-band
- Utilise un numéro de port UDP impair

- RTP Control Protocol
- Protocole de signalisation permettant de surveiller la qualité de la distribution des données. La transmission en temps réel nécessite la surveillance du réseau.
- RTCP fournit les informations suivantes :
  - ➔ Qualité de transmission
  - ➔ Statistiques
  - ➔ Participants de la session
  - ➔ Contrôle des informations
- L'émetteur envoie des messages sender reports (SR) au récepteur à intervalle régulier afin de fournir une indication d'horodatage absolue au récepteur.
- Le récepteur envoie des messages receive reports (RR) à l'émetteur à intervalle régulier, qui fournissent des informations sur les conditions de réception des données.
- Le contrôle est de type out-of-band, hors bande, ce qui permet d'utiliser des algorithmes adaptatifs. Il est ainsi possible d'adapter dynamiquement le débit du codage et la taille des tampons en cas de congestion ou de problème sur le réseau.
- Utilise un numéro de port UDP impair.

H323

Standards H323

- Signalisation end-to-end
- Rôles : Initiation, négociation, établissement, maintient et fermeture d'une connexion
- Standard ITU
- Version actuelle : 6
- Orienté conférence interactive
- Développé pour les environnement connectionless, les LANs
- Flexible
- Complexe

- H323 est un ensemble de protocoles fournissant une signalisation end-to-end, développé et standardisé par l'ITU (International Telecommunication Union).
- H323 définit comment combiner plusieurs protocoles distincts afin de disposer d'un système téléphonique opérationnel.
- Ils viennent compléter RTP, qui est très pauvre en signalisation pour établir des connexions évoluées ou faire de la ToIP (Telephony over IP).
- Le rôle de H323 est de permettre l'initiation, la négociation, l'établissement, le maintien et la fermeture d'une connexion.
- La première version date de 1996, la dernière (la sixième) date de 2006.
- H323 a été développé pour la gestion des conférences interactives dans des environnements hors connexion, de type LAN.
- Ses principaux avantages sont sa maturité et sa flexibilité.
- Son principal défaut est sa complexité.

Composants de H323

Composants de H323

- H225.0 signalisation d'appel
- H245 contrôle et retour d'information (feedback) en cours d'appel
- RTP transfert de données en temps réel :séquencement et horodatage
- T.120 échange de données associées à un appel
- T.38 : fax
- Utilise les port UDP 1718, UDP 1719 et TCP 1720

Les protocoles composants l'architecture H323 sont les suivants :

- H225.0. C'est le protocole chargé de la signalisation d'appel et d'enregistrement. H225.0 utilise pour cela respectivement les protocoles Q931 et RAS (Registration Admission Status).
- H245. Protocole de la signalisation de contrôle de connexion.
  - ➔ Ouverture du canal de contrôle
  - ➔ Etablissement du canal de transmission
  - ➔ Négociation des paramètres (codecs notamment)
  - ➔ Contrôle de flux
  - ➔ Fermeture du canal de contrôle
- RTP, qui est utilisé, comme nous l'avons vu, pour permettre le transport de données en temps réel sur les réseaux hors connexion. Il fournit :
  - ➔ Le séquencement des paquets
  - ➔ L'horodatage des paquets
- T.120 : Spécifications pour l'échange de données lors des conférences.
- T.38 : Relais des communications pour les fax.
- Les ports utilisés en standard sont les suivants :
  - ➔ UDP 1718 pour Gatekeeper Discovery
  - ➔ UDP 1719 pour Gatekeeper Registration
  - ➔ TCP 1720 pour H225 (Call Setup)

Composants de H323

Architecture H323

- Terminaux : éléments permettant d'émettre et de recevoir des appels
- Gatekeeper : localisation des utilisateurs, gestion et contrôle des communications
- Gateway : passerelle permettant l'interconnexion avec d'autres environnements : RNIS, RTC, ATM.
- MCU (Multipoint Control Unit) : gestion de conférences.

L'architecture H323 définit quatre entités :

LES TERMINAUX

Les terminaux sont les éléments permettant aux utilisateurs d'émettre et de recevoir des appels. Il en faut un minimum de deux pour établir une communication.
Un terminal doit respecter les points suivants :

- Support des protocoles H225.0 et H245.
- Support de G.711. Optionnellement, il peut supporter d'autres codecs.
- Support des liaisons asymétriques : utilisation de codecs différents en émission et en réception.
- Support optionnel du multicasting.

GATEKEEPER

Ou garde-barrière. Elément facultatif de l'architecture H323. Cet élément est chargé :

- De la localisation des utilisateurs. Notamment la conversion entre les alias et les adresses IP. Pour les utilisateurs hors réseau IP, on peut également utiliser les adresses téléphoniques de type E164, une adresse URL, une adresse IP associée à un numéro de port.
- De la gestion et du contrôle des communications :
  - ➔ Contrôle d'admission.
  - ➔ AAA : Authentication Authorisation Accounting. Permet d'authentifier un utilisateur, de lui accorder des autorisations et d'enregistrer des événements qui lui sont associés.
  - ➔ Gestion des coûts.
  - ➔ Services d'annuaire.

- ➔ Gestion des appels et des services associés. Transferts d'appels, restrictions, mise en attente, limitations horaires…
- ➔ Historique des appels.
- ➔ Statistiques d'utilisation.

GATEWAY

Une passerelle est chargée de l'interconnexion avec les autres environnements téléphoniques : RNIS, RTC et ATM.

MCU

Multipoint Control Unit. Ou pont multipoint. Cet élément est chargé de la gestion des conférences, c'est-à-dire des communications multimédia à plusieurs intervenants. Trois modes existent :

- Centralisé, en unicast
- Décentralisé, en multicast
- Hybride, unicast et multicast

SIP

SIP

- Session Initiation Protocol
- Protocole de signalisation end-to-end
- Standard IETF
- Fonctionne avec les protocole HTTP et SMTP
- Protocoles associés : SAP & SDP
- Utilise les ports TCP et UDP 5060
- Conférences interactives et non-interactives
- Plus simple et plus évolutif que H323, moins mature

- SIP, Session Initiation Protocol, est le protocole de signalisation téléphonique end-to-end standard de l'IETF.
- SIP gère aussi bien les conférences interactives que non-interactives.
- Un de ses atouts est de pouvoir s'intégrer avec d'autres protocoles standards, notamment :
  - ➔ RTP / RTCP.
  - ➔ RTSP (Real-Time Streaming Protocol), qui permet de contrôler la diffusion de flux multimédias en temps réel.
  - ➔ SDP (Session Description Protocol). Fournit les paramètres, la description, utilisés dans une communication SIP.
  - ➔ SAP (Session Advertisement Protocol). Utilisé pour les communications multicasts.
  - ➔ MIME, pour la description des contenus.
  - ➔ RSVP (Resource Reservation Protocol). Protocole de réservation de bande passante.
  - ➔ HTTP. Ce qui permet d'inclure directement des adresses SIP dans des pages WEB.
  - ➔ MGCP (Media Gateway Control Protocol).
- SIP utilise les ports TCP et UDP 5060.
- SIP est plus simple et plus évolutif que H323, mais moins mature.

MGCP

MGCP

- Media Gateway Control Protocol
- Standard IETF
- Permet l'interopérabilité entre les protocoles de signalisation
- Permet la signalisation de contrôle entre les passerelles
- RFC 2705
- Utilise les ports UDP 2427 et UDP 2727

- MGCP, Media Gateway Control Protocol, permet la communication entre les passerelles (gateway). Le fait qu'il existe désormais des protocoles de signalisation concurrents, à savoir H323 et SIP, pose le problème de l'interopérabilité.
- MGCP permet de faire communiquer entre eux des réseaux utilisant H323, SIP ou SS7 (signalisation des réseaux téléphoniques des opérateurs).
- MGCP est un standard de l'IETF. Il est défini par la RFC 2705.
- MGCP utilise les ports UDP 2427 et UDP 2727.
- Un usage récent est le contrôle des boitiers multiservices des opérateurs Internet, les fameuses box.

- *Firewalls*
- *Proxies*
- *IDS*
- *Corrélation*
- *VPN*
- *IPSec*
- *Traduction d'adresses*

9

Sécurité

Objectifs

Ce module traite de la sécurité réseau.

Connaissances

- Niveaux de sécurité
- Sécurité réseau
- Les firewalls
- Les proxies
- IDS
- Le NAT
- Le PAT
- IPSec
- L2TP

Progression

Les bases de la sécurité réseau

Les éléments de la sécurité réseau

La traduction d'adresse

Les VPNs

Les VPDNs

Problématiques de la sécurité

- Se protéger de qui ?
  - Déterminer le degré d'exposition de l'entreprise, de l'organisation ou de l'administration
  - Quelles sont les motivations potentielles des pirates ?
- Protéger quoi ?
  - L'infrastructure, les systèmes et les applications
  - Les données
- A quel prix ?
  - Déterminer le ratio entre la protection des données et le coût intrinsèque des données
  - Les types de coûts :

    Ponctuels : achat, mise à jour du matériel et des logiciels

    Récurrents : personnel, audit…

Quelles sont les problématiques de la sécurité informatique ? Quelles sont les questions qu'il se faut se poser ?

SE PROTEGER DE QUI ?

Dans un premier temps, il faut essayer de déterminer contre qui on essaye de se protéger. Tenter d'évaluer le degré d'exposition de l'entreprise. Plus une entreprise est exposée, plus grand est le risque qu'elle soit piratée. Pour cela, il faut tenter de déterminer les motivations potentielles des pirates.

Les motivations potentielles des pirates peuvent être classées en trois grandes catégories :

- La motivation pseudo-intellectuelle. C'est en réalité de l'orgueil pur et simple. C'est une des motivations les plus répandues, une des plus tenaces. Le pirate tente de se prouver qu'il est plus fort que ceux qui ont écrit un logiciel de sécurité, que les responsables de la sécurité, que l'architecte qui a défini la politique de sécurité… Cette catégorie de pirate n'est pas la plus dangereuse en soi, mais peut provoquer des dégâts considérables. On y trouve les faiseurs de virus, les chercheurs de failles, les apprentis pirates, les taggeurs de site, les vengeurs masqués…
- La motivation vénale. Un moteur de motivation très puissant. L'argent constitue le noyau principal des pirates dans le monde. Ce ne sont pas forcément les plus exposés médiatiquement. Ce sont les voleurs de numéros de cartes bancaires, de code d'accès, de détournements de tous bords, les spécialistes du phishing… Aujourd'hui, les plus dangereux sont structurés autour d'organisations mafieuses très organisées et très puissantes.

- La motivation idéologique. La catégorie la plus dangereuse. On y trouve les pirates les plus extrêmes. Ce sont également les plus incontrôlables. Cela peut aller des anti-OGM jusqu'aux fanatiques religieux ou politiques de tous bords.

PROTEGER QUOI ?

Une entreprise se doit de protéger ce qui est aujourd'hui devenu un outil de travail à part entière, son système d'information. Cela englobe :

- Les éléments d'infrastructure : commutateurs, routeurs, firewalls, proxies… Si l'accès aux serveurs est inopérant, l'accès aux données l'est également.
- Les systèmes d'exploitation. Un plantage ou des failles dans la sécurité peuvent entrainer des dysfonctionnements dans les applications ou rendre les données vulnérables.
- Les applications elles-mêmes. Les applications sont les éléments les plus fragiles, car elles ont souvent été, et sont bien souvent encore, développées sans souci de sécurisation particulier. On a longtemps cru que sécuriser l'infrastructure et les systèmes était suffisant pour protéger les applications. Il n'en est rien, et les attaques actuelles les plus courantes le démontrent : phishing, SQL injection, attaques DNS, spam SMTP, attaques http…
- Les données. C'est le but final de la sécurité, faire en sorte que seuls les utilisateurs habilités aient accès aux données, qu'elles ne soient pas détruites par malveillance, altérées volontairement… On recourt de plus en plus à la protection directe des données : sauvegardes multiples et systématiques, cryptage, audit…

A QUEL PRIX ?

Enfin, autre point important, voir parfois capital, le coût de la sécurité. Le but est d'essayer de déterminer le bon ratio entre le coût engendré par la sécurité et la valeur intrinsèque des données protégées. Souvent un gain mineur en sécurité entraine des dépenses qui ne sont plus en adéquation avec cette règle.

Il existe deux types de coûts liés à la sécurité :

- Les coûts ponctuels : achat de matériel, de licences, mises à jour…
- Les coûts récurrents : personnel, audit, conseil…

Buts de la sécurité informatique

Buts de la sécurité informatique

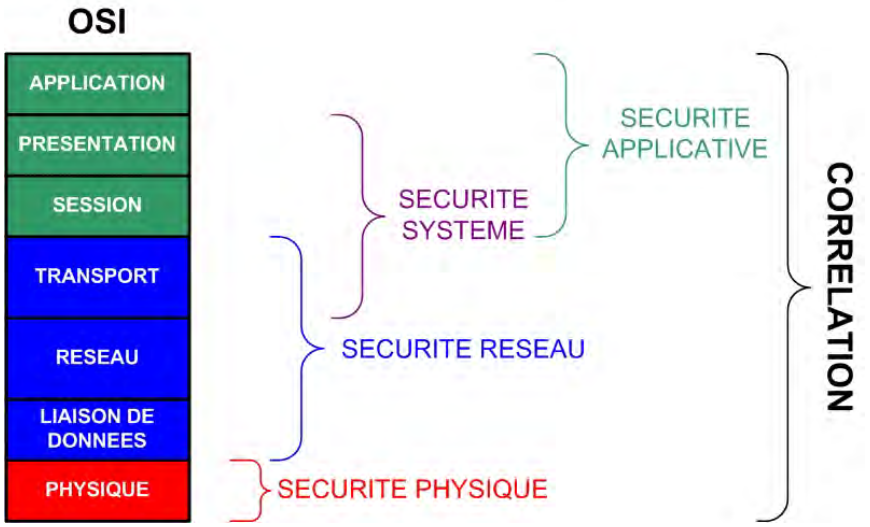
- Protection du matériel
- Protection du réseau
- Protection des systèmes
- Protection des applications
- Protection des données informatiques

BUTS DE LA SECURITE INFORMATIQUE

Les buts de la sécurité informatique sont les suivants :

- La protection du matériel. Ce qui recoupe la protection physique sous toutes ses formes : accès, redondance d'alimentation, protection électrique…
- La protection du réseau. Aussi bien physique que logique : les firewalls, les proxies, les systèmes de détection d'intrusion et les outils de corrélation ont en charge cette tâche essentielle de la sécurité.
- La protection des systèmes. Cela passe par les anti-virus, les firewalls personnels, les sondes HIDS, les stratégies systèmes…
- La protection des applications. La plus difficile, car il existe une double problématique :
  - ➔ Les logiciels propriétaires sont très difficilement modifiables. Le niveau de sécurisation dépend bien souvent de l'éditeur.
  - ➔ Les logiciels libres sont eux beaucoup plus faciles à modifier, mais ils doivent rester compatibles, ce qui limite le champ d'action.
- Enfin, la protection des données elles-mêmes. La marge de manœuvre est beaucoup plus grande en local. La difficulté réside surtout dans leur transport à travers le réseau, et plus particulièrement à travers Internet, ce qui sera du ressort des techniques VPNs.

Niveaux de sécurité



Il existe globalement quatre niveaux de sécurité correspondant chacun à des objectifs de la sécurité informatique et un niveau connexe qui est la corrélation.

SECURITE PHYSIQUE

La sécurité physique correspond à la couche physique du modèle OSI.

La sécurité physique regroupe tous les moyens protégeant l'accès aux ressources informatiques sensibles : serveurs, firewalls, routeurs, commutateurs…

Les moyens utilisés :

- Vérification visuelle d'identité
- Clés d'accès
- Cartes d'identification
- Biométrie

SECURITE RESEAU

La sécurité réseau englobe les couches liaison de données, réseau et transport. Les buts de la sécurité réseau sont :

- Authentification : vérification de l'identité des partenaires. Très souvent, on y associe les fonctions d'audit et les droits et autorisations des utilisateurs authentifiés.
- Intégrité : empêcher toute modification des données durant leur acheminement.
- Confidentialité : les données ne doivent être accessibles en clair que par le(s) destinataire(s).

Moyens de protection utilisés :

- Firewalls
- Systèmes d'authentification : RADIUS, Kerberos, TACACS+, PAP, CHAP, EAP…
- Technologies de cryptage
- Détecteurs d'intrusions (IDS et HIDS)
- VPN et VPDN

SECURITE SYSTEME

La sécurité système regroupe les couches transport à présentation.

Le but de la sécurité système est d'empêcher l'utilisation non conforme du système d'exploitation.

Les utilisations non conformes sont :

- Utilisation de droits système non autorisés
- Usurpation d'identité
- Violation des règles de fonctionnement
- Récupération de données protégées
- Utilisation de services non conforme
- Blocage ou corruption du système

Les moyens de protections utilisés :

- Configuration avancée du système et des services
- Stratégies des droits utilisateurs
- Stratégies d'accès
- Stratégies d'audit
- Anti-virus

SECURITE APPLICATIVE

La sécurité applicative s'étend de la couche session à la couche application.
La sécurité applicative est chargée de protéger le fonctionnement des applications.
Les attaques visent à rendre une application inopérante ou à en perturber fortement le fonctionnement.

Les attaques sont basées sur les éléments suivants :

- Faiblesse d'écriture des applications
- Complexité croissante des fonctionnalités
- Mauvaise configuration
- Activation de services ou de fonctionnalités automatiques
- Mauvais respect des règles de sécurité de la part des utilisateurs

Moyens de protections utilisés :

- Anti-virus
- Configurations strictes et systématiques
- Sensibilisation des utilisateurs
- Technologies de cryptage applicatives (PGP, SSL…)

- Firewalls applicatifs

CORRELATION

Un des problèmes de la sécurité informatique est que nous disposons d'outils plus ou moins efficaces pour chacun de ces niveaux, mais ces outils communiquent peu ou mal entre eux. Et encore, parfois des outils d'un même niveau ne communiquent pas du tout entre eux. Cela s'améliore lentement mais insuffisamment.

Une évolution importante de ces dernières années a été l'apparition des outils dits de corrélation. Un outil de corrélation est capable d'analyser les informations remontant des différents éléments de sécurité, des systèmes et des applications, et de les corréler afin de tenter de reconnaitre une attaque, qui ne serait pas détectée individuellement par les éléments précédemment cités.
Certaines informations prises isolément, par les éléments de sécurité, ne déclencheront aucune alarme. Elles ne seront pas considérées comme critiques. En établissant des relations entre ces informations non critiques, les outils de corrélation vont être en mesure de détecter les attaques les plus structurées, les plus dangereuses.
Les seuls freins à l'utilisation de ces outils sont leur coût et la complexité de leur déploiement.

Généralement, les informations recueillies proviennent :

- Des systèmes d'exploitation
- Des applications
- Des firewalls
- Des sondes de détection d'intrusion
- Des routeurs
- Des anti-virus

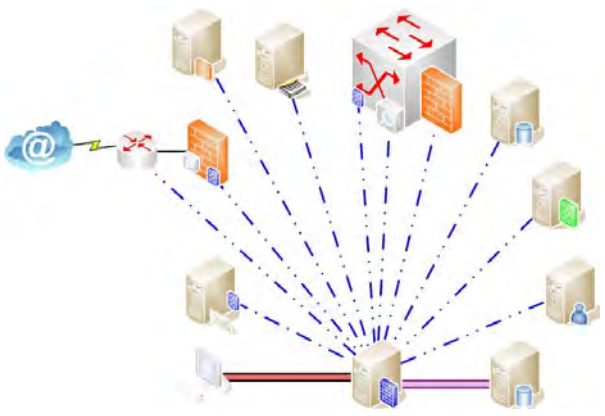
La détection peut provoquer soit une simple alerte, soit une action conséquente :

- Modification temporaire des règles de filtrage des firewalls
- Suspension de services ou d'applications
- Modification du fonctionnement d'un système d'exploitation
- Blocage de l'acheminement de certaines données

Composants d'un système de corrélation :

- Un gestionnaire ou collecteur central
- Une base de données contenant les données analysées ainsi que les rapports
- Des sources d'information :
- Des remontées d'informations via SNMP
- Des connecteurs spécifiques
- Des clients propriétaires
  ✓

Correlation



Les firewalls

Les Firewalls

- Un firewall a les caractéristiques suivantes :
  - C'est un filtre réseau entre plusieurs réseaux
  - Il contrôle uniquement le trafic qui le traverse
  - C'est, à la base, un élément discret du réseau
  - Il existe sous forme applicative et sous forme embarquée
- Le fonctionnement, polarisé, s'appuie sur des règles
- Il existe trois générations de firewalls
  - Première génération : firewalls statiques
  - Deuxième génération : les proxies
  - Troisième génération : firewalls statefull

CARACTERISTIQUES PRINCIPALES

Un firewall est un élément d'infrastructure du réseau. Présent maintenant dans la quasi-totalité des entreprises, il est le rempart de sécurité minimum pour se protéger des attaques provenant d'Internet. Son utilisation est quasiment exclusivement réservée à TCP/IP.

Son rôle essentiel est le filtrage réseau. Un firewall vérifie, contrôle le trafic en provenance et à destination d'un ou de plusieurs réseaux, ou VLANs, qui le traverse (un firewall n'a pas de rôle au sein d'un réseau). Actuellement, les firewalls sont également capables de vérifier le fonctionnement de certaines applications standard mais en aucun cas le contenu applicatif.

Un firewall, à la base, était un élément discret du réseau. Ce n'est plus le cas aujourd'hui car les fonctionnalités qui lui ont été attribuées ne sont plus les mêmes qu'il y a quelques années.

Les firewalls existent sous deux formes :

- ➔ Applicative. Dans ce cas, il est installé sur un système d'exploitation préexistant. Il est fortement conseillé, voir pour certains produits obligatoire, de dédier la machine à cette fonction. C'est sous cette forme que les firewalls sont les plus évolutifs et les riches en fonctionnalités. Ils sont, en revanche, généralement moins performants que les systèmes embarqués.
- ➔ Embarquée. Sous cette forme, le firewall se présente sous la forme d'un boitier intégrant. :
  - ✓ Un système d'exploitation dédié ou spécifique ;
  - ✓ Le firewall lui-même ;

- ✓ Des composants dédiés à certaines tâches spécifiques : coprocesseurs mathématiques, processeurs de cryptage, d'analyse…

Cette forme de firewalls est la plus performante, mais, bien souvent, la moins évolutive.

FONCTIONNEMENT

Le fonctionnement d'un firewall est polarisé. Généralement, on définit des niveaux de sécurité pour chacun des réseaux que l'on veut sécuriser :

- ➔ Le trafic d'un réseau de niveau de sécurité forte vers un niveau de sécurité inférieur est dit sortant ;
- ➔ Le trafic d'un réseau de niveau de sécurité faible vers un niveau de sécurité supérieur est dit entrant ;
- ➔ Souvent, par défaut sur de nombreux firewalls, tout le trafic sortant est autorisé et tout le trafic entrant est interdit.

Le fonctionnement de base d'un firewall s'appuie sur des règles testées séquentiellement, et ce, pour chaque datagramme susceptible d'être transmis à travers lui.

Il existe deux catégories de règles :

- ➔ Prédéfinies, variables selon les éditeurs. Ce sont les règles génériques qui sont normalement valables sur tous les réseaux. Par exemple, une adresse source ne peut pas être une adresse de broadcast ou de multicast.
- ➔ Manuelles, définies par l'administrateur.

On utilise quatre types de règles :

- ➔ Trafic entrant autorisé
- ➔ Trafic entrant interdit
- ➔ Trafic sortant autorisé
- ➔ Trafic sortant interdit

Une règle possède deux composants :

- ➔ Une ou plusieurs conditions de test ;
- ➔ Une action. L'action n'est exécutée qu'en cas de correspondance de toutes les conditions d'une règle. Si ce n'est pas le cas, le firewall passe à la règle suivante. Il existe deux actions principales :
- ➔ PERMIT. Le datagramme est autorisé à transiter.
- ➔ DENY. Le datagramme n'est pas autorisé à transiter, il est donc détruit.

Le filtrage peut s'appuyer sur divers paramètres de test :

- ➔ Les adresses IP source et destination
- ➔ Les ports source et destination
- ➔ Le contenu de certains champs spécifiques
- ➔ Les protocoles de niveau 4 utilisés
- ➔ La reconnaissance des modes opératoires de certaines applications

Le filtrage peut être réalisé de deux façons, selon le rôle que joue le firewall dans le réseau :

- ➔ Tout ce qui n'est pas explicitement autorisé est interdit. L'administrateur devra donc édicter les règles adéquates. La plupart des firewalls actuels procèdent de cette manière. Quand un nouveau filtre est créé, par défaut la dernière règle est un DENY ANY.
- ➔ Tout ce qui n'est pas explicitement interdit est autorisé. On procède ainsi en plaçant un PERMIT ANY en dernière règle.

Un filtre bien écrit possède toujours au moins un PERMIT et un DENY.

Il faut positionner les règles les plus précises avant les règles les plus générales, autrement elles ne seront jamais appliquées.

