Introduction aux réseaux

Introduction aux réseaux

Pythagore F.D.

FH/950805/1/120820

Sommaire

I

Introduction

Besoin

Les premiers besoins de réseaux ont été des besoins d'accès entre deux terminaux (téléphone) ou entre un central et des terminaux distants:

- accès à certaines ressources spécialisées: imprimante, autre terminal, etc,...
- accès à certaines ressources multiples: bandes, disques, services centraux, etc,...

La communication entre ordinateurs est à l'origine de l'apparition de nouvelles fonctionnalités:

- messagerie, courrier électronique,
  Ex: Transpac
- traitement transactionnel: client <==> serveur;
  Ex: lecteur de cartes bancaires
- surveillance et pilotage de traitements industriels,
  Ex: gestion d'une chaîne de robots
- accès à des fichiers partagés,
- accès à des bases de données réparties.

L'aspect réseau

Un réseau définit un ensemble de machines informatiques (ordinateurs, terminaux, routeurs, contrôleurs, etc...) reliées entre elles par différents moyens. Il en existe de nombreux comme les liaisons satellites, infra-rouges, etc,...

Jusqu'au début des années 80, une distinction est à faire entre un réseau de communications et un réseau informatique: un réseau informatique est un réseau constitué uniquement de matériel informatique qu'il ne faut pas confondre avec un réseau téléphonique (RTC) par exemple.

Actuellement, ces deux réseaux se rapprochent, soit au travers de la téléphonie mobile, soit de la CTI (Couplage Téléphonie/Informatique).

Quelques définitions

Terminal

On appelle *terminal* le principal moyen d'accès à un réseau; il s'agit souvent de l'ensemble écran et clavier, ou encore d'un téléphone portable, d'un PDA, ... Les terminaux travaillent principalement soit en mode page ou caractère dans le cas d'une transmission numérique, soit en mode analogique.

Hôte

On appelle *hôte*, un calculateur du réseau. Les hôtes et les terminaux peuvent communiquer par un canal de communication, qui permet d'assurer la liaison physique (le type le plus courant est la liaison téléphonique).

Ligne

Pour utiliser ce canal, il faut transformer les données informatiques (bus parallèle) en données "physiques". On passe alors par des modems (modulateurs/démodulateurs) qui sont des appareils effectuant l'interface entre un ordinateur et un canal de communication de type téléphonique. Le coût de mise en place d'une ligne étant souvent élevé, on essaye de la partager grâce à un multiplexeur (MUX) qui est un appareil assurant le partage d'un même canal par plusieurs utilisateurs. Le multiplexage peut être fréquentiel (allocation d'une bande de fréquence par utilisateur), ou temporel (allocation d'un temps déterminé pour chaque utilisateur).

Définitions: transmissions

ETTD/ETCD DTE/DCE

Dans un réseau tous les équipements se comportant comme un terminal sont nommés ETTD (Equipement Terminal de Traitement des Données) ou DTE (Data Terminal Equipement).
Tous les équipements servant pour les connexions intermédiaires sont appelés ETCD (Equipement Terminal de Circuit de Données) ou DCE (Data Communication Equipement).
Cette distinction sert principalement pour le câblage: croise-t-on les fils d'émission et réception ou non?

Exemple:
Câble "droit" pour se raccorder à un concentrateur Ethernet
Câble "croisé" pour établir une liaison directe entre 2 machines

Half/Full duplex

Indique une communication à sens unique (2 fils, 1 voie) ou à double sens (4 fils, 2 voies)

Définitions: unités de mesure

Bit

Le réseau de données transporte les informations sous forme d'une suite de valeurs (0 et 1) nommées "bits" (binary digits) et symbolisées *b*. On parle de *langage binaire* (base à deux états).

Octet

Un octet (symbole *o*) est une suite d'exactement 8 bits.

Byte

Le byte (symbole *B*) est une suite de bits. Souvent confondue avec l'octet, il s'agit d'un terme anglais désignant la taille du plus petit élément traité par un processeur.

> ➢L'usage systématique est le suivant: **1B=1o=8bits**

Sur-multiples

Unités S.I.: 1000=**10^3**=**1k** définit le kilo et 1024=**2^10**=**1ki** définit le.**ki**lo **bi**naire ou kibi.
Par approximation (1000≈1024 soit 10^3≈2^10), on emploie les sur-multiples k, M, G,... pour les unités d'information, tout en conservant la valeur réelle dans les calculs.

> ➢L'usage est *d'écrire* **1ko=1024o** (impropre) et *d'évaluer* 1ko=1000o (techniquement non concevable).

Modulation

La modulation est un ensemble de techniques visant à former un signal électrique interprétable (mise en onde).

Sur la couche 1 (physique), on lui associe un ensemble de règles destinées à coder les bits reçus en niveaux de tensions, transmettre le signal, reconstituer les suites de bits et contrôler l'intégrité de la transmission.

Exemple:
La modulation CSMA/CD code et transporte souvent les données d'un réseau local.

La modulation doit donc assurer la chaîne numérique:
- la conversion numérique/analogique (CNA ou DAC),
- le transport sur le support physique,
- la conversion analogique/numérique (CAN ou ADC),
- le contrôle d'intégrité.

Protocole

Un protocole est un ensemble de règles décrivant la manière de transmettre des données.

Les protocoles interviennent à tous les niveaux d'un échange réseau.

Exemples:
au niveau liaison, LLC (Logical Link Control) et MAC (Media Access Control),
au niveau réseau, IP, Internet Protocol,
au niveau transport, TCP, Transmission Control Protocol,
au niveau session, présentation et application, FTP, File Transfer Protocol

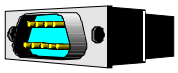
Le protocole doit assurer:

- l'identification des données
- le séquencement des blocs de données
- la synchronisation des différents intervenants
- la détection des erreurs de transmission
- les procédures de reprise
- la régulation du débit (contrôle de flux)

Protocoles

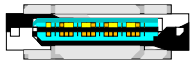
Transmission asynchrone

Les *fréquences d'horloges* de l'*émetteur* et du *récepteur* ont des fréquences *différentes*.
Le récepteur synchronise son compteur sur le débit du paquet reçu grâce au préambule de trame



L'interêt d'une transmission asynchrone est de ne pas nécessiter d'horloge très précise pour chacun des équipements.
Cet interêt est compensé par la diminution de la vitesse de transmission qui est plus faible que pour le mode synchrone (dans un rapport de 1 à 10).

Transmission synchrone



Les *fréquences d'horloges* de l'*émetteur* et du *récepteur* sont *synchronisées*:

- soit car elles sont alignées sur une fréquence de référence
- soit par le flux de données

Le signal d'horloge permettant la synchronisation est reconstitué par le récepteur à partir des transitions du flux des données reçues.
Ce système de communication supprime le besoin des bits de start et de stop utilisés en transmission asynchrone.

En revanche, il nécessite la présence d'une horloge précise dans les matériels.

Protocoles

PDU

Protocol Data Unit: l'*unité de données transférée* est un paquet de données. La couche du PDU est généralement précisée: un PDU réseau ou 3-PDU. Les données d'un PDU sont un SDU (*Service Data Unit*).

Medium, trame/cellule, paquet, message/segment

Le **medium** (couche 1, physique) est à la fois le *support physique* qui assure le transport des données et également la *modulation* utilisée pour leur conversion en signal électrique. (paires de cuivre torsadées, câbles coaxiaux ou encore fibre optique).

Les **trames** sont un 2-PDU (liaison de données). La couche 1 transporte des données sans signification que la couche 2 découpe en trames par reconnaissance de séquence d'initialisation (préambule et SDC) et accord sur le protocole d'échange.

Les **cellules** sont des trames très petites et de longueur fixe.

Exemple: la cellule ATM (Asynchronous Transfer Mode) utilise 5 octets pour l'en-tête et 48 octets pour les données, donc 53 octets au total.

Les **paquets** sont des PDU de couche 3 (réseau) de taille variable.

Exemple: sur IP, les paquets sont de taille maximum 65 536 octets.

Les **messages** ou **segments** (4-PDU, transport) qui morcellent les données applicatives (couches 5, 6 et 7).

Détection d'erreur (PCI)

Pour transmettre de couche à couche, le PDU de couche supérieure est encapsulé dans en PDU de couche inférieure en tant que données SDU adjointes d'un PCI (*Protocol-Control Information*).
Le PCI a pour objectif le contrôle de l'intégrité des données à transmettre (le PDU de couche supérieure): c'est la détection d'erreur.

CD (Collision Detection)

Sans être à proprement parler une technique de détection d'erreur, la détection de collision vérifie la disponibilité du medium avant et pendant l'émission des données.

Parité (Parity)

Détection d'erreurs de transmission: envoi d'un bit de parité à la suite des bits de données (couche 1):

- en parité paire (even), le bit de parité vaut 0 si le nombre (la *somme*) de bits de données à 1 est pair,
- en parité impaire (odd), le bit de parité vaut 0 si nombre (la *somme*) de bits de données à 1 est impair.

Détection d'erreur (PCI)

CRC (Cyclic Redundancy Check)

Le *contrôle de redondance cyclique* est le reste de la *division* modulo 2 du PDU supérieur (données ou SDC). Il est utilisée sur la couche 2 (liaison) en vérifiant l'unicité du résultat de l'opération avant et après transmission.

Checksum

La *somme de contrôle* est une extension du principe de calcul du bit de parité sur des alphabets à plus de deux états et s'exprimant sur plusieurs bits dans les couches 3 avec IP par exemple, et 4 avec TCP ou UDP.

Mesures

Mesures

Les caractéristiques principales d'une transmission peuvent se mesurer par le délai, le débit et la disponibilité.

Le délai de transmission d'une trame peut avoir plusieurs définitions différentes. Entre autres, le délai peut représenter:

- le temps écoulé entre l'émission du premier caractère d'une requête et la réception du premier caractère de la réponse,
- le temps écoulé entre l'émission du premier caractère d'une requête et la réception du dernier caractère de la réponse.

Mesures

Débit

Le débit d'un réseau est le taux de transfert de ce réseau. C'est une valeur qui se compte en ***bits par seconde*** (bps ou b/s) à cause de la signification particulière de certains bits intégrés à la trame. Néanmoins, on peut aussi le compter en "bits utilisateurs" effectivement transmis. En général, on divise par 10 le nombre de bits par seconde pour obtenir le nombre de caractères par seconde.

Remarque: le nombre de bits transmis par seconde n'est pas forcément égal au nombre de signaux transmis par seconde. En effet, un signal peut transmettre plus d'un bit à la fois (voir en particulier la norme V29).

Exemples de débits:

64 kbits/s ou 64kbauds
1,544 Mbits/s

On exprime en ***bauds***, le nombre de changements d'états physiques que la liaison peut supporter.

En norme V29, un signal transmet 4 bits à la fois (2 amplitudes, 2 déphasages). Dans ce cas 2400bauds valent 9600bits/s.

Mesures

Disponibilité

La disponibilité est le temps pendant lequel un système informatique est effectivement utilisable. Elle est déterminée par le temps moyen entre pannes et le temps moyen de réparation. La disponibilité globale d'un système peut être déterminée en multipliant les taux de disponibilité des différents éléments composant une ligne. Cependant, lorsqu'il existe plus d'un chemin pour aller d'un élément à un autre (par exemple, chemin de secours entre 2 modems), il est nécessaire de composer les taux:

Exemple:

chemin normal t1=95%
chemin secours t2=90%

==> disponibilité composée=1-(1-t1)(1-t2)=0,995*

Fiabilité

La fiabilité d'un réseau dépend de la sécurité et du taux d'erreurs. Quand on parle de sécurité sur un réseau, cela englobe tous les systèmes de protection contre les lectures, modifications ou envois non autorisés de données. Le taux d'erreurs est la probabilité de transmission d'un bit erroné. Celle-ci va en général de 10^{-5} à 10^{-9}. Toute transmission nécessite des mécanismes de reprise en cas d'erreur.

Couches ISO

La constitution d'un réseau passe par la définition:

- du support physique,
- du codage ou de la technique de transmission (Ex: transport de la voix sur le câble téléphonique),
- du mode de fonctionnement pour gérer les conflits, les surcharges (les règles de circulation, les protocoles réseaux),
- de l'architecture.

Les 7 couches ISO

Les différentes étapes de définition d'un réseau (suppport physique, codage, protocole,etc ...) ont amené l'ISO (International Standards Organization) à produire les spécifications en couches d'un réseau.

Les couches sont définies suivant les critères suivants :

- chaque couche doit réaliser une fonction spécifique parfaitement définie,
- les fonctions d'une couche doivent pouvoir être l'objet d'un standard.

Le modèle à 7 couches

Nom	Fonction	Objets manipulés	Contrôle	Exemple
7-Application	Fournit aux applications les services spécifiques de mise en correspondance des demandes utilisateurs. Apporte tous les services directement compréhensibles entre applications et gère les contenus des messages.			
6-Présentation	Mise en forme des données pour les rendre "portables" d'un système à un autre. Les données sont mises sous forme commune compréhensible par les applications (conversion ASCII -> EBCDIC, cryptage).			
5-Session	Gestion des connexions et mécanismes de reprise de session (check point). Effectue le contrôle du dialogue (half ou full duplex). Sécurité.			
4-Transport	Communication transparente d'un noeud à l'autre. Contrôle de transmission point-à-point. Gère le contrôle de flux et le contrôle de séquencement. Permet l'adressage au niveau du processus. Communication inter-réseaux.	Messages	cohérence des numéros et checksum	TCP
3-Réseau	Contient les mécanismes de contrôle de congestion ainsi que les services de routage. Effectue aussi la segmentation et le réassemblage.	Paquets	checksum de paquet	IP
2-Liaison	Gestion de la ligne physique. Contient les mécanismes de détection et de correction d'erreurs, et le contrôle du flux (protocole HDLC le plus utilisé).	Trames	checksum horizontal, CRC	Ethernet 802.3
1-Physique	Couche permettant d'effectuer le codage, puis la transmission physique des bits sur le canal de communication.	bits, octets	parité	CSMA/CD

➢ Remarque: dans le modèle TCP, les couches 5,6 et 7 du modèle ISO sont confondues en une seule couche "Application" de niveau 5.

II

Supports de transmission

Présentation

Les différents supports de transmission:

- les paires torsadées,
- les paires coaxiales,
- les fibres optiques,
- les faisceaux hertziens,
- les satellites.

Les équipements d'interconnexion:

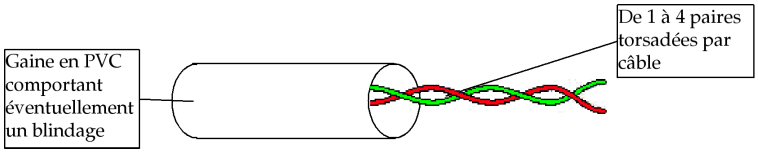
- les répéteurs,
- les concentrateurs (hubs),
- les commutateurs (switches),
- les ponts (bridges),
- les routeurs/passerelles (router/gateway).

Les types de commutation:

- la commutation de circuit (circuit switching),
- la commutation de paquets (paquet switching).

Paires torsadées

Les câbles à paires métalliques ou "paires torsadées" regroupent jusqu'à 4 paires de fils chacune spécifiquement enroulée en hélice afin de réduire les réflexions de signaux, la diaphonie et maintenir une impédance caractéristique.



Chaque paire peut être blindée (*Shielded Twisted Pair*, câbles STP) ou non (*Unshielded Twisted Pair*, câble UTP). Le câble peut également être blindé (*Foiled Twisted Pair*, câbles FTP et SFTP), on parle d'*écrantage*.
Ce câble est largement répandu du fait de sa présence dans les PABX téléphoniques et réseaux Ethernet.

Paires torsadées

Avantages:

- son coût modique,
- sa facilité d'installation.

Inconvénients:

- débit limité: de 64 Kbps en liaison point à point entre modems, jusqu'à 10 Gbps pour un réseau éthernet(en fonction de la longueur), 4 ou 16 Mbps en Token Ring, etc.. selon le type de réseau local
- longueurs utilisables limitées, (1,5 Kms en point à point, une centaine de mètres sur la plupart des réseaux locaux), du fait de problèmes de diaphonie, sensible aux interférences électromagnétiques, aux parasites.

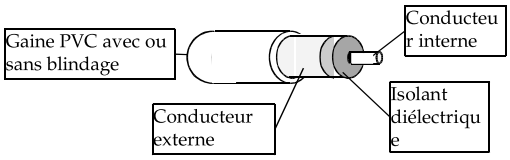
Catégories de paires torsadées

Catégorie / Classe	Paires	Bande passante	Débit max.	Réseaux utilisés
CAT-3 / C	2	16 MHz	100 Mbps	10BASE-T, 100BASE-T2, 100BASE-T4, téléphonie
CAT-4 / D		20 MHz	100 Mbps	TR 16Mbps, 10BASE-T
CAT-5 / D	4	100 MHz	100 Mbps	TR, ATM, 100BASE-TX, téléphonie
CAT-5e / D			1 Gbps	TR, ATM, 100BASE-TX, 1000BASE-T, téléphonie
CAT-6 / E		250 MHz	10 Gbps	10BASE-T, 1000BASE-T, 100BASE-TX, 10GBASE-T
CAT-6a / Ea		500 MHz		
CAT-7 / F		600 MHz		Télévision VHF et UHF
CAT-7a / Fa		1 GHz	*en cours de normalisation*	

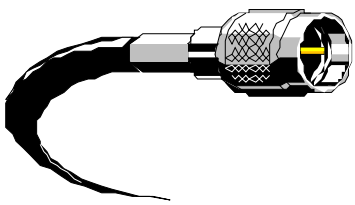
Les catégories 1 et 2 sont obsolètes. La catégorie 3 est en passe de le devenir.
Le standard actuel *de facto* est la catégorie 5/5e.
Seules les catégories à 4 paires de fils sont éligibles au transport de l'alimentation par POE (Power Over Ethernet).
La longueur maximale d'un *segment* est de *100m*.

Paires coaxiales

Les câbles coaxiaux



Il en existe de très nombreux types. On peut citer le 75 Ω à 400 Mhz pour la télévision, le 93 Ω d'IBM pour la connexion des terminaux 3270, les 50 Ω pour les anciens réseaux thick et thin éthernet.



Paires coaxiales

Avantages:

- large bande passante, garantie de débits élevés,
- faible diaphonie,
- bonne immunité aux parasites, (surtout les câbles à double blindage).

Inconvénients:

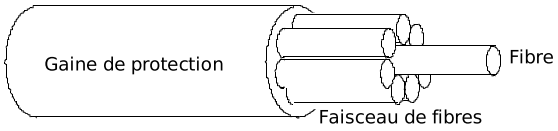
- nettement plus onéreux que la paire torsadée,
- pose plus difficile du fait d'une assez grande rigidité.

Exemples d'interfaces

- **RS-232C:** la plus répandue entre 0 et 20 kbps jusqu'à 15 m. équivalent à V.24, V.28 et ISO IS-2110.
- **RS-449:** conçue pour porter le débit des transmissions à 2 Mbps jusqu'à 60 m.
- **RS-530:** remplace le RS-449 et complète le RS-232. Les débits vont de 10 kbps à 2 Mbps.
- **RS-422:** sert fréquemment dans les communications point-à-point pilotées par des circuits à deux états. Débits et portées sont importants. RS-422 est équivalent à la norme CITT V.11.
- **RS-485:** ressemble au RS-422, mais avec un maximum de 64 noeuds.
- **CITT V.35:** débits jusqu'à 256 kbps. Service numérique (Transpac®, Transfix®).
- **IEEE-488** (GPIB): interface digitale pour les instruments de mesure programmables. Connexion d'un micro-ordinateur et d'un multi-mètre.
- **Interface Parallèle Centronics:** interface en mode caractère qui est devenue standard pour les communications d'un ordinateur vers une imprimante. L'interface comprend 8 lignes qui acheminent en parallèle chacune un bit de donnée.
- **X.25:** protocole d'accès à un réseau. Utilise X.21 comme interface numérique directe.
- **X.21:** L'interface traditionnelle DTE à modem a été remplacée par un "adaptateur" de ligne. L'adaptateur joue alors le rôle d'un appareil inintelligent qui transmet sur la ligne numérique les données du DTE. X.21 définit la procédure de transmission synchrone en full-duplex entre DTE et DCE jusqu'à 64 kbits/s.
- **RJ11**: le *registered jack 11* est le connecteur traditionnel des lignes téléphoniques analogiques (modems, combinés, PABX,...).
- **RJ45**: le *registered jack 45* est le connecteur traditionnel des réseaux ethernet sur paires torsadées. Lorsque le brochage des paires émission et réception est inversé de part et d'autre d'un câble, on parlera de câble croisé (interconnexion d'équipements du même type), de câble droit sinon (interconnexion d'équipements différents).

Fibres optiques

Schéma de principe d'un faisceau optique:



Les fibres optiques (FO) se présentent groupées en faisceau à l'intérieur d'une gaine.
Les liaisons entre faisceaux sont réalisées à l'aide de jarretières monofibres.
La propagation étant unidirectionnelle, une liaison nécessite l'utilisation de deux fibres.
Les fibres non utilisées dans un faisceau sont dites *fibres noires* ou *mortes*.

Chaque fibre propage l'onde lumineuse au travers du *cœur*.

L'onde y est maintenue par réfraction grâce à la *gaine optique* qui entoure le cœur (la fibre est un guide d'onde).

La nature de la gaine optique (son indice de réfraction) permet de distinguer deux grands types de fibres.

Fibres multimodes

Une fibre *multimodes* (MMF: MultiMode Fiber) autorise de *multiples trajets* pour l'onde lumineuse car le diamètre du cœur est important (50 ou 62,5 µm).
Ces fibres autorisent la propagation de *plusieurs ondes lumineuses* dans un même cœur (multiplexage en longueur d'onde ou WDM:Wavelength Division Multiplexing).

L'onde est émise par une simple LED dans le rouge visible (l=850nm) ou dans l'infrarouge (l=1300nm).

La perte d'énergie résultant de la réfraction sur la gaine optique (dispersion modale) n'autorise que de *courtes distances* (<2km) et du *bas débit* (bande passante: 200 à 1500MHz/km). Cela induit par ailleurs une importante déformation du signal à mesure que la distance augmente.

La distance de propagation peut être augmentée par insertion de répétiteurs optiques sur la ligne, augmentant le coût de déploiement.

Il existe deux types de fibres multimodes:

- **à saut d'indice**: les indices de réfration du cœur et de la gaine diffèrent fortement.
  L'onde rebondit sur la gaine, augmentant le trajet parcouru: il en résulte une perte d'énergie.

- **à gradient d'indice**: le cœur est constitué de couches de verre successives ayant un indice de réfraction proche.
  L'onde oscille autour de l'axe longitudinal: le chemin parcouru est plus court, la perte d'énergie moindre.

Fibres monomodes

Ces fibres véhiculent les ondes lumineuses sur un *trajet unique* (SMF: Single Mode Fiber) du fait de la finesse du cœur (9µm de diamètre).

La source lumineuse nécessite alors une grande puissance, on utilise des lasers dans l'infrarouge (l=1300 ou 1550nm).

Le trajet optique étant quasi rectiligne, la perte d'énergie est très réduite.

Cette dispersion modale quasi nulle autorise son utilisation pour de très hauts débits sur de très longues distances (liaisons trans et intercontinentales, câbles sous-marins).

Un segment peut atteindre 60km sans répétiteur, mais le débit maximum diminue avec la distance. Une fibre monomode courante peut mesurer 5km.

La bande passante est quasi infinie (> 10GHz/km).

Actuellement, il est possible de multiplexer jusqu'à 256 canaux dans une seule fibre monomode: multiplexage WDM dense ou D-WDM (espacement <100GHz entre les longueurs d'ondes).

En théorie, il sera possible de multiplexer jusqu'à 400 canaux avec des longueurs d'ondes très rapprochées: multiplexage WDM ultra-dense ou U-DWDM.

Synthèse

Avantages:

- très faible poids et un faible encombrement,
- totale insensibilité aux parasites,
- forts débits liés à une large bande passante et sur de très longues distances,
- pas de phénomènes électromagnétiques ou électrostatiques.

Inconvénients:

- pertes de transmissions dues au matériau (atténuation et héterogénéité du verre), aux imperfections dimensionnelles du coeur et de la gaine, à la précision de la connectique et à l'état de surface des extrémités.
- la résistance mécanique des câbles est faible, ils sont peu souples,
- mauvaise tenue au feu ou à la température,
- la pose de la connectique reste une affaire de spécialistes.

Faisceau hertzien

Un faisceau hertzien permet la transmission de signaux radioélectriques entre deux antennes directives (en ligne droite) et terrestres.

Il est donc sensible au masquage (arbres, bâtiments), à l'ionisation de l'atmosphère (réflexion, réfraction) ou encore aux intempéries.

Les fréquences transmises varient de 1 à 40GHz (micro-ondes).

L'émetteur joint le récepteur par des bonds entre stations relais.
Les antennes sont à la fois émettrices et réceptrices (bidirectionnelles), chaque sens utilisant une fréquence de transmission distincte.

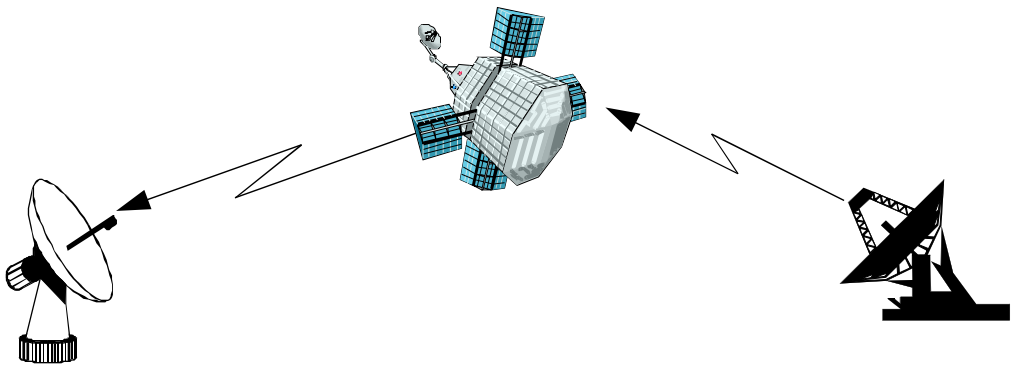
La distance maximale pour un bond est de l'ordre de 100km.

Liaison satellite

Pour les transmissions de très longue distance:
utilisation d'un satellite géostationnaire qui sert de relais de transmission.

Une antenne émet les signaux vers le satellite qui a en charge de convertir le type de signal (changement de phase) et de reémettre les données.
Une antenne au sol peut alors capter les informations.

Les données contiennent un code qui permet d'adresser une antenne parmi d'autres.



Equipements d'interconnexion

L'interconnexion des réseaux est assurée au moyen d'équipements opérant à différents niveau du modèle OSI:

- **Répéteur - couche 1 - Physique:**
  régénère le signal électrique reçu sur le medium (couche 1) ***à l'identique***.

- **Concentrateur ou Hub – couche 1 - Physique:**
  diffuse le signal reçu sur toutes les interfaces raccordées. T***opologie bus***.
  Exemple: un hub 100Mbps partage le débit sur l'ensemble de ses interfaces raccordées.

- **Commutateur ou Switch – couche 2 – Liaison de données:**
  connecte ses interfaces deux à deux. T***opologie étoile*** entre les interfaces raccordées.
  Exemple: un switch 100Mbps garantit un débit de 100Mbps sur chacune de ses interfaces raccordées.

- **Pont ou Bridge- couche 2 – Liaison de données:**
  connecte des réseaux de nature (liaison) différente.
  Exemple: un point d'accès Wi-Fi est un pont entre les réseaux Ethernet 802.3 et WiFi 802.11

- **Routeur / Passerelle ou Router / Gateway – couche 3 - Réseau:**
  interconnecte des réseaux IP différents entre eux. La passerelle agit jusqu'au niveau 7.
  Exemple: un routeur reçoit une trame, compare l'adresse IP de destination à ses tables et renvoie le datagramme vers l'interface de sortie correspondante.

Commutation

La *commutation* réalisée par les switches est de deux types: sur le *mode d'acheminement (circuit/paquet)* et sur le *type de données* acheminées *(trames/cellules)*.

Commutation de circuit

Utilisée principalement pour les communications téléphoniques, elle établit et maintient un **chemin unique** entre la **source** et la **destination**..

Exemple:
Le Réseau Téléphonique Commuté Public (RTCP) est un réseau à commutation de circuit (1 chemin par numéro).

Commutation par paquets

Les paquets de données sont transmis sur le chemin optimum à tout instant: il existe de **multiples chemins** entre la **source** et la **destination**.

Exemple:
Internet est un réseau de machines et équipements interconnectés. La commande 'traceroute google.fr' lancée à quelques secondes d'intervalle montre des chemins différents pour une même requête.

Commutation de trames/cellules

Le type de données acheminées distingue la commutation de trames (taille variable) de celle des cellules (taille fixe et réduite).

III

Protocoles de liaison

Démarche

Le besoin en bande passante est issu du type d'application et du volume de données à transférer.

- Les applications deviennent de plus en plus "visuelles"
- Le nombre de postes clients est en augmentation constante
- Certaines applications nécessitent une intégrité totale des données, d'autres acceptent les pertres d'informations (voix)

Exemple:

Visualisation point à point	10Mo-1Go
Vidéo en broadcast	3M-100M
Transfert de fichier multimédia	1M-100M
Vidéo conférence	600k-10M
CD Audio	500k-1M
Image haute définition	100k-10M
Facsimile	50k-500k
Image basse définition	10k-100k
Voix	20k-50k

Il faut ensuite évaluer les besoins, puis définir une architecture et enfin sélectionner les technologies appropriées.

Ethernet

Né en 1970

Résultat des recherches de DEC et Intel et Xerox (ethernet DIX).

Modulation CSMA/CD (couche 1):

Carrier Sense Multiple Access/Collision Detection

transmission lorsque la voie est libre avec détection de collisions

Caractéristiques

- Protocole non déterministe
- temps aléatoire avant retransmission.
- 10 Mbps
- Coaxial, STP/UTP ou fibre optique
- Standard IEEE 802.3

Ethernet

Une trame Ethernet 802.3 contient:

- un préambule sur 7 octets valant chacun 10101010 permettant au récepteur de synchroniser son horloge (le rapport cyclique de 50% est égal à la demi-fréquence de transmission),
- le SFD (Starting Frame Delimiter): 1 octet valant 10101011 indiquant le début de trame,
- l'adresse physiques de destination, puis de source codées sur 6 octets,
- le champ "Ether Type" sur 2 octets (IPv4=0x0800, ARP=0x0806, RARP=0x8035, VLAN 802.1Q=0x8100, IPv6=0x86DD) indiquant le type de protocole dans les données,
- si EtherType=0x8100, on lui ajoute 4 octets définis comme suit:
  - priorité: 3 bits de priorité de trame (basse=000, haute=111) représentant 8 niveaux,
  - CFI: 1 bit Canonical Format Indicator systématiquement à 0 pour compatibilité Ethernet/Token Ring,
  - VLAN ID: 12 bits numérotant le VLAN (4096 possibilités); le 0 indique qu'il n'y a pas de VLAN tout en gardant une priorité dans la trame,
  - Ether Type: 2 octets de type de protocole dans les données,
- le MTU précisant la longueur des données comprise entre 46 et 1500 octets (sinon padding, bits de bourrage), généralement 1492 octets pour optimisation,
- les données,
- des codes de contrôle d'erreur le FCS (Frame Check Sequence) qui est de type CRC, calculé à l'émission et à la réception (la comparaison indique s'il y a eu altération).

L'adresse physique est nommée adresse MAC.

Structure de l'adresse MAC

L'adresse MAC ou Media Access Control est un identifiant unique d'interface réseau codé sur **6 octets** et représentée par 12 caractères hexadécimaux **dans le cas d'Ethernet** car elle dépend du protocole de couche 1 utilisé.

Caractéristiques de l'adresse MAC:

- Unicité,
- Structurée selon les normes en vigueur chez le constructeur de l'interface,
- En théorie non modifiable pour ethernet, car inscrite au niveau matériel (mais de nombreux constructeurs autorisent un changement dynamique).

Les **trois premiers octets** identifient le **constructeur** tel que référencé par l'IEEE: cette table regroupe les **OUI** (Organizationally Unique Identifier), identifiant unique de constructeur.

Les **trois octets suivants** identifient un **matériel** unique.

Les constructeurs respectent certaines normes, par exemple, six caractères pour un type de matériels d'un constructeur, plus six caractères pour le matériel:

- 080002 + 6 chiffres pour les stations réseau de 3COM (référencé "Bridge Communications inc.")*,
- 02608C + 6 chiffres pour les serveurs de terminaux 3COM (référencé "3COM Corporation"),
- 080020 + 6 chiffres pour les stations SUN (référencé "Sun Microsystems inc.").

L'adresse MAC 08 00 20 A0 42 5B, désigne donc une station SUN.

* *Bridge Communications et 3COM Corporation ont fusionné en 1987.*

Standards Ethernet

Ethernet 802.3 offre une large variété de standards, tant au niveau des débits proposés que des supports utilisables.

Ethernet 10Mbps

La norme historique se décline en 4 standards toujours utilisés actuellement:

- 10BASE2 (ThinNet ou Cheapernet): ancien standard dominant sur câble coaxial et prises BNC en T,
- 10BASE-T: standard dominant à l'heure actuelle, 2 paires de fils torsadées catégorie 3 ou 5, connecteurs RJ45,
- FOIRL: Fiber-Optic Inter-Repeater Link (lien inter-répéteur sur fibre optique), première norme à support fibre optique, obsolète,
- 10BASE-FL: successeur de FOIRL.

Débit: 10Mbps

Fast Ethernet

Fondé sur la norme 802.3, donc compatible quant à la méthode d'accès.

Il se décline en trois versions regroupées sous le terme générique 100BASE-T:

- 100BASE-TX: sur du câble cuivre en paires torsadées catégorie 5 et 6, connecteurs RJ45, standard dominant,
- 100BASE-T4: semi-duplex, sur du câble cuivre en paires torsadées catégorie 3, connecteurs RJ45,
- 100BASE-FX: sur fibre optique.

Débit: 100Mbps

Gigabit Ethernet

Déclinaisons:

- 1000BASE-T: sur du câble cuivre en paires torsadées catégorie 5e et plus, connecteurs RJ45, standard dominant, 100m maximum, très répandu,
- 1000BASE-X: interfaces modulaires (GBIC) adaptées au média (fibre multi ou monomode, cuivre),
- 1000BASE-SX: sur fibre optique multimodes à 850nm, diode rouge,
- 1000BASE-LX: sur fibre optique monomodes et multimodes à 1300nm, diode laser,
- 1000BASE-LH: sur fibre optique, longues distances.
- 1000BASE-ZX: sur fibre optique monomodes, très longues distances.

Distances sur fibre multimode: 100m / 300m
Distances sur fibre monomode: 2 / 10 / 40 km

Débit: 1Gbps

Ethernet 10Gbps

Norme 802.3ae, déclinée de 802.3 et interopérable.

Ratifiée en mars 2002, elle devrait être incorporée à une révision de 802.3.

Se destine aux réseaux LAN, MAN et WAN (locaux, métropolitains, étendus).

Les infrastructures FTTx (Fiber To The..., Home pour le FTTH) utilisent l'ethernet 10Gbps à support fibre.

Définit 2 familles de couches physiques (PHY):

- LAN PHY opérant à 10Gbps,
- WAN PHY à modulation compatible avec la porteuse optique OC-192/STM-64 à 9.95328Gbps des télécommunications (multiplexage de lignes S0 à 64kbps), ce qui permet de réutiliser les infrastructures téléphoniques (SONET).

Ethernet 10Gbps

Déclinaisons:

Norme	Support	Distance	Couche physique
10GBASE-CX4	Cuivre InfiniBand 4x	15m	LAN PHY
10GBASE-T	Cuivre CAT-6 et plus	100m	
10GBASE-LX4	MMF, multiplexage WDM	240 à 300m	
	SMF, multiplexage WDM	10km	
10GBASE-SR	MMF 850nm	26 à 82m	
	MMF 2GHz	300m	
10GBASE-LR	SMF 1310nm	10km	
10GBASE-ER	SMF 1550nm	40km	
10GBASE-SW	MMF 850nm	300m	WAN PHY / SONET
10GBASE-LW	SMF 1310nm	10km	
10GBASE-EW	SMF 1550nm	40km	

Débits: 10Gbps sur commutateurs informatiques, 9.95328Gbps sur commutateurs téléphoniques.

Token Ring (TR)

Le droit d'émettre est matérialisé par une trame particulière " le jeton ou Token ". Celui-ci circule en permanence sur le réseau. Une station qui reçoit le jeton peut émettre une ou plusieurs trames (station maître). Si elle n'a rien à émettre, elle se contente de répéter le jeton (station répéteur).

Dans un tel système, les informations (trames) transitent par toutes les stations actives.

Chaque station du réseau répète ainsi le jeton ou le message émis par la station maître, il n'y a pas de mémorisation du message, un bit reçu est immédiatement retransmit.

Sans le jeton, on devra attendre son tour, matérialisé par le passage d'une configuration particulière de bit appelée jeton.

Publiée en 1985, la norme IEEE 802.5 fut implémentée par IBM dès 1986. IBM est resté le principal acteur du monde Token Ring.

Protocole déterministe.
Débits: 4/16/100 Mbps

En cours de désengagement. IBM ne vend plus de matériel Token Ring mais en assure encore le support.