Dans la mesure du possible, il faut essayer de positionner le plus haut les règles les plus populaires. Le but étant d'améliorer le temps de traitement des datagrammes par le firewall.

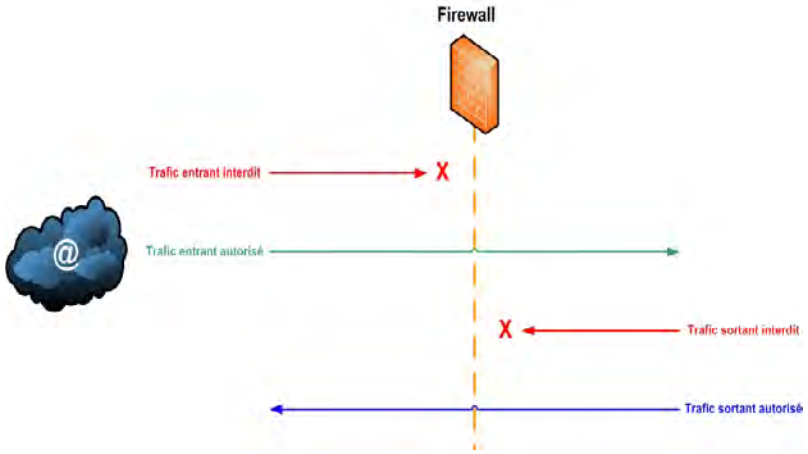
GENERATIONS DE FIREWALLS

Il existe trois générations de firewalls :

- ➔ Première génération : firewalls statiques. Complètement obsolètes, il fallait explicitement autoriser tout trafic entrant et sortant. Lents et peu sûrs.
- ➔ Deuxième génération : les proxies. Ils subsistent car ils sont complémentaires de la génération de firewalls actuelle, la troisième.
- ➔ Troisième génération : firewalls statefull. Ces firewalls fonctionnent en « dynamique », ils sont capables de mémoriser les états des sessions afin d'adapter au mieux leur action. Ils sont capables, par exemple, d'ouvrir et de fermer dynamiquement les ports de la couche transport selon l'antériorité ou non d'une demande de connexion.

Exemple

Exemple



Dans cet exemple, nous avons la topologie réseau la plus simple : un réseau interne et Internet. Dans ce cas, le firewall doit contrôler :

- Les datagrammes sortants. Ils ont pour source le réseau interne et pour destination Internet. Généralement, les routeurs appliquent cette règle par défaut. Il est bien évidemment possible d'ajouter des règles afin de limiter les flux applicatifs entre les deux réseaux.
- Les datagrammes entrants. Ils ont pour source Internet et destination le réseau interne. Généralement, par défaut, les routeurs ont une règle qui interdit ce trafic inconditionnellement.

Fonctionnalités des firewalls

- Un firewall peut avoir deux rôles principaux :
  - Internet
  - Interne
- Il existe plusieurs niveaux de sécurité :
  - Le réseau interne a toujours le niveau de sécurité le plus élevé
  - Internet a toujours le niveau de sécurité le plus faible
  - Des niveaux de sécurité intermédiaires : les DMZ (zones démilitarisées)
- Fonctionnalités des firewalls :
  - Filtrage
  - Traduction d'adresses
  - Connexions VPNs
  - Redirections/Publications

ROLES DES FIREWALLS

Un firewall peut avoir deux rôles principaux :

- Firewall Internet : il est généralement placé entre le routeur de connexion à Internet et le réseau interne. Son rôle sera de protéger le réseau interne contre les éventuelles attaques provenant d'Internet. C'est le rôle tenu par la grande majorité des implémentations.
- Firewall interne : il est au cœur du réseau interne et contrôle les flux de données échangées sur les différents réseaux, ou les différents VLANs de l'entreprise. De plus en plus, il est présent sous forme de carte d'extension des commutateurs backbone.

NIVEAUX DE SECURITE

Le niveau de sécurité attribué à un réseau peut être explicite ou non pour un firewall. Néanmoins, c'est ce qui caractérise généralement sa sensibilité. L'affectation de ces niveaux permettra une écriture plus évidente des règles de filtrage.
En effet, le principe général est d'interdire tout ce qui n'est pas autorisé par défaut pour les flux de données entre un niveau de sécurité faible et un niveau de sécurité fort, plus élevé. A l'opposé, on autorise par défaut ce qui n'est pas explicitement interdit entre un niveau de sécurité fort et un niveau de sécurité faible, inférieur.
Il existe plusieurs niveaux de sécurité :

- Le réseau interne a toujours le niveau de sécurité le plus élevé. On l'appelle aussi Zone Militarisée (MZ, Military Zone).
- Le réseau extérieur (souvent Internet) a toujours le niveau de sécurité le plus faible. On le nomme également Dirty DMZ (Demilitarized Zone).

- Il peut y avoir des niveaux de sécurité intermédiaires : les DMZ (zones démilitarisées).

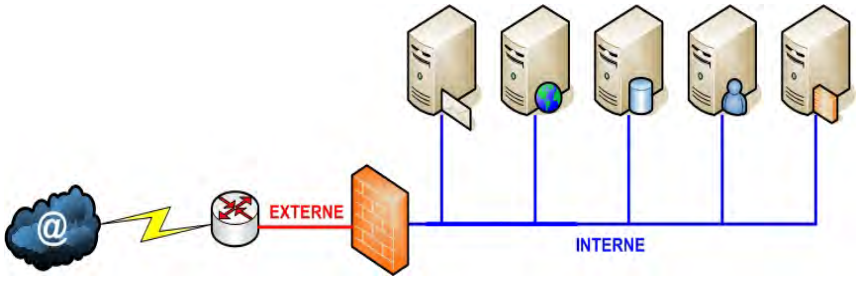
FONCTIONNALITES

Les firewalls actuels assument de nombreuses fonctionnalités :

- Filtrage, la fonctionnalité de base.
- Traduction d'adresse. Ces techniques permettent de traduire une adresse interne en adresse externe. Pour l'accès Internet par exemple.
  Il existe trois techniques de traduction :
  - ✓ Le NAT, traduction des adresses une à une.
  - ✓ Le PAT, traduction avec une adresse extérieure unique et mappage de ports.
  - ✓ Le SAT, ou NAT statique, mappage en dur entre une adresse externe et une adresse interne.
- Les connexions VPNs. Les VPNs permettent l'échange sécurisé entre deux entités IP. Les firewalls sont de plus en plus utilisés comme extrémité des tunnels VPNs pour les accès externes.
- Redirections / Publications. Cette fonctionnalité permet de rendre un serveur interne accessible depuis l'extérieur. On parle de publication lorsque les ports ne sont pas modifiés et de redirection dans le cas inverse.

Firewall Internet à deux niveaux de sécurité

Firewall Internet à deux niveaux de sécurité



L'architecture la plus simple est constituée d'un seul firewall connectant deux zones :

- La zone interne qui recoupe tous les réseaux internes à l'entreprise.
- La zone externe, représentée par Internet.

La marge de manœuvre est relativement limitée, il est juste possible de définir ce qui est interdit et ce qui est autorisé dans chaque sens.

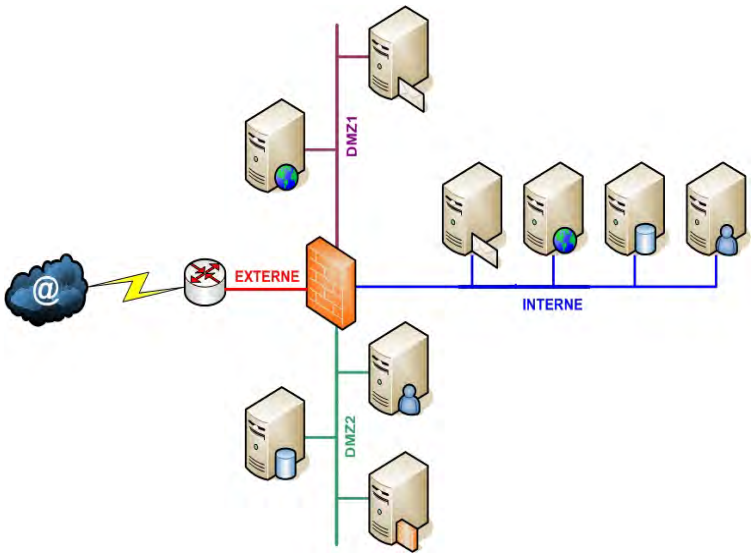
Pour assurer un maximum de sécurité, il est conseillé :

- De tout interdire par défaut et de n'autoriser que le strict nécessaire pour le trafic sortant.
- De n'effectuer aucune publication ou redirection, donc d'interdire tout trafic entrant direct.

Le trafic entrant est le trafic autorisé explicitement par le firewall d'Internet vers le réseau interne.
Le trafic retour est le trafic généré par une requête sortante. Par exemple, si une machine interne tente d'établir une connexion TCP avec un serveur WEB externe, elle émettra un segment SYN, auquel le serveur répondra par un SYN, ACK. Ce dernier ne sera pas considéré comme du trafic entrant, car il existe une demande antérieure interne qui l'a provoqué. En revanche, si un segment SYN, ACK se présente et qu'aucune antériorité ne corresponde à cette réponse, il sera détruit.

Firewall Internet à quatre niveaux de sécurité

Firewall Internet à quatre niveaux de sécurité



L'architecture à plusieurs interfaces, c'est-à-dire quant leur nombre est supérieur à deux, permet d'obtenir des solutions intéressantes.

Nous avons pris ici 4 interfaces, car c'est une solution très répandue :

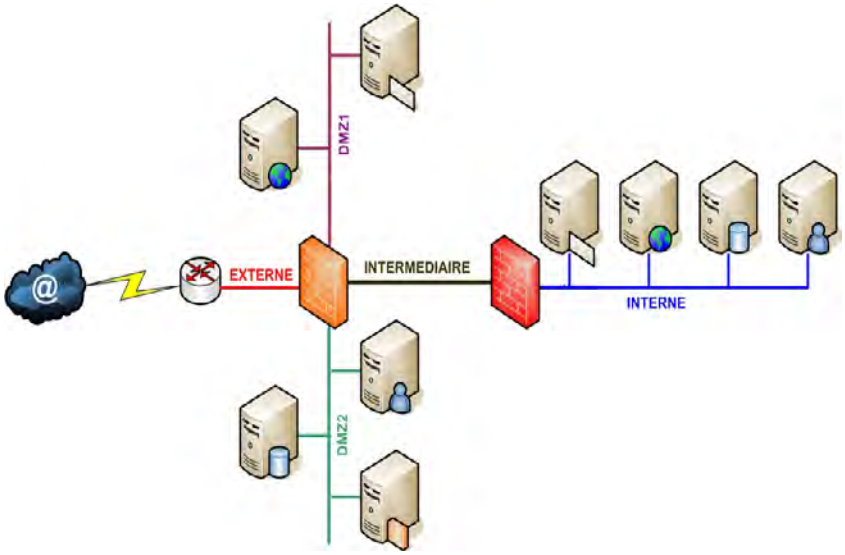
- Une interface interne à laquelle nous attribuerons le niveau de sécurité 100.
- Une interface externe à laquelle nous attribuerons le niveau de sécurité 0.
- Une interface DMZ1 avec un niveau de sécurité 50 contenant le serveur WEB publié et un relais de messagerie.
- Une interface DMZ2 avec un niveau de sécurité 50 contenant un proxy, une base de données et un serveur d'authentification.

Les règles qu'il est conseillé d'appliquer sont les suivantes :

- Par défaut, aucun trafic entre un niveau de sécurité faible vers un niveau de sécurité plus fort. Bien entendu, des exceptions seront autorisées au cas par cas.
- Pas de trafic direct entre Internet et le réseau interne. Plus généralement pas de trafic direct entre le niveau de sécurité le plus faible et le plus fort. La solution idéale est de n'avoir aucune exception.
- Obligation pour les utilisateurs de passer par le proxy afin d'accéder à Internet pour les protocoles http et ftp.
- Les mails entrants sont redirigés par le firewall vers le relais de messagerie.
- Tout autre trafic doit être explicitement autorisé et contrôlé.

Architecture à deux firewalls

Architecture à deux firewalls



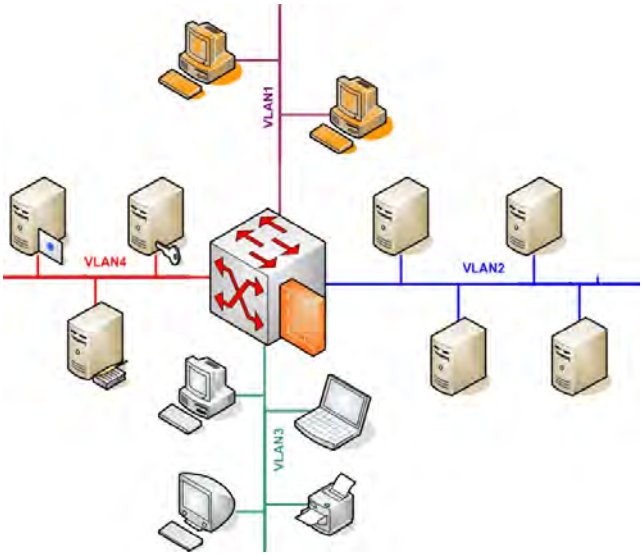
Nous reprenons la topologie précédente en y ajoutant un second firewall, dit intermédiaire, entre le réseau interne et le firewall d'accès Internet. Ce dernier est souvent désigné par externe ou Internet.

Règles conseillées :

- Une règle élémentaire dans ce genre d'architecture : les deux firewalls ne doivent pas être identiques, ils devraient être d'éditeurs ou de fabricants différents. La raison en est simple : une faille éventuelle sera commune aux deux firewalls s'ils sont identiques. C'est un peu comme protéger une salle bancaire avec deux portes blindées identiques, avec des serrures également identiques. Quelqu'un connaissant une faiblesse ou ayant une copie de la clé, ouvrira les deux portes.
- Certaines banques, certaines sociétés exigeant un niveau de sécurité maximal ont jusqu'à 4 ou 5 firewalls alignés de la sorte. Très souvent, on place des sondes d'intrusion sur les réseaux intermédiaires reliant les firewalls.
- Certains architectes préfèrent positionner les serveurs relais sur les réseaux intermédiaires plutôt que sur les DMZ.

Firewall interne

Firewall interne



Les firewalls internes contrôlent les échanges de données entre les réseaux de l'entreprise. Bien souvent dans les topologies actuelles, ce sont les échanges entre les VLANs qui sont contrôlés. N'oublions pas que les firewalls Internet et intermédiaires protègent ce qui est échangé entre Internet et les réseaux internes de l'entreprise. Autrement dit, une attaque réseau initiée en interne ne sera pas détectée par ce type de firewall. Par exemple, un cheval de Troie à partir d'une machine infectée par un mail ou un téléchargement.

Comme le firewall devient à ce moment un élément central de l'infrastructure interne de l'entreprise, ses performances deviennent un paramètre critique. Les fonctionnalités, en revanche, sont moindres que celles des firewalls Internet et intermédiaires.

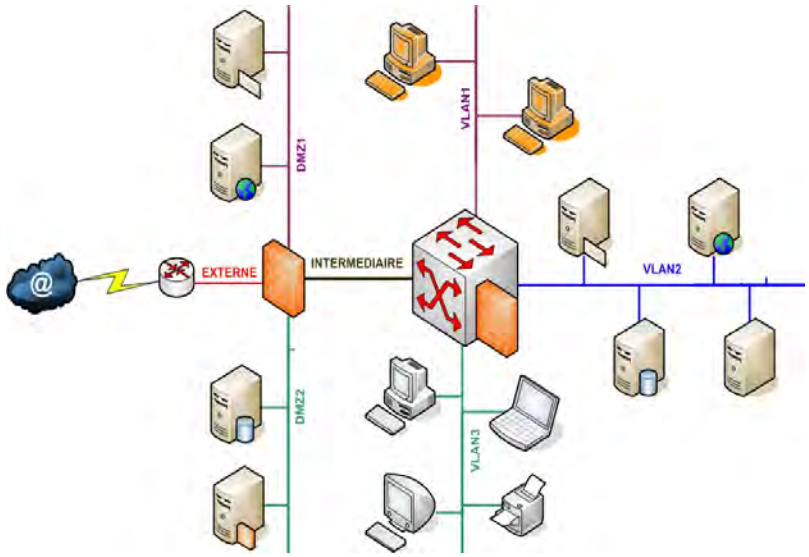
Posons le problème dans les réseaux modernes : comment permettre à un firewall de contrôler tous les échanges entre les VLANs sans constituer un goulet d'étranglement dans le fonctionnement du réseau ? Nous connaissons la réponse pour le routage : l'intégrer dans les commutateurs. La solution est identique pour les firewalls internes, ils sont intégrés sous forme de carte supplémentaire (ou blade) dans les commutateurs fonctionnant au niveau distribution.

Le fait de les intégrer aux commutateurs permet de résoudre le problème du goulet d'étranglement constitué par les interfaces physiques normalisées. En effet, le firewall est relié au réseau, à travers le commutateur, à la vitesse du fond de panier de celui-ci, qui est sans commune mesure avec celles des interfaces standards.

Cela n'implique en rien une amélioration interne, intrinsèque, des performances des firewalls. Pour les mettre à niveau, les constructeurs ont simplifié les fonctionnalités des firewalls internes et augmenté considérablement leur puissance de traitement par forte adjonction de processeurs, de RAM et d'optimisation de traitement.

Architecture intégrée

Architecture intégrée



Pour obtenir un niveau de sécurité élevé, l'idéal est de contrôler tous les échanges entre réseaux ou VLANs. Nous avons ici un exemple d'architecture dite intégrée :

- ➔ Tous les échanges entre les VLANs, en interne, sont contrôlés par le ou les firewalls internes.
- ➔ Tous les échanges entre les réseaux internes et Internet sont contrôlés par le firewall Internet.

Sur le schéma, un seul commutateur et un seul firewall sont représentés, mais en réalité ces éléments d'infrastructure sont doublés afin de disposer d'une tolérance de panne. Les éventuels firewalls intermédiaires n'ont pas non plus été représentés afin de ne pas alourdir le schéma.

Cette architecture fournit un niveau de sécurité réseau élevé, mais est-ce suffisant ? La réponse en clairement non. Un firewall ne peut rien contre une attaque interne à un VLAN par exemple. Rappelons qu'un firewall ne filtre que les flux qui le traversent. Si l'attaque est interne à un réseau ou un VLAN, le firewall ne pourra pas la détecter. Pour compléter les fonctionnalités d'un firewall et augmenter la sécurité réseau, il faut disposer d'un système de détection d'intrusion qui va analyser ce qui se passe en interne dans les réseaux.

Présentation des proxies

Présentation des Proxies

- Un serveur proxy est un mandataire, un agent de relais, qui récupère sur Internet les documents requis par ses clients
- Fonctionne en client/serveur, élément visible du réseau, nécessite la configuration des navigateurs Internet
- Les clients proxy n'accèdent pas directement à Internet, les requêtes sont envoyées au serveur qui les traite et stocke les données dans un cache
- Il existe trois standard de proxy
  - Web Proxy (CERN), le proxy le plus répandu
  - WinSock Proxy, propriétaire Microsoft
  - SOCKS, répandu dans le mode Unix

PRESENTATION

Les proxies sont la deuxième génération de firewalls. Leur installation et leur utilisation perdurent néanmoins, car ses fonctionnalités complètent, plus qu'elles ne concurrencent, les firewalls de troisième génération.

Un serveur proxy est un mandataire, ou agent de relais, qui permet de naviguer sur Internet sans contact direct entre les clients, les navigateurs Internet et les serveurs distants.

Un serveur proxy est constitué de modules :

- Une partie cliente intégrant http, ftp et gopher. C'est ce module qui accède à Internet.
- Une partie serveur fournissant les services http, ftp et gopher. C'est à ce module que se connectent les clients.

Les requêtes http, ftp et gopher sont envoyées par le client au serveur proxy, qui est chargé de récupérer les données demandées et de les transmettre en interne.

Le fonctionnement utilise le principe du client/serveur. Ce qui signifie que les clients, les navigateurs Internet, doivent être configurés explicitement pour utiliser un serveur proxy. De ce fait, celui-ci n'est pas un élément discret du réseau.

Les données récupérées par le proxy sont généralement mises en cache pour une éventuelle demande identique.

Comme un serveur proxy est souvent un point de passage obligatoire pour la navigation Internet, on complète fréquemment ses fonctionnalités en installant des outils tels qu'un anti-virus, un filtre URL…

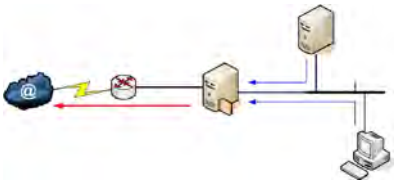
STANDARDS

Il existe trois standards pour les serveurs proxy :

- Web Proxy, ou compatible CERN. En effet, c'est dans les laboratoires du *Conseil européen pour la recherche nucléaire* qu'il a été développé. De loin le plus répandu, souvent intégré dans les navigateurs Internet.
- WinSock, propriétaire Microsoft. Il nécessite l'installation d'un client et de disposer de Proxy Server / ISA Server. Son intérêt réside surtout dans le fait qu'il permette une gestion intégrée aux réseaux Windows et notamment à Active Directory.
- SOCKS, moins répandu que les deux précédents, on le rencontre surtout dans le mode Unix/Linux. La plupart des navigateurs Internet du marché intègrent le client.

Architecture

Architecture



- Deux utilisations possibles :
  - En solo, le serveur proxy est alors le seul rempart entre les réseaux internes et Internet

  - En amont du firewall Internet, ce qui leur permet de se compléter. Généralement il est placé sur une DMZ.

Globalement, deux architectures sont possibles pour les serveurs proxy :

- En solo. Le serveur proxy est en prise directe avec Internet, ce qui signifie qu'il est le seul rempart entre les réseaux internes de l'entreprise et Internet. Cette solution est de plus en plus rarement utilisée. ISA Server de Microsoft n'échappe pas à la règle, car il intègre un serveur proxy ET un firewall de troisième génération.
- En amont du firewall Internet. Généralement, on le place dans un DMZ. Au pire, en interne s'il n'y a pas de zone démilitarisée.
  Dans ce cas, le serveur proxy complètera les fonctionnalités du firewall.
  Celui-ci fournira :
  - ➔ Le filtrage de tout le trafic web
  - ➔ Les fonctionnalités avancées en termes de sécurité
  - ➔ Les services d'accès distant et de VPN.
  - ➔ Le serveur proxy fournira :
  - ➔ Le filtrage et le relais pour les protocoles http, ftp et gopher
  - ➔ Les services de mise en cache
  - ➔ Les éventuels services annexes : anti-virus, filtre URL…

Avantages

- Mutualisation des accès :
  - Un seul point de contact avec Internet
  - Une seule adresse publique nécessaire
  - Utilisation de la bande passante plus efficace
- La structure d'adressage interne est invisible sur Internet
- Filtrage du niveau 3 au niveau 7
- Fonctions avancées de cache
- Contrôle de l'accès par authentification des utilisateurs
- Prise en charge de la publication (*Proxy Reverse*)

Les avantages et fonctionnalités d'un serveur proxy sont les suivants :

MUTUALISATION DES ACCÈS

La mutualisation des accès fournit les avantages suivants :

- Il n'y a qu'un seul point de contact avec Internet. Du point de vue de la sécurité, il est bien évidemment beaucoup plus facile de contrôler et de surveiller un point unique.
- Une seule adresse publique est nécessaire pour l'accès de l'ensemble des internautes.
- L'usage de bande passante est plus efficace et, surtout, elle est plus facile à évaluer et à améliorer.

ADRESSAGE

- Les accès à Internet se font en utilisant l'adresse externe du proxy. Du point de vue d'Internet, il y a un seul client : le serveur proxy. Une seule adresse officielle est donc nécessaire pour permettre l'accès à tous les clients du proxy.
- Cette unicité de contact permet également une configuration plus simple et plus efficace des règles de filtrage des firewalls et de contrôle des sondes IDS.
- De plus, ce mécanisme d'accès masque l'adressage réel des machines clientes. La structure interne d'adresses est donc inconnue, masquée sur Internet. Ce qui est toujours un plus du point de vue de la sécurité.

FILTRAGE

Les serveurs proxy permettent de contrôler les flux de données, du niveau 3 (IP) au niveau 7 (Application). Cela assure un bon niveau de sécurité pour les applications que

prennent en charge les serveurs proxy.
Les possibilités d'évolutions de ces filtres sont un autre avantage :

- Il est possible d'en modifier certains ;
- On peut en créer d'autres ;
- Certaines applications installent leurs propres filtres complémentaires de ceux du proxy. C'est le cas pour les anti-virus et les filtres URL.

CACHE

C'est une des fonctionnalités les plus appréciée des utilisateurs. Les serveurs proxy intègrent un cache qui stocke les pages et les objets déjà chargées sur le disque dur. Ainsi, si deux utilisateurs demandent la même page, un seul chargement sera effectué par le serveur.

Le cache dispose des fonctionnalités suivantes :

- On peut définir les types d'objets autorisés à être stockés, ainsi que leur taille maximale.
- Il est possible de définir un temps de présence maximum absolu ou relatif par type ou par taille de fichiers stockés. Par exemple, un temps absolu de 2 minutes pour les fichiers .jpeg, et un temps relatif de 50% du TTL d'origine pour un fichier .gif. Nous aurons donc les cas suivants :
  - ➔ Si un fichier .jpeg est chargé, sa durée de vie dans le cache sera de deux minutes quelque soit son TTL ;
  - ➔ Si un fichier .gif est chargé avec un TTL de 60s, sa durée de vie dans le cache sera de 30s.
- On peut activer la fonction de mise à jour par anticipation. Le serveur n'attendra pas que le TTL d'un objet soit à 0 pour le mettre à jour.
  On peut définir :
  - ➔ Un pourcentage, par rapport au TTL, à partir duquel le serveur vérifiera l'état de fraicheur d'un objet sur son serveur d'origine. Il vérifiera la date et la taille de l'objet ;
  - ➔ Un intervalle de vérification récurrente ;
  - ➔ Une ou des plages autorisées pour les actions de mise à jour.
- Il est possible de définir les utilisateurs ayant le droit d'utiliser le cache.

Toutes les fonctionnalités ne sont pas disponibles sur tous les serveurs proxy. La liste n'est pas exhaustive, certaines fonctionnalités étant spécifiques à un serveur ou un environnement.

CONTRÔLE D'ACCES

Les serveurs proxy intègrent des fonctions d'authentification.
Généralement, les possibilités sont les suivantes :

- Authentification locale. Par mot de passe en clair ou mieux, via https.
- Authentification centralisée. Dans ce cas le serveur proxy s'appuie sur un serveur LDAP ou, plus rarement, RADIUS pour effectuer cette opération.

- Authentification intégrée. On utilise les mécanismes d'authentification intégrés au système d'exploitation. C'est le cas d'ISA Server avec Windows pour Microsoft et de Border Manager avec NetWare pour Novell.
- Accès invité ne nécessitant pas d'authentification, mais ne disposant d'aucun privilège.

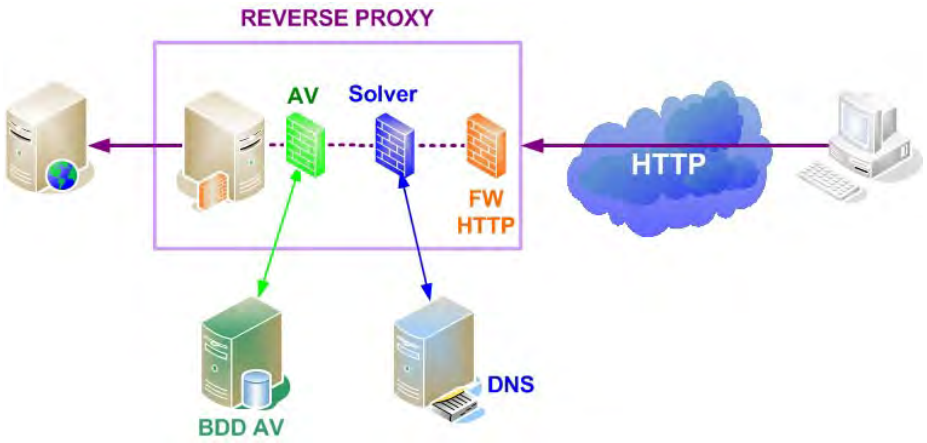
L'authentification peut bien évidemment s'accompagner de restriction sur :

- Les privilèges d'accès
- Les plages horaires d'accès
- Le filtrage des protocoles et des objets
- De filtrage URL
- D'audit des accès…

PUBLICATION

Certains serveurs proxy disposent de la fonction de publication. On les nomme Proxy Reverse. Leur fonctionnement est inversé par rapport à celui d'un serveur proxy « normal » : les clients sont des internautes externes et le serveur web ou ftp est interne.

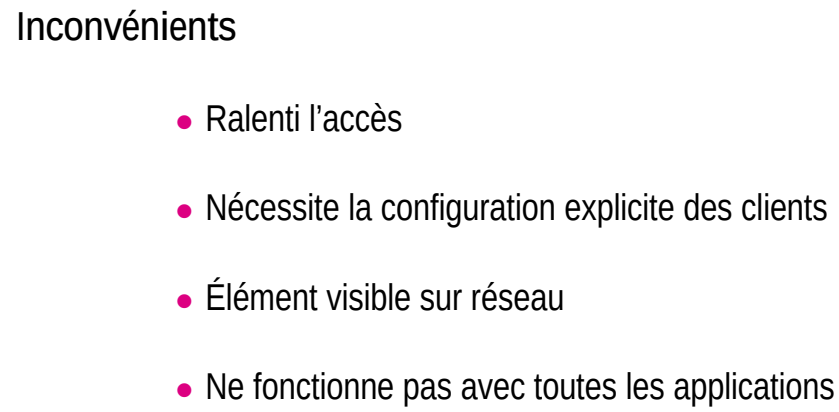
Reverse proxy



Souvent, les reverses proxy intègrent également d'autres éléments permettant de renforcer le niveau de sécurité d'accès au serveur interne :

- Un firewall applicatif http. Ces firewalls dédiés permettent de contrôler les données échangées entre le client et le serveur, et ce, page par page, champs par champs.
- Un client DNS sécurisé (Solver).
- Un anti-virus autonome ou un client compatible avec un standard du marché.

Inconvénients

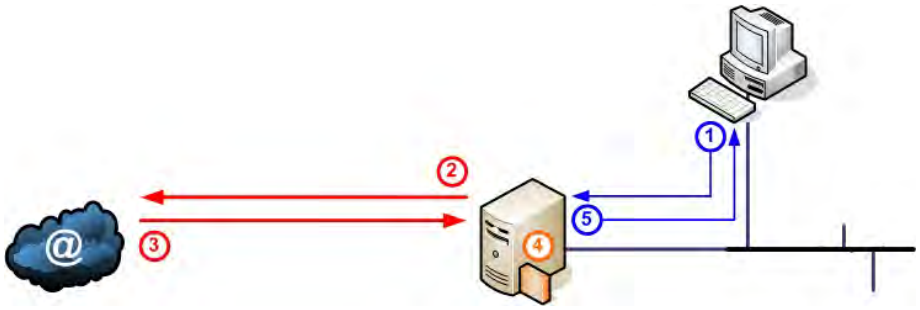


L'utilisation d'un serveur proxy a également quelques inconvénients :

- L'accès Internet peut être parfois plus long qu'un accès direct, dans proxy, ce qui est dû au temps de traitement du serveur. Globalement, avec la puissance des machines actuelles, le gain de temps est quand même en sa faveur.
- Les clients doivent être explicitement configurés et paramétrés, ce qui pour les grands comptes, n'est pas forcément une affaire simple.
- Le serveur proxy, de par sa fonction même, est un élément visible sur le réseau. Il peut donc devenir aisément une cible pour une attaque, interne ou externe.
- Enfin, un serveur proxy ne fonctionne qu'avec trois protocoles : http, ftp et gopher. Pour les autres protocoles, on utilisera les fonctions spécifiques du firewall.

Fonctionnement

Fonctionnement

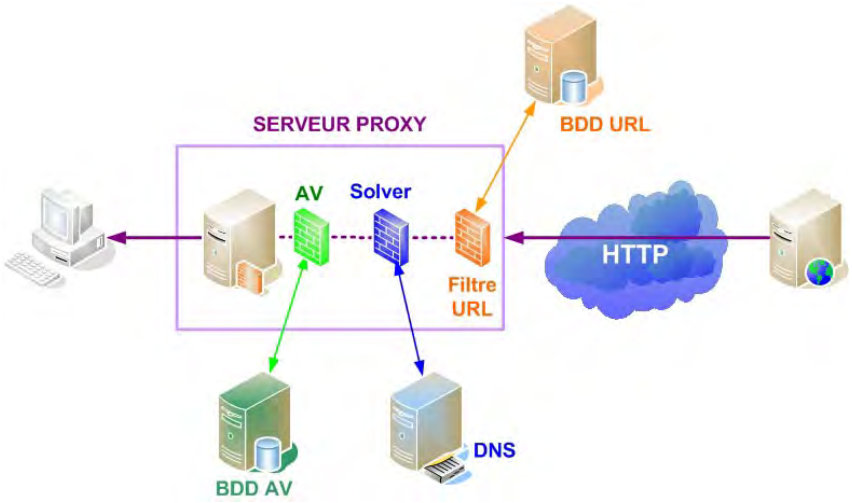


Étudions maintenant les étapes du fonctionnement d'un serveur proxy :

1) Le client émet une requête vers le serveur. En http, on utilise souvent les ports 8000 ou 8080 pour les requêtes clientes, car les ports 80 et 443 sont utilisés pour l'administration du serveur lui-même.
2) Le serveur vérifie que la page ou l'objet demandé(e) n'est pas présent(e) dans son cache. Si ce n'est pas le cas, il le (la) récupère sur Internet.
3) La réponse parvient au serveur.
4) Le serveur enregistre la page, ou le fichier, dans son cache, en conformité avec les règles de fonctionnement définies.
5) La page ou l'objet est transmis(e) au client.

Composants complémentaires

Composants complémentaires



Il est très courant actuellement d'installer des composants complémentaires sur les serveurs proxy. La centralisation de l'accès Internet permet très facilement d'augmenter le niveau de contrôle sur les échanges de données.

ANTI-VIRUS

Généralement, ils sont dédiés et spécifiques à une plate-forme donnée. Ils fonctionnent en mode interception, c'est-à-dire qu'ils contrôlent le contenu des données reçues sur le port d'écoute du serveur. Si le contenu est « propre », il sera transmis au serveur, dans le cas contraire, il est détruit.
Ils se présentent sous deux formes :

- Autonome, complète. Ils fonctionnent comme n'importe quel anti-virus système classique.
- Client. Seul le client est installé, il faut ensuite le configurer pour qu'il aille charger les règles et les signatures virales sur le serveur AV central.

CLIENT DNS SECURISE

Les attaques DNS étant faciles à réaliser et de plus en plus nombreuses, de plus en plus d'éditeurs de produits de sécurité intègrent des clients DNS sécurisés. Ils apparaissent parfois sous le qualificatif d'outil anti-fishing. Ces clients intègrent des routines de contrôle, qui permettent le recoupement des informations en interrogeant plusieurs serveurs DNS, y compris ceux de l'éditeur afin de limiter au maximum les piratages de source (les serveurs) ou d'injection (le pirate répond plus vite à une requête que le serveur DNS) lui-même.

FILTRES URL

Ces programmes permettent de contrôler l'accès aux sites web et ftp des clients du proxy. Ils sont généralement très impopulaires.
Le principe est le suivant : l'éditeur qualifie tout nouveau site créé sur Internet en utilisant un certain nombre de critères, quelques dizaines en général. Citons, par exemple, le type de site (sport, information, jeux, adulte, bourse…), le contenu de violence visuelle, verbale, raciale, érotique…

Il est possible, utilisateur par utilisateur, de définir des règles incluant :

- Les types de sites autorisés
- Les valeurs maximales de chaque critère. Le niveau de violence par exemple.
- Les horaires de validités de chaque règle. Ainsi, selon la tranche horaire, différentes règles s'appliqueront.
  Par exemple, l'accès aux sites de jeux et de sports ne sera autorisé, pour tout le monde, que le matin avant 8h, de 12h à 14h et le soir après 17h.
- La granularité des enregistrements d'activité des utilisateurs…

Enfin, des outils statistiques sont fournis :

- Les sites les plus accédés
- Les types de sites les plus demandés
- La durée moyenne de connexion…

IDS

IDS

- IDS : Intrusion Detection System
- Un système de détection d'intrusion est chargé de détecter des attaques réseaux qui ne peuvent l'être par les autres outils de sécurité
- Un système de détection d'intrusion est composé de trois parties :
  - Des sondes qui analysent en temps réel le trafic réseau
  - Un serveur, ou gestionnaire, qui analyse les informations remontées par les sondes
  - Une base de données contenant les signatures des attaques

PRESENTATION

Un IDS, Intrusion Detection System, est chargé de détecter les attaques réseaux qui ne peuvent l'être par les autres éléments de sécurité. Un anti-virus s'occupe des attaques virales sur les systèmes et les applications, les firewalls contrôlent les flux de données échangés entre les réseaux ou les VLANs.

Mais, si une attaque a lieu à l'intérieur d'un réseau à partir, par exemple, d'un cheval de Troie non encore répertorié par l'anti-virus, le firewall interne ne détectera rien.
Les IDS analysent, précisément, en temps réel ce qui se passe à l'intérieur des réseaux.

COMPOSANTS

Un IDS est constitué des éléments suivants :

- Des sondes d'intrusion, chargées d'analyser en temps réel le trafic du réseau. En général, elles réalisent une première analyse très simple et ne remontent que les informations sur d'éventuels mécanismes suspects. Elles existent sous plusieurs formes :
  - ➔ Boitier dédié, intégrant un OS embarqué, un outil d'analyse réseau et un moteur d'analyse d'attaque.
  - ➔ Intégré au système d'exploitation d'un routeur ou d'un firewall
  - ➔ Sous forme de lame (blade) insérable dans un commutateur modulaire
  - ➔ De logiciels clients installables sur divers OS
- Un serveur, ou gestionnaire, qui analyse les informations que lui remontent les sondes. Cette analyse, plus fine, permet également de procéder à d'éventuels recoupements. Certains gestionnaires ont des fonctions intrusives, c'est-à-dire qu'ils peuvent agir en cas d'attaque sur certains éléments du réseau.

Enfin, les gestionnaires peuvent alerter les administrateurs lorsqu'un événement critique survient sur le réseau.

- Une base de données contenant les signatures d'attaques, similaire à la base des signatures virales existantes sur les systèmes anti-virus. Le serveur y stocke également la plupart du temps les rapports et l'historique des incidents.

Les sondes d'intrusion

Les sondes d'intrusion

- Certaines sondes sont intégrées aux firewalls ou aux routeurs
- Leur objectif est de détecter tout trafic anormal :
  - Un trafic réseau ne correspondant pas aux règles de fonctionnement applicatif
  - Un trafic reconnu comme une intrusion réseau
- Les sondes d'intrusion se basent sur des fichiers de signature d'attaque afin de reconnaître le mode opératoire des intrusions réseau

FONCTIONS DES SONDES

- Les sondes d'intrusion sont des analyseurs réseau très performants. Une sonde peut analyser du niveau 2 jusqu'au niveau 7, pour certaines applications.
  De plus en plus, elles sont intégrées aux routeurs, au firewall ou aux commutateurs modulaires. La raison en est simple et logique : ces éléments constituent l'infrastructure des réseaux, ils permettent un accès simultané à plusieurs réseaux logiques ou physiques.

```
Par exemple, sur un firewall on peut avec une seule sonde intégrée
analyser tous les réseaux (interne, externe, DMZs) auxquels il est
connecté.
Même chose pour un routeur. Si, de plus, ce routeur est lui-même
intégré à un commutateur modulaire, une seule interface, le fond de
panier, permet l'accès à tous les VLANs.
```

- L'objectif principal des sondes est la détection de tout trafic anormal :
  - ➔ Du trafic réseau qui ne correspond pas aux règles et modes opératoires de l'application ou du protocole utilisé ;
  - ➔ Du trafic reconnu comme intrusif. Les sondes s'appuient sur un fichier de signatures d'attaques qu'elles chargent au démarrage ou, lorsqu'une nouvelle version est disponible, sur le gestionnaire central.

Fonctionnement

Fonctionnement

- Les communications entre les sondes et le gestionnaire sont cryptées pour éviter toute interférence, et souvent sur un réseau dédié
- On distingue deux types de systèmes :
  - Les NIDS, qui analysent l'ensemble du réseau
  - Les HIDS, qui sont des systèmes intégrés sur un serveur et qui analysent uniquement le trafic réseau lié au serveur sur lequel ils sont implémentés. Généralement ils sont installés sur des serveurs critiques
- De plus en plus, les détecteurs dialoguent avec les firewalls pour bloquer en temps réel tout trafic suspect
- Les outils de corrélation permettent une approche plus générale encore

COMMUNICATION

- Les communications entre les sondes et le gestionnaire sont, au minimum, cryptées, afin d'éviter impérativement toute interférence, volontaire ou non.
  Une solution complémentaire et très efficace est la mise en place d'un réseau hors production, en parallèle. Sur ce réseau ne transitent que des données administratives ou relatives à la sécurité. Ce réseau peut être un simple VLAN ou, mieux, un réseau câble séparément.

  Les sondes sont connectées aux réseaux via des commutateurs. Les interfaces sur lesquelles elles se connectent doivent être configurées en port mirroring ou port SPAN.

- Pourquoi toutes ces précautions ? Prenons deux exemples :
- Supposons que le gestionnaire et les sondes communiquent entre eux en in-band, c'est-à-dire via le réseau de production. Imaginez une attaque qui sature le réseau, plus aucun trafic ne peut être acheminé en continu. Cela affectera également les échanges entre le gestionnaire et les sondes. Le cryptage garantit la sécurité, pas la disponibilité.
- Supposons maintenant que les communications entre le gestionnaire et les sondes se fassent via un VLAN dédié. Une attaque sature un des commutateurs, ou un des liens, entre le gestionnaire et les sondes. Les communications seront également interrompues. C'est toujours de l'in-band, on utilise toujours les composants physiques du réseau. Le VLAN garantit l'isolation des flux, pas la disponibilité physique du réseau.
- Enfin, prenons la topologie la plus fiable : le réseau physiquement séparé. Dans ce cas, les sondes possèdent deux interfaces réseau :

- Une interface sur le réseau surveillé. Cette méthode est la seule garantissant la discrétion complète sur le réseau de production, car cette interface n'y émet aucun trafic.
- Une interface sur le réseau physique dédié. Toute communication avec le gestionnaire se fera par l'intermédiaire de cette interface.

TYPES D'IDS

On distingue deux types de systèmes IDS :

- Les NIDS, Network IDS, qui analysent l'ensemble du trafic réseau.
- Les HIDS, Host IDS, qui sont des systèmes intégrés sur un serveur. Autrement dit, la sonde, le gestionnaire et la base de données sont intégrés sur le serveur. Ils analysent uniquement le trafic réseau reçu ou généré par leur hôte. On les installe sur des serveurs critiques pour l'entreprise. Pour quelle raison ?
  Supposons l'attaque suivante : un pirate parvient à bloquer le port qu'utilise la sonde pour analyser le trafic réseau. Ensuite, il lance une attaque contre un serveur critique. Que peut faire le NIDS ? Rien, car il ne voit rien. Une alerte sera lancée, mais le temps de réaction sera favorable au pirate.

Remarque :
Une évolution actuelle est apportée par les sondes IPS, qui intègrent une sonde et un outil d'analyse. Ces sondes sont très performantes et fonctionnent en interception, à la différence des sondes IDS « classiques » qui fonctionnent en dérivation. Elles existent principalement sous forme de boîtiers dédiés ou de carte d'extension (de « blade ») pour les routeurs ou les commutateurs.

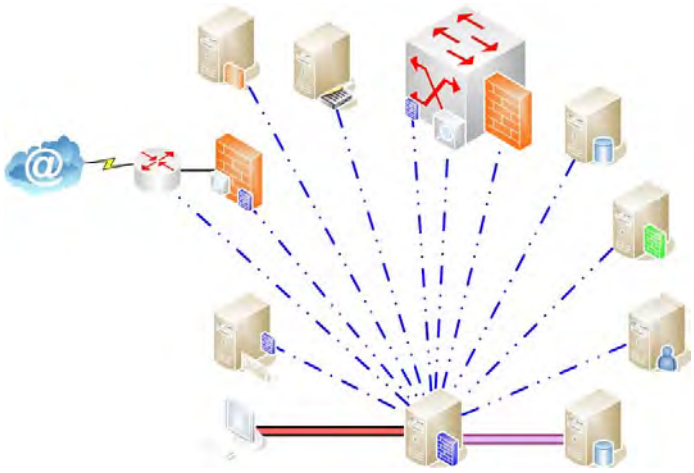
INTERACTION

La tendance actuelle est à l'interaction entre les éléments réseau. Le but est de faire communiquer les IDS avec les firewalls, les routeurs, les commutateurs…

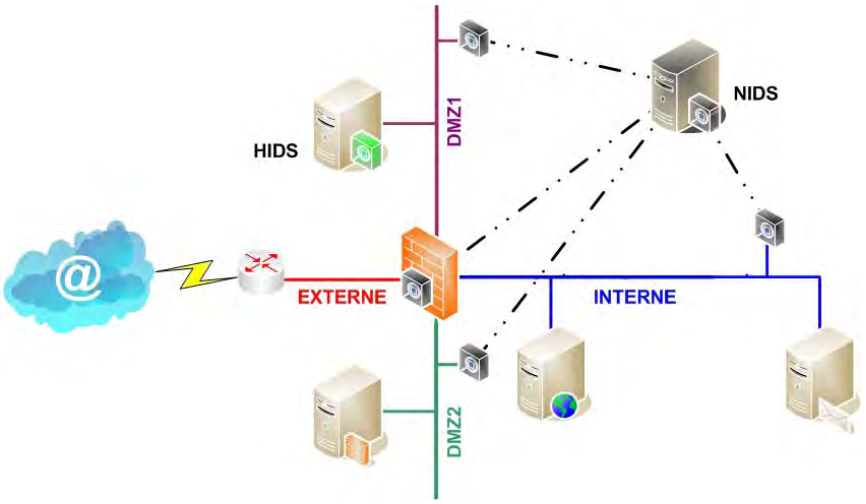
L'interaction entre les IDS et les firewalls est le point le plus important, le plus décisif. Cela permet de bloquer des attaques qui ont une origine externe. Si l'IDS détecte et identifie ce genre d'attaques, il peut la bloquer en remontant l'information au firewall. Il existe déjà des standards de communication entre IDS et Firewalls :

- OPSEC de CheckPoint permet d'interréagir avec les firewalls FireWall-1 et Nokia (FW-1 embarqué).
- CISCO. Permet au matériel… CISCO d'interréagir avec du matériel… CISCO.
- L'IETF travaille sur la normalisation d'un protocole de normalisation entre les éléments de sécurité.

Enfin, les outils de corrélation permettent de centraliser les informations collectées sur les éléments du réseau, les OS, les applications critiques, les anti-virus. Ces puissants outils permettent, comme leur nom l'indique, d'établir des corrélations entre des événements qui, pris individuellement, n'auraient pas une signification critique. Ces outils permettent également de disposer de tout un arsenal pour réagir en cas d'attaque avérée. Le seul frein à leur expansion actuellement, hormis le coût, est la complexité de la mise en place. Mais les évolutions récentes permettent de prévoir une nette amélioration dans ce sens dans les années à venir.



Exemple



Dans cet exemple nous avons un NIDS et un HIDS :

- Le HIDS protège un serveur critique présent sur la DMZ1
- Le NIDS est composé, en plus du gestionnaire et de la base de données non représentée ici, de quatre sondes :
  - ➔ Une sur la DMZ1 où est présent le serveur critique ;
  - ➔ Une sur la DMZ2 où il y a le serveur proxy ;
  - ➔ Une sur le réseau interne ;
  - ➔ Et une sur le firewall, qui peut paraitre redondante, mais qui accroit de façon significative le niveau de sécurité de l'ensemble. Il est en effet possible de faire des recoupements avec les autres réseaux.
- Les sondes et le gestionnaire communiquent via un réseau physique distinct du réseau de production. Ce trafic est également crypté, pour plus de sécurité.

Quelques références

- En Firewall :
  - Embarqués : CISCO PIX, Watchguard, Raptor, Netasq
  - Applicatifs : CheckPoint FireWall 1, Libre : IPChains / IPTable
- En proxy :
  - Microsoft : Proxy Serveur / ISA Serveur
  - Novell : Border Manager
  - Netscape/SUN : Proxy Server
  - Linux, libre : Squid
- IDS :
  - ISS
  - CISCO IDS
  - NFR
  - Libre : Snort

Traduction d'adresses

Définitions

- Le principe de la traduction d'adresse :
  - Une adresse source est traduite en une autre adresse à la traversée d'un élément traducteur
- Les rôles de la traduction d'adresse :
  - Sécurité
  - Extension de l'espace d'adressage
- Les différentes techniques :
  - NAT ou NAT dynamique : adresses traduites une à une, il faut autant d'adresses publiques que d'adresses utilisées simultanément
  - PAT : une seule adresse publique est utilisée, on multiplexe les ports
  - SAT ou NAT statique: une adresse interne est toujours associée à la même adresse publique

PRINCIPE

Le principe de la traduction d'adresses est de mapper une adresse IP source dite interne avec une autre adresse IP dite externe. La plupart du temps, il s'agit d'une adresse IP privée vers une adresse IP publique.

A l'origine, la traduction d'adresses permet d'accéder à Internet avec une adresse IP publique, officielle, tout en utilisant une adresse privée sur le réseau interne.