FDDI

Fiber Distributed Data Interface

topologie de base:
anneaux doubles contre-rotatifs

Caractéristiques

Fonctionne sur la base d'un anneau primaire et d'un anneau secondaire contre-rotatif.

- Trames: 4500 octets maximum (longueur variable),
- Débit: 100Mbps,
- Transmission: 125 Mbps (horloge à 125MHz +/- 0.005%),
- Charge utile: 90%,
- Tolérance aux pannes par rebouclage automatique,
- Fibre optique multimode (MMF),
- Distance maximale couverte: 100km,
- Supporte jusqu'à 1000 stations distantes,
- Distance maximale entre deux stations: 2km (atténuation 11dB).

Fonctionnement

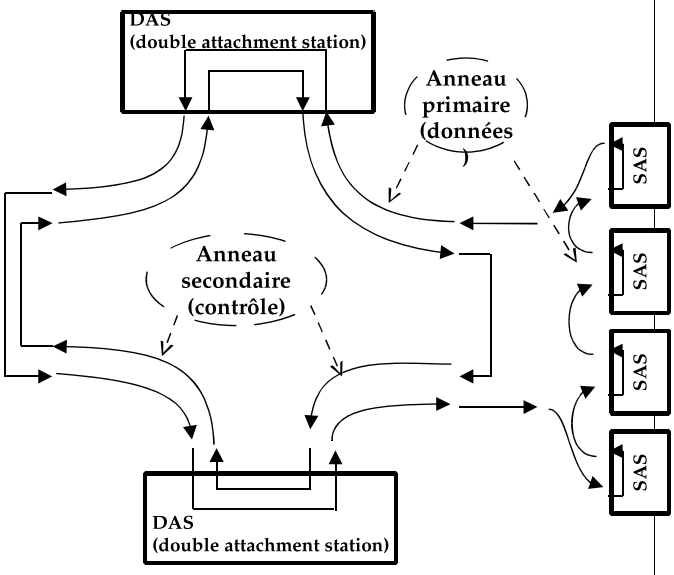
Similaire au TokenRing 16 MBps. Toutes les stations sont des répéteurs. Pour accéder au support, une station doit posséder le jeton. Elle émet ses données et génère un nouveau jeton. Chaque station retire de l'anneau les données qu'elle y a déposées.Plusieurs trames de données issues de stations différentes peuvent circuler sur l'anneau, mais il n'y a qu'un seul jeton.

- si un câble est coupé, les stations les plus proches se reconfigurent et le réseau est alors constitué d'un seul anneau
- si deux coupures surviennent, le réseau se fragmente

FDDI utilise un mode synchrone pour les données urgentes et un mode asynchrone pour les données courantes.

Quatre types de stations sont définis:

SAS	les stations à accès unique
DAS	Les stations à double accès
SAC	les concentrateurs à accès unique
DAC	les concentrateurs à double accès



Frame Relay (FR)

Le Frame Relay (relais de trames) est une évolution de la commutation par paquets X25. Il établit, en mode connecté, une liaison virtuelle entre les deux extrémités.

Cette liaison est soit permanente (PVC: Permanent Virtual Circuit), soit établie à la demande (SVC: Switched Virtual Circuit).

Le Frame Relay couvre les couches 1 et 2 du modèle OSI mais n'est pas conforme à ce dernier.

Le Frame Relay permet un débit de 2 à 45 Mbps et des temps de réponse très faibles.
Il est particulièrement bien adapté aux forts trafics aléatoires tels que les trafics d'interconnexion de réseaux locaux.

Délais de transmission variables: le Frame Relay n'est pas adapté aux applications vidéo et voix.

RNIS / ISDN

Réseau Numérique à Intégration de Services

ISDN: Integrated Services Digital Network

Il a été pensé pour remplacer les lignes téléphoniques analogiques actuelles, tout en permettant l'acheminement de services évolués ainsi que la visioconférence bas-débit.

RNIS bande étroite (Narrowband ISDN) permet l'intégration de services pour des débits de 56 Kbps à 2 Mbps (accès S2) par aggrégation (bundling ou bonding) de canaux S0 (1 ligne téléphonique) de 64kbps.

RNIS large bande (Broadhand ISDN) est basé sur des cellules évoluées de la technologie ATM pour des débits de 2 à 600 Mbps (transporté par Sonet/SDH). Il est conçu pour utiliser le réseau téléphonique en transportant du numérique de bout en bout.

Avantages:

- souplesse d'utilisation,
- support de plusieurs canaux à haute vitesse,
- l'allocation dynamique de bande passante.
- robuste (chemin dédié),
- QoS garantie à 200ms d'acheminement après connexion (contrainte téléphonique de retard).

RNIS / ISDN

Inconvénients:

- Multiples protocoles,
- Complexité des échanges,
- Peu sécurisé (chemin statique)

Fonctionnement

Ce réseau est à commutation de circuit (circuit switching, évolution des lignes RTC) sur des canaux B (64kbps) et un canal D à 16kbps pour l'accès de base et à 64bps pour l'accès primaire.

- Accès de base (ISDN-BRI/BRA: Basic Rate Access): 2B+D16 = 144kbps,

- Accès primaire (ISDN-PRI/PRA: Primary Rate Access):
  - 30B+D64+synchro64 = 2,048Mbps en Europe (accès E1 improprement appelé T2 à 32 canaux),
  - 23B+D64+synchro8 = 1,544Mbps en Amérique du Nord (accès T1).

Le canal D transporte les signaux servant à l'établissement de la communication et toutes les informations de service ; il peut aussi transporter des informations à bas débit (protocole x31.b à 16kbps).

Les canaux B transportent les données. Ils sont utilisables indépendemment les un des autres. Avec un accès de base, on peut téléphoner tout en surfant sur le Web (offre Numéris de France Télécom).

ATM

ATM est conçu pour la transmission et la commutation d'informations numériques de nature quelconque: voix, données, images.

Le problème de la synchronisation est de l'étalement de la bande passante est assurée par un découpage en cellule de petites tailles, 53 octets:
- 5 octets pour l'en-tête,
- 48 octets pour les données.

ATM construit des chemins virtuels en point à point.

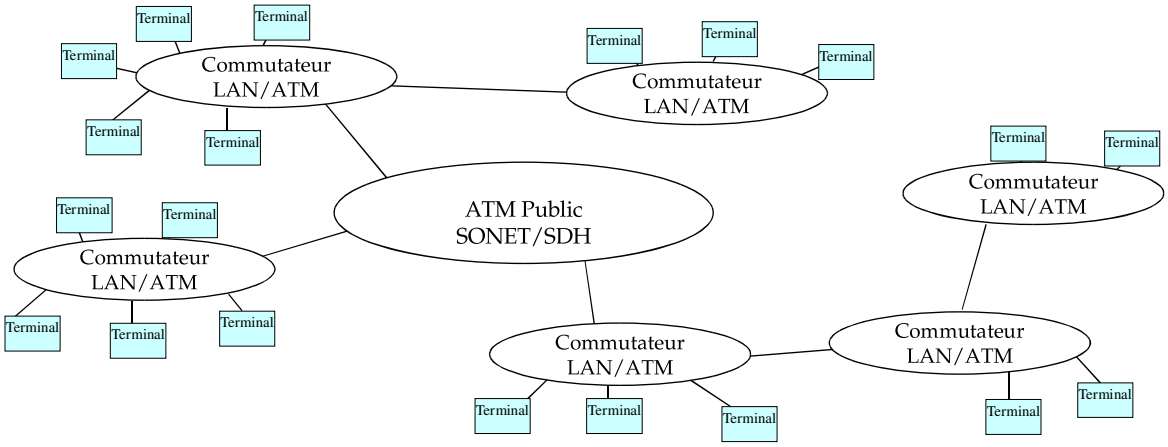
ATM ne connaît pas la notion de broadcast d'où des problèmes d'interopérabilité avec IP.

ATM permet de supporter tous les services actuels: téléphonie, multimedia, données diverses,...

Débit

Le débit est évalué en nombre de cellules émises par seconde:
- 53 Mbps = 138 000 cellules/s,
- 2,5 Gbps = 6 510 000 cellules/s

Architecture



Voies Virtuelles (VC) et Conduits Virtuels (VP)

Les voies virtuelles (Virtual Channels) VC sont des connexions de noeud à noeud.
Les conduits virtuels (Virtual Paths) VP sont un regroupement de plusieurs voies virtuelles.

Les VC et VP définissent les circuits virtuels (VCC), et permettent de garantir la bande passante.

Les identifiants sont stockés dans des tables de routage au niveau des noeuds du réseau.

Adressage

L'adresse d'un terminal lui est donnée par le commutateur (informations de signalisation).

Une adresse ATM tient sur 20 octets:

Exemple:
47.0023.0100.0003.0010.205a.2a01.0123.5678.9abc.00

Plusieurs formats d'adresse existent.

Au format ICD, cette adresse se décompose de la façon suivante:

AFI	*47 (ICD)*
IDI	*0023 (NORDUnet)*
Version	*01*
Network	*000003 (Finland, Funet)*
Tele Traffic area	*00*
Funet member identifier	*1020*
Member access point	*5a*
Area	*2a*
Switch	*01*
Mac address	*01236789abc*
Selector	*00*

DSL

ATM est souvent utilisé par les technologies DSL (Digital Subsciber Line).

Il existe plusieurs types de DSL:

- ADSL (Asymmetric DSL): basée sur un débit asymétrique, le flux descendant (du réseau vers l'utilisateur) étant plus important que le flux montant. ADSL préserve le canal de voix et convient bien aux applications interactives du type "accès à Internet" ou "vidéo à la demande".
- HDSL (High data rate DSL): permet un canal T1 ou E1 sur une boucle locale sans répéteur. HDSL peut être utilisé par les opérateurs pour l'interconnexion de PABX, par exemple.
- SDSL (Symmetric DSL): version monoligne de HDSL (qui utilise les deux paires téléphoniques).
- VDSL (Very high data rate DSL): permet des débits de l'ordre de 50 Mbps pour le flux descendant (utilisé par Erenis sur Paris).
- VDSL2: comme VDSL mais en 100Mbps en Full duplex.
- RADSL (Rate Adaptive DSL): technique asymétrique qui a la particularité d'adapter le débit en fonction des capacités de la ligne.

Comparatif

	ADSL	HDSL	SDSL	VDSL	RADSL
Mode	Asymétrique	Symétrique	Symétrique	Asymétrique	Asymétrique
Débit descendant (kbps)	1544-9000	1544-2048	768	13000-51000	600-7000
Débit ascendant (kbps)	16-640	1544-2048	768	1544-2300	128-1024

Chacune de ces techniques utilise des modes de séparation des canaux différents:
- AdE, Annulateur d'écho,
- FDM, modulation de fréquence...

...et des codages différents:
- DMT, Discrete Multitone, qui divise le signal en 256 sous-canaux,
- CAP, Carrierless Amplitude Modulation, qui module en phase et en amplitude,
- le codage 2B1Q, 2 Binary 1 Quaternary, qui est le codage à 4 états utilisé par RNIS.

WAN: ppp

Conçu principalement pour les réseaux TCP/IP.
Permet la connexion point-à-point entre deux équipements d'interconnexion.
De multiples protocoles peuvent être véhiculés sur un lien PPP.
De multiples équipements de constructeurs différents peuvent être reliés par des liaisons séries.
PPP apporte une véritable interopérabilité dans les environnements WAN en pontage et en routage.

Interface	**Débit**
RS-232	< 19,2 Kbps
V.35	< 2,048 Mbps
X.21	< 2,048 Mbps
RS-449	< 2,048 Mbps
T1 / E1	1,544 / 2,048 Mbps
T3 / E3	45 / 34 Mbps
HSSI (50 broches)	8-53 Mbps
OC- N (fibre)	> 51 Mbps

Récapitulatif

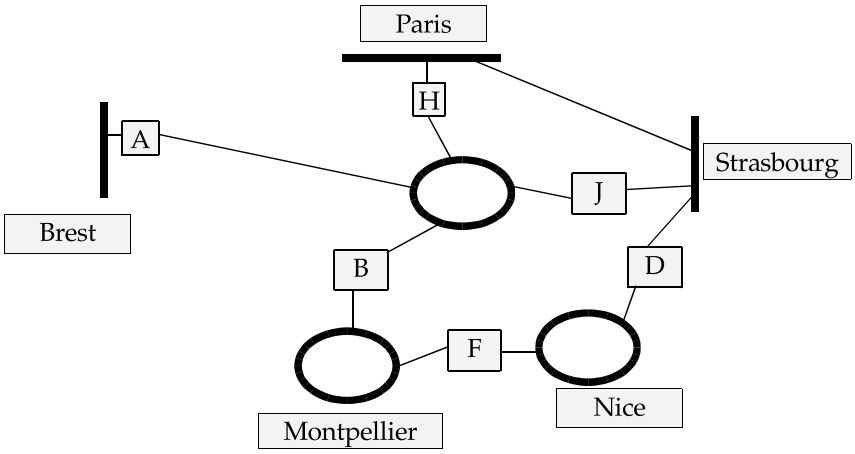
Technologie	**Débit**	**Utilisation**	**Câble**
Token Ring	4,16,100 Mbps	Réseaux IBM	Type 1
Ethernet	10 Mbps	Généraliste	Coaxial, UTP, STP, fibre optique
Fast Ethernet	100 Mbps	Fédérateurs, serveurs, stations de travail	UTP, STP, fibre optique
Giga Ethernet	1/10 Gbps	Fédérateurs	fibre optique
FDDI	100 Mbps	Fédérateurs sécurisés	UTP, STP, fibre optique
ATM	25, 155, 622, 2400 Mbps	Voix/vidéo/données	Coaxial, UTP, fibre optique
RNIS	64/128 kbps	Point-à-point numérique	RTC
Frame Relay	2-45 Mbps	WAN	LS

IV

Architectures de base

Architectures

Les possibilités d'architecture sont variées, depuis un simple bus, un réseau en étoile, ou un anneau, jusqu'à un mélange de tous ces types de réseaux.



Paris, Brest et Strasbourg sont sur des réseaux de type bus équipés de concentrateurs.
A, D, H et J sont des équipements de type 'ponts'.
B et F sont des équipements de type 'commutateur' ou 'routeur' (possibilité de pont).

Lien architecture/protocole

L'architecture du réseau et le protocole de liaison sont fortement liés: ainsi, le système de jeton devra être utilisé sur un anneau.

En revanche, un protocole de transport se doit d'être indépendant de l'architecture. C'est le cas de TCP/IP.

Remarque:
il est possible de boucler un brin Ethernet par un pont et d'ouvrir un anneau Token-Ring.
Dans ce cas, il faut que la boucle Ethernet soit ouverte, par exemple, automatiquement avec le STA (Spanning Tree Algorithm). Ouvrir un anneau TokenRing nécessite un rebouclage automatique en utilisant un double anneau.

Topologies filaires

Liaison point à point

Servent pour des dialogues d'ordinateur à ordinateur, entre commutateurs de paquets et de manière générale entre deux équipements de même "niveau".
Les liaisons Multipoint sont utilisées pour des dialogues d'ordinateur (primaire) à terminaux (secondaire).

Bus

Un réseau en bus est un réseau dont tous les noeuds sont reliés à une même artère centrale. L'intérêt de ce type de réseau est que les pannes d'un élément sont peu pénalisantes.

Anneau

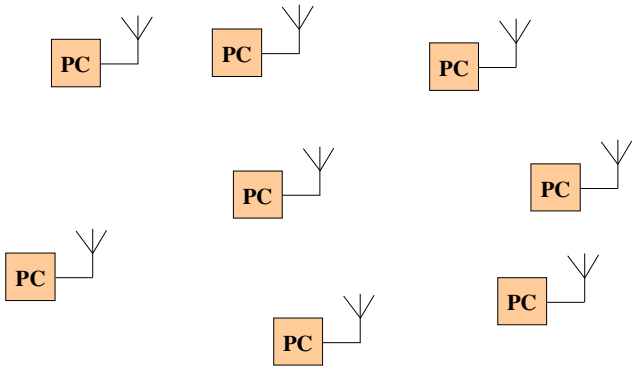
Un réseau en anneau est un réseau dont chaque noeud est relié à deux et seulement deux noeuds. L'intérêt de ce type de réseau est que les temps de transferts sont relativement indépendants de la charge. La fiabilité en cas de panne d'un noeud est assurée par la déconnexion automatique de ce noeud.

Etoile

Un réseau en étoile est un réseau dont les secondaires ne sont pas connectés sur une même ligne, mais en étoile autour d'un primaire. Cette organisation nécessite un système central performant et fiable.

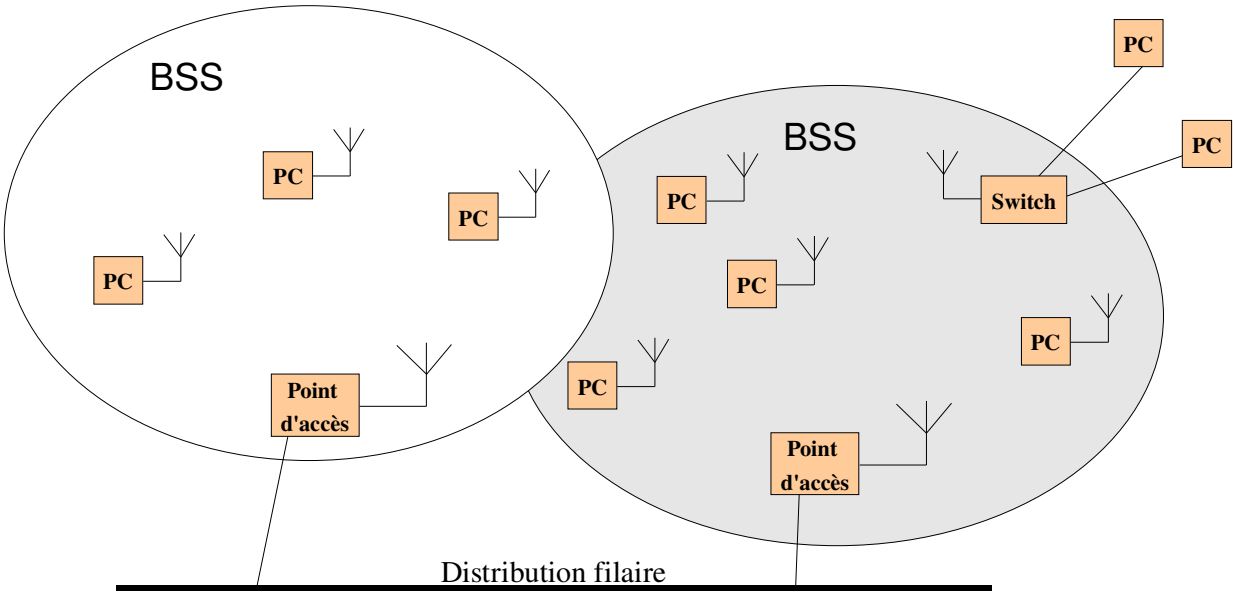
Topologies sans fil

Un réseau sans fil est un réseau dans lequel les stations ne sont pas connectées par des liens solides. Les réseaux à courant porteur sont ici considérés comme un réseau de type bus.



Architecture sans fil 802.11

Architecture cellulaire où chaque cellule (appelée Basic Service Set ou BSS dans la nomenclature 802.11), est contrôlée par une station de base (appelée Access Point ou AP, Point d'Accès en français).



Mode ad'hoc

Si l'on souhaite disposer d'un réseau local sans fil sans infrastructure (surtout sans Point d'Accès), on peut utiliser le mode ad'hoc du standard 802.11.

Ceci peut permettre le transfert de fichiers entre deux utilisateurs d'agenda ou pour une rencontre hors de l'entreprise.

Dans ce mode, il n'y a pas de Point d'Accès, et une partie de ses fonctionnalités sont reprises par les stations elles-mêmes (comme les trames balise pour la synchronisation).

D'autres fonctions ne sont pas utilisables dans ce cas (relayage des trames ou mode d'économie d'énergie).

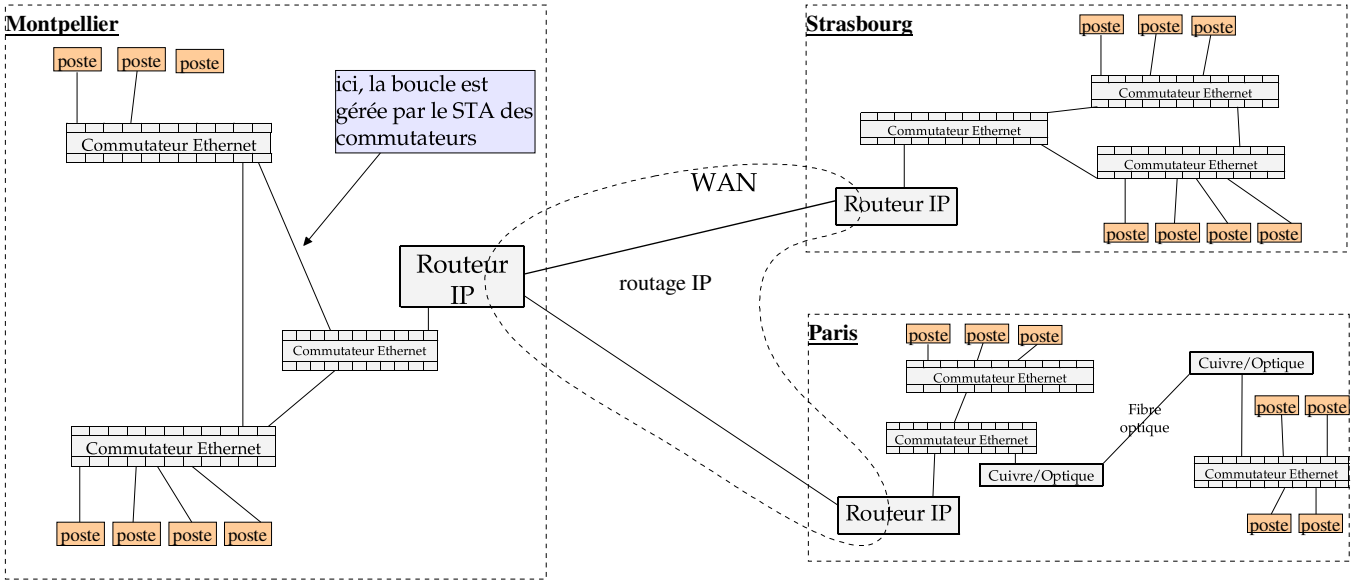
Réseau maillé

Un réseau maillé est un réseau pour lequel tout noeud peut être atteint par un autre noeud et ce, quel que soit le nombre de noeuds intermédiaires.

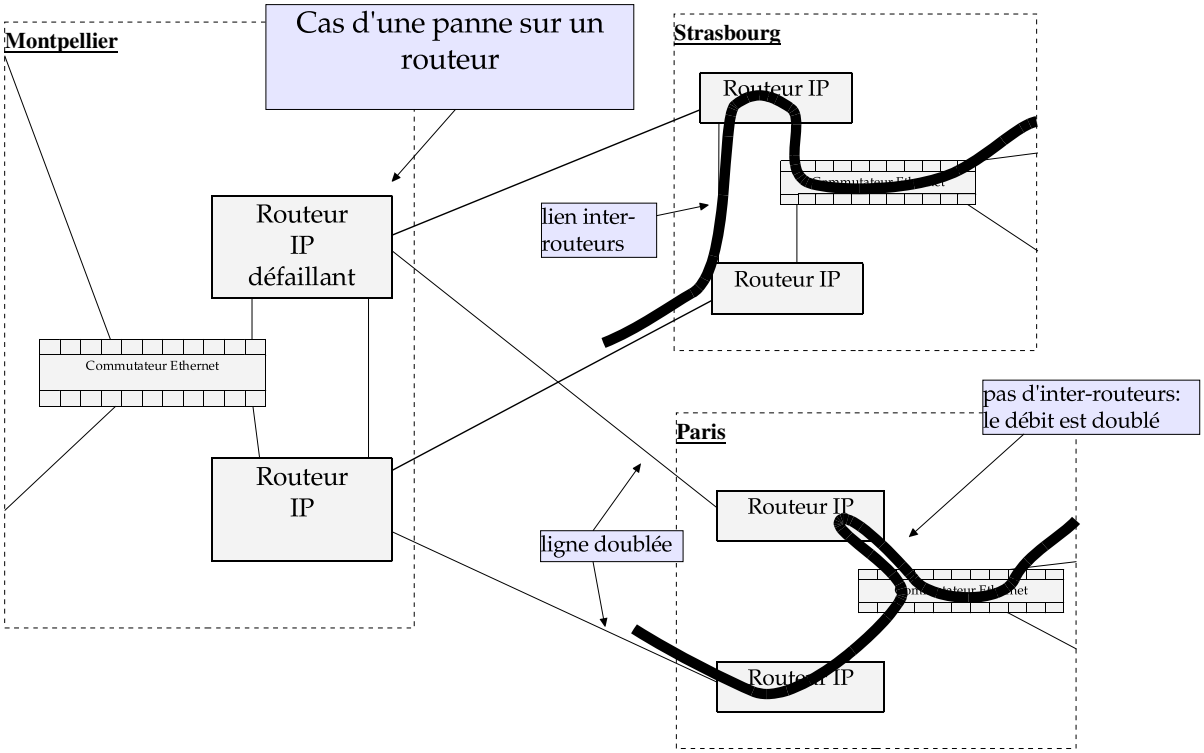
Un réseau complètement maillé est un réseau pour lequel tout noeud est relié à tous les autres. Autrement dit, entre 2 noeuds quelconques du réseau, il existe toujours une ligne de communication directe.

Réseau maillé

De manière générale, les architectures d'aujourd'hui s'appuient sur des liaisons point-à-point pour relier les sites distants et sur des architectures en étoile pour les connexions locales.
Lorsqu'un site s'étend sur une grande surface (approchant le kilomètre carré), les commutateurs sont reliés entre eux par des fibres optiques.



Doublement de ligne



V

Réseaux sans fil

Généralités

Basés sur une technologie qui utilise les ondes radio électriques et infrarouges, les réseaux sans-fil sont de plus en plus utilisés en entreprise.

Suppression des câbles

- Suppression des coûts liés à l'installation des câbles. Evite les lourds aménagements du filaire.
- Encombrement moindre.

Mobilité accrue

L'autonomie des utilisateurs est augmentée.
La mobilité est uniquement limité à la portée de l'émetteur, excepté pour les appareils ne fonctionnant pas sur batterie (raccordement aux prises électriques).
Les technologies sans fil permettent de se passer de la plupart des câbles, mais pas encore de ceux d'alimentation. Les futures normes POE+ permettront d'alimenter les points d'accès WiFi par leur câble ethernet.

Flexibilité

Le réseau peut être rapidement modifié, l'ajout ou la suppression de stations au réseau s'effectue rapidement et ne nécessite aucun matériel hormis les cartes réseau sans fil.

Problèmes de sécurité

En contrepartie de cette mobilité, comme les signaux ne sont pas "contenus" dans les câbles leur propagation n'est pas contrôlable, c'est pourquoi la sécurité prend une place importante pour les réseaux sans fil.

Catégories de réseaux sans fil

WPAN (Wireless Personal Area Network)

La technologie **Bluetooth** appartient à cette catégorie de réseaux, dont l'objectif principal est de relier des appareils et périphériques (tels que téléphones portables, appareils photo numériques, claviers, souris...) à des ordinateurs. La portée et le débit sont généralement peu élevés (environ 10 m de portée et un débit de 1 Mbps).

WLAN (Wireless Local Area Network)

C'est dans cette catégorie que se situe le **WiFi**. L'objectif des WLAN est d'offrir les mêmes prestations que les LAN avec les avantages du sans-fil. La portée d'un réseau de ce type est en général d'une cinquantaine de mètres.

WMAN (Wireless Metropolitan Area Network)

D'une portée de plusieurs kilomètres, seules les grandes agglomérations sont équipées des antennes nécessaires.

WWAN (Wireless Wide Area Network)

Réseau cellulaire mobile.

VI

Réseaux sans fil

Généralités

Basés sur une technologie qui utilise les ondes radio électriques et infrarouges, les réseaux sans-fil sont de plus en plus utilisés en entreprise.

La suppression des câbles évite de lourds aménagements, réduit l'encombrement et accroît mobilité et flexibilité.

En contrepartie de cette mobilité, la propagation des signaux aériens n'est pas contrôlable: la sécurité prend une place importante pour les réseaux sans fil.

Catégories de réseaux sans fil

Il existe 4 catégories de réseaux sans fil:

- WPAN (Wireless Personal Area Network): portée et débit peu élevés (10m et 1Mbps), Bluetooth,
- WLAN (Wireless Local Area Network): le WiFi ou LAN sans fil, de portée 50m environ,
- WMAN (Wireless Metropolitan Area Network): réseau sans fil d'agglomération d'une portée de plusieurs kilomètres,
- WWAN (Wireless Wide Area Network): réseau cellulaire mobile.

Norme WiFi

Un réseau WiFi (contraction de Wireless Fidelity) est un réseau répondant à la norme IEEE 802.11.

Le comité 802 de l'IEEE (Institute of Electrical and Electronics Engineers), organisation à but non lucratif opérant dans le domaine des télécommunications, s'occupe de normalisation et établissent les normes WiFi, dont les plus utilisées sont les 802.11a, 802.11b, 802.11g et 802.11n.

La première, 802.11, date de 1997.

Couche physique

Représentation de 802.11 dans la couche physique du modèle ISO:

<table>
<tr><td rowspan="2">Couche 2: liaison de données
Protocole de transmission des données</td><td colspan="4">LLC 802.2</td></tr>
<tr><td colspan="4">MAC</td></tr>
<tr><td>Couche 1: PHY
Encodage du signal</td><td>FHSS</td><td>DSSS</td><td>IR</td><td>MIMO OFDM = WWiSE ou TGn Sync</td></tr>
</table>

Le WiFi est donc indépendant du protocole de réseau (couche 3) et de transport (couche 4) bien que l'on utilise communément TCP/IP.

Normes 802.11

Norme	Caractéristiques
802.11a	Haut débit (30 Mbit/s effectifs) sur la bande des 5 GHz
802.11b	Haut débit (6 Mbit/s effectifs) sur la bande des 2,4 GHz
802.11c	Travaux suspendus
802.11d	Travaux suspendus
802.11e	Travaux sur la qualité de service (QoS) dans les normes existantes. Par exemple, la transmission synchrone (voix)
802.11f/r	Travaux sur le protocole Inter Access Point Protocol, qui doit permettre aux bornes d'accès de dialoguer entre elles
802.11g	Haut débit (54 Mbit/s théoriques) sur la bande des 2,4 GHz
802.11h	Adoption des technologies DFS (Dynamic Frequency Solution) et TPC (Transmit Power Control), pour une conformité avec les normes européennes
802.11i	Travaux sur la sécurité des transmissions sur les bandes de fréquence 2,4 GHz et 5 Ghz. Amélioration de l'algorithme WPA
802.11j	Convergence des standards américain 802.11 et européen Hiperlan, tous deux fonctionnant sur la bande de fréquence des 5 GHz
802.11n	540Mbit/s. Portée 50m. Validée le 19 janvier 2006 par l'IEEE

Encodages du signal

Caractéristiques des modulations utilisées utilisées pour le WiFi:

- **FHSS: Frequency Hopping Spread Spectrum (étalement de spectre par évasion (saut) de fréquence)**
  Changement de la fréquence porteuse en cas d'encombrement. Cela réduit les interférences.

- **DSSS: Direct Sequence Spread Spectrum (étalement de spectre à séquence directe)**
  Codage sur plusieurs fréquences. Implique une résistance au bruit accrue. Dans les applications militaires, dissimulation du signal utile par ressemblance à un bruit. Encodage aléatoire.

- **IR: Infra-Rouges**
  Lien visuel (lumière, ligne droite). Réduction des interférences.

- **OFDM: Orthogonal Frequency Division Multiplexing/Modulation (multiplexage par répartition en fréquence orthogonale)**
  Le signal utile, envoyé dans le bruit, perturbe moins les autres. La bande passante de 5GHz réduit les interférences. Possibilité de multiplexage (MIMO 802.11n) longues distances (WiMax, 802.11n).

- **WWiSE: World-Wide Spectrum Efficiency (ou TGn Sync)**
  Utilise OFDM et MIMO par emploi de plusieurs antennes. Longue portée, amélioration du débit et de la spatialisation (utilisation du rebond du signal).

Caractéristiques 802.11a,b,g, n et i

Norme	Débit théorique / réel	Encodage	Portée int./ext.	Compatibilité
802.11	1 à 2Mbps	FHSS	50m	aucune
		DSSS 2,4GHz	50m	802.11b et g
802.11b	11/1Mbps	DSSS 2,4GHz	50/300m	interopérable 802.11g
802.11a	54/27Mbps	OFDM 5GHz	50m	aucune
802.11g	54/30Mbps	OFDM 5GHz et DSSS 2,4GHz	70m	802.11b
802.11n	540/100Mbps	WWiSE 2,4 et 5 GHz	90m	802.11b et g

Les normes sont représentées chronologiquement.

La norme 802.11n est à l'état de draft (brouillon), mais des matériels sont disponibles. Elle ne sera finalisée qu'en avril 2009.
La norme 802.11b introduit le chiffrement WEP par algorithme RC4 (peu robuste).

La norme **802.11i** est une norme de sécurité comprenant:

- WPA: WiFi Protected Access,
- TKIP: protocole chiffré à échange dynamique de clés,
- CCMP: protocole à chiffrement AES (meilleur, WPA2),
- 802.1X: méthode d'utilisation d'un serveur d'authentification qui distribue les clés aux utilisateurs. Définit EAP (Extensible Authentication Protocol) utilisable avec un serveur Radius (EAP-TLS).

Architectures 802.11

Les deux architectures définies par la norme 802.11 sont:

- le mode infrastructure: les postes clients sans fil se connectent à un point d'accès,
- le mode ad'hoc: il n'y a pas de point d'accès, les postes clients se connectent directement entre eux.

Mode infrastructure

- Le mode infrastructure utilise des bornes de concentration appelées points d'accès ou PA ("access point" ou AP) qui gèrent l'ensemble des communications dans une même zone géographique.
- Chaque ordinateur du réseau se connecte à un point d'accès via une liaison sans fil.
- **L'ensemble des stations** utilisant un même point d'accès est un **BSS** (Basic Service Set).

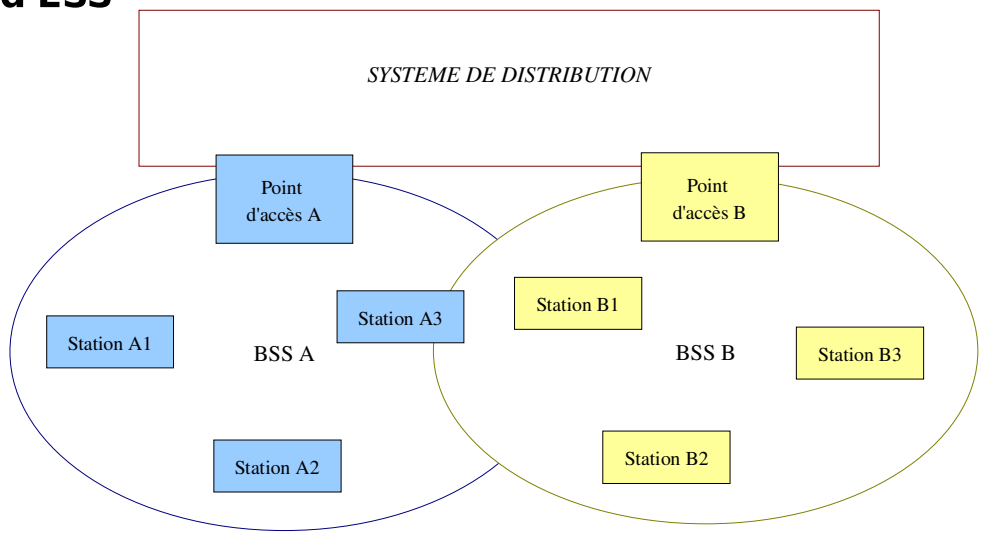
ESS (Extended Service Set)

Il est possible de relier des points d'accès entre eux par une liaison appelée système de distribution: ce peut être un réseau filaire, sans fil ou un câble entre 2 PA. **L'ensemble des BSS** reliés entre eux est appelé **ESS**.

Un ESS est représenté par un ESSID (Service Set Identifier, souvent abrégé SSID), identifiant de 32 caractères de long au format ASCII servant de nom pour le réseau.

Architectures 802.11

Exemple d'ESS



Les 6 stations du schéma font partie du même ESS.
Le système de distribution peut être n'importe quel type de réseau (filaire ou sans fil).
Toute station mobile peut se déplacer tant qu'elle reste dans la zone de couverture totale des 2 points d'accès, le changement de BSS s'effectuant de manière transparente. Ceci est appelé itinérance (ou roaming en anglais), normalisée dans 802.11r (anciennement 802.11f).

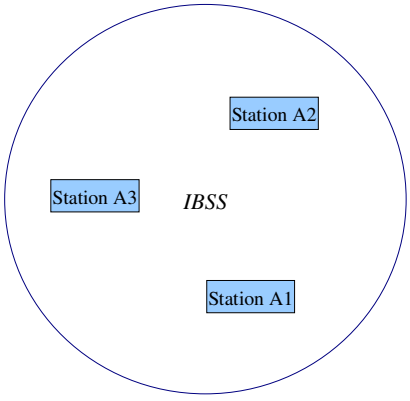
Architectures 802.11

Le mode ad hoc

Dans ce cas de figure, les machines clientes se connectent les unes aux autres. Il n'y a plus d'infrastructure fixe, le signal est transmis par l'intermédiaire des stations et routé dynamiquement. Les stations jouent à la fois le rôle de client et de point d'accès, c'est un réseau point-à-point (peer-to-peer en anglais).