ROLES

Le premier avantage est évident : il n'est plus nécessaire de posséder autant d'adresses officielles que de postes utilisant Internet, mais autant d'adresses que de connexions simultanées. Or, sur un réseau, de par le fonctionnement même de HTTP, seule une fraction des machines est réellement connectée à un instant donné.

Ceci permet une extension très importante de l'espace d'adressage :

- D'une part, l'adressage interne n'est plus tributaire de la disponibilité et de la quantité d'adresses publiques disponible ;
- D'autre part, il est possible de définir sa structure d'adresse interne librement : il n'est plus nécessaire de tenir compte des règles d'adressage publiques ;
- Enfin, une modification de l'adressage interne n'a pas d'impact sur l'extérieur.

Autre avantage important, seules les adresses publiques utilisées sont visibles sur Internet, la structure d'adressage interne n'étant pas accessible. Du point de vue de la sécurité ce point est crucial, car cela implique deux conséquences :

- Il est toujours plus difficile d'attaquer un réseau dont on ignore les structures physiques et logiques ;

- Il est aisé de mettre en place un filtre interdisant par défaut tout ce qui veut « entrer » et autoriser ce qui veut « sortir », ce que font les firewalls.

La traduction d'adresse permet donc d'établir une polarisation de l'accès réseau à Internet :

- Le coté publique, peu sûr ;
- Le coté interne, mieux contrôlé et, a priori, plus sûr.

La plupart des firewalls s'appuie sur la traduction d'adresse afin de définir les différents niveaux de sécurité constitutifs d'un réseau d'entreprise.

Pour réaliser la traduction d'adresses, il est nécessaire d'avoir un composant réseau adéquat, qui peut être par exemple :

- Un routeur
- Un firewall
- Un proxy (implicite)
- Un serveur RAS
- Un serveur jouant l'un des rôles précédents

METHODES DE TRADUCTION

Il existe trois méthodes de traduction d'adresse :

- Le NAT, Network Address Translation. C'est la technique du « une à une » : pour chaque adresse privée accédant à Internet, il faut une adresse publique.
- Le PAT, Port Address Translation. Pour cette technique, dite de « plusieurs à une », une seule adresse est utilisée afin de permettre à toutes les adresses internes d'accéder à Internet.
- Le SAT, Static Address Translation, encore appelée NAT Statique. Cette technique consiste à réaliser une réservation d'adresse publique pour une adresse privée. Elle est souvent associée à la publication de serveurs ou la redirection.

Les trois techniques peuvent coexister sur une même machine et/ou un même réseau. Par exemple, les utilisateurs accèdent à Internet grâce au PAT, et un serveur de messagerie interne est publié sur Internet afin d'assurer la gestion des mails de l'entreprise.

Implémentation de la traduction d'adresses

Implémentation

- Dans quels cas utiliser la traduction d'adresse ?
  - Accès à Internet
  - Communication entre réseaux ayant la même adresse majeure
  - Répartition de charge simple en TCP
- Avantages :
  - Indépendance de l'adressage interne vis-à-vis de l'adressage externe
  - Augmentation du niveau de sécurité par polarisation des accès
- Inconvénients :
  - Délais de transit supplémentaires
  - Problèmes avec certaines applications
  - Pas de traçabilité de bout en bout

USAGE

Dans quels cas allons-nous utiliser la traduction d'adresses ?

- La première raison est la plus répandue : pour accéder à Internet sans avoir l'ensemble de son parc informatique en adressage public. Ce que permet également un serveur proxy, mais uniquement pour les protocoles http, ftp et gopher. La traduction fonctionne indépendamment des protocoles utilisés.
- La seconde raison est moins courante mais peut se révéler problématique : deux réseaux ayant la même adresse majeure doivent communiquer entre eux. Cela est plus fréquemment que l'on ne pense et ce pour les raisons suivantes :
  - ➔ Fusion de sociétés ;
  - ➔ Utilisation par les entreprises des mêmes adresses privées, souvent les plus « confortables », notamment 10.0.0.0, 172.16.0.0, 192.168.1.0 (vérifiez chez vous…) ;
  - ➔ L'augmentation de l'utilisation des VPNs, que ce soit en inter-entreprise ou en extra-entreprise. De plus en plus de sociétés établissent des liens privilégiés (friendly access) sécurisés afin de faciliter et accroître leurs échanges en toute sécurité.
- La troisième raison est de permettre la mise en place facile d'un système de répartition de charge simple en TCP. Il est en effet possible de mapper des adresses externes avec des adresses internes en utilisant la traduction d'adresse et les fonctionnalités de round robin.

AVANTAGES

Les avantages apportés par la traduction d'adresses sont les suivants :

- Un espace d'adressage interne privé, plus souple et indépendant de l'extérieur. Il est possible de modifier son adressage interne —changement de masque de sous-réseau ou de réseau majeur— sans interférences avec l'extérieur.
- Une sécurité accrue : pas de visibilité du réseau interne, par polarisation. Il en résulte un niveau de sécurité plus élevé et une facilité de configuration des firewalls notamment. Il est plus simple de lier les niveaux de sécurité avec la traduction des adresses.

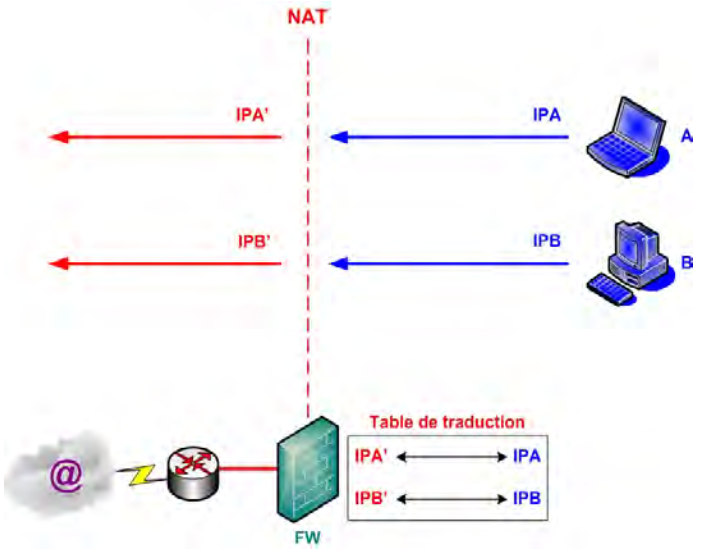
INCONVENIENTS

Il existe néanmoins des inconvénients à la traduction d'adresse :

- Les VPNs, réseaux privés virtuels, ne supportent généralement pas la traduction d'adresse.
- Les opérations nécessaires à sa réalisation par l'élément traducteur rendent inévitable un délai de transit supplémentaire :
  - ➔ Changement de l'adresse source dans le datagramme IP
  - ➔ Recalcul du CRC
  - ➔ Enregistrement du mappage
- Certaines applications, notamment celles utilisant des ports dynamiques ou négociés, ne supportent pas toujours la traduction d'adresse. C'est surtout le cas avec le PAT.
- Intrinsèquement, il n'est évidemment pas possible d'avoir une vision d'ensemble du cheminement de bout en bout d'un datagramme IP. Néanmoins, c'est aussi le but recherché d'un point de vue sécuritaire : ce qui n'est pas visible est plus difficile à attaquer.

Présentation du NAT

Présentation du NAT



PRESENTATION

Le NAT a été la première technique de traduction d'adresse développée. C'est la plus simple, celle qui pose le moins de problèmes, mais la plus gourmande en adresses publiques. Elle est en voie de disparition pour les accès Internet, supplantée par le PAT. En revanche, elle est encore couramment utilisée pour les traductions internes. Les traductions internes sont utilisées afin de créer des zones de sécurités de niveau élevé.

CARACTERISTIQUES DU NAT

- Les adresses sont traduites une à une. A chaque adresse interne va correspondre une adresse externe. En général, une adresse publique pour chaque adresse privée souhaitant accéder à Internet.
- Il doit donc y avoir autant d'adresses publiques disponibles (le pool) que de machines connectées simultanément.
- La machine traductrice mémorise les correspondances, les mappages, dans un cache d'adresses ou cache NAT (cache XLATE chez CISCO). La durée de présence d'un mappage dans ce cache est limitée par défaut à quelques minutes et configurable la plupart du temps.
- Supporté par la plupart des applications, y compris multimédia, les ports source et destination n'étant pas modifiés.

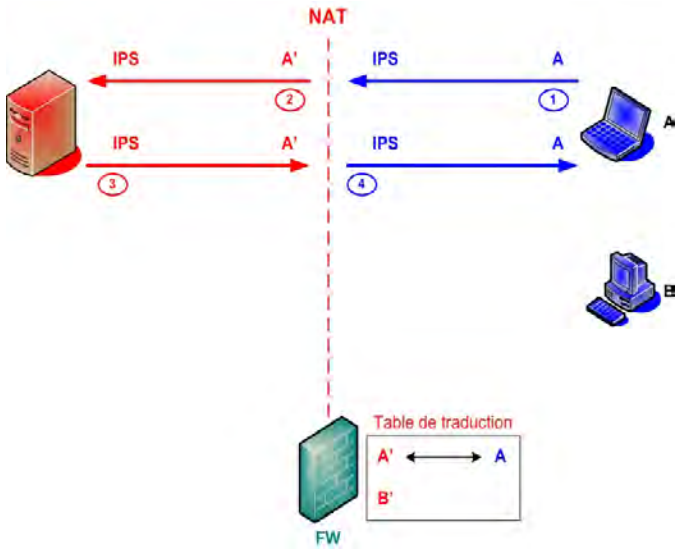
CONFIGURATION

Les étapes de configuration sont simples :

- On définit un pool, c'est-à-dire l'ensemble des adresses publiques que l'on va utiliser pour la traduction des adresses internes. Une adresse peut être réservée pour l'élément traducteur lui-même. Ces adresses doivent impérativement appartenir au sous-réseau extérieur auquel est directement connectée la machine traductrice.
- On spécifie quelles adresses internes seront traduites. Il est possible, pour des raisons de sécurité, de ne pas autoriser toutes les adresses à être traduites : serveurs « sensibles » (outils de sécurité, d'analyse, base de données confidentielles…), commutateurs, routeurs, firewall interne…

Fonctionnement du NAT (1)

Fonctionnement du NAT (1)



EXEMPLE

Prenons le cas le plus simple : un réseau d'entreprise accédant à Internet et protégé par un firewall. Ce dernier est l'élément traducteur.

Nous traiterons l'exemple de deux machines A et B présentes sur le réseau interne se connectant à un serveur externe accessible via l'adresse publique IPS.

FONCTIONNEMENT

Les étapes de fonctionnement du NAT sont les suivantes :

1) Émission du datagramme IP :

- ➔ La machine A émet un datagramme IP avec l'adresse source A et l'adresse destination IPS vers Internet.
- ➔ Ce datagramme parvient à la machine traductrice. Dans ce cas précis, A est présente dans un sous-réseau auquel la machine traductrice est directement reliée, sur lequel elle possède une adresse. Nous verrons un exemple dans lequel le réseau source n'est pas forcément directement relié au firewall.

2) Traduction de l'adresse source interne :

- ➔ La machine traductrice change l'adresse IP source privée A en adresse officielle A' et l'expédie sur Internet à destination de IPS.
  A' est la première adresse ***disponible*** dans le pool d'adresses officielles. Si un filtre de traduction a été configuré, la machine vérifie que l'adresse source est bien autorisée à être traduite. Si ce n'est pas le cas, soit l'adresse source du datagramme n'est pas traduite, soit le datagramme est purement et simplement détruit.

- ➔ Elle enregistre le mappage dans son cache, ou table de traduction. La durée de vie de présence d'un mappage dans ce cache est en général configurable via la définition de deux paramètres : la durée de vie initiale du mappage et la durée totale de présence dans le cache. Par exemple, si on définit une durée de vie initiale de 2 minutes et une durée totale de 10 minutes, le mappage sera conservé durant 2 minutes. S'il est réutilisé, il est crédité à chaque nouvelle utilisation de 2 minutes supplémentaires dans la limite de 10 minutes de présence maximale dans le cache. De même, il est possible d'effacer manuellement le contenu de ce cache : pour des raisons de sécurité ou pour valider instantanément un changement de configuration.

3) Réponse :

- ➔ Le serveur contacté répond à la demande (une demande de connexion TCP pour du trafic HTTP par exemple) en envoyant un datagramme IP à l'adresse A', seule adresse visible pour le moment. L'adresse interne A n'est pas visible comme nous l'avons vu précédemment.
- ➔ Le datagramme parvient à la machine traductrice sur son interface extérieure.

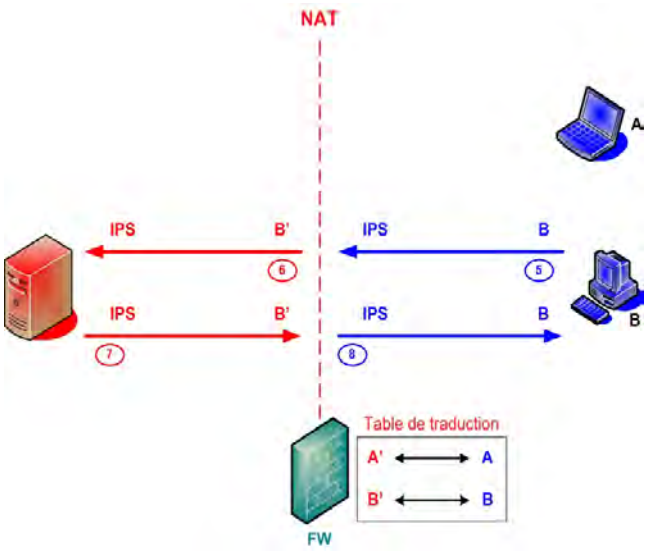
4) Traduction « inverse » :

- ➔ Pour le datagramme retour, de réponse, la machine traductrice change l'adresse de destination publique en adresse privée en utilisant la table de traduction. Elle l'expédie au destinataire interne. Il faut noter que c'est fréquemment à ce moment précis qu'il est possible de définir des règles d'accès spécifiant que le trafic entrant n'est autorisé que s'il y a antériorité d'une demande. Autrement dit, nous pouvons définir le trafic directement entrant comme interdit et le trafic « en réponse à une demande interne » comme autorisé.
- ➔ Le datagramme est expédié en interne vers l'adresse A. Il est à noter que l'on traduit l'adresse source dans le sens interne vers externe et l'adresse destination dans le sens externe vers interne.

La machine traductrice joue en fait un rôle plus complexe qu'il n'y paraît. Elle traduit bien sûr les adresses mais remplit également les fonctions suivantes :
- Elle est la passerelle par défaut du réseau interne, que ce soit directement ou par l'intermédiaire d'un routeur interne,
- Elle répond aux requêtes ARP IP pour chacune des adresses externes qu'elle gère dans son pool d'adresses.

Fonctionnement du NAT (2)

Fonctionnement du NAT (2)



Prenons maintenant une seconde machine B, qui a elle aussi besoin d'accéder à Internet. Les étapes de fonctionnement sont les suivantes :

1) L'étape est identique à (1) : le datagramme est émis et parvient à la machine traductrice.
2) Traduction :
   - ➔ La machine traductrice change l'adresse IP source privée B en adresse officielle B' et l'expédie sur Internet. B' est la première adresse disponible dans le pool. Si le mappage entre A et A' n'était plus présent dans le cache, l'adresse serait dite libérée et serait de nouveau disponible dans le pool.
     B aurait dans ce cas utilisé A' pour accéder à Internet. Les traductions se font une à une de manière ***dynamique*** et non statique.
     Nous verrons qu'avec le PAT, il est possible de mapper deux sous-réseaux entre eux en point à point.
   - ➔ La machine traductrice enregistre le mappage dans son cache.
3) Réponse du serveur à B'.
4) Traduction « inverse » : l'adresse de destination publique B' est traduite en adresse privée B en utilisant le cache et expédiée au destinataire interne.

Le fonctionnement même de la traduction d'adresses a un impact non négligeable sur la sécurité interne, car si la traduction est réalisée par un firewall, il cesse d'être un élément transparent du réseau. C'est une des raisons pour lesquelles leur fonctionnement et leurs capacités ont évolués de conserve.
Néanmoins, les autres aspects sécuritaires tels que la polarisation de l'accès et le masquage de la structure réseau interne permettent au NAT d'être un élément essentiel pour la sécurité actuelle de l'accès à Internet.

PAT

PAT

- Le PAT est une variante à un du NAT
- Il n'y a qu'une adresse officielle utilisée pour la traduction, on va donc « multiplexer » les ports source pour identifier les différents flux de données
- La limite théorique est de 64512 connexions simultanées sur une seule adresse publique, en pratique on ne dépasse pas 4000
- Certaines applications multimédia ne supportent pas le PAT, notamment les applications utilisant des ports clients fixes, prédéfinis ou négociés

PRESENTATION

Le PAT, Port Address Translation, est une variante du NAT. Alors que le NAT utilise autant d'adresses officielles que de connexions simultanées à Internet, le PAT n'en utilise qu'une. Cette adresse peut être l'adresse externe de la machine traductrice ou une adresse externe supplémentaire gérée par la machine.

Cela représente évidemment une économie de moyens et une souplesse beaucoup plus grande que celle du NAT.

PROBLEMATIQUE

Un problème apparaît immédiatement : comment différentier les différents flux de données ?

- Pour caractériser les flux de données, il est possible d'utiliser plusieurs éléments : adresse et port source, adresse et port destination. Dans le cas du NAT, la tâche est relativement facile : les adresses sont traduites une à une. Caractériser un flux de données en utilisant les adresses source et destination est donc plus facile.
- Pour le PAT, on doit utiliser autre chose, l'adresse source traduite étant la même pour tous les flux de données. On ne peut jouer sur les ports de destination : si deux machines internes se connectent simultanément au même serveur, cela ne fonctionne pas. De même, on ne peut utiliser les ports source d'origine : et si par hasard deux machines accédaient au même serveur avec le même protocole en même temps en utilisant les mêmes ports source ? C'est plus fréquent qu'on ne pourrait le supposer : les ports clients sont normalement aléatoires, mais, très souvent, les applications clientes utilisent de préférence les mêmes ports, quitte à en prendre un autre s'il n'est pas disponible.

SOLUTION

La solution est simple : il suffit de changer les ports sources en même temps que l'on traduit l'adresse source et de mémoriser le mappage entre le socket interne (adresse + port) et le socket externe. Très souvent, comme la traduction est associée à des fonctionnalités de sécurité, l'adresse et le port de destination sont également mémorisés (mémorisation de l'antériorité).

Fonctionnement du PAT (1)

Fonctionnement du PAT (1)

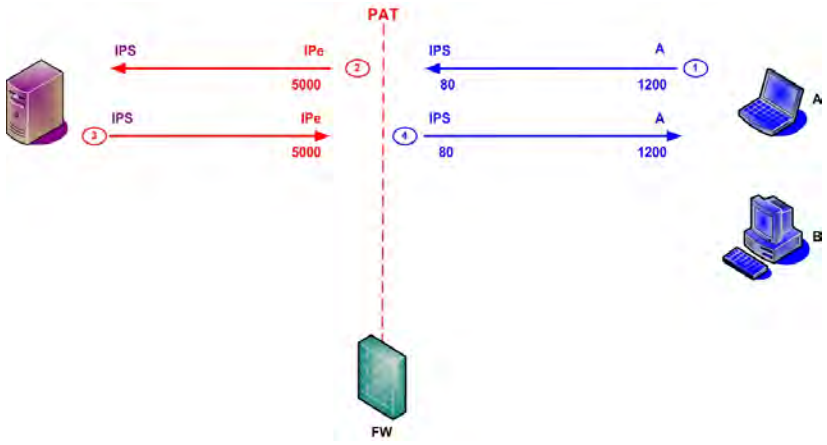


Table de traduction

Adr cible	port cible	Protocole	Adr externe	Port externe	Adr interne	Port interne
IPS	80	TCP	IPe	5000	A	1200

EXEMPLE

Prenons un exemple similaire à celui utilisé pour le NAT : un réseau d'entreprise accédant à Internet et protégé par un firewall.

Nous traiterons l'exemple de deux machines A et B présentes sur le réseau interne se connectant à un serveur externe accessible via l'adresse publique IPS.

Nous supposerons que la connexion utilise TCP, choisir UDP n'aurait pas modifié l'exemple. La traduction PAT utilisera l'adresse externe IPe, qui est soit l'adresse assignée au firewall, soit une adresse supplémentaire utilisée spécifiquement pour le PAT.

FONCTIONNEMENT DU PAT

Les étapes de fonctionnement du PAT sont les suivantes :

1) Émission du datagramme IP :

- ➔ La machine A émet un datagramme IP avec l'adresse source A et l'adresse destination IPS vers Internet
- ➔ Ce datagramme parvient à la machine traductrice

2) Traduction de l'adresse et du port source internes. La machine traductrice :

- ➔ Change l'adresse IP source privée A en adresse externe IPe du datagramme
- ➔ Change le port source TCP 1200 en TCP 5000
- ➔ Enregistre le mappage dans son cache ou table de traduction. Les paramètres enregistrés sont :
  - ✓ Adresse et port source internes, paramètres de la machine émettrice

- ✓ Adresse et port source externes « traduits »
- ✓ Adresse et port de destination, utilisés ensuite pour la vérification de l'antériorité d'une requête

➔ Expédie le datagramme via Internet à destination d'IPS

3) Réponse du serveur :

➔ Le serveur contacté répond à la demande (une demande de connexion TCP pour du trafic HTTP par exemple) en envoyant un datagramme IP à l'adresse IPe et au port client 5000

➔ Le datagramme parvient à la machine traductrice sur son interface extérieure

4) Traduction « inverse ». La machine traductrice, en utilisant la table de traduction, effectue les opérations suivantes sur le datagramme de réponse :

➔ Elle change l'adresse de destination externe IPe en adresse interne A

➔ Elle change le port externe 5000 en port interne 1200

➔ Elle expédie le datagramme au destinataire interne

Fonctionnement du PAT (2)

Fonctionnement du PAT (2)

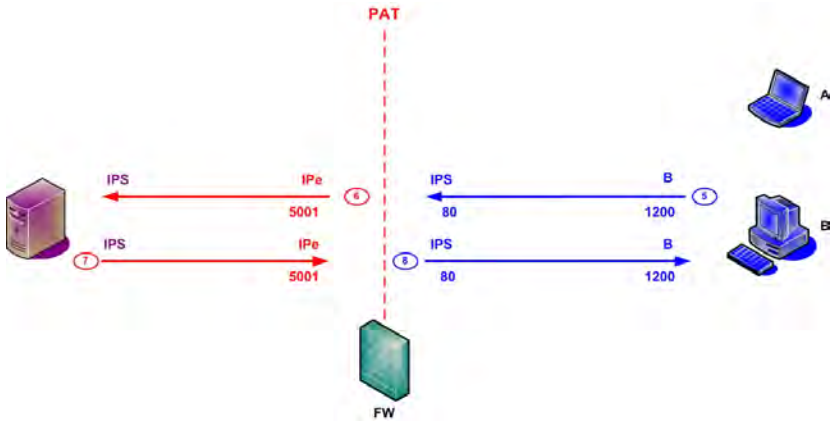


Table de traduction

Adr cible	port cible	Protocole	Adr externe	Port externe	Adr interne	Port interne
IPS	80	TCP	IPe	5000	A	1200
IPS	80	TCP	IPe	5001	B	1200

Prenons maintenant une seconde machine, B, qui a elle aussi besoin d'accéder à Internet. Nous avons volontairement pris le même port source afin de montrer ce qui se passe lorsque deux machines utilisent le même port source en accédant au même serveur simultanément.
Les étapes de fonctionnement sont les suivantes :

1) L'étape est identique à (1) : le datagramme est émis et parvient à la machine traductrice.
2) Traduction. La machine traductrice :
   - ➔ Change l'adresse IP source privée B en adresse externe IPe
   - ➔ Change le port source interne TCP 1200 en port source externe 5001
   - ➔ Enregistre le mappage dans son cache
   - ➔ Expédie le datagramme sur Internet
3) Réponse du serveur à IPe sur le port 5001
4) Traduction « inverse ». La machine traductrice :
   - ➔ Consulte sa table de traduction et établit la correspondance entre IPe:5001 et B:1200
   - ➔ Change l'adresse externe de destination IPe en adresse interne B
   - ➔ Change le port externe de destination TCP 5001 en port de destination interne TCP 1200
   - ➔ Expédie le datagramme au destinataire interne

SAT

SAT

- Le SAT, ou NAT statique, permet un mappage statique entre une adresse externe, souvent publique, et une adresse interne
- Le SAT est utilisé afin de publier, c'est-à-dire rendre visible, un serveur sur Internet
- Un serveur, pour être accessible depuis Internet, doit toujours l'être via la même adresse
- Il faut donc au minimum autant d'adresses publiques que de serveurs à publier

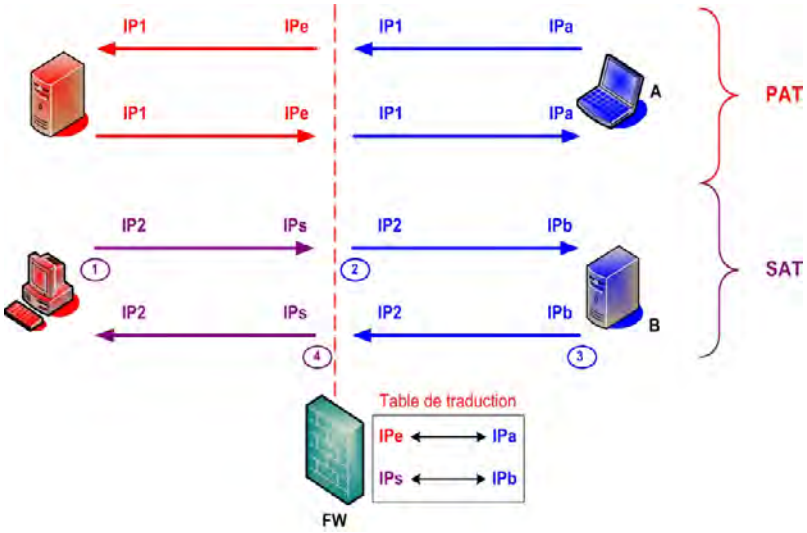
PRESENTATION DU SAT

- Le SAT (Static Address Translation), ou NAT statique, permet de mapper « en dur » une adresse interne avec une adresse externe. Le plus souvent, l'adresse externe est une adresse publique. Ce mappage, contrairement au NAT, n'a pas de limite de durée, comme son nom l'indique d'ailleurs.
  Cette technique permet de réserver une adresse publique afin de publier un serveur, c'est-à-dire le rendre accessible depuis Internet. La publication permet à un serveur interne d'être toujours vu à partir d'Internet avec la même adresse externe et le même port de destination.
- Le mappage est exclusif : l'adresse interne sera toujours traduite avec cette adresse publique et, réciproquement, l'adresse publique sera réservée pour cette adresse interne.