L'ensemble formé par les stations de ce réseau est appelé IBSS (independant basic service set).
Tout comme un ESS, un IBSS est identifié pau un SSID.

Ne disposant pas de point d'accès, le mode ad hoc est généralement utilisé pour créer un réseau éphémère.



OLSR

Présentation

OLSR (Optimized Link State Routing Protocol) est un protocole de routage destiné aux réseaux mobiles "ad hoc". De nombreux systèmes Unix et Windows implémentent ce protocole.
OLSR a été développé de façon à fonctionner indépendamment de tout autre protocole.

Principe de fonctionnement

Contrairement à d'autres protocoles où les noeuds envoient l'intégralité de leur table de routage, avec OLSR seules sont envoyées des informations nécessaires à établir la "carte" du réseau.

A partir de celle-ci chaque noeud effectue, en local, le calcul du plus court chemin vers chacun des autres noeuds du réseau, ceci permettant d'établir la table de routage. Cette méthode nécessite plus de puissance de calcul pour les noeuds mais permet une utilisation moindre de la bande passante.

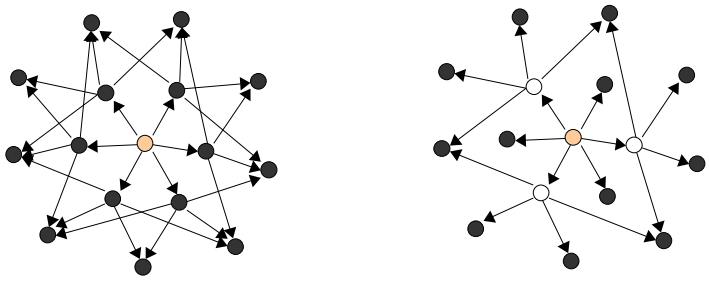
Principal avantage de cette méthode de routage : une grande rapidité de réaction lors de changements dans la topologie du réseau.

OLSR

MPR

Chaque noeud sélectionne un ensemble de noeuds voisins comme "multipoint relays" (MPR). Dans le cas du WiFi, les voisins d'un noeuds sont ceux qui sont à portée radio. Avec OLSR, les noeuds sélectionnés comme MPR sont les seuls responsables de la gestion du trafic et de la diffusion des informations à l'ensemble du réseau.

L'utilisation des MPR permet de réduire au maximum le nombre de transmissions nécessaires et ainsi de ne pas surcharger le réseau.



Contrairement à un fonctionnement classique (à gauche), les relais multipoints (en blanc sur la figure de droite) sont les seuls à pouvoir transmettre les informations.

Le matériel

Point d'accès et routeurs WiFi

- On trouve sur certains routeurs un modem ADSL intégré.
- Certains routeurs WiFi disposent de plusieurs sorties RJ45 et peuvent faire office de commutateur (switch) filaire en plus de leur fonction de routeur WiFi.

Cartes et adaptateurs WiFi

Les matériels les plus répandus pour les clients WiFi sont :

- Carte réseau WiFi PCI (pour les ordinateurs de bureau)
- Carte réseau WiFi PCMCIA (pour les ordinateurs portables)
- Adaptateur réseau sans fil USB

Points d'accès et ponts extérieurs

Ces équipements faits pour l'extérieur sont conçus pour résister au froid et aux intempéries.

Le matériel

Les antennes

Les principales catégories d'antenne 2,4 GHz du commerces utilisées pour le WiFi:

- Le dipôle : omnidirectionnel, équipe la plupart des points d'accès, cartes et adaptateurs WiFi.
- L'antenne tige extérieure: omnidirectionnelle, gain de 7 à 15 dBi lié à sa dimension verticale (2m).
- L'antenne panneau (ou plate): directionnelle, gain de 9 à 21 dBi (10x12 à 45x45x4.5 cm). Meilleur rapport gain/encombrement et rendement (de 85 à 90%).
- L'antenne type parabole pleine ou ajourée (grille): directionnelle, rendement moyen (45 à 55%), gain de 18 à 30 dBi, volumineuse.
- Autres types d'antennes: à fentes, sectorielle, à gain.

Les antennes à plateaux sont souvent préférées grâce à leur faible encombrement, et les paraboles sont à utiliser si de meilleures performances sont recherchées.

Les antennes Wi-Fi sont généralement dotées de connecteurs SMA, RP-SMA ou N selon le constructeur, nécessitant parfois l'utilisation d'adaptateur d'antenne.

Interopérabilité

Des problèmes d'incompatibilité

L'utilisation du WiFi s'étant généralisée, de nombreuses marques fabriquent du matériel WiFi.
Tous les matériels certifiés WiFi assurent les mêmes fonctions propres à la norme 802.11, mais proposent aussi souvent des fonctions supplémentaires.
Il y a alors risque d'incompatibilité avec des matériels de marques différentes. Il faut s'assurer que tous les matériels du réseau supportent les outils utilisés.

Il est nécessaire de vérifier les points suivants lors de l'achat de matériel WiFi :

- Les matériels doivent supporter la norme utilisée pour le réseau (prendre en compte la compatibilité du 802.11g avec le 802.11b).
- Longueur de clé WEP supportée (le WEP est l'outil de sécurité standard du WiFi). La clé WEP a une longueur de 40 bits selon les spécifications de la norme 802.11b, mais sur la plupart des matériels il est possible de fixer une clé WEP plus longue (64, 104, 128 bits...). Il faut veiller à ce que tous les matériels du réseau supportent la longueur de clé désirée.
- Support du WPA. Le WPA est un autre standard de sécurité mais n'est pas supporté par tous les matériels WiFi.

Utilisation du WiFi

Modes de fonctionnement

La plupart des points d'accès propose 4 modes de fonctionnement :
- Point d'accès (AP),
- Point d'accès client (AP Client),
- Répéteur (AP Repeater),
- Pont (Wireless Bridge).

Mode point d'accès

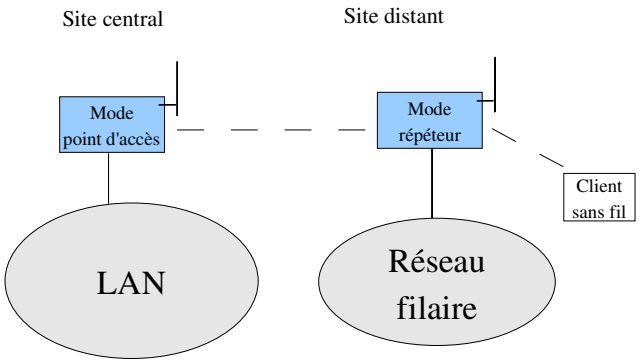
Mode par défaut. Sans sécurité, tous les postes clients peuvent se connecter aux points d'accès mis en place. Par défaut le SSID est diffusé librement, ce qui signifie que si un poste client est à portée d'un point d'accès, il connait le SSID du réseau et peux se connecter.

Mode point d'accès client

Dans ce mode le matériel se comporte en carte d'interface réseau sans fil (carte WiFi).

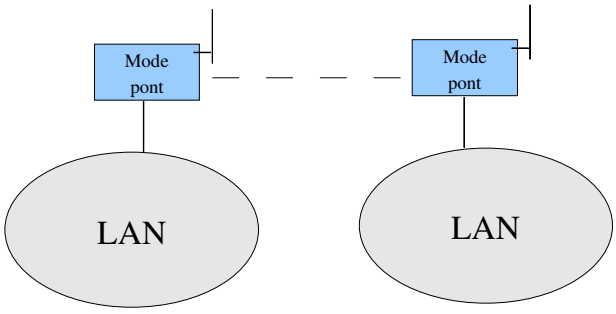
Mode répéteur

Avec ce mode, le matériel conserve son rôle de point d'accès, tout en *élargissant la couverture réseau* en se connectant à un autre point d'accès.



Mode pont

Ce mode permet de connecter un ou plusieurs réseaux locaux distants (LAN) en un seul réseau, en supprimant le rôle de point d'accès (aucun client WiFi).
Le mode pont permet l'*extension du réseau filaire par un lien WiFi*.



Alignement d'antennes

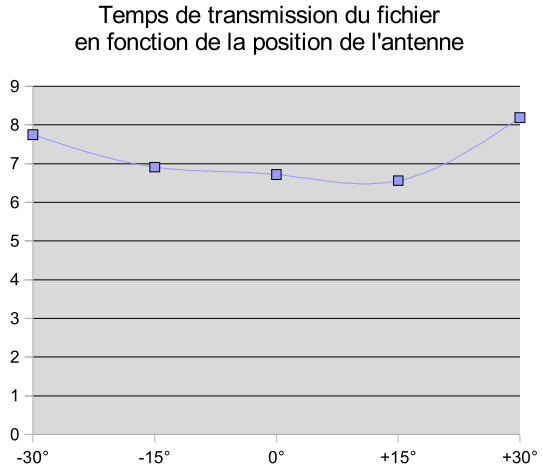
Utilisation des paliers de transfert

Avec un matériel WiFi assurant le rôle de pont et des antennes ayant un gain suffisant il est possible de relier des sites distants.
Pour aligner des antennes à grande distance, une astuce consiste à utiliser les paliers de taux de transfert. En effet, le débit est adapté en fonction de la qualité du signal.
Par exemple, les paliers de la norme 802.11g sont 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 et 54 Mbps.

Méthode d'étude des changements de paliers:
envoyer un même fichier par la connexion sans fil,
modifier la position de l'antenne entre les envois,
relever cette position,
relever le temps mis pour l'envoi complet.

Plus le signal est bon, plus le point d'accès augmente le débit de la transmission (et plus l'envoi sera court).

Dans le cas ci-contre, il faut tourner l'antenne de +15°.



Supervision de réseaux WiFi

Wavemon

Outil Linux mesurant de la force du signal au cours du temps.
Il établit les performances de la carte WiFi en utilisant les informations de /proc/net/wireless.

/proc/net/wireless

Fichier d'informations diverses sur les cartes réseau sans fil:

- *status* est la valeur d'état renvoyée par la carte,
- *Link quality* correspond à la qualité de la modulation (maximum=16),
- *Level* et *Noise* correspondent aux niveaux de signal et de bruit (maximum=64).

NetStumbler

Equivalent Windows de Wavemon. Il détecte et affiche les réseaux sans fil en détails. Cet outil génère un retour MIDI de la puissance du signal, facilitant l'alignement d'antennes sur une longue distance.

MacStumbler et iStumbler

Outils d'analyse de réseaux sous Mac OS X: collectent des renseignements sur les réseaux détectés (SSID, cryptage WEP activé ou non, canal utilisé, etc...) et fournissent puissance du signal et quantité de bruit en temps réel.

Sécurité des réseaux sans fil

La propagation des ondes

La sécurité est une notion particulièrement importante pour les réseaux sans fil, les ondes radio pouvant traverser les obstacles et se propager au-delà du proche voisinage.
Un point d'accès de faible puissance dans le but de limiter la couverture du réseau n'est pas une solution correcte: une antenne suffisamment puissante capte de faibles signaux à grande distance.

Sécuriser le réseau

Le principal, pour les utilisateurs, est d'être sûr qu'un intrus ne pourra pas:

- accéder aux ressources du réseau en utilisant le même équipement sans fil,
- capturer le trafic du réseau sans fil (écoute clandestine).

La *restriction d'accès* est obtenue par *authentification*: une station doit *prouver sa connaissance d'une clef*, ce qui est similaire à la sécurité sur réseaux câblés. L'intrus doit entrer dans les lieux en utilisant une clef physique pour connecter son poste au réseau.

Il existe deux types de chiffrements basés sur de telles clés:

- WEP: Wired Equivalent Privacy,
- WPA/WPA2: WiFi Protected Access.

L'*écoute clandestine* exploite une *faiblesse de l'algorithme WEP* permettant de reconstituer la clé.

WEP

Le WEP (Wired Equivalent Privacy) est un protocole sécurisé pour les réseaux WiFi. Il fait partie du standard 802.11, tous les matériels WiFi le supportent donc.

Principe de fonctionnement

Le chiffrage WEP utilise l'algorithme RC4: chiffrement continu symétrique à clés de longueur variable:

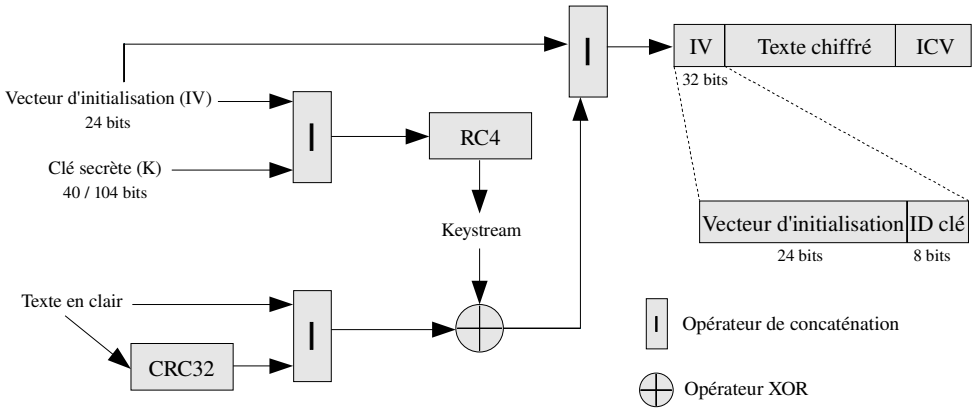
- chiffrement en continu: exécuter la fonction de cryptage ou de décryptage sur une unité du texte en clair (ici, la trame 802.11).
- chiffrage symétrique: la clé est un élément d'information qui doit être partagé par les unités d'extrémité pour réaliser le cryptage et le décryptage.

Chaque paquet 802.11 est chiffré dans un flux codé RC4, généré par une clé de 64 bits. Cette clé est composée d'un vecteur d'initialisation (Initialization Vector, noté IV) codé sur 24 bits et de la clé WEP de 40 bits (ou plus). Le vecteur d'initialisation n'est pas généré par l'utilisateur, il fait partie intégrante de l'algorithme WEP.

Il est en général possible de choisir la longueur de la clé WEP de son réseau : 40, 64, 104 bits (bien que la spécification originale fixe la longueur de la clé à 40 bits).

Chiffrage RC4

Construction du texte chiffré



ICV : Integrity Check Value (Cyclic Redundancy Code sur 32 bits)
K : clé secrète partagée par le point d'accès et les clients (40 ou 104 bits)
Key-stream : résultat de l'algorithme RC4 initialisé par IV et K

Recommandations

Exploiter au mieux le WEP:

- Ne pas utiliser de clé évidente. Les attaques par dictionnaire contre les clés WEP seront d'autant plus difficiles que la clé est complexe.
- Utiliser la plus longue clé supportée par le matériel, après avoir vérifié que tous les matériels du réseau supportent cette longueur de clé.
- Changer souvent de clé (ce n'est pas toujours réalisable, notamment pour les grands réseaux, à cause du problème de diffusion de la clé).
- Combiner le WEP à d'autres fonctionnalités de sécurité.

Les faiblesses du WEP

4 faiblesses du WEP

- Chiffrage au niveau liaison: Le cryptage se situe au niveau de la couche Liaison et non Application. Les données sont protégées entre le client et la passerelle, mais pas au-delà. Lorsque les données atteignent un câblage, elles transitent en clair.
- Clé partagée: tous les clients d'un même réseau partagent la même clé. Il est possible de lire les paquets des autres clients.
- Longueur de clé: plusieurs équipes de cryptographes ont identifié des faiblesses dans l'implémentation WEP, démontrant qu'une longueur de clé plus importante ne garantissait pas, dans tous les cas, une meilleure sécurité.
- Casser une clé WEP: des logiciels (AirSnort,...) permettent de casser une clé WEP très facilement. Le principe consiste à capturer les paquets circulant sur un réseau sans fil. L'opération prend quelques heures, durée fonction de l'intensité du trafic sur le réseau.

Le vrai objectif du WEP

Le WEP n'a pas été conçu pour faire office de protection parfaite mais pour, comme son acronyme l'indique, fournir une protection équivalente à celle d'un réseau cablé non chiffré.
Le WEP est une solution simple de dissuasion contre les accès non autorisés.

Précautions supplémentaires

En complément du WEP, les opérations suivantes renforcent la sécurité.

Cacher le SSID

Sur les points d'accès, désactiver l'émission en clair du SSID (nom du réseau). Ainsi toute personne voulant se connecter devra au préalable connaître le SSID.

Filtrage par adresse MAC

Généralement il est possible de configurer sur un point d'accès une liste de droits d'accès (appelée ACL) basée sur les adresses MAC. Seuls les équipements dont l'adresse MAC est présente dans l'ACL sont autorisés à se connecter.

WPA

Présentation

WPA (WiFi Protected Access) et WPA2 sont des standards de sécurisation proposés par la WiFi Alliance pour combler les faiblesses du WEP. WPA et WPA2 fonctionnent avec toutes les normes WiFi standards (802.11a/b/g/n) mais sont uniquement destinés aux réseaux en mode infrastructure et ne sont pas utilisables en mode ad-hoc.

802.11i

WPA implémente une grande partie de la norme IEEE 802.11i et a été créé comme une étape intermédiaire pour remplacer le WEP en attendant que la norme 802.11i soit finalisée. Le WPA peut être utilisé avec toute carte d'accès sans fil mais pas avec les poins d'accès de première génération.

WPA2 est la version de la norme 802.11i certifiée par la Wi-Fi Alliance. WPA2 inclut tous les éléments obligatoires de la norme 802.11i. En particulier, les algorithmes Michael et RC4 sont remplacés respectivement par CCMP, un algorithme d'authentification de message qui est considéré comme complètement sécurisé, et par AES. WPA2 ne fonctionne pas avec certaines anciennes cartes sans fil.

WPA et WPA2 fournissent un bon niveau de sécurité et doivent être préférés au WEP.

Il existe deux modes de fonctionnement pour WPA et WPA2: l'un utilisant une clé partagée (WPA-PSK) et l'autre un serveur d'authentification (WPA-EAP).

WPA-PSK

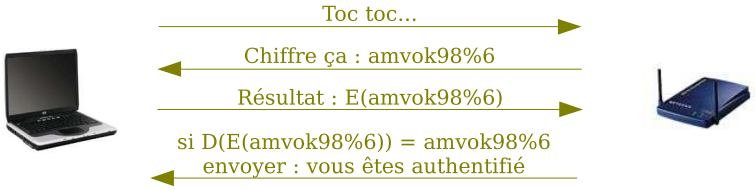
Clé partagée

Ce mode, appelé également *WPA-Personnal*, ne nécessite pas la mise en place d'un serveur d'authentification et est donc moins couteux et plus facile à mettre en place que l'autre mode WPA, mais offre un moins bon niveau de sécurité.