LIMITATIONS

- La seule limite à cette technique est le nombre d'adresses publiques dont on dispose.
- Le SAT est rarement utilisé seul, il est souvent utilisé simultanément avec du NAT dynamique ou du PAT. Il est même possible sur certaines plateformes qu'une adresse publique puisse être utilisée pour différentes techniques.

Fonctionnement du SAT



EXEMPLE

Dans cette configuration, deux techniques de traduction d'adresse sont utilisées simultanément :

- Le PAT pour l'accès interne des machines à Internet
- Le SAT pour l'accès depuis Internet au serveur B

L'adresse IPs est mappée statiquement, réservée, avec l'adresse interne du serveur B. L'adresse IPe est utilisée pour le PAT.

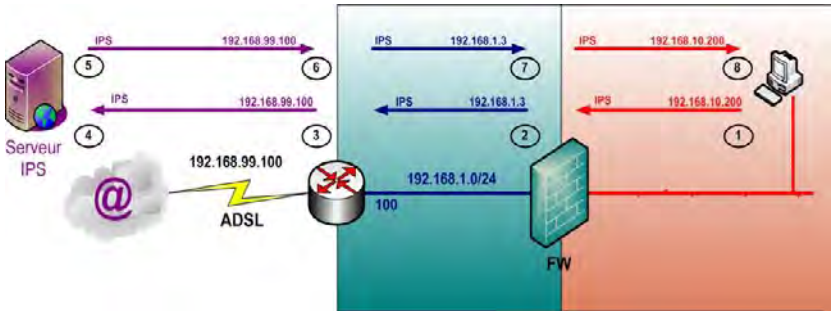
FONCTIONNEMENT

Le fonctionnement du SAT est le suivant :

1) Lorsqu'une machine IP2 veut accéder au serveur B, elle envoie un datagramme à l'adresse IPs.
2) Le firewall reçoit ce datagramme :
   - ➔ Il consulte sa table de mappage et détermine :
     - ✓ Si le trafic entrant est autorisé : selon les firewalls, cela peut être implicite ou, à l'inverse, nécessiter une règle entrante spécifique. Autrement, le datagramme est détruit.
     - ✓ L'adresse interne correspondant au mappage.
   - ➔ Il traduit l'adresse de destination du datagramme IPs en IPb
3) Le serveur B répond à destination d'IP2.
4) Le firewall traduit l'adresse source interne IPb en adresse destination externe IPs et l'expédie à IP2.

Exemple du « double NAT »

Exemple du « double NAT »



Adresse externe	Adresse interne
192.168.99.100	192.168.1.3

Adresse externe	Adresse interne
192.168.1.3	192.168.10.200

EXEMPLE

Le double NAT consiste à réaliser deux traductions d'adresses avant l'accès à Internet. Cette technique apporte un surcroît de sécurité ainsi qu'une simplification du routage. Il est intéressant de l'étudier car :

- C'est un cas de plus en plus fréquent ;
- Il mêle des problèmes de routages à des problèmes de traduction ;
- Il permet de voir des cas de figures particuliers de la traduction :
  - ➔ Du NAT réalisé par le firewall
  - ➔ Du PAT réalisé par le routeur ADSL

Dans cet exemple, nous avons un réseau d'entreprise typique composé de :

- Un réseau interne, 192.168.10.0/24 ;
- Un réseau dit intermédiaire, entre le firewall et le routeur d'accès à Internet, 192.168.1.0 ;
- Une adresse IP publique 192.168.99.100/24. Nous prenons cette adresse pour des raisons de commodité. Il est évident que cette adresse n'est pas une adresse publique mais nous ferons comme si elle l'était dans l'exemple présent.

FONCTIONNEMENT

Les étapes suivantes ont lieu :

1) Émission : la machine 192.168.10.200 émet une requête vers l'adresse officielle IPS.

2) Traduction NAT : le firewall reçoit le datagramme, traduit l'adresse interne 192.168.10.200 en adresse externe 192.168.1.3 et enregistre le mappage dans le cache NAT : adresse source interne et adresse traduite.
3) Traduction PAT : le routeur ADSL traduit l'adresse 192.168.1.3 en 192.168.99.100 et mémorise les paramètres dans son cache de traduction.
4) Réception : le serveur reçoit la requête.
5) Le serveur émet une réponse à la requête à destination de l'adresse 192.168.99.100.
6) Le routeur ADSL, après vérification, effectue une traduction « inverse » de l'adresse destination 192.168.99.100 en 192.168.1.3.
7) Le firewall effectue une traduction inverse de l'adresse de destination 192.168.1.3 en 192.168.10.200.
8) La machine 192.168.10.200 reçoit la réponse à sa requête.

AVANTAGES

La technique du double NAT présente les avantages suivants :

- Augmentation du niveau de sécurité :
  - ➔ Ni le réseau intermédiaire, ni le réseau interne ne sont visibles de l'extérieur
  - ➔ Le réseau interne n'est pas visible du réseau intermédiaire
  - ➔ Deux protections valent mieux qu'une seule
- Augmentation de la souplesse d'adressage :
  - ➔ Il est possible de changer la structure d'adressage du réseau intermédiaire ou interne sans répercutions directes sur les autres réseaux. La seule modification concernera la définition des pools d'adresses.
  - ➔ Seule l'interface externe nécessite une ou plusieurs adresses externes.
- Simplification des règles de routages :
  - ➔ Le réseau interne utilise l'adresse interne du firewall afin d'accéder au réseau intermédiaire et à Internet. Souvent, le firewall est la passerelle par défaut du réseau interne.
  - ➔ Le réseau intermédiaire n'a pas besoin de connaître le réseau interne : les datagrammes traversant le firewall en ressortent avec une adresse source appartenant au réseau intermédiaire. L'accès est donc considéré comme local.
  - ➔ Le firewall utilise comme passerelle par défaut l'interface interne du routeur d'accès, c'est-à-dire l'adresse qu'utilise le routeur sur le réseau intermédiaire.

Redirections

Redirections

- La redirection permet l'accès extérieur à des serveurs internes
- Il existe trois techniques de redirection :
  - La publication ou redirection complète
  - Redirection avec mappage de ports
  - Redirection avec traduction de ports
- Il est possible d'utiliser simultanément plusieurs techniques de redirection

PRINCIPES

Les redirections permettent de rediriger un flux de données particulier entrant vers un serveur interne, ce flux étant initié par une source externe, sans antériorité.
En général, on fait correspondre :

- Une adresse de destination externe avec une adresse de destination interne
- Un port de destination externe avec un port de destination interne

REDIRECTIONS

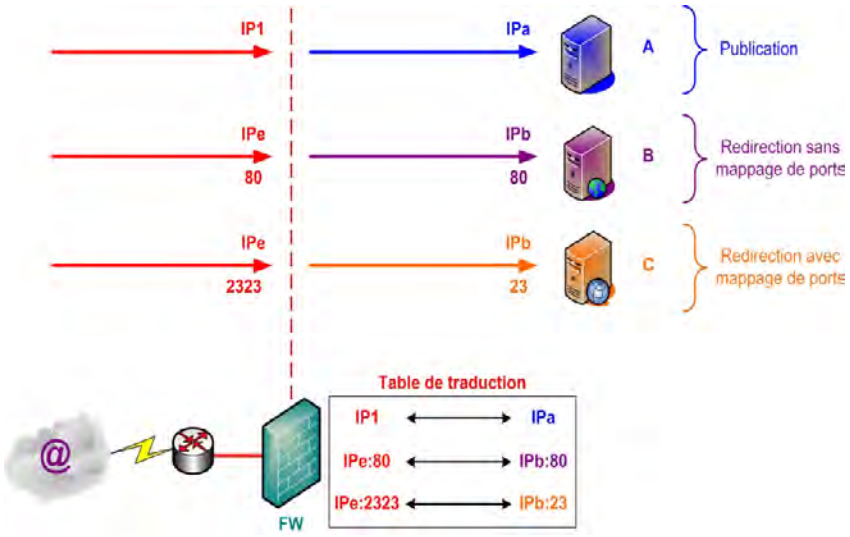
Il existe deux types de redirections :

- La publication ou redirection complète : tout trafic à destination de l'adresse externe publiée est redirigé vers l'adresse interne mappée.
- Redirection avec mappage de ports : le port de destination externe est le même que le port de destination interne. Seul le trafic entrant sur ce port est transmis au serveur interne.
- Redirection avec traduction de ports : le port de destination externe est différent du port de destination interne. Seul le trafic entrant sur ce port est transmis au serveur interne.

Il est possible d'utiliser simultanément plusieurs techniques de redirection.

Fonctionnent des redirections

Fonctionnent des redirections



Dans l'exemple ci-dessus, nous avons les trois possibilités techniques des redirections :

- Une publication d'adresse IP :
  - ➔ L'adresse externe IP1 est mappée en statique avec l'adresse interne IPa ;
  - ➔ Tout trafic IP à destination d'IP1 sera redirigé vers l'adresse interne IPa par le firewall.
- Une redirection avec mappage de ports :
  - ➔ La socket externe IPe:80 est mappée en statique avec la socket interne IPb:80 ;
  - ➔ Tout trafic à destination de l'adresse IPe sur le port 80 est redirigé vers l'adresse interne IPb sur le port 80.
- Une redirection avec traduction de ports :
  - ➔ La socket externe IPe:2323 est mappée en statique avec la socket interne IPc:23 ;
  - ➔ Tout trafic à destination de l'adresse IPe sur le port 2323 est redirigé vers l'adresse interne IPc sur le port 23.

Présentation des VPNs

Présentation des VPNs

- Permettent une interconnexion sécurisée
- Avantages :
  - Coûts
  - Souplesse
  - Contrôle
- Inconvénients
  - Débit pas toujours garanti
  - Complexité
  - Overhead

Les VPNs, Virtual Private Networks, sont très utilisés dans les réseaux modernes. Le principe d'un lien VPN est la mise en place d'une connexion logique sécurisée entre deux entités. Généralement, entre un micro-ordinateur et un réseau ou entre deux réseaux, à travers Internet. Pour cela, il est nécessaire d'utiliser des protocoles spécifiques tels que IPSec, PPTP ou encore L2TP. Souvent, les VPNs remplacent les LS/LL (Lignes Spécialisées/Lignes Louées).

Intéressons nous aux avantages, autres que l'évidence de la sécurité, et aux inconvénients apportés par les VPNs.

AVANTAGES DES VPNs

- Le coût constitue l'avantage le plus évident et le plus parlant. Les VPNs remplacent souvent les LS/LL, dont le coût est parfois prohibitif au regard des nécessités. Pour établir un lien VPN entre deux réseaux d'une même entreprise, il suffit d'avoir un bon accès à Internet et le matériel adéquat. Plus la distance entre les entités est grande, plus significatif sera le gain pour l'entreprise.
- La souplesse n'est pas forcément la qualité première à laquelle on pense avec les VPNs. Pourtant, il est aujourd'hui très simple de mettre en place des liens VPNs, de les arrêter, de les faire évoluer, de changer les protocoles utilisés…
- Le contrôle est un facteur beaucoup moins technique, mais très important du point de vue de la sécurité. Quand une entreprise utilise une LS/LL, le niveau de sécurité repose sur la confiance dans l'opérateur. Or, les opérateurs sous-traitent de plus en plus un certains nombre de tâches, avec une dilution des responsabilités et un contrôle opérationnel moindre. Les VPNs n'ont pas ce problème, le niveau de sécurité est intrinsèque à l'entreprise, en dehors des éventuelles faiblesses des fabricants ou des éditeurs.

INCONVIENTS DES VPNs

- Les VPNs ne garantissent aucun débit. Ce qui peut être problématique pour certaines applications ou certains protocoles. Il est toujours possible, pour pallier cette faiblesse, d'utiliser :
  - ➔ Une LS/LL pour de courtes distances en WAN ;
  - ➔ La labellisation avec MPLS, qui permet de disposer des mêmes avantages qu'un LS/LL, mais à un coût moindre et surtout une souplesse infiniment supérieure ;
  - ➔ Une stratégie de QoS, de qualité de service, pour des VPNs internes.
- Autre point délicat, la complexité des protocoles VPNs. Même si les interfaces de configuration se sont nettement améliorées, la configuration avancée d'un VPN est toujours une opération complexe et délicate.
- L'overhead. Le fait de crypter des données augmente leur taille. Cela peut aller jusqu'à 20% supplémentaire pour les options les plus puissantes. Pour limiter ce facteur, on compresse les données avant de les crypter. Ce qui entraine deux phénomènes :
  - ➔ La MTU réelle des données diminue ;
  - ➔ Le cryptage et la compression entrainent des délais de traitement supplémentaires.

Technologies VPN

- *Virtual Private Network* : les protocoles de *tunneling* permettent de transporter d'autres protocoles de même niveau ou de niveaux supérieurs.
- Ces protocoles fonctionnent généralement au niveau 3 et/ou 4
- Fonctionnalités :
  - Authentification
  - Intégrité
  - Confidentialité
- Exemples :
  - GRE
  - IPSec (IKE, ISAKMP, AH, ESP)
  - CET : propriétaire CISCO

TECHNOLOGIES VPN

Les protocoles VPNs permettent de transporter d'autres protocoles de même niveau ou de niveaux inférieurs en sécurisant leur transport.

La plupart des protocoles VPNs fonctionnent au niveau 4 et permettent de sécuriser des protocoles de niveau 3 ou 4.

Les fonctionnalités fournies par les protocoles VPNs sont les suivantes :

- Authentification : vérification de l'identité des intervenants. Elle peut être unidirectionnelle ou réciproque.
- Intégrité : on garantit que les données n'ont pas été altérées durant leur acheminement.
- Confidentialité : les données ne seront visibles en clair que par le ou les destinataires.

EXEMPLES

Quelques exemples de protocoles fréquents :

- ➔ GRE, qui n'est pas à proprement parlé un VPN, mais que l'on rencontre très souvent chez les opérateurs et les FAI/ISP. Libre et standardisé.
- ➔ IPSec, le plus puissant, le plus complexe, le plus modulaire. Libre et standardisé, c'est CISCO qui l'a développé à partir de CET.
- ➔ CET, Cisco Encrypted Technology, l'ancêtre de IPSec. Propriétaire CISCO.

GRE

GRE

- Protocole 47
- « IP dans IP »
- RFC 2784
- Permet d'interconnecter des réseaux entre eux de façon transparente
- Utilisé tel quel surtout par les opérateurs
- Utilisé dans PPTP pour les connexions clientes

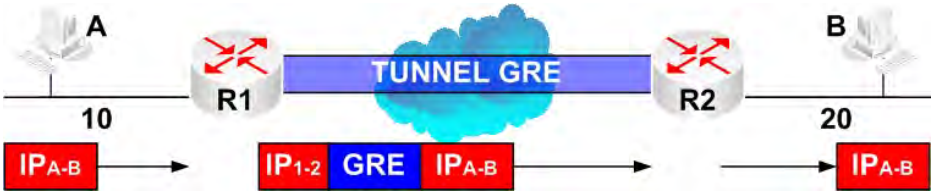
GRE, Generic Routine Encapsulation, est un protocole de niveau 4, ayant le numéro de protocole IP n°47 et défini dans la RFC 2784.

Les caractéristiques de GRE sont les suivantes :

- Permet de transporter de façon transparente des datagrammes IP entre deux réseaux. D'un point de vue IP, les réseaux intermédiaires sont transparents.
- Il n'offre aucune sécurité de transport. GRE est juste un protocole de tunneling pur et dur.
- Utilisé surtout par les opérateurs pour précisément masquer leurs réseaux internes.
- GRE est également utilisé dans PPTP et pour transporter IPSec afin de lui permettre de traverser des éléments traducteurs.

Tunnel GRE

Tunnel GRE



EXEMPLE

Prenons un exemple typique : Une machine A dans le réseau privé 10 veut envoyer des datagrammes à une machine B présente dans le réseau privé 20. Nous supposerons que R1 et R2 disposent d'adresses publiques pour accéder à Internet.
En fonctionnement normal :

- Le réseau 10 doit être connu du routeur R2 et de tous les routeurs intermédiaires. Or, comme le réseau 10 est un réseau privé, c'est impossible.
- Le réseau 20 doit être connu du routeur R2 et de tous les routeurs intermédiaires. Or, comme le réseau 20 est un réseau privé, c'est impossible.

En utilisant GRE :

- Pour atteindre le réseau 20, R1 utilise le tunnel établi avec le routeur R2. Le tunnel est vu par le routeur comme une interface logique virtuelle.
- Pour atteindre le réseau 10, R2 utilise le tunnel établi avec le routeur R2.

FONCTIONNEMENT DU TUNNEL

- A émet un datagramme IP ayant pour adresse source A et destination B.
- Le datagramme parvient à R1.
- R1 cherche dans sa table de routage comment atteindre le réseau 20, le réseau de B.
- La table de routage pointe vers l'interface logique virtuelle du tunnel GRE entre R1 et R2.
- R1 encapsule le datagramme original dans un autre datagramme ayant pour adresse source l'adresse publique de R1 et destination l'adresse publique de R2. Ce

datagramme transporte du GRE, qui lui-même encapsule le datagramme entre A et B.

- R1 émet ce datagramme sur Internet, qui sera routé en tenant compte uniquement du destinataire, à savoir R2.
- R2 reçoit le datagramme de R1, le désencapsule , et le transmet à destination du réseau de B.
- B reçoit le datagramme.

Comme nous le voyons, GRE simplifie le routage. Les routeurs intermédiaires n'ont pas besoin de connaitre les réseaux 10 et 20, puisqu'ils acheminent, d'un point de vue IP, des datagrammes entre R1 et R2 qui possèdent des adresses publiques.
Pour A et B, les réseaux intermédiaires sont transparents. Pour elles, c'est comme si les réseaux 10 et 20 étaient directement connectés via un routeur unique.

IPSec

IPSec

- *IP Security*
- Standard RFC 2401, 2402, 2406 et 3168
- Composants de IPSec
  - AH
  - ESP
  - Mode : transport ou tunnel
  - Transformation
  - SA
  - IKE
  - ISAKMP

PRESENTATION

IPSec, IP Security, est un protocole libre et normalisé, développé à partir du protocole propriétaire de CISCO CET. A l'origine, il était destiné à n'être utilisé que sur IPv6. Mais, la demande étant très forte, et la migration prenant du retard, il a été porté sur IPv4.

IPSec est défini dans les RFCs suivantes : 2401, 2402, 2406 et 3168. De nombreuses autres RFCs concernent d'autres protocoles amenés à utiliser IPSec.

C'est, actuellement, le protocole libre le plus sûr et le plus riche en fonctionnalités. Il est largement utilisé pour interconnecter des réseaux, un peu moins pour les postes de travail. Néanmoins, la spectaculaire augmentation de puissance des machines actuelles et les débits d'accès à Internet disponibles rendent son utilisation plus aisée.
Même les militaires et les banques abandonnent au fur et à mesure leurs protocoles propriétaires pour migrer en IPSec.

COMPOSANTS

IPSec est composé des éléments suivants :

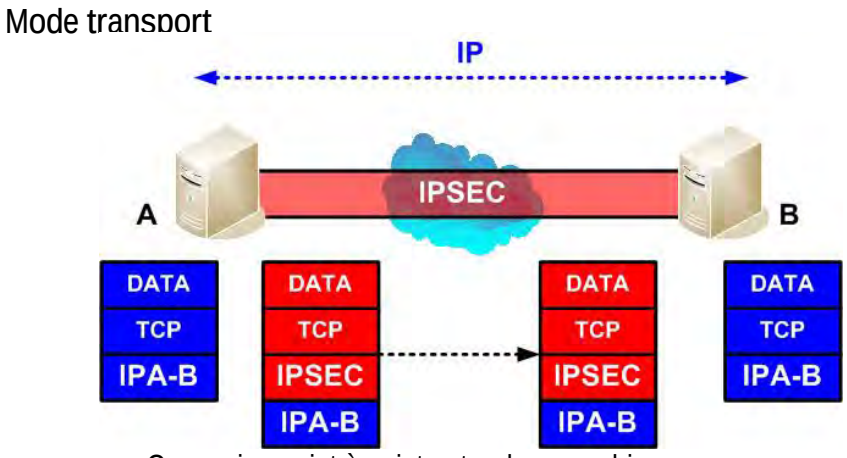
- Les protocoles de niveau 4 AH et ESP sont utilisés pour transporter les données sécurisées
- Deux modes sont définis en IPsec : transport et tunnel. Ils sont adaptés aux types d'usages courants d'IPsec.
- On appelle transformation l'ensemble des opérations réalisées par IPSec sur les datagrammes protégés. AH réalise une seule transformation, ESP une ou deux.
  Il est possible pour un lien VPN d'utiliser :
  - ➔ AH uniquement

- ➔ ESP uniquement
- ➔ AH, puis ESP
- ➔ ESP, puis AH

Au maximum, il est possible de réaliser trois transformations et d'utiliser une seule fois chaque protocole.

- Les SA, Security Associations, définissent les paramètres de sécurité utilisés par le tunnel IPSec : algorithme utilisé, protocoles, durée de validité, intervalle de renégociation…
- IKE/ISAKMP sont utilisés à l'initialisation pour négocier les SAs entre les machines intervenantes.

Mode transport



CARACTERISTIQUES DU MODE

IPSec supporte deux modes : le mode transport et le mode tunnel.
Quant on définit les propriétés d'un lien VPN, il faut impérativement en définir le mode.
Le mode est exclusif pour un lien VPN donné, il n'est pas possible de les mixer.
Autrement dit, on ne peut pas, par exemple, utiliser AH en mode transport puis ESP en mode tunnel.

MODE TRANSPORT

Le mode transport consiste à protéger les données de la couche transport. L'en-tête de la couche transport et les données sont protégés par IPSec. L'en-tête IP d'origine est conservé, seul le champ protocole est modifié et le checksum recalculé.

Le mode transport est adapté :

- Pour la connexion entre deux machines. A travers le réseau interne de l'entreprise ou à travers un WAN. Attention toutefois, IPSec ne supporte pas la traduction d'adresse.
- Pour la connexion entre une machine et un réseau. Cette solution est moins fréquente, mais elle est encore utilisée. Généralement on préfère la solution du mode tunnel dans ce cas de figure.

Les avantages du mode transport sont :

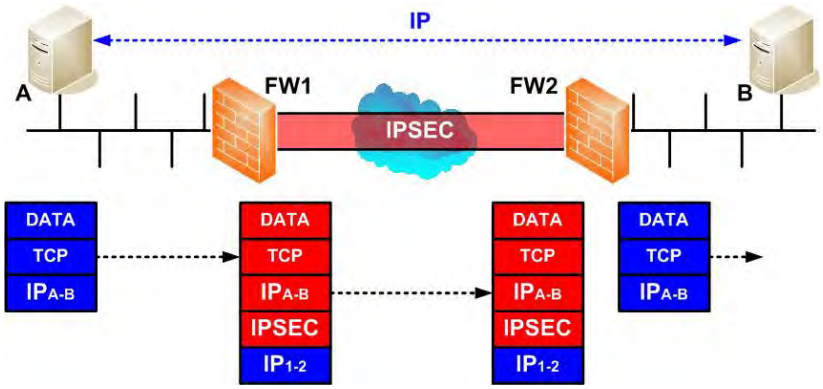
- ➔ Nécessite moins de ressources (RAM, CPU) que le mode tunnel
- ➔ Facile à mettre en place
- ➔ N'est pas tributaire d'un tiers

- Les inconvénients sont les suivants :

- Ne fonctionne qu'en point à point. S'il faut, par exemple, sécuriser les échanges entre un serveur et 50 machines, il faudra 50 VPNs.
- Le niveau de sécurité est inférieur au mode tunnel.