Il utilise une clé partagée appelée PSK (Pre-Shared Key) qui est renseignée dans le point d'accès et dans les postes clients. Cette clé n'a pas de longueur prédéfinie et WPA réserve la possibilité de saisir une "passphrase" qui sera traduite en PSK. Il est conseillé de choisir une clé d'au moins 20 caractères.

Processus d'authentification par clé partagée

- Un client tente de s'associer à un point d'accès,
- l'AP lui répond en envoyant une chaîne de caractères aléatoire,
- le client utilise sa clé pour chiffrer le texte et envoie le résultat à l'AP,
- l'AP déchiffre avec sa clé partagée,
  si le résultat est le texte d'origine,
  les deux clés sont identiques,
  le client est authentifié.



WPA-EAP

Le mode WPA-EAP, également nommé *WPA-Enterprise,* impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification et d'un contrôleur réseau.

802.1x

Le protocole 802.1x utilisé par WPA décrit une méthode pour l'authentification par port qui peut être appliquée à différents types de réseaux, filaires ou non. Attention à ne pas confondre le 802.1x avec la notation 802.11x parfois utilisée pour abréger 802.11a/b/g/n.

802.1x définit un mécanisme d'authentification au niveau de la couche 2 du modèle ISO pour les réseaux physiques de type IEEE802 (Ethernet, Token Ring, radio) et PPP. Le mécanisme d'authentification 802.1x intervient avant d'éventuels mécanismes d'auto-configuration tels que DHCP (Dynamic Host Configuration Protocol) ou PXE (Pre-Boot Execution Environment).

WPA-EAP

Processus d'authentification

L'authentification 802.1x comporte trois composants principaux: le client ("supplicant"), l'authentificateur (PA par exemple) et le serveur d'authentification (souvent Radius).
RADIUS (Remote Authentication Dial-in User Service), n'est pas imposé par la norme.

Avant que tout accès réseau soit permis le client doit s'authentifier. Il ne peut communiquer sur le réseau qu'avec l'authentificateur,.qui vérifie les droits d'accès et autorise ou interdit l'accès au réseau.

1. *Requête d'identification à l'authentificateur* (le point d'accès WiFi dans ce cas).
2. *Demande d'identification et bloquage* de tout autre trafic tant que le client n'a pas été identifié: le port du client est ainsi imperméable à tout le trafic hors 802.1x.
3. *Réponse du client au serveur d'authentification via l'authentificateur*: le type d'identification n'est pas spécifiée par le protocole, elle peut être de n'importe quelle forme.
4. *Réçeption de la reponse et vérification d''identité*. Un message est envoyé à l'AP pour indiquer si le client est accepté ou rejeté. L'AP transmet la réponse au client.
5. Dans le cas où le client est accepté, l'AP met le *port du client à l'état "autorisé"* et permet tout trafic.

WPA-EAP

EAP

802.1x est basé sur le protocole d'authentification EAP (Extensible Authentication Protocol) qui est une extension de PPP (point-to-point protocol). EAP est un framework d'authentification mais ne constitue pas un mécanisme spécifique d'authentification.

EAP est le socle de base, de nombreuses autres méthodes d'authentification peuvent venir se greffer par-dessus. Au départ uniquement le mécanisme EAP-TLS (Transport Layer Security) était certifié par la Wi-Fi Alliance, puis elle a annoncé l'inclusion de mécanismes supplémentaires. Les produits certifiés *WPA-Enterprise* peuvent interopérer entre eux.

Certification

Les mécanismes EAP inclus dans le programme de certification pour les modes *WPA-Enterprise* et *WPA2-Enterprise* sont les suivants :

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

D'autres mécanismes EAP peuvent être supportés par les clients et les serveurs 802.1X.

VII

Interconnexions de réseaux

Matériels d'interconnexion

Le besoin

Dès qu'il existe plusieurs réseaux apparaît le besoin de communication.

Cela a nécessité le développement de matériels d'inter-connexion de réseaux différents et opérants à différents niveaux du modèle OSI:

- soit de techniques identiques (Ethernet/Ethernet),
- soit complètement différents en architecture, protocole, ... (Ethernet/Token-Ring).

Comment?

Liste des différents types d'équipements d'interconnexion:

- les répéteurs *(repeater)*,
- les concentrateurs *(hubs)*,
- les ponts *(bridges)*,
- les commutateurs *(switches)*,
- les routeurs *(routers)*,
- les passerelles *(gateways)*.

Répéteur / Repeater

Un répéteur agit sur la couche 1 (la couche physique): il ***régénère le signal*** électrique reçu sur le medium (couche 1) ***à l'identique***.

Cela augmente la distance physique de transmission, mais l'absence de contrôle et de filtrage fait qu'il répète également le bruit avec le signal.

Caractéristiques:

- opère sur la couche 1
- régénère le signal à l'identique

Avantages:

- aucune perte de signal
- augmente la distance couverte par un réseau

Inconvénients:

- répète également le bruit

Concentrateur / Hub

Le concentrateur agit sur la couche 1 (physique).
Son rôle est d'interconnecter plusieurs interfaces entre elles.
Le signal reçu est diffusé sur toutes les interfaces raccordées.

La ***topologie*** réseau résultante est de type ***bus***.

*Exemple: un hub 100Mbps **partage** le débit sur l'ensemble de ses interfaces raccordées.*

Caractéristiques:

- opère sur la couche 1
- diffuse un signal reçu sur toutes ses autres interfaces
- topologie bus de données

Avantages:

- simplicité de mise en œuvre

Inconvénients:

- générateur de collisions (non directif, rapport signal/bruit faible)

Pont / Bridge

Un pont agit au niveau de la couche 2 (liaison de données).

Il permet de connecter des réseaux de nature (liaison) différente et retransmet si nécessaire sur un segment de sortie les trames après traduction.
Si l'adresse destinataire appartient au réseau origine, le message sera filtré.
Si l'adresse destinataire est inconnue, le message sera envoyé à tous sauf le réseau d'origine.

Exemple: un point d'accès Wi-Fi est un lien entre les réseaux Ethernet 802.3 et WiFi 802.11.

Caractéristiques:

- opère sur la couche 2,
- interconnecte des réseaux de nature différente; utilisé pour l'expansion d'un même réseau

Avantages:

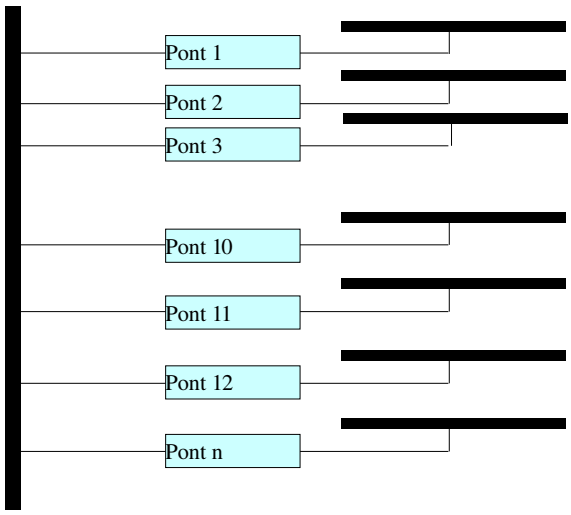
- reconnaissance des stations,
- filtrage,
- transmission

Inconvénients:

- introduction d'un délai de transmission non négligeable

Commutation

Imaginons un pont que l'on réduit à la traduction d'un seul protocole en un autre.
Le programme permettant de réaliser cette fonction devient suffisamment simple pour être gravé dans un circuit intégré.
Il est ainsi facile de développer des machines multi-ponts qui sont équivalentes au schéma:



Commutateur / Switch

Un commutateur opère sur la couche 2 (liaison de données).

C'est un ensemble de circuits et de machines permettant de créer au moins un chemin entre deux points (c'est-à-dire entre deux de ses interfaces).

Cela constitue une ***topologie*** réseau en ***étoile*** *autour du commutateur* entre les interfaces raccordées.

*Exemple: un switch 100Mbps **garantit** un débit de 100Mbps sur chacune de ses interfaces raccordées.*

Caractéristiques:

- opère sur la couche 2
- connecte deux interfaces l'une à l'autre
- topologie étoile

Avantages:

- débit garanti *dans chaque sens*
- peu collisionneur (directif, rapport signal/bruit élevé)

Inconvénients:

- opère sur une couche liaison identique sur chaque interface (Ethernet/Ethernet, par exemple)

Commutation

Globalement, il existe 2 types de commutation :

- La commutation de trames (au vol et bufférisée)
- La commutation de cellules (utilisée dans la téléphonie numérique, ATM)

commutation au vol

on ouvre le circuit dès que l'adresse de destination est connue.

==> temps de traitement très court
==> mais les erreurs ne sont pas traitées: reémission

commutation bufferisée

le commutateur agit comme un pont : l'ensemble des trames est reçu avant d'être analysé, ce traitement est effectué au niveau matériel, ce qui améliore les performances.

La commutation à des vitesses différentes ne peut être réalisée que si la structure de trame est fixe et compatible avec les 2 réseaux à interconnecter

Ethernet 10MB et Ethernet 100 MB

Routeur / Router

Un routeur agit au niveau de la couche 3 (réseau).
Il voit le réseau comme l'ensemble des adresses et des chemins pour accéder aux différents objets.

Exemple: un routeur reçoit une trame, compare l'adresse IP de destination à ses tables et renvoie le datagramme vers l'interface de sortie correspondante.

Caractéristiques:

- opère sur la couche 3,
- interconnecte des réseaux IP entre eux
- gestion de la table des adresses et des chemins (ARP)
- sélection de la meilleure route pour chaque paquet (RIP, OSPF,...)

Avantages:

- fonctionnalités de qualité de service (DiffServ, RSVP, ToS,...)
- filtrage,
- transmission

Inconvénients:

- complexification de la configuration

Passerelle / Gateway

Une passerelle permet des conversions de protocoles, et agit sur n'importe quelle couche du modèle OSI (généralement de 3 à 7).

Caractéristiques:

- opère sur toutes les couches OSI,
- interconnecte
- gestion de la table des adresses et des chemins (ARP)
- sélection de la meilleure route pour chaque paquet (RIP, OSPF,...)

Avantages:

- fédération de réseaux hétérogènes
- peut assumer un rôle de proxy/firewall dédié (proxy SIP par exemple)

Inconvénients:

- configuration spécifique au type de passerelle
- gourmande en ressources

Résumé

Fonction

Un	connecte	OSI
Répéteur	des segments ou des stations	1
Concentrateur	de nombreux segments en partageant le débit	1
Commutateur	de nombreux segments ou stations à très grande vitesse	2
Pont	des réseaux similaires (en terme de protocole de communication)	2
Routeur	des réseaux avec un ou plusieurs protocoles de communication	3
Passerelle	des réseaux hétérogènes	7

Comparaison

Répéteur	+des types de support physiques différents, -ne filtre pas le trafic. Limite l'extension du nombre de segments
Concentrateur	+simple à installer, économique, -débit partagé
Commutateur	+très grande vitesse, simple à installer, économique
Pont	+simple à installer et à configurer, indépendant des protocoles. STA
Routeur	+gère plusieurs protocoles de communications simultanément
Passerelle	+relie des environnements totalement différents -lent et coûteux. Souvent spécifique.

Comparatif Ethernet partagé/commuté

Nous allons comparer un concentrateur 24 ports avec un commutateur 24 ports Ethernet 100

100M partagé

Bande passante totale: 100Mbps x 30% (en moyenne par suite des collisions)= 30Mbps, c'est à dire environ 3Mo/s pour l'ensemble des postes.

Par poste, on dispose de 3/24= **125ko/s par poste**

100M commuté

Bande passante par poste 100Mbps x 90% (en moyenne pour le traitement interne)= 90Mbps, c'est à dire environ **9Mo/s par poste**

D'autre part, il est difficile d'écouter un réseau commuté, ce qui améliore le degré de sécurité.

La commutation semble donc un bon atout pour améliorer le débit et la qualité de service.

Dédier un brin ethernet 10Mbps par poste est plus efficace que partager un brin 100Mbps. Dans le premier cas, chaque poste dispose de 10Mbps sans collision ce qui porte la bande passante utilisable à 90% du total soit environ 1Mo/s de taux de transfert.

VIII

TCP/IP

Définitions

IP = Internet Protocol
TCP = Transmission Control Protocol

Objectif

Fournir un moyen de communication universel, indépendant des machines et des réseaux physiques.

Développé au début sur Ethernet.

Internet = INTERNETWORKING
= interconnexion de réseaux

TCP/IP définit la communication entre machines, l'interconnexion de réseaux différents et le routage des informations entre des réseaux.

Naissance et historique

- 1969 : création du réseau ARPANET (Advanced Research Project Agency Network)
= réseau longue distance à commutation de paquets

- 1975 : définition de TCP

TCP/IP a été développé par BBN (Bolt Beranek and Newman)

- 1980 : version d'Unix Berkeley contenant TCP/IP
- 1983 : toutes les machines du réseau ARPANET utilisent TCP/IP.

Les universités sont progressivement équipées de systèmes Unix et se connectent au réseau ARPANET par TCP/IP, il en est de même pour les laboratoires de recherche, etc ...

IP dans le modèle ISO

IP est un protocole réseau et s'intègre dans un modèle normalisé décrivant les fonctionnalités réseaux

Rappel sur le modèle à 7 couches

Les différentes étapes de définition d'un réseau (suppport physique, codage, protocole,etc ...) ont amené l'ISO (International Standards Organization) à produire les spécifications en couches d'un réseau.

Les couches sont définies suivant les critères suivant :

- chaque couche doit réaliser une fonction spécifique parfaitement définie
- chaque couche rend des services aux couches supérieures et doit donc lui fournir les renseignements nécessaires au décodage des trames reçues
- les fonctions d'une couche doivent pouvoir être l'objet d'un standard.

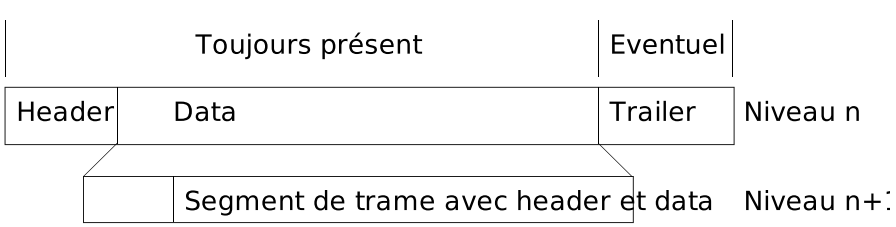
Structure des trames

Une trame comprend toujours :

- Un *header*, entête en français,
- Des données,

éventuellement :

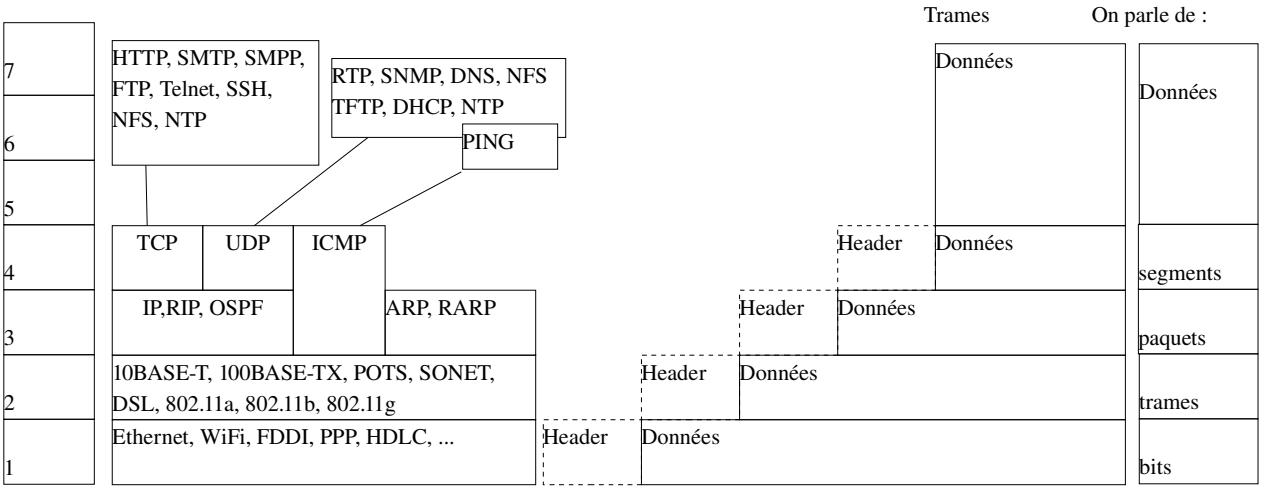
- Un *trailer*, une queue.



La trame d'un niveau fait partie des données du niveau inférieur. Si elle est trop grande elle sera segmentée par la machine émettrice, puis reconstituée par la machine réceptrice.
Il y a imbrication des trames lors des traversées de niveaux.

Empilement des trames

Les données du niveau n comportent toujours les données du niveau n+1 plus leur header (en-tête).
Les différentes couches ne connaissent et ne s'occupent que des informations liées à leur niveau.
TCP/IP donne un format à chaque header pour chaque niveau de protocole.



Exemple d'application

A titre d'exemple, on considère l'application FTP qui permet de transférer des fichiers.
Soit à transférer un fichier de 10000 octets entre une machine A vers une machine B.

Que se passe-t-il lors d'un transfert?

Connexion FTP

- obtention d'un port de la part de TCP (permet d'identifier ce transfert parmi d'autres. Cette identification permet le multiplexage TCP)
- demande à TCP de la connexion vers B
- IP réalise le transfert des informations

TCP doit réaliser la connexion et la maintenir:

- envoi d'une demande de connexion à B
- demande à FTP des références de l'utilisateur (Nom, Mot de passe)
- envoi des références à la machine B
- réponse de B et remontée à FTP
- IP réalise le transfert des informations

Exemple d'application

FTP envoie son fichier à TCP

- découpage en éléments simples
- numérotation des paquets, calcul des CRC
- transmission à IP
- attente des accusés de réception du TCP distant
- reémission de toute trame qui n'est pas acquittée

Sur la machine distante B:
le processus FTPD reçoit les informations du TCP et fabrique le fichier utilisateur.