Mode tunnel

Mode tunnel



- Connexion entre deux réseaux
- Connexion entre une machine itinérante et un réseau
- L'en-tête IP original fait partie du *payload* d' IPSec
- Un autre en-tête est créé

MODE TUNNEL

Le mode tunnel consiste à protéger les données d'IP. L'en-tête IP d'origine est réencapsulé dans IPSec et un nouvel en-tête est généré :

- La machine A émet un datagramme IP à destination de B ;
- FW1 reçoit le datagramme et le réencapsule dans un nouveau datagramme IP ayant pour adresse IP source sa propre adresse et pour adresse IP destination celle de FW2 ;
- FW2 reçoit le datagramme et le désencapsule. Il transmet en interne le datagramme d'origine émis par A.

Le mode tunnel est adapté :

- A la connexion entre deux réseaux
- A la connexion entre une machine itinérante et un réseau

Les avantages du mode tunnel sont :

- Le niveau de sécurité fourni est supérieur au mode transport
- Fonctionne en mode point à point, mais est transparent pout les machines des réseaux connectés. Pour sécuriser les échanges entre 50 serveurs d'un réseau et 50 clients d'un autre réseau, un seul lien VPN suffit. Alors qu'il en faudrait 2500 en mode transport.

Les inconvénients sont les suivants :

- Nécessite plus de ressources (RAM, CPU) que le mode transport
- Parfois complexe à mettre en place
- Overhead plus élevé qu'en mode transport

AH

AH

- *Authentication Header*
- Protocole 51
- RFC 2402
- Utilisé afin de protéger les datagrammes ou les segments
- Protection à deux niveaux :
  - Intégrité
  - Authentification
- Pas de cryptage des données

CARACTERISTIQUES DE AH

AH, Authentication Header, est un des deux protocoles de sécurité utilisés par IPSec.

AH est défini dans la RFC 2402.

AH utilise le numéro de protocole IP numéro 51.

Selon le mode défini, AH protégera les datagrammes ou les segments

FONCTIONNALITES DE AH

AH fournit deux fonctionnalités de sécurité :

- ➔ Contrôle de l'intégrité des données échangées. La signature numérique calculée par l'expéditeur permettra au destinataire de vérifier que les données n'ont pas été altérées, volontairement ou pas, durant leur parcours.
- ➔ Authentification des intervenants. L'expéditeur et le destinataire doivent prouver leur identité respective. Cela peut être réalisé via des mots de passe secret, des clés pré-partagées, ou bien via l'utilisation d'une paire de clé publique/clé privée.

Ces deux fonctionnalités sont très souvent couplées, réalisées simultanément par un seul algorithme

Attention toutefois à un point important : AH n'intègre pas les algorithmes pour réaliser les opérations de cryptage, AH s'appuie sur des algorithmes publiques existants. Parmi ceux-ci citons les plus courants :

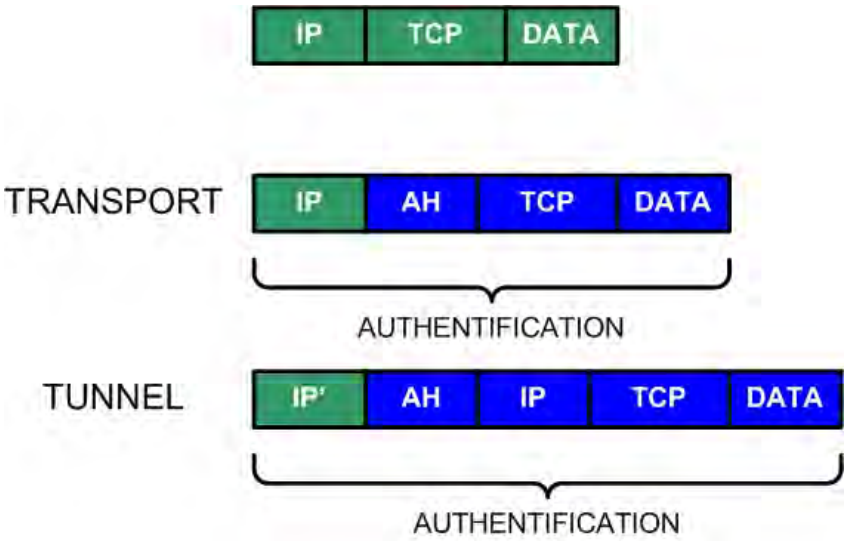
- ➔ MD5
- ➔ SHA-1

- ➔ HMAC, qui n'est pas à proprement parlé un algorithme à part entière, mais une surcouche pour MD5 et SHA dont il améliore la fiabilité.

Enfin, autre point important, AH ne fournit pas de fonctions de confidentialité. AH ne crypte pas les données.

AH

AH



AUTHENTIFICATION & INTEGRITE

L'authentification et l'intégrité, indissociables en AH, sont effectuées sur l'ensemble du datagramme IP quelque soit le mode utilisé.
Plus précisément, sur l'ensemble du datagramme sauf :

- Les champs considérés comme variables dans l'en-tête IP :
  - ➔ ToS/DSCP
  - ➔ TTL
  - ➔ FLAGS (SYN, ACK, PSH, FIN, RST)
  - ➔ Fragment offset
  - ➔ Header Checksum
- Le champ de AH contenant les données d'authentification

Voici la raison pour laquelle IPSec est incompatible avec la traduction d'adresse : l'adresse source est considérée comme un paramètre fixe. Si cette adresse est modifiée, le contrôle d'intégrité échouera et le datagramme sera détruit par le destinataire.

MODE TRANSPORT

Dans ce mode, le datagramme original est modifié pour transporter du AH.

Les données originales sont ré-encapsulées par AH.

L'authentification et l'intégrité sont réalisées sur l'ensemble du nouveau datagramme, sauf les champs précédemment cités.

MODE TUNNEL

Dans ce mode, le datagramme original complet est ré-encapsulé dans AH et un nouvel en-tête IP est créé.

L'authentification et l'intégrité sont réalisées sur l'ensemble du nouveau datagramme, sauf les champs précédemment cités du nouvel en-tête IP et de AH.

ESP

ESP

- *Encapsulating Security Payload*
- Protocole 50
- RFC 2406
- Utilisé pour protéger l'intégralité des datagrammes IP
- Protection à trois niveaux :
  - Intégrité
  - Authentification
  - Confidentialité : cryptage des données

CARACTERISTIQUES DE ESP

ESP, Encapsulating Security Payload, est l'autre protocole utilisé par IPSec.

ESP est défini dans la RFC 2406.

ESP utilise le numéro de protocole IP 50.

Selon le mode défini, ESP protégera les datagrammes ou les segments.

FONCTIONNALITES DE ESP

ESP fournit trois fonctionnalités de sécurité :

- ➔ Contrôle de l'intégrité des données échangées. La signature numérique calculée par l'expéditeur permettra au destinataire de vérifier que les données n'ont pas été altérées, volontairement ou pas, durant leur parcours.
- ➔ Authentification des intervenants. L'expéditeur et le destinataire doivent prouver leur identité respective. Cela peut être réalisé via des mots de passe secrets, des clés pré-partagées, ou bien via l'utilisation d'une paire de clé publique/clé privée.
- ➔ Confidentialité des échanges. Les données échangées ne seront lisibles que par le ou les destinataires.

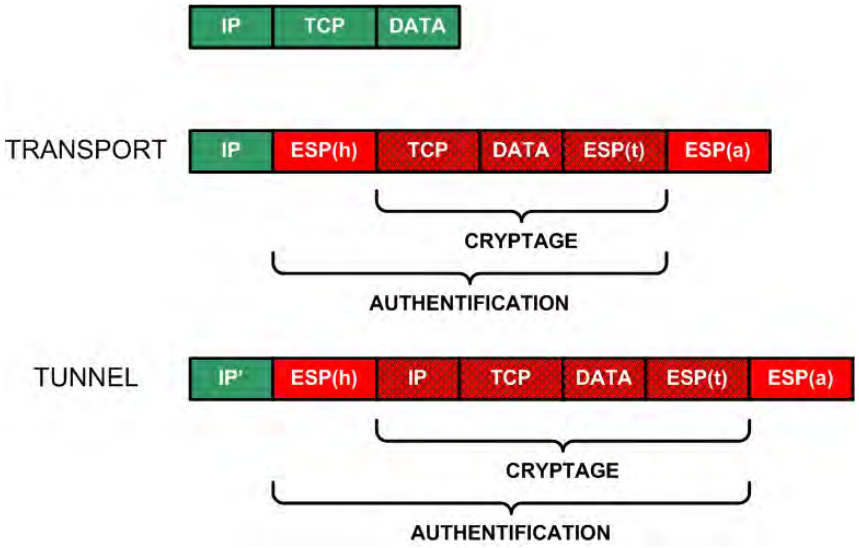
Comme pour AH, les fonctionnalités d'authentification et de contrôle d'intégrité sont très souvent couplées, réalisées simultanément par un seul algorithme. En revanche, elles ne sont pas réalisées sur l'ensemble du datagramme.

Les algorithmes supportés par ESP sont :

- ➔ Pour l'authentification et l'intégrité :
  - ✓ MD5
  - ✓ SHA-1
  - ✓ HMAC
- ➔ Pour la confidentialité :
  - ✓ DES sur 56 bits
  - ✓ DES 128 sur 128 bits
  - ✓ 3DES sur 168 bits, mais 112 bits en puissance réelle
  - ✓ AES qui utilise des clés de 128, 192 ou 256 bits
  - ✓ IDEA sur 128 bits
  - ✓ Blowfish avec des clés de 40 ou 448 bits
  - ✓ RC5 de 40 à 2040 bits
  - ✓ CAST 128 de 40 à 128 bits
- ➔ PCKS et X509v3 de RSA pour la gestion des paires de clé publique/clé privée et le format des certificats.

ESP

ESP



PROTECTION

L'authentification et l'intégrité sont effectuées sur l'ensemble du payload IP, quelque soit le mode utilisé, sauf le champ d'authentification de ESP.

Le cryptage des données est effectué sur une partie seulement du datagramme, le payload de ESP et le trailer.

ESP est divisé en trois champs distincts :

- ➔ Le HEADER ou en-tête, ESP(h)
- ➔ Le TRAILER, ou en-queue, ESP(t)
- ➔ Le champ AUTHENTICATION, d'authentification, ESP(a)

MODE TRANSPORT

Dans ce mode, le datagramme original est modifié pour transporter de l'ESP.

Les données originales sont ré-encapsulées par ESP.

L'authentification et l'intégrité sont réalisées sur l'ensemble de la partie payload du nouveau datagramme, sauf le champ d'authentification de ESP.

Le cryptage est effectué sur le payload de ESP, c'est-à-dire les données originales transportées par IP et le trailer de ESP, ESP(t).

MODE TUNNEL

Dans ce mode, le datagramme original complet est ré-encapsulé dans ESP et un nouvel en-tête IP est créé.

L'authentification et l'intégrité sont réalisées sur l'ensemble du nouveau datagramme, sauf le champ d'authentification de ESP.

Le cryptage est effectué sur l'ensemble du datagramme d'origine et le champ ESP(t).

Transformation

Transformation

- Transformation : action sur le datagramme ou le segment
- AH :
  - Une transformation, l'authentification
- ESP :
  - Une transformation
    - Authentification seule
    - Cryptage seul
  - Ou deux transformations
    - Authentification et cryptage

DEFINITION

Une transformation est définie comme une action de sécurité effectuée sur un datagramme ou un segment. L'authentification couplée au contrôle d'intégrité constitue une transformation. Le cryptage des données constitue une autre transformation.

En IPSec, il est possible de définir pour un lien VPN un maximum de trois transformations. Mais, on ne peut utiliser qu'une seule fois chaque protocole pour un type de transformation. Autrement dit, on ne peut utiliser AH qu'une seule fois et ESP qu'une seule fois. De plus, pour ESP on ne peut crypter qu'une seule fois les données et procéder à l'authentification qu'une seule fois également.

AH

AH ne peut effectuer qu'une seule transformation : authentification et contrôle d'intégrité.

ESP

Avec ESP on peut réaliser une ou deux transformations :

- ➔ Authentification et contrôle d'intégrité uniquement, une seule transformation
- ➔ Cryptage des données seules, une seule transformation
- ➔ Authentification et cryptage, deux transformations

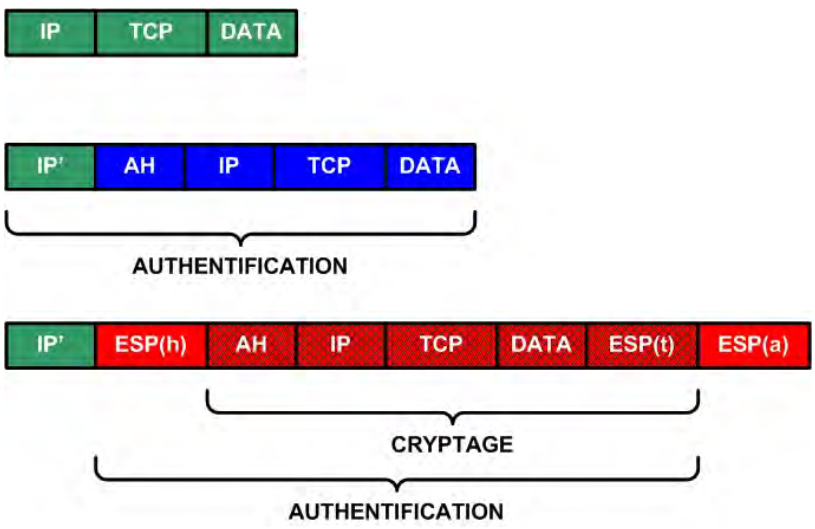
AH + ESP

Il existe vingt combinaisons possibles en utilisant AH, ESP et le mode :

- ➔ AH seul, en mode transport ou tunnel. Deux combinaisons.

- ESP seul, avec une transformation ou deux, en transport ou tunnel. Six combinaisons.
- AH et ESP, en mode tunnel ou transport. On procède à une première transformation avec AH, puis une ou deux avec ESP. La combinaison la plus fiable, surtout en mode tunnel, la plus sûre, mais également la plus lourde. Six combinaisons.
- ESP et AH, en mode tunnel ou transport. On procède à une ou deux transformations avec ESP, puis une AH. Six combinaisons.

AH-ESP en mode tunnel



La combinaison AH-ESP en mode tunnel est la plus puissante dont dispose IPSec.

Voyons le processus de transformation avec trois transformations :

- Transformation AH :
  - ✓ Le datagramme IP est intégralement ré-encapsulé dans AH.
  - ✓ Un nouvel en-tête, IP', est crée. Il transporte AH et le datagramme original.
  - ✓ AH authentifie l'ensemble du nouveau datagramme, sauf les champs considérés comme variables et le champ d'authentification de AH.
- Transformation ESP :
  - ✓ AH est à son tour ré-encapsulé dans ESP.
  - ✓ Le nouvel en-tête IP' est conservé mais modifié, le protocole IP indique maintenant ESP.
  - ✓ Le payload d'IP', à l'exception du champ ESP(a) est authentifié par ESP.
  - ✓ Le payload de ESP plus le champ ESP(t) sont cryptés par ESP. C'est-à-dire que AH lui-même est crypté par ESP.

SA

SA

- *Security Association*
- Permet la négociation des paramètres de sécurité :
  - Algorithmes : authentification, intégrité, cryptage, hachage
  - Longueur des clés
  - Périodicité de renouvellement : temps ou débit
  - Mode
- Une SA pour chaque transformation et dans chaque sens

Les SAs, Security Associations, définissent les paramètres pour établir un lien VPN :

- ➔ Algorithmes utilisés pour l'authentification, l'intégrité, le cryptage, le hachage.
- ➔ La longueur des différentes clés utilisées.
- ➔ La périodicité de renouvellement des clés et des SAs elles-mêmes. Le critère peut porter sur le temps ou le débit. Par exemple, une clé peut être renouvelée toutes les heures ou tous les 100Mo échangés. Au premier terme échu, la clé sera changée.
- ➔ Le mode utilisé : tunnel ou transport.

Les SAs sont négociées par les deux intervenants en utilisant IKE/ISAKMP avant l'établissement du lien IPSec proprement dit. Il faut qu'il existe deux SAs se correspondant de chaque côté. On peut définir plusieurs SAs pour une même connexion IPSec, mais une seule, en finalité, sera utilisée.

Il faut une SA pour chaque transformation et chaque sens. En fait, les SAs fonctionnent par paires qui doivent se correspondre. Ce qui signifie que l'on peut définir des règles de cryptage asymétriques entre deux entités utilisant un lien IPSec. Par défaut, toutefois, les règles sont symétriques.

Par exemple, supposons que nous ayons un lien IPSec entre A et B en AH-ESP avec trois transformations. En tout, il faut 6 SAs :

- ➔ Une SA entre A et B pour AH
- ➔ Une SA entre B et A pour AH
- ➔ Une SA entre A et B pour l'authentification ESP
- ➔ Une SA entre B et A pour l'authentification ESP
- ➔ Une SA entre A et B pour le cryptage ESP
- ➔ Une SA entre B et A pour le cryptage ESP

IKE - ISAKMP

IKE - ISAKMP

- *Internet Key Exchange*
  - RFC 2409
  - Ensemble des règles de négociation des SAs
  - On attribue des niveaux de priorité à chaque SA négociable
  - Lié intrinsèquement à ISAKMP
- *Internet Security Association and Key Management Protocol*
  - RFC 2408 et 2412
  - UDP 500
  - Protocole utilisé pour la négociation dynamique

IKE

IKE, Internet Key Exchange, définit l'ensemble des règles de négociation des SAs.

IKE est défini par la RFC 2409.

Le principe est d'attribuer des niveaux de priorité à chaque SA négociable.

ISAKMP/OAKLEY

ISAKMP, Internet Security Association and Key Management, est un protocole permettant d'établir un tunnel sécurisé avant la mise en place du lien IPSec proprement dit. Son rôle est de permettre la négociation dynamique sécurisée des SAs, et l'échange éventuel de clé.

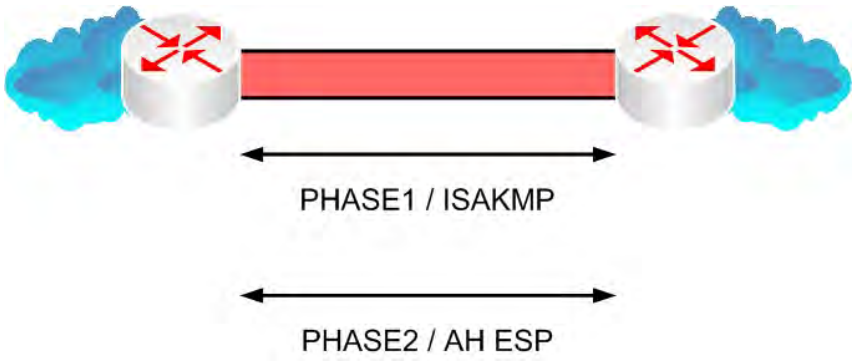
ISAKMP est défini par les RFCs 2408 et 2412.

ISAKMP utilise le port UDP 500.

L'usage de ISAKMP n'est pas obligatoire, il est tout à fait possible de configurer des paramètres en dur pour un lien VPN IPSec. Toutefois, le niveau de sécurité s'en trouve affaibli. N'oubliez pas que plus longtemps une clé est utilisée plus il y a de risque qu'elle soit dévoilée. Avec ISAKMP, il est possible de changer de stratégie de sécurité IPSec à intervalles réguliers de manière entièrement dynamique.

Établissement des tunnels

Etablissement des tunnels



Il existe deux phases d'établissement d'un lien VPN en IPSec :

PHASE 1

La phase 1 utilise IKE et un tunnel ISAKMP pour les négociations des SAs. La phase 1 est utilisée initialement avant l'établissement du VPN IPSec lui-même. On peut définir un intervalle de validité de cette négociation (Main Mode). A échéance de l'intervalle, les SAs seront renégociées.

PHASE 2

La phase 2 correspond à l'établissement du VPN IPSec lui-même, c'est-à-dire à l'utilisation de AH et/ou de ESP.

Il est possible de ne renouveler que les clés utilisées pour le lien, sans être obligé de relancer tout le processus complet d'ISAKMP, en utilisant un intervalle de validité prédéfini… dans la négociation des SAs (Agressive Mode).

VPDN

- *Virtual Private Dialup Network*. Par rapport au VPN, la différence se situe au niveau des couches transportées : en VPDN, on transporte du niveau 2 dans du niveau 3, 4 ou 5
- Fonctionnalités :
  - Authentification locale ou déportée
  - Intégrité
  - Confidentialité
- Exemples :
  - PPTP, TCP 1723, développé notamment par Microsoft
  - L2TP, UDP 1701, évolution standardisée du protocole L2F de CISCO

Les VPDNs, Virtual Dialup Private Networks, se différentient des VPNs par le niveau d'encapsulation qu'ils fournissent. Un VPDN permet de transporter et de sécuriser des protocoles de niveau 2 en utilisant des protocoles de niveau 3, 4 ou 5.

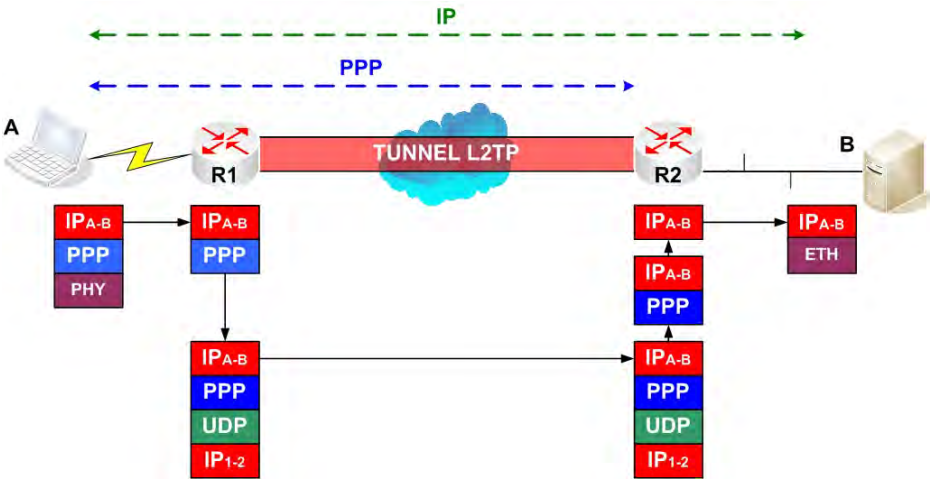
Les fonctionnalités sont les mêmes que celles fournies par les VPNs :

- ➔ Authentification, locale ou déportée. Une authentification déportée permet d'effectuer cette opération par une entité extérieure au réseau d'accueil.
- ➔ Intégrité
- ➔ Confidentialité

Exemple de protocoles VPDN :

- ➔ PPTP qui utilise le port TCP 1723 et le protocole GRE. Ce protocole a été développé afin de permettre de s'affranchir de la limite principale de PPP, le fait qu'il soit point à point. Avec PPTP, on peut « traverser » Internet, ou plus simplement des réseaux IP, pour établir une connexion sécurisée avec un routeur, un firewall ou un serveur. De fait, les trames PPP sont encapsulées par GRE. Le port TCP 1723 étant utilisé pour la signalisation. Sa simplicité de mise en place et de configuration le prédestine à un usage sur les postes nomades, ce qui était d'ailleurs son but original.
- ➔ L2TP. Dérivé du protocole L2F de CISCO. Contrairement à ce dernier, L2TP est libre et normalisé. L2TP permet lui aussi de s'affranchir de la limitation point à point de PPP. Il est destiné à un usage interne chez les opérateurs, beaucoup plus rarement pour un usage direct itinérant.

L2TP



La problématique qui a initialement conduit à développer L2TP (en fait son ancêtre L2F, pour être tout à fait exact) est la suivante :

Comment faire en sorte qu'un utilisateur itinérant (roaming) puisse se connecter à distance partout dans le monde au réseau de son entreprise, dans les conditions suivantes :

- Il ne faut pas que cela coûte une fortune à son employeur
- La qualité de liaison doit être un minimum garantie
- L'authentification d'accès doit pouvoir être déportée chez le client, qui peut ainsi garder le contrôle de ses accès
- Garantir un niveau de sécurité adapté
- Que cet accès itinérant ne nécessite pas l'installation d'un nouveau protocole sur les portables et reste simple à configurer

La solution a été apportée de la manière suivante par L2TP : on simule un lien PPP entre la machine itinérante et le point d'accès au réseau à travers n'importe quel réseau IP en transportant les trames PPP sur UDP. En effet, PPP ne fonctionne qu'en point à point mais offre les autres fonctionnalités demandées.