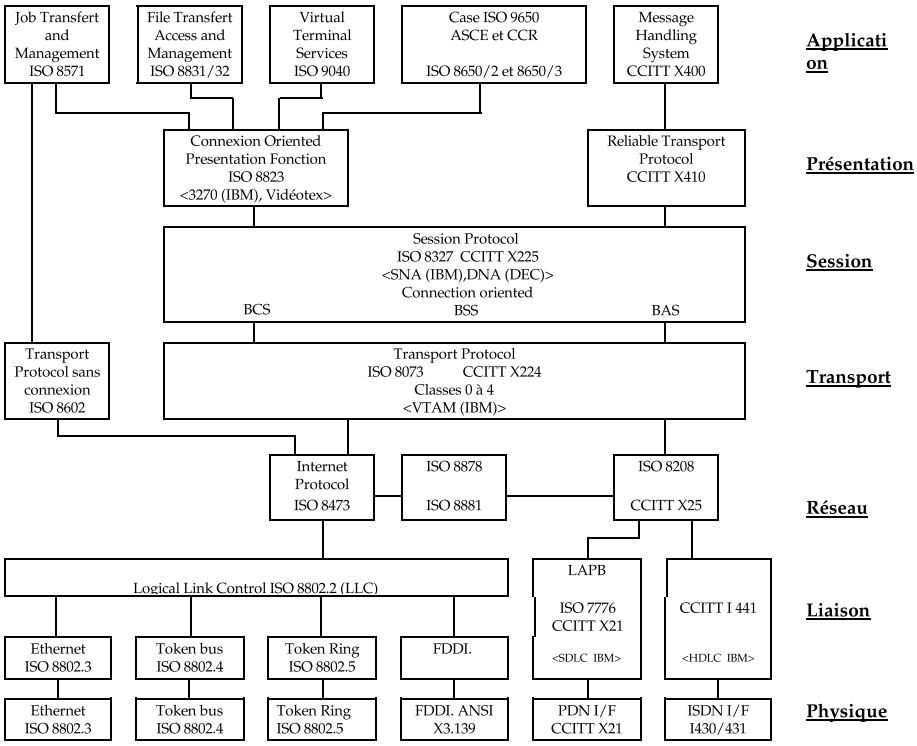
Toute transmission par IP se fait selon:

- IP indique dans la trame que celle-ci vient de TCP
- IP la transmet à Ethernet
- Lors du transit par des routeurs, cette trame pourra éventuellement être fragmentée
- l'IP de la machine B (IP2) réalise le réassemblage
- Cet IP2 transmet la trame à TCP
- Le TCP de B transmet les données à FTP

Le modèle à 7 couches

Nom	Fonction	Objets manipulés	Contrôle
7-Application	Fournit aux applications les services spécifiques de mise en correspondance des demandes utilisateurs. Apporte tous les services directement compréhensibles entre applications et gère les contenus des messages.		
6-Présentation	Mise en forme des données pour les rendre "portables" d'un système à un autre. Les données sont mises sous forme commune compréhensible par les applications (conversion ASCII -> EBCDIC, cryptage).		
5-Session	Gestion des connexions et mécanismes de reprise de session (check point). Effectue le contrôle du dialogue (half ou full duplex). Sécurité.		
4-Transport	Communication transparente d'un noeud à un autre. Contrôle de transmission point-à-point. Gère le contrôle de flux et le contrôle de séquencement. Permet l'adressage au niveau du processus. Communication inter-réseaux.	Messages	cohérence des numéros
3-Réseau	Contient les mécanismes de contrôle de congestion ainsi que les services de routage. Effectue aussi la segmentation et le réassemblage.	Paquets	checksum de paquet
2-Liaison	C'est la gestion de la ligne physique. Contient les mécanismes de détection et de correction des erreurs, et le contrôle du flux (protocole HDLC le plus utilisé).	Trames	checksum horizontal
1-Physique	C'est la couche permettant d'effectuer le codage, puis la transmission physique des bits sur le canal de communication.	bits octets	parité

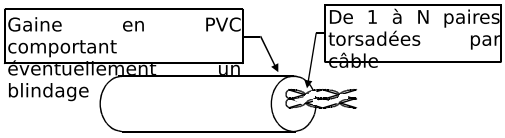
Le modèle à 7 couches



Ethernet

Ethernet couche 1:

Décrit la partie physique.
Par exemple, Ethernet sur câble catégorie 6



Ethernet couche 2:

Décrit la trame:

- un préambule
- les adresses physiques source et destination
- la longueur des données
- les données
- des codes de contrôle d'erreur

L'adresse physique est nommée adresse MAC.

L'adresse MAC

MAC ou Media Access Control.

Comment une machine est-elle connue d'un réseau ?

- Par une adresse ⟶ l'adresse MAC

Qu'elles sont ses caractéristiques ?

- Elle est unique.
- Elle est structurée selon les normes en vigueur chez le constructeur de l'interface.
- Elle n'est pas modifiable pour ethernet, car inscrite au niveau matériel.

Structure de l'adresse MAC

Elle dépend du protocole de niveau 1 utilisé.

Dans le cas d'un réseau Ethernet elle est constituée de 12 caractères hexadécimaux.

Les constructeurs respectent certaines normes, par exemple, six caractères pour un type de matériels et un constructeur, plus six caractères pour le matériel :

- 080002 + 6 chiffres pour les stations réseau de 3COM.
- 02608C + 6 chiffres pour les serveurs de terminaux 3COM.
- 080020 + 6 chiffres pour les stations SUN.

L'adresse MAC, 0800 20A0 425B, désigne donc une station SUN.

Le protocole IP

Rôle d'IP :

acheminement de datagrammes sans mécanisme de reprise, ni de contrôle de flux et sans garantie de réception.

IP est un protocole de niveau réseau (3).

Couche réseau (3) :

Gestion des trames:

IP = Internet Protocol
ICMP = Internet Control Message Protocol

Gestion des adresses :

ARP = Address Resolution Protocol
RARP = Reverse Address Resolution Protocol

Adresse IP

Pour acheminer des données depuis une origine jusqu'à un destinataire, IP doit savoir comment accéder au destinataire
=> nécessité de l'adressage.

Pourquoi IP ne peut-il pas utiliser les adresses MAC ?

Adresse IP

C'est l'adresse réseau par excellence.

Quelles sont ses caractéristiques ?

- Elle doit être unique au sein d'un même réseau,
- Elle est normalisée au niveau international,
- Elle est attribuée par une autorité unique, le Network Information Center, (pour Internet)
- Elle est codée sur 32 bits.

Une machine peut avoir plusieurs adresses IP.

La représentation de l'adresse IP

La décomposition des 32 bits en quatre groupes de 8 bits a permis trois représentations :

- Binaire, c'est l'exemple précédent,
- Décimal,
- Hexadécimal.

L'exemple précédent donne :

Binaire	10111100	00101011	01001001	10110110
Décimal	188	043	073	182
Hexadécimal	BC	2B	49	B6

La notation décimale améliore la lisibilité de l'adresse,
la notation hexadécimale correspond au format utilisé par la plupart des analyseurs de trames.

Structure de l'adresse IP

Le déploiement de machines sur un réseau IP oblige à regrouper les adresses en blocs. Un bloc d'adresses IP s'appelle un réseau. Les réseaux sont reliés entre eux par des routeurs.

Pour définir un bloc d'adresses, deux techniques existent aujourd'hui:

- les classes d'adresses
- la définition de masques réseaux

Classes d'adresses

L'adresse IP se divise en trois champs.

- Les deux premiers désignent le réseau, (il comprend 8, 16 ou 24 bits): le Netid
- Le dernier précise la machine recherchée sur le réseau: le Hostid.

Les machines d'un même réseau se partagent un même radical adresse. C'est la partie gérée au niveau international.
La position de la frontière de partage de l'adresse IP détermine la classe du réseau. C'est le propriétaire du réseau qui fixe la classe de son adresse en fonction de ses besoins.

Adresse IP de 32 bits, par exemple		
10	11110000101011	0100100110110110
2 bits	14 bits	16 bits

Classe du réseau	Adresse du réseau	Indicatif de station
Partie commune à toutes les stations		

Classes

Classe		nb octets/net	nb octets/hosts
A	0xxxxxxx	1	3
B	10xxxxxx	2	2
C	110xxxxx	3	1
D	1110xxxx	multicast	
E	11110xxx		
F	111110xx		
G	1111110x		

Remarque: les classes d'adresses deviennent obsolètes.

Masque réseaux

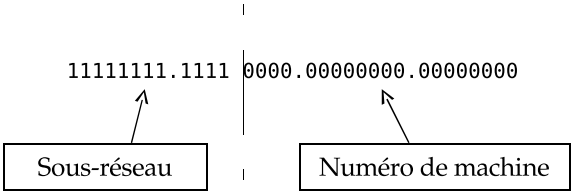
La notion de classes sert à découper le jeu d'adresses en zones.
Le nombre de ces zones est trop faible

==> normalisation de la notion de masque de réseau

Masque de sous-réseau

Dans une adresse IP, la séparation entre la partie "numéro de réseau" et "numéro de machine" ne se fait plus par la classe mais par une valeur binaire:
Chaque "un" du masque indique une partie du sous-réseau
Chaque "zéro" du masque indique une partie du numéro de machine

Exemple:
`255.240.0.0`
se traduit en binaire en



Calcul du numéro réseau

Le numéro de réseau est déterminé par le Subnet Mask. Celui-ci forme un masque qui, appliqué à l'adresse IP, 'extrait' le numéro réseau.

Soit l'adresse IP: `18.35.217.21` et le masque à `255.240.0.0`

Nous cherchons à déterminer sur quel réseau se trouve cette machine.

Etape 1

La séparation entre réseau et numéro de machine va se faire sur le deuxième octet à partir de la gauche.
L'adresse du réseau sera donc de la forme 18.X.0.0

Etape 2

Il nous reste à trouver X

`35` en décimal est représenté par `0010 0011` en binaire.
`240` en décimal est représenté par `1111 0000` en binaire.

Il ne nous reste qu'à prendre en compte les 1 du 35 qui sont aussi dans les 1 du 240.
Ce qui donne:

```
  0010 0011
  1111 0000
  ----------
= 0010 0000
```

nombre qui vaut `32` en décimal.

Calcul du numéro réseau

Le réseau est donc `18.32.0.0`

La valeur initiale `255.240.0.0` s'appelle le masque réseau. Cette valeur pourrait aussi s'écrire `/12`, qui signifie: "on prend en compte les 12 premiers bits à partir de la gauche".

L'adresse IP dans ce cas s'écrit `18.35.217.21/12`.

La machine `18.35.217.21/12` se trouve sur le réseau `18.32.0.0`

Broadcast

La notion de broadcast permet de représenter à l'aide d'une adresse IP unique, l'ensemble des machines d'un même réseau IP.

Le broadcast est défini lorsqu'on met à 1 tous les bits correspondant au numéro de la machine.

Pour un réseau de classe:
A: la destination `x.255.255.255` représente toutes les machines du réseau `x`
B: la destination `x.y.255.255` représente toutes les machines du réseau `x.y`
C: la destination `x.y.z.255` représente toutes les machines du réseau `x.y.z`

Ce mécanisme permet de transférer les tables de routage, et plus généralement de faire de la diffusion globale de messages.

L'adresse de broadcast de 10.16.0.1/12 est 10.31.255.255.

Remarque

Les noms logiques

Même en notation décimale les adresses précédentes présentent le même inconvénient, le manque de lisibilité.

Comment s'affranchir de ce problème ?

- Par l'emploi de noms logiques ou noms symboliques.

Quelles sont ses caractéristiques ?

- Aucune contrainte, le gestionnaire du réseau est libre d'appliquer ses propres normes,
- Il ne peut-être utilisé qu'à l'intérieur d'un réseau connu, en général le sien,
- En inter-réseau il y a risque d'ambiguïté (plusieurs administrateurs)

La gestion de ces noms logiques est réalisée par DNS.

Nous verrons que les URL utilisés pour le Web s'appuient principalement sur ces noms.

Fonctionnalités

La fonctionnalité principale d'IP est l'interconnexion de réseaux hétérogènes, ce qui nécessite du routage.

Chaque réseau a des caractéristiques propres, comme la taille maximum des trames.

La fragmentation

Si le réseau accepte une taille maximum de paquets inférieure à la taille du datagramme, il faut fragmenter le datagramme.

Les "datagram fragments" sont routés indépendamment les uns des autres.

Ils sont réassemblés par l'IP de la machine destinataire.

La fiabilité

IP ne garantit pas l'acheminement des trames.

Quelques sources d'erreur :

- un datagramme peut être détruit par le destinataire en cas de manque de ressources
- IP ne détecte pas la perte de datagrammes par les couches liaison
- Un pirate peut facilement prendre un datagramme et le remplacer par un autre avec la même adresse destination.

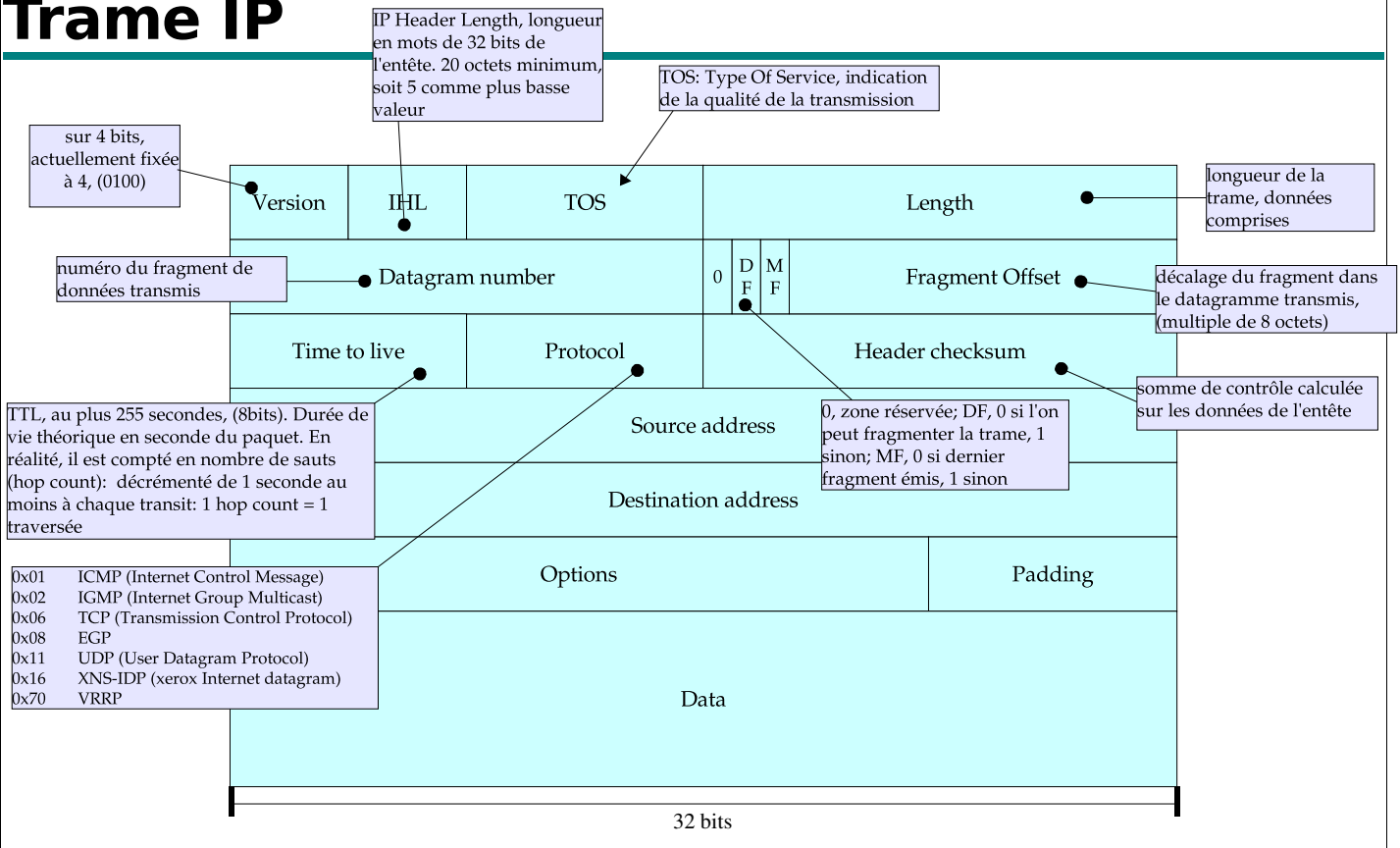
Remarques :

Cette absence de garantie est nécessaire puisqu'il s'agit d'un routage dynamique

La destruction de datagrammes par un destinataire en cas de surcharge peut être un avantage en cas de surcharge du réseau.

La garantie d'acheminement nécessaire aux applications sera apportée par les couches supérieures (TCP)

Trame IP



TCP

TCP = Transmission Control Protocol

Besoin : fiabilisation des communications
En effet, IP assure le transfert, le routage des datagrammes, mais sans aucune assurance, ni vérification d'arrivée à destination.

TCP est un protocole de transport.

Rôle d'un protocole de transport (couche 4) :

- assurer une communication transparente d'un noeud à l'autre
- gérer le contrôle de flux et le contrôle de séquencement

Le mode connecté

Pour assurer une connexion de "bout en bout", TCP fonctionne en mode connecté.

Un process se connecte à un autre process : c'est une communication inter-process.

Notion de port :

un process est identifié par un numéro de port.
On s'adresse au numéro de port, et non pas au process directement.

Plusieurs moyens pour connaître le numéro de port associé à un service :

- soit on fixe une convention à l'avance
- soit un crée un serveur de ports, qui gère les associations process/ports
- soit on utilise la table des "well known ports", qui réserve des numéros de ports pour les services les plus courants.

Note : sur un système UNIX, cette table peut être stockée dans le fichier `etc/services`.

TCP

Remarques :

TCP assure le multiplexage

certaines données peuvent être prioritaires, un drapeau l'indique dans le segment

La fiabilité TCP

La fiabilité est assurée par la numérotation des octets à transmettre.

La numérotation :

TCP numérote tous les octets qu'il doit transférer
Dans le segment, est indiqué le numéro du premier octet du segment, et le nombre d'octets contenus dans le segment.

L'acquittement :

Le récepteur indique à l'émetteur le numéro de l'octet attendu
(numéro de l'octet transféré + nb d'octets transférés dans le segment)

En cas d'absence d'acquittement au bout d'un temps T, TCP réemet son segment.

Ce temps T est calculé automatiquement par TCP et adapté de façon dynamique.

Les fenêtres glissantes

Principe :

L'émetteur envoie des segments sans attendre l'acquittement tant qu'il reste dans la fenêtre.

A chaque acquittement, il y a renégociation de la taille de la fenêtre.