Prenons un exemple :

- Une machine itinérante A veut accéder à son réseau d'entreprise afin de pouvoir joindre le serveur B.
- L'entreprise dispose d'un abonnement roaming, itinérant pour son utilisateur. L'opérateur lui a fourni :
  - ✓ Une liste de numéros de téléphones à utiliser dans différents états ou pays selon l'abonnement

- ✓ Un login et un mode passe. Le login est généralement du genre xxxx@codeoperateur.yy

➔ Lorsque l'utilisateur veut accéder à son réseau d'entreprise, il compose le numéro fourni par l'opérateur correspondant à sa localisation physique et utilise toujours le même login et le même mot de passe.

➔ Le portable va alors tenter d'établir une connexion PPP avec le point d'accès au réseau distant, R2… en appelant R1.

➔ Quand R1 reçoit l'appel de A, il reconnait « codeoperateur » et va établir un tunnel L2TP avec R2. C'est R2 qui authentifiera l'ouverture de session avec A. D'un point de vue PPP, la session est établie entre A et R1, R2 jouant le rôle de relais.

➔ Les données PPP reçues par R1, une fois la session établie, seront encapsulées dans des paquets L2TP et envoyées à R2. Celui-ci les désencapsulera et récupérera les données et les transmettra en interne à destination du serveur B.

- *Fonctions*
- *Testeur de câbles*
- *Analyse de trames*
- *SNMP*
- *MIB*

10

Administration

Objectifs

Ce module traite de l'administration des réseaux.

Connaissance

- Présentation des tâches et fonctions d'un administrateur réseau
- Les testeurs de câbles
- L'analyse de trames
- SNMP

Progression

Fonctions des administrateurs réseau	Présentation de SNMP
Testeurs de câbles	Composants
Analyse de trame	MIB

Fonctions des administrateurs réseaux

- Gestion de la configuration
- Gestion de la sécurité
- Gestion des pannes
- Audit des performances
- Gestion de la comptabilité

L'administration des réseaux devient une tâche de plus en plus complexe. Car les réseaux eux-mêmes le sont devenus. Aujourd'hui, un administrateur peut rarement faire face seul, et ce, malgré sa bonne volonté et ses compétences. Les outils et les logiciels d'administration ont connu un développement symétrique à la complexification des réseaux.

Nous allons étudier les différentes tâches qui incombent à un administrateur réseau :

- Gestion de la configuration.
- Gestion de la sécurité.
- Gestion des pannes.
- Audit des performances.
- Gestion de la comptabilité.

Fonctions des administrateurs réseaux

- Gestion de la configuration
  - Collecte des informations d'état des systèmes
  - Contrôle des états des systèmes
  - Sauvegarde et historique de l'état
  - Présentation de l'état du système
- Gestion de la sécurité
  - Mécanismes de détection
  - Mécanismes de protection
  - Procédures

GESTION DE LA CONFIGURATION

La gestion de la configuration est une tâche essentielle des réseaux actuels. Il est, et il sera, de plus en plus difficile de maitriser l'ensemble des paramètres des différents systèmes. Il faut donc être apte à remettre en l'état le plus rapidement possible tout élément constitutif du réseau.

La gestion de la configuration englobe les points suivants :

- Collecte des informations d'état des systèmes. Cette opération peut être réalisée manuellement ou automatiquement. La plupart des logiciels d'administration proposent cette fonctionnalité, ce qui permet une gestion plus efficace et plus pertinente.
- Contrôle des états des systèmes. Cette tâche permet de vérifier la cohérence des états et de la configuration. Et, éventuellement, d'en détecter les interférences.
- Sauvegarde et historique de l'état. Cette opération doit être réalisée à intervalles réguliers ou avant et après une modification importante du paramétrage. L'historique permettra de constituer une base de données permettant de déterminer l'origine d'un problème ou d'une panne.
- Présentation de l'état du système. Ce qui peut prendre diverses formes :
  - ➔ Rapport rédigé ou directement édité par le logiciel d'administration.
  - ➔ Graphiques synthétiques. Plus lisibles, plus compréhensibles par les décideurs et les autres intervenants.
  - ➔ Des statistiques brutes réutilisées par d'autres applications.

GESTION DE LA SECURITE

Un domaine de plus en plus vaste. La sécurité est un domaine transversal, de plus en plus intrusif et contraignant. Son administration l'est tout autant.

La forte tendance actuelle est d'utiliser des outils puissants et centralisés qui permettent à l'administrateur de se libérer des tâches les plus lourdes et rébarbatives comme l'analyse de log, la classification des attaques et les procédures réactives. Néanmoins, l'humain garde plus que jamais sa place, car une attaque structurée et efficace a toujours une origine humaine, dont le but est justement de mettre en défaut la logique automatisée des applications de sécurité. Le vrai rôle de ces applications est de libérer le temps et l'énergie de l'administrateur pour pouvoir réagir promptement et efficacement en cas de crise non gérable logiciellement.

La gestion de la sécurité inclut les éléments suivants :

- Les mécanismes de détection. Comment détecter une intrusion ? L'altération d'un service ? La violation d'une règle ? La perturbation d'un service ? La modification de données ? L'usurpation d'identité ?... comme nous l'avions dit, le domaine est vaste. Les outils, firewalls, sondes d'intrusion, anti-virus, logiciels de corrélation, sont de plus en plus performants et efficaces.
- Mécanismes de protection. Ils sont à la hauteur de la complexité de la tâche : nombreux et complexes :
  - ➔ Les mécanismes d'authentification. Ce qui permet de s'assurer de l'identité des intervenants.
  - ➔ Les mécanismes d'intégrité. Garantir l'acheminement des données sans altération et sans modification.
  - ➔ Les mécanismes de confidentialité. Seuls les intervenants destinataires des données pourront les visualiser en clair.
  - ➔ Les mécanismes d'autorisation. Souvent implémentés dans les éléments dits filtrants (firewalls, ACL, routeurs filtrants...). Leur rôle est d'autoriser le transit des données de sources préalablement autorisées ou authentifiées.
  - ➔ Les mécanismes de comptabilité. Ce qui inclut l'audit, la facturation, le suivi des utilisateurs et de leurs privilèges.
- Les procédures. Quelles procédures mettre en place ? Quant une attaque est détectée ? Quant une ressource critique du réseau ou de l'entreprise est en péril ? L'établissement, le respect et l'évolution de ces procédures doivent tenir compte :
  - ➔ Du fonctionnement du réseau
  - ➔ Du caractère critique de chaque élément exposé
  - ➔ De l'état du système
  - ➔ De l'historique des attaques
  - ➔ Du facteur humain
  - ➔ Des contraintes légales…

Fonctions des administrateurs réseaux

- Gestion des pannes
  - Signalisation de fonctionnement anormal
  - Localisation / isolation
  - Défaut internes / externes
  - Réparation / contournement
  - Confirmation du retour à la normale ou contraintes
- Audit des performances
  - Statistiques
  - Performances
  - Prévisions

GESTION DES PANNES

La gestion de pannes est une des tâches habituelles et ingrates des administrateurs réseaux.

Les points suivants sont inclus dans la gestion des pannes :

- Signalisation de fonctionnement anormal. Quels outils et quelles procédures sont en place pour la détection d'un fonctionnement anormal d'un élément du réseau ? Quels seuils ont été définis pour quels critères ? Quel est le niveau critique de chaque disfonctionnement ?
- Localisation / isolation. Le premier objectif n'est pas toujours la résolution immédiate de la panne. Sauf, bien entendu, si la panne est triviale. Autrement, il faut tenter de l'isoler en éliminant les causes possibles une à une. La complexité croissante des réseaux contraint fortement à appliquer des procédures structurées et efficaces. Les pannes complexes impliquent généralement plusieurs facteurs simultanément, car l'imbrication des fonctionnalités est de plus en plus grande. Par exemple, s'il n'y a plus de ToIP sur votre réseau. Le problème peut provenir des machines d'extrémité, de la QoS, de la Gatekeeper, des routeurs, des commutateurs, de la sécurité… le champ d'investigation est vaste. De plus, la QoS peut mal fonctionner parce qu'un routeur fonctionne mal, lui-même fonctionnant mal, car un commutateur a un problème, etc.
- Réparation. Une fois la panne localisée ou isolée, il faut :
  - ➔ La réparer si c'est possible ;
  - ➔ Etablir un diagnostic et définir les conditions de réparation. Une pièce qui ne peut être changée immédiatement, une modification de la configuration trop délicate à effectuer en production, une mise à jour obligatoirement réalisée hors ligne…

- ➔ Remonter le problème au support de niveau supérieur. Il peut être interne, chez le distributeur, une société de service ou directement chez le constructeur.

- Confirmation du retour à la normale. Vérifier que tout fonctionne de nouveau normalement. Dans le cas contraire, identifier les contraintes provisoires ou permanentes que cela va engendrer.

Audit des performances

L'audit des performances est une partie parfois laissée pour compte. Ce qui est fort dommage et souvent préjudiciable pour le bon fonctionnement d'un réseau. Cet audit permet souvent de déceler des dysfonctionnements qui ne le seraient pas par les moyens conventionnels. De plus, les informations recueillies permettent souvent d'anticiper les évolutions nécessaires ou possibles d'un réseau.

Les éléments constitutifs de l'audit des performances sont les suivants :

- Gestion des statistiques :
  - ➔ Collecte. Quels moyens sont utilisés pour remonter, collecter les informations des éléments constitutifs des réseaux ? Quelles informations collecter ? Quelle granularité ?
  - ➔ Contrôle. Comment ces performances sont contrôlées ? Sur quels critères ? Sur quelles procédures d'évaluation ?
  - ➔ Stockage. Il est indispensable afin d'avoir un base référentielle et évolutive de l'état du réseau.
  - ➔ Présentation. Diverses formes sont possibles : données brutes, graphiques…
- Les performances proprement dites. Elles sont logiquement basées sur des statistiques. Les valeurs mesurées sont en général :
  - ➔ Les temps de réponse. Par tranche horaire, selon la charge, selon le nombre d'utilisateurs…
  - ➔ Les débits. En bis/s, en caractères/s, en trames/s, selon les tranches horaires…
  - ➔ Les taux d'erreur. Absolus, pondérés, relatifs…
  - ➔ La disponibilité. Critère qui a pris une place très importante, voire cruciale ces dernières années. Le 100% est illusoire.
    On vise soit les quatre 9 : 99,99% sur une année. Soit les cinq 9 : 99,999 % sur une année. Ce qui nous donne, respectivement, 52' et 5' d'indisponibilité sur une année !

Fonctions des administrateurs réseaux

- Gestion de la comptabilité
  - Relevés
  - Réseau
  - Déroulement de la comptabilité

GESTION DE LA COMPTABILITE

La gestion de la comptabilité consiste à établir les coûts, facturables ou non, d'utilisation des services et ressources du réseau. Les éléments en sont les suivants :

- Les relevés :
  - ➔ Par réseau.
  - ➔ Par application ou service.
- Le réseau :
  - ➔ Les unités reçues et envoyées. Ce qui est souvent noté : PDUs E/R.
  - ➔ Les caractères reçus et envoyés.
  - ➔ Dates de début et de fin des connexions ou des sessions.
- Déroulement de la comptabilité :
  - ➔ Négociation. Quels sont les protocoles en place ? Quelles sont les modalités d'application de ces protocoles ?
  - ➔ Activation. Comment et quand sera activée la comptabilité ?
- Collecte :
  - ➔ Modalités. Granularité, pondération, étalement…
  - ➔ Report. Sous quelle forme seront effectués les reports.
  - ➔ Contrôle. Quelles garanties sur les reports ?

Testeurs

- Testeurs de câbles :
  - Vérification des paramètres physiques
  - Détection des coupures ou les altérations
  - Réalisation de tests
  - Génération de rapports

TESTEURS DE CABLES

Les testeurs de câbles sont des appareils permettant de réaliser un certain nombre d'opérations matérielles sur les réseaux filaires, optiques, radio ou satellite :

- Vérification des paramètres physiques. Impédance, atténuation, déperdition, déphasage, longueur…
- Détection des coupures ou des altérations. Câbles sectionnés, fibre trop courbée…
- Réalisation de tests. En charge, en provoquant des erreurs, des trames trop longues, etc.
- Génération de rapports. Sous forme graphique ou brute.

Analyse de trafic réseau

- L'analyse de trame permet l'analyse des couches réseaux, 2 à 4
- Certains outils permettent également l'analyse de certaines couches applicatives standard
- Plusieurs utilisations :
  - Analyse globale du trafic
  - Analyse du trafic réseau d'une application ne fonctionnant pas normalement
  - Recherche, surveillance de certains mécanismes suspects
  - Meilleure compréhension du fonctionnement d'une application

ANALYSE RESEAU

- L'analyse de trame consiste à décortiquer ce qui se passe sur le réseau au niveau des couches 2 à 4, les couches réseaux proprement dites. Voir, pour certains outils, de permettre également l'analyse au niveau de certaines couches applicatives standard.
- L'analyse réseau permet plusieurs utilisations :
  - ➔ Analyse globale du trafic : détection des dysfonctionnements, des goulets d'étranglement, des serveurs congestionnés…
  - ➔ Analyse du trafic réseau d'une application ne fonctionnant pas normalement
  - ➔ Recherche, surveillance de certains mécanismes suspects
  - ➔ Meilleure compréhension du fonctionnement d'une application dans un but d'optimisation

Analyseurs de trafic réseau

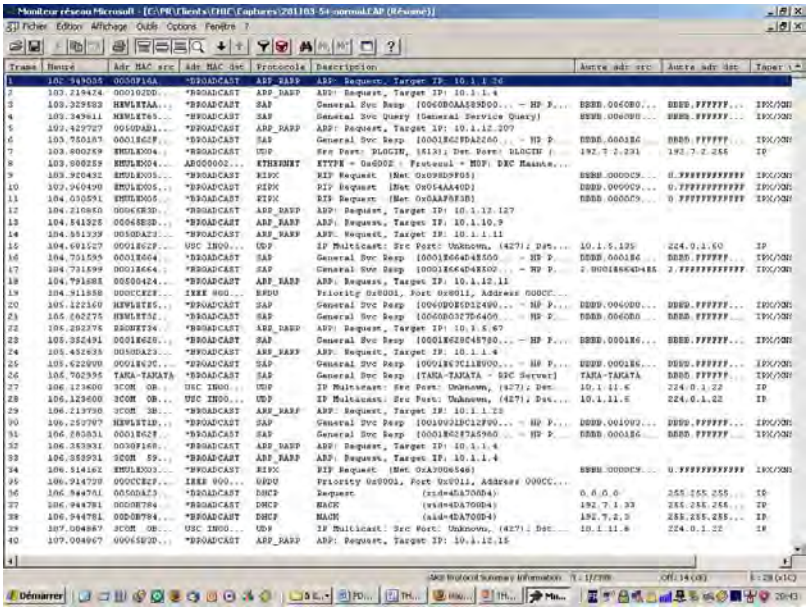
- Outils permettant d'analyser le trafic réseau des couches 2 à 4 et certaines couches 5
- Deux types :
  - Logiciels : s'installent sur un OS. Souples d'utilisation, moins contraignants.
  - Matériels : boîtier dédiés. Très performants. Contraignants. Coût important.
- Généralement installés sur un poste d'administration ou sur un portable
- Grâce au SPAN et RSPAN, l'analyse du trafic réseau est devenue beaucoup plus souple
- Quelques références : Sniffer Pro, Network Monitor, Ethereal, TCP Dump

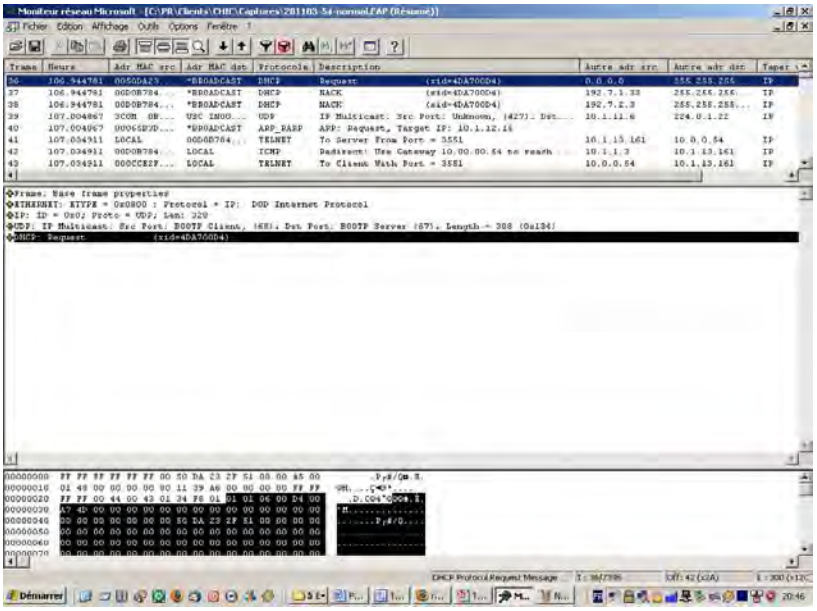
---

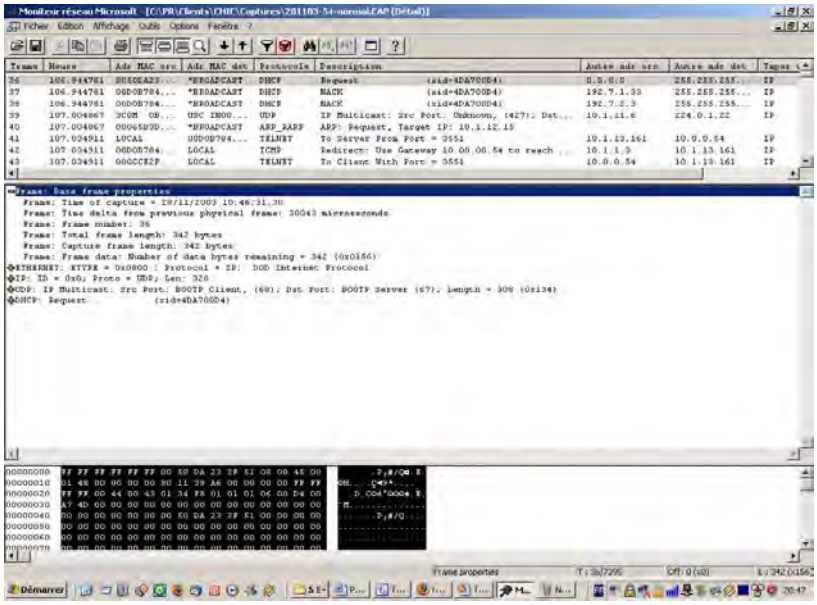
ANALYSEUR DE TRAFIC RESEAU

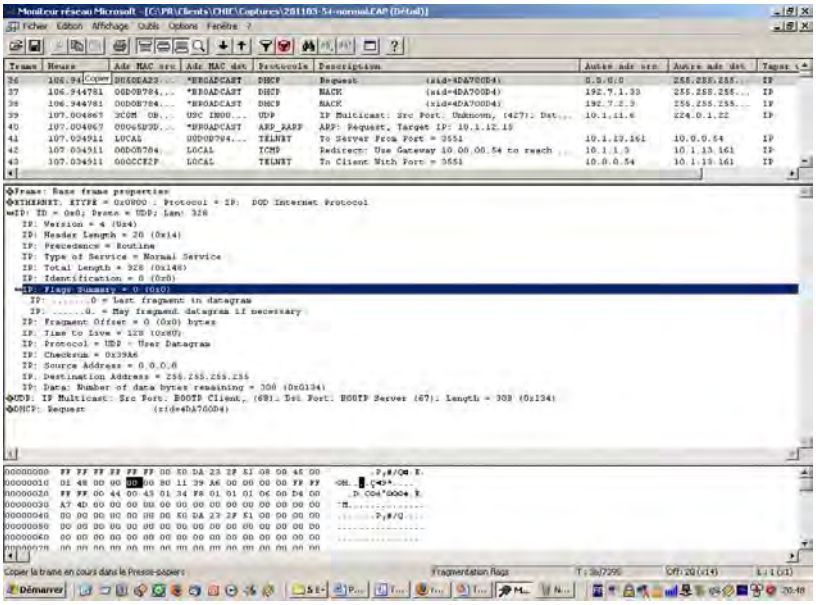
- Outils permettant d'analyser le trafic réseau des couches 2 à 4 et certaines couches 5
- Deux types :
  - ➔ Logiciels : s'installent sur un OS. Souples d'utilisation, moins contraignants.
  - ➔ Matériels : boîtier dédiés. Très performants. Contraignants. Coût important.
- Généralement installés sur un poste d'administration ou sur un portable
- Grâce au SPAN et RSPAN, l'analyse du trafic réseau est devenue beaucoup plus souple
- Quelques références : Sniffer Pro, Network Monitor, Ethereal, TCP Dump

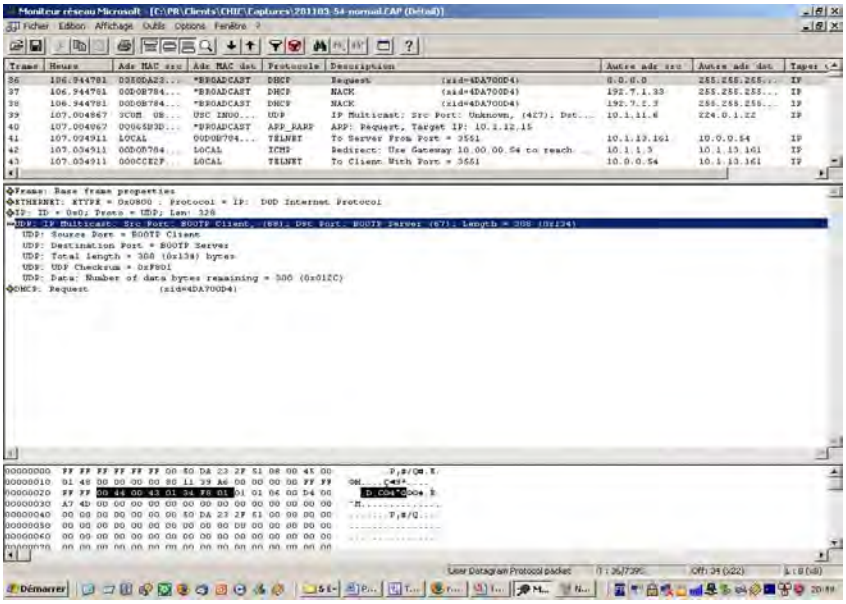
QUELQUES EXEMPLES

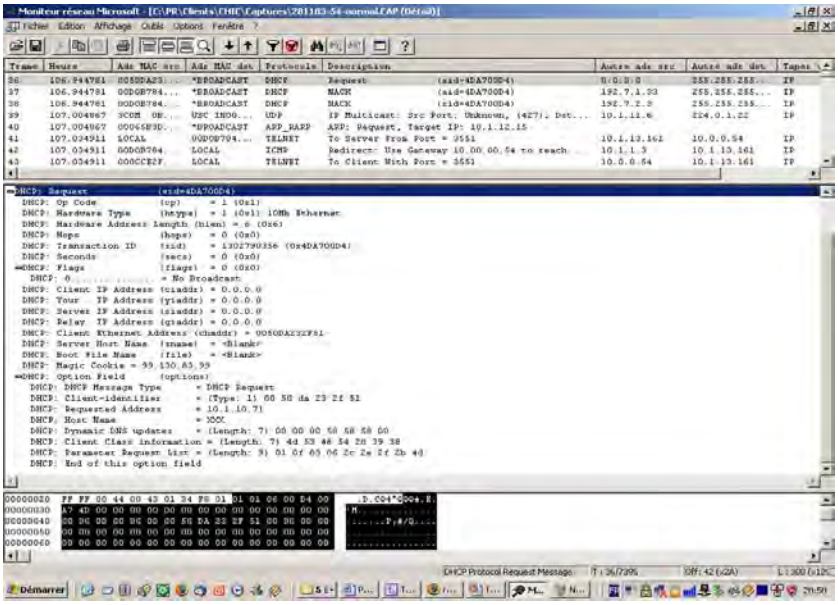


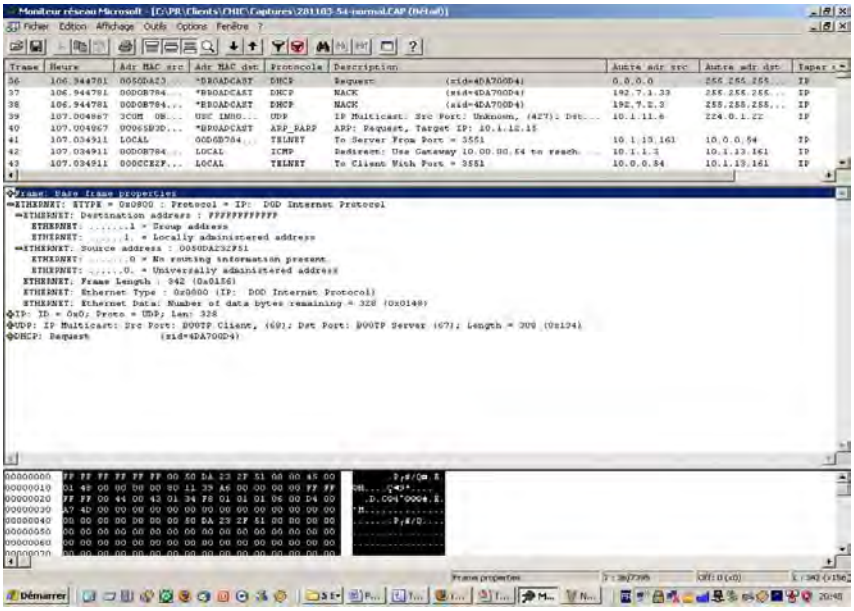


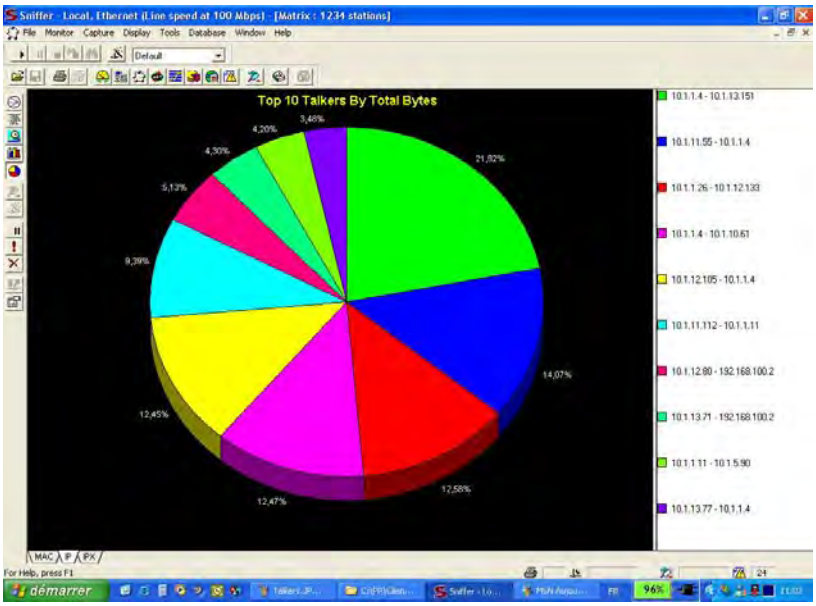


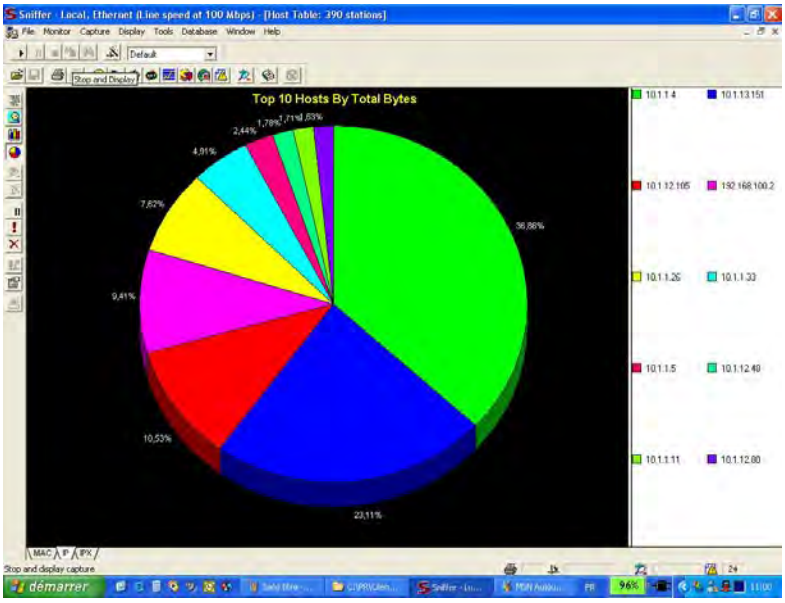


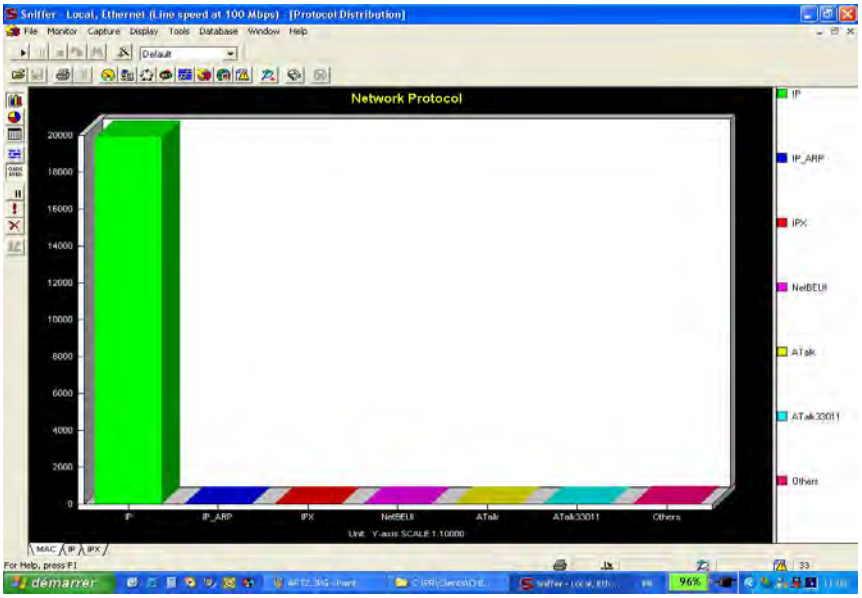


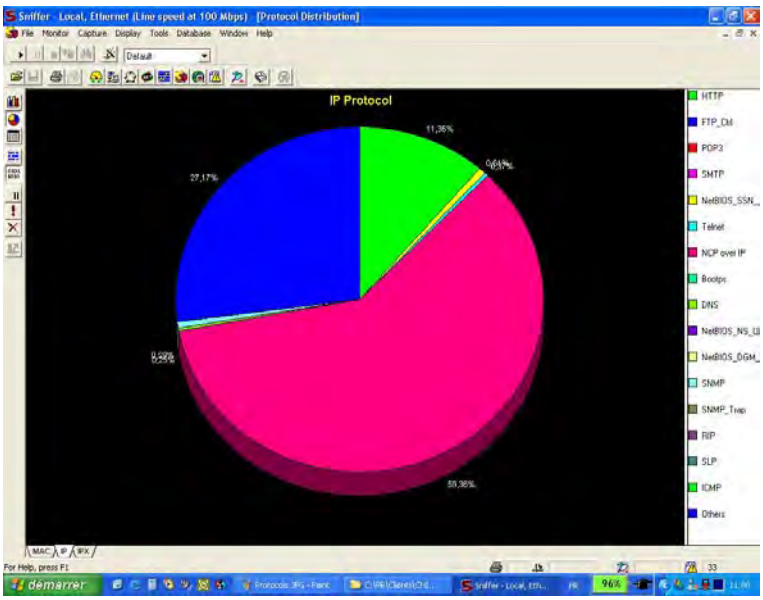


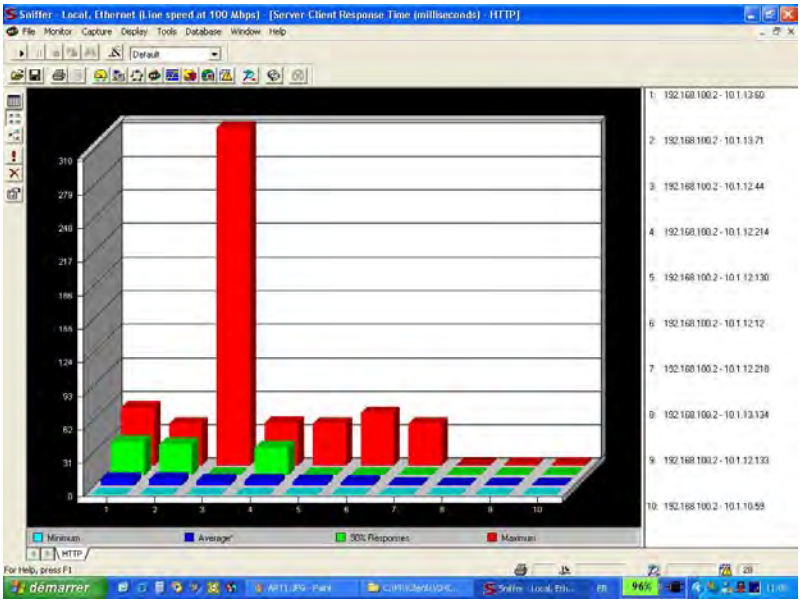



Top 10 Talkers By Total Bytes
21,82%
14,07%
12,58%
12,47%
12,45%
9,39%
5,12%
4,50%
4,20%
3,46%
10.1.1.4 - 10.1.12.151
10.1.11.55 - 10.1.1.4
10.1.1.26 - 10.1.12.133
10.1.1.4 - 10.1.10.61
10.1.12.105 - 10.1.1.4
10.1.11.112 - 10.1.1.11
10.1.12.80 - 192.168.100.2
10.1.13.71 - 192.168.100.2
10.1.1.11 - 10.1.5.90
10.1.13.77 - 10.1.1.4


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Host Table: 390 stations]
Top 10 Hosts By Total Bytes
36,86%
23,11%
10,53%
9,41%
7,82%
4,91%
2,44%
1,78%
1,71%
1,53%
10.1.1.4
10.1.13.151
10.1.12.105
192.168.100.2
10.1.1.26
10.1.1.33
10.1.1.5
10.1.12.40
10.1.1.11
10.1.12.80
démarrer


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Protocol Distribution]
Network Protocol
IP
IP_ARP
IPX
NetBEUI
ATalk
ATalk33011
Others
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
démarrer


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Protocol Distribution]
IP Protocol
11,36%
27,17%
59,36%
HTTP
FTP_Ctl
POP3
SMTP
Telnet
DNS
SNMP
RIP
SLP
ICMP
Others
démarrer


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Server Client Response Time (milliseconds) - HTTP]
Minimum
Average
50% Responses
Maximum
démarrer

SNMP

- Présentation
- Commandes
- Configuration
- MIB
- Produits

SNMP est un protocole standard de gestion des réseaux IP.

Nous allons voir dans cette partie :

- Une présentation de SNMP, son rôle et ses intérêts.
- Les principales commandes des différentes versions de SNMP.
- Les étapes de configuration d'un client et d'un serveur SNMP.
- Ce qu'est la MIB, son rôle et les différents types existants.
- Un tour d'horizon des principaux produits disponibles sur le marché.

Présentation de SNMP

- Protocole d'administration centralisée, libre et normalisé
- Fonctionne en client/serveur sur les ports UDP 161 et 162
- Permet d'administrer des machines sans en connaitre les interfaces et les commandes
- Utilise des tables MIB afin de remonter les informations des agents vers le gestionnaire central ou serveur
- Activable sur la quasi totalité des machines IP
- Trois messages serveur : GetRequest, GetNextRequest, SetRequest
- Deux messages agent : GetResponse, TRAP

Les caractéristiques essentielles de SNMP sont les suivantes :

- SNMP (Simple Network Managemet Protocol) est un protocole d'administration centralisée, libre et normalisé.
- La version actuelle est la 3.
- SNMP fonctionne en client/serveur, le serveur utilise le port UDP 162, le client utilise le port UDP 161.
- Le serveur est appelé gestionnaire et le client agent.
- La quasi-totalité des machines IP d'aujourd'hui inclut un agent SNMP.
- Il faut une application spécifique pour le gestionnaire SNMP.
- SNMP peut remonter des informations, des statistiques et modifier la configuration des machines.
- Le principe de base de SNMP est de pouvoir administrer des machines IP sans en connaitre les interfaces ou les commandes, en revanche il faut connaitre les variables que supportent les machines administrables. Ce rôle est alloué aux tables MIB (Management Information Base).
- Les tables MIB permettent de connaitre les variables supportées par un matériel donné. Les informations utiles concernant un routeur ne sont pas les mêmes que celle d'un serveur par exemple.
- SNMP n'utilise, de base, que cinq types de messages :
  - ➔ Trois entre le gestionnaire et l'agent : GetRequest, GetNextRequest, SetRequest
  - ➔ Deux entre l'agent et le serveur : GetResponse, Trap

Messages SNMP

- GetRequest : permet d'obtenir une information de la part de l'agent. Des codes spécifiques sont utilisés
- GetNextRequest : permet d'obtenir l'information suivante, dans le cas de plusieurs réponses
- SetRequest : permet de modifier des paramètres de la machine cliente
- GetResponse : message de l'agent en réponse à une requête du gestionnaire
- Trap : message initié par l'agent en cas de dépassement d'un seuil ou d'une valeur fixée par le gestionnaire

Les messages de base de SNMP sont les suivants :

- GetRequest : envoyé par le gestionnaire à l'agent, il permet d'obtenir des informations ou des statistiques. On utilise des codes prédéfinis et normalisés en utilisant les tables MIB. On peut obtenir toutes sortes d'informations sur la configuration IP, les flux de données, les erreurs, les interfaces, les statistiques de fonctionnement, le système, les applications, le matériel, etc.
- GetNextRequest : permet d'obtenir l'information suivante. Par exemple, pour obtenir toutes les adresses IP d'un routeur, ce message sera envoyé séquentiellement jusqu'à ce que le gestionnaire reçoive une réponse nulle, signifiant que l'information concernant cette variable était la dernière.
- SetRequest : permet au gestionnaire de modifier des paramètres IP, système, etc. sur la machine administrée.
- GetResponse : réponse de l'agent à une requête GET ou SET du gestionnaire.
- Trap : envoyé par l'agent lorsqu'un seuil préalablement défini par une commande Set est atteint. Par exemple, l'espace disque dur disponible sur une partition donnée, un taux d'erreur sur une interface réseau…

MIB

- Management Information Base
- Décrit les informations que l'on peut collecter sur les machines
- Présente sur les machines administrables
- Nécessite leur compilation sur le gestionnaire
- Plusieurs types :
  - Standards : MIB II
  - Spécifiques : routage, téléphonie, serveurs…
  - Propriétaires : CISCO, Microsoft…

PRESENTATION

La MIB (Management Information Base) est la base de données normalisée qui contient les informations de gestion, toutes les variables utilisables par le gestionnaire pour gérer les agents SNMP.

Il y a trois catégories de données :

- Les informations, collectables sur l'agent via les commandes GET et GETNEXT.
- Les paramètres, modifiables via la commande SET.
- Les alarmes, dont les valeurs et les seuils peuvent être définis par la commande SET.

Cette table MIB est présente sur l'agent et sur le gestionnaire, ce qui permet au gestionnaire d'administrer les machines indépendamment du matériel et des logiciels, dont le système d'exploitation.

Les échanges entre le gestionnaire et les agents sont normalisés, l'agent étant chargé de « traduire » les requêtes au format adéquat sur la machine.

Un client peut intégrer plusieurs MIB. L'intégration supplémentaire d'une MIB au gestionnaire est appelée compilation.

TYPES DE MIB

Comme il existe différents types de machines, il existe plusieurs types de MIB. Chaque type correspondant aux spécificités des machines administrées.

Les types sont :

- Standard : la MIB II, qui contient les données communes aux machines IP les plus usuelles.
- Spécifiques : routage, téléphonie, serveurs… Ces MIB sont dédiées à des usages spécifiques correspondant aux types de machines administrées.
- Propriétaires : certains constructeurs ou éditeurs publient des tables permettant d'administrer leurs matériels ou leurs logiciels avec un gestionnaire SNMP, c'est le cas de CISCO, MICROSOFT…

Configuration

- Sur le client :
  - Définition des adresses IP des gestionnaires dont l'agent acceptera les requêtes
  - Définition des mots de passe (community) :
    - Un mot de passe en lecture (GET, GET NEXT)
    - Un mot de passe en écriture (SET)
- Sur le gestionnaire :
  - Déclaration des agents à administrer
  - Compilation éventuelle des tables MIB spécifiques

Pour configurer un système SNMP, il faut effectuer les étapes suivantes :

SUR LE CLIENT

Déclaration des adresses IP des gestionnaires pour lesquels l'agent acceptera des requêtes. Il est possible d'autoriser toutes les adresses, dans ce cas ce seront les mots de passe qui permettront l'accès ou non.

Définition des mots de passe ou communauté (community). Il y a deux niveaux de privilèges, chacun accessible selon la communauté :

- READ : autorise les commandes GET et GET NEXT.
- READ/WRITE : autorise en plus la commande SET.

SUR LE GESTIONNAIRE

- Déclaration des agents à administrer. Pour chaque agent, les paramètres suivants sont définissables :
  - ➔ L'adresse IP par laquelle la machine est joignable. Dans certains cas, il peut y en avoir plusieurs, pour les routeurs par exemple.
  - ➔ Le ou les mots de passe. On peut définir un mot de passe pour l'accès READ et un pour l'accès READ/WRITE.
  - ➔ Les tables MIBs utilisables avec l'agent.
- Compilation éventuelle des tables MIBs supplémentaires nécessaires.

Evolutions

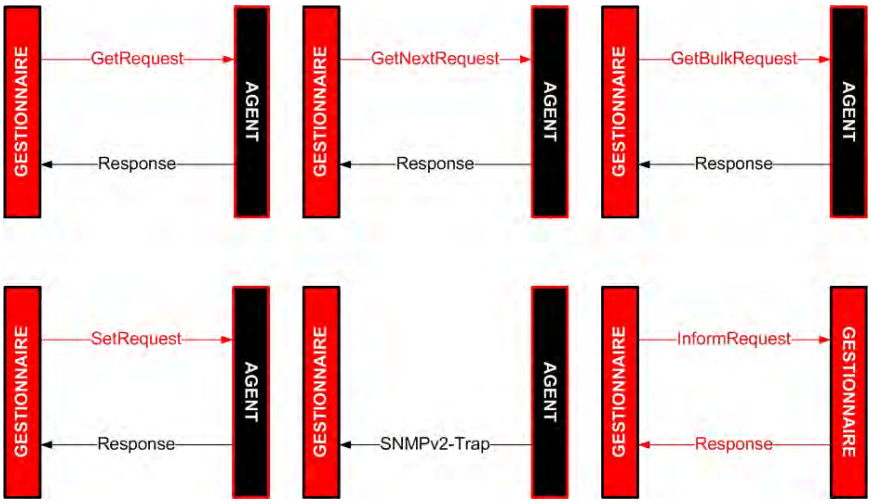
- SNMPv2
  - GetBulkRequest, permet la recherche d'un bloc de données
  - InformRequest
  - GetResponse devient Response
  - SNMPv2-Trap remplace Trap
  - Evolution des MIBs vers plus de souplesse et de richesse
- SNMPv3
  - Authentification des messages (MD5-HMAC et SHA1-HMAC)
  - Confidentialité des messages : DES 128 bits

EVOLUTIONS DE SNMPv2

La version 2 de SNMP a apporté les évolutions suivantes :

- De nouveaux messages :
  - ➔ GetBulkRequest qui permet la recherche d'un bloc de données. On peut ainsi, notamment, récupérer toutes les valeurs d'une table plutôt que la parcourir séquentiellement avec GET et GETNEXT.
  - ➔ InformRequest qui est utilisé entre les gestionnaires afin d'échanger des informations.
  - ➔ SNMPv2-Trap qui remplace le Trap de la version 1.
  - ➔ Report, qui n'est pas défini. Comme précisé dans les spécifications de SNMPv2, l'usage et la sémantique sont à la charge de l'administrateur.
- Une évolution des tables MIBs, qui apporte plus de souplesse et de richesse. Surtout, elles sont plus en adéquation avec les réseaux actuels.

Messages SNMPv2



EVOLUTIONS DE SNMPv3

La troisième version apporte surtout des fonctionnalités de sécurité, qui faisaient cruellement défaut dans les versions précédentes.

Les fonctions de sécurité sont les suivantes :

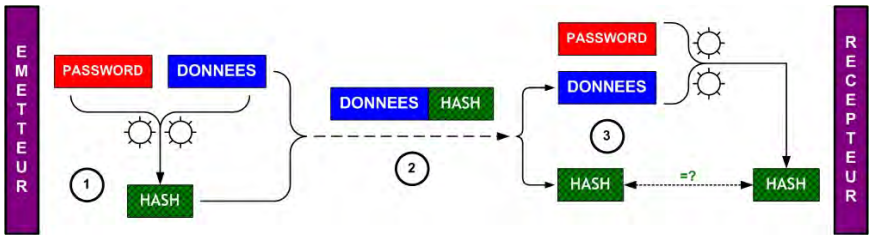
- Authentification des messages échangés. Ce qui permet de s'assurer que l'expéditeur est bien celui qu'il prétend être.
- Vérification de l'intégrité des données. On s'assure par ce moyen que les données n'ont pas été altérées durant leur transport.
- Confidentialité des échanges. Seul le destinataire du message pourra le lire en clair.

Bien évidemment, il est possible d'utiliser les trois fonctions de sécurité simultanément, c'est même fortement recommandé.

Les algorithmes utilisés sont :

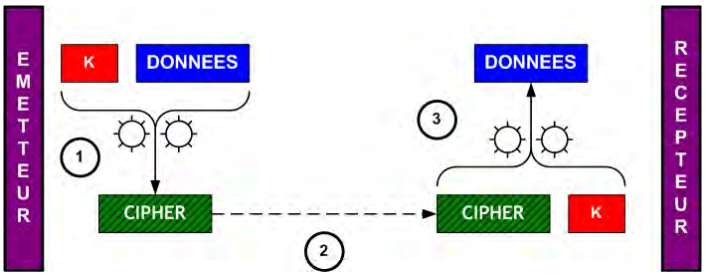
- MD5-HMAC et SHA1-HMAC pour l'authentification et l'intégrité, dont les fonctions sont groupées.
- DES 128 bits pour la confidentialité.

Authentification & intégrité



1. L'émetteur utilise l'algorithme de hachage (MD5 ou SHA1) avec le mot de passe secret d'authentification et les données du message pour obtenir un HASH
2. Les données et le HASH sont envoyés au destinataire
3. Le récepteur utilise les données reçue avec le mot de passe secret d'authentification avec le même algorithme que l'émetteur et obtient un HASH qu'il compare avec celui qu'il a reçu. Si les deux correspondent cela signifie que le message n'a pas été modifié et que l'émetteur à bien utilisé le même mot de passe secret que le récepteur.

Confidentialité



1. L'émetteur crypte les données à expédier en utilisant la clé secrète partagée avec le destinataire.
2. Les données cryptées sont envoyées au destinataire.
3. Le récepteur décrypte les données en utilisant la clé secrète partagée avec l'émetteur et obtient les données en clair

Produits

- Principaux produits :
  - HP OpenView
  - TNG de Computer Associate
  - Tivoli d'IBM
  - MRTG libre
  - SMS de Microsoft
  - CISCO Works
  - SNMPc
  - SunNet de SUN

Terminons par une liste des gestionnaires SNMP les plus répandus :

- HP OpenView, la référence, orienté grand réseaux. Un gestionnaire lourd et puissant capable d'administrer à peu près n'importe quelle machine IP. Très modulaire et évolutif.
- TNG de Computer Associate, très bien implémenté chez leurs clients mainframe.
- Tivoli d'IBM, l'autre référence pour les grandes sociétés. Très modulaire et évolutif.
- MRTG, libre, gratuit. Nécessite un développement plus important que les produits payants. Fonctionnalités de base plus restreintes, mais suffisantes dans la plupart des besoins des PME/PMI.
- SMS de Microsoft. Orienté Windows et réseaux Microsoft.
- CISCO Works. Existe sous plusieurs offres. Modulaire et évolutif, orienté CISCO et réseau.
- SNMPc. Plus simple que ses concurrents payants, il offre les fonctionnalités essentielles au quotidien.
- SunNet de SUN est l'outil SNMP de SUN.

Vos critiques et suggestions sont indispensables !

TSOFT fait la mise à jour de ses ouvrages dès que vous nous transmettez vos remarques. Nous comptons sur vous pour nous faire part de toute correction à effectuer ou de toute amélioration à apporter.

Vous avez choisi les ouvrages TSOFT pour vous former ou former d'autres personnes. Vous êtes donc les premiers concernés pour qu'à votre prochaine commande, le guide de formation ait été rectifié si nécessaire ou complété s'il le faut.

Titre de l'ouvrage :.....

Date d'achat ou d'entrée en possession de l'ouvrage : .....

Erreurs relevées (notez les pages concernées)

Sujets à ajouter (précisez éventuellement le chapitre)

Critiques et suggestions

M. Mme Mlle..... Prénom .....

Société ..... Profession .....

Adresse .....

.....

Code postal ..... Ville ..... Pays.....

A télécopier ou découper/envoyer à :
TSOFT – Service lecteurs – 10 rue du Colisée 75008 Paris
Fax : 01 53 76 03 64 - email : lecteur@tsoft.fr
Consultez tous nos ouvrages sur le site Web : **www.tsoft.fr**

Guide de formation Tsoft
TCP/IP de l'essentiel à la maîtrise
Référence : TS0083
Version 1 – septembre 2015