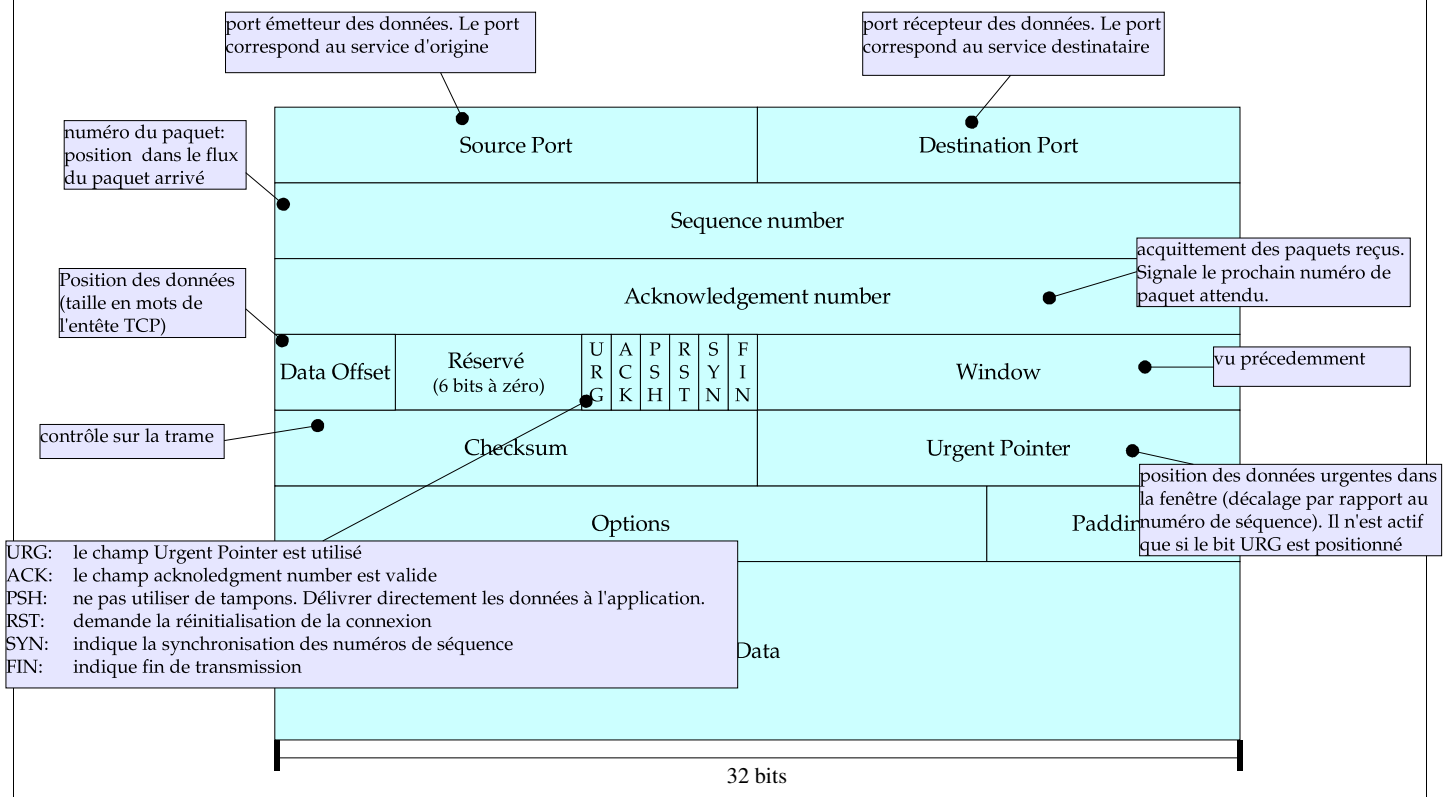
La fenêtre "est" le nombre de trames envoyées nécessitant 1 seul acquittement

Ce champ sert à calculer le nombre d'octets de données que l'on doit émettre avant de recevoir l'autorisation d'en envoyer de nouveau. Il sert à s'assurer que les octets sont bien reçus. L'émetteur et le récepteur utilisent cette valeur pour contrôler le flux.

Apports :

- transmission plus fiable
- contrôle de flux
- "rentabilité" du transfert

Dessin de la trame TCP



UDP

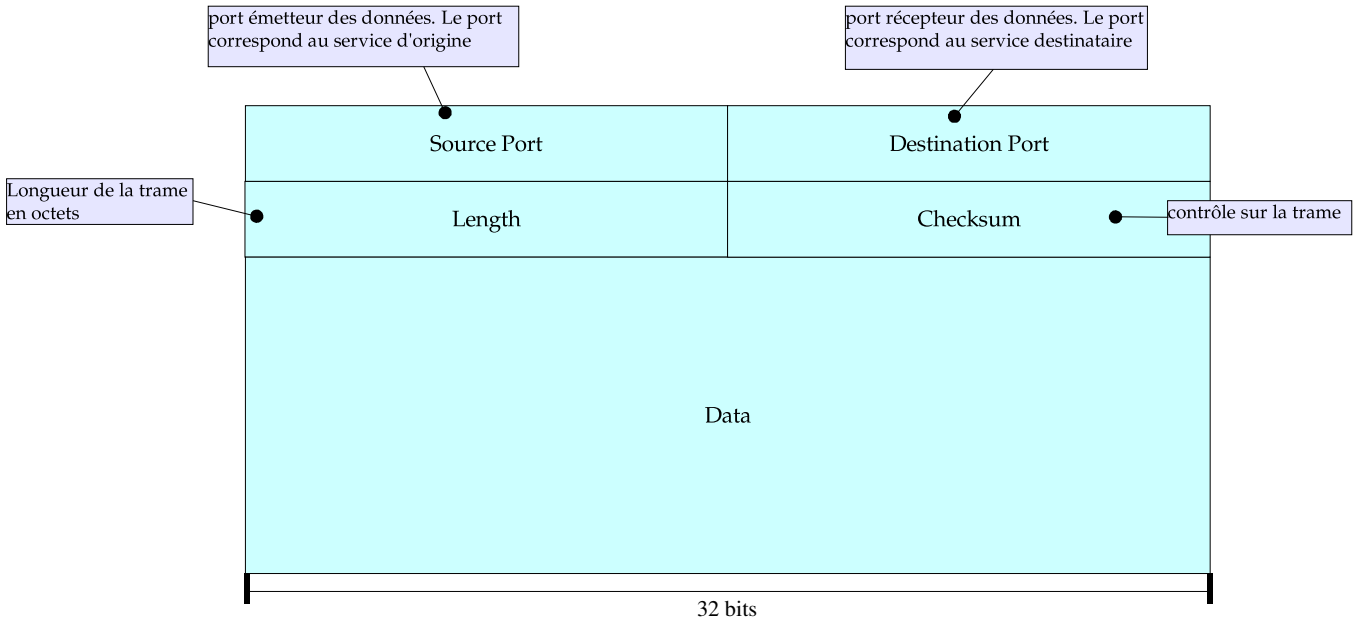
User Datagram Protocol

Protocole de transport parallèle à TCP mais avec des fonctionalités restreintes

UDP, User Datagram Protocol, utilise une trame simplifiée par rapport à TCP.
Des services, comme SNMP, s'appuient dessus.

Permet de transférer des informations de manière rapide (pas de connexion), sans forcer le maintien d'une liaison (pas d'amplification de surcharge).

Dessin de la trame UDP

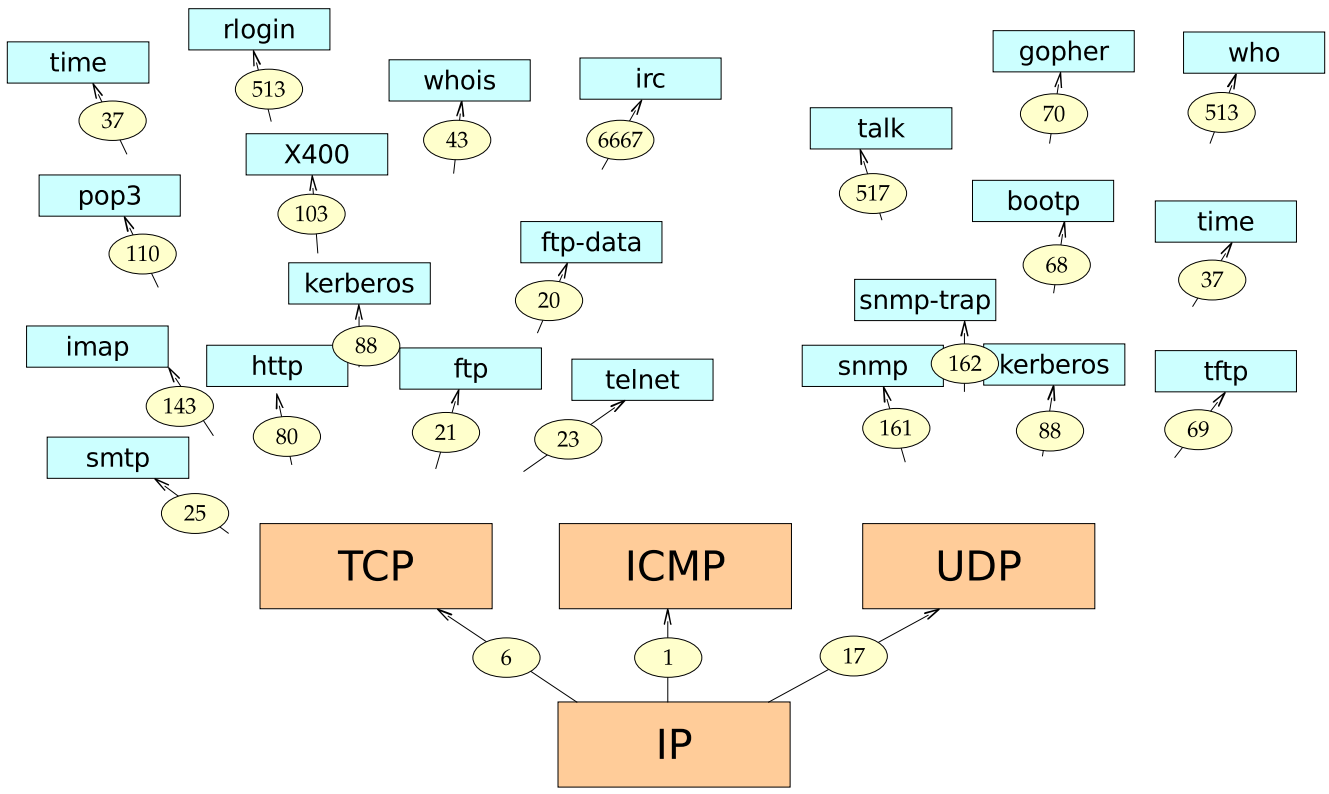


Commandes

Au dessus de TCP ou UDP, il existe un certain nombre d'applications conçues pour réaliser de nombreuses tâches.

- `ftp`, basé sur TCP, qui permet le transfert de fichier entre 2 sites.
- `telnet`,basé sur TCP, qui permet de se connecter à un site distant.
- `SMTP`, basé sur TCP, qui permet l'échange de courrier à travers l'outil mail.
- `tftp`, basé sur UDP, qui permet du transfert de fichier (sans assurer la cohérence du transfert de la même manière que `ftp`).
- `nfs`, basé sur UDP, qui permet le partage de fichiers entre plusieurs sites.

Vue globale de quelques ports



Exercice

Port telnet

Par défaut telnet est sur le port 23. On peut spécifier un autre port sur la ligne de commande (fonctionne aussi avec ftp).

La syntaxe est dans le mode ligne la suivante :

```
telnet monadresse port
```

Par exemple :

```
telnet 130.21.1.1 80
```

vous fera passer comme un navigateur WEB

- Comment faire pour connaître l'adresse du fournisseur d'accès?
- Comment faire pour rapatrier un document?

Les ports liés à la sécurité

Il s'agit essentiellement des ports attribués au protocole kerberos

749	tcp	udp	Kerberos-adm	administration/changement mot de passe
750	tcp	udp	Kerberos-sec	authentification
751	tcp	udp	Kerberos-master	authentification
754	tcp	udp	kb5-prop	Slave propagation
1109	tcp	kpop	pop sur kerberos	
2105	tcp	eklogin	mot de passe codé	
4444	tcp	kb524	traducteur de ticket k5->k4	

IX

Routage IP

Principe

- Routage = établissement d'un chemin entre deux points A et B.

Opération simple pour un réseau peu maillé, mais dont la complexité augmente avec le nombre de noeuds.

Principe

Les matériels d'interconnexion sont souvent des ponts ou des routeurs.
Pont : l'interconnexion aboutit à la création d'un réseau logique unique
Routeur : l'interconnexion est réalisée en conservant l'indépendance de chaque réseau

Par analogie

Ponter, c'est changer de type de roues quand on change de type de surface (modification de la couche liaison)
Router, c'est changer de véhicule (les données quittent une trame et sont écrites dans une nouvelle trame)

➢Le routage sur IP s'apparente au réseau routier:

Les lignes inter routeurs correspondent aux routes
Les routeurs correspondent aux carrefours

Contrairement aux ponts, les routeurs n'écoutent pas en permanence les segments auxquels ils sont attachés.

Les stations d'un réseau connaissent le routeur auquel elles doivent s'adresser

Algorithme

Contrairement à un pont, un routeur ne dispose pas d'une liste de machines, mais d'une liste de routes.

Un routeur essaye donc d'avoir la connaissance du réseau.

Il fonctionne par dialogue avec les autres routeurs.

Ce dialogue s'appuie sur un protocole de routage, qui doit être supporté par tous les routeurs du réseau.

Les caractéristiques d'un tel protocole sont:
- la vitesse de convergence
- la bande passante utilisée
- la capacité de reprise en cas d'erreur

Typiquement:
- si le temps de transfert des données est grand devant le temps de connexion, on aura intérêt à avoir un algorithme qui optimise le chemin afin de diminuer les temps de transfert entre A et B.
  Ex : réseau téléphonique
- si le temps de transfert des données est petit devant le temps de connexion, on aura intérêt à avoir un algorithme qui trouve le plus rapidement possible un chemin pour relier A et B.
  Ex : réseau de cartes bancaires

Routage

Routage dynamique/statique

Le routage dynamique est un routage capable d'évoluer dans le temps :

- restauration rapide du réseau en cas de problèmes
- mais implique un trafic important

Le routage statique est un routage constant dans le temps :

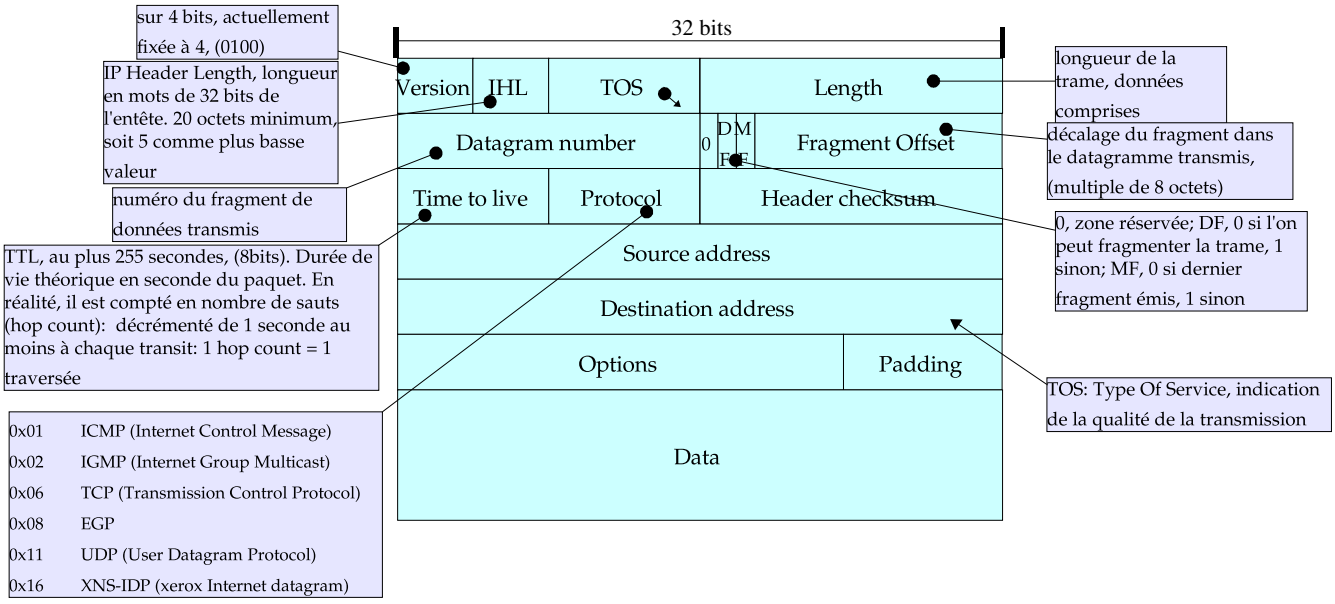
- nécessite une intervention manuelle en cas de modification du réseau.

Routage IP

Un routeur considère que chaque segment qui lui est attaché forme un réseau à part entière.

Un réseau est désigné par une partie de l'adresse IP.

Rappel sur la trame IP



Fonctionnement

Le travail d'un routeur consiste à
- accepter un datagramme
- l'examiner
- l'envoyer sur le bon réseau

Eléments connus du routeur:
- As l'adresse IP source
- Rs le numéro de réseau source
- Ad l'adresse IP destination
- Rd le numéro de réseau destination
- une table de routage qui contient une liste de numéros de réseaux et pour chacun d'entre eux, une autre destination et le coût du transfert et d'autres informations, suivant le protocole de routage

Les numéros de réseaux sont obtenus par l'extraction à l'aide du masque réseau.

Algorithme

L'algorithme de routage procède généralement aux opérations:

Si Rs est égal à Rd, alors As et Ad sont sur le même réseau, on oublie la trame
Si Rd est connecté directement au routeur, on envoie le datagramme sur le port correspondant
Si Rd est connu du routeur, on envoie le datagramme conformément à la table de routage
Si une route par défaut est indiquée, on lui transmet le datagramme
sinon on renvoie à la source une erreur (par ICMP)

Le plus compliqué est de mettre à jour la table de routage

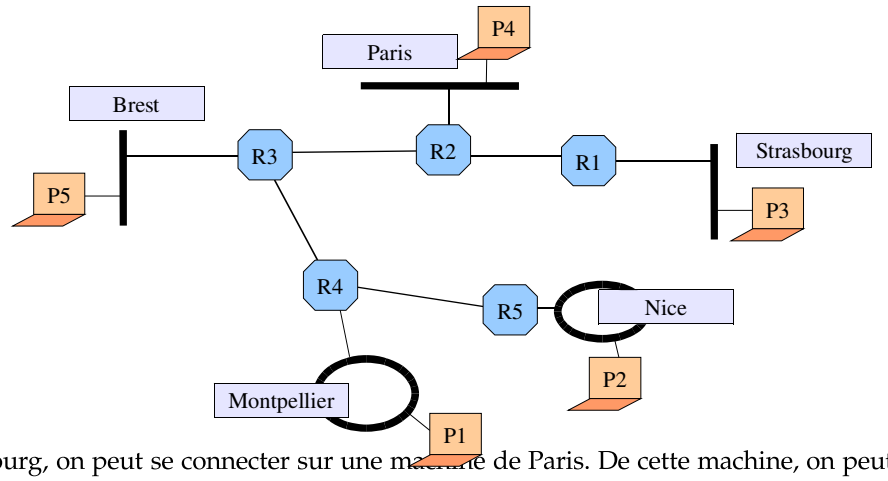
Route par défaut

La notion la plus importante est celle de route par défaut.

C'est la route qui est prise dans le cas où aucun routeur n'a été affecté à un réseau.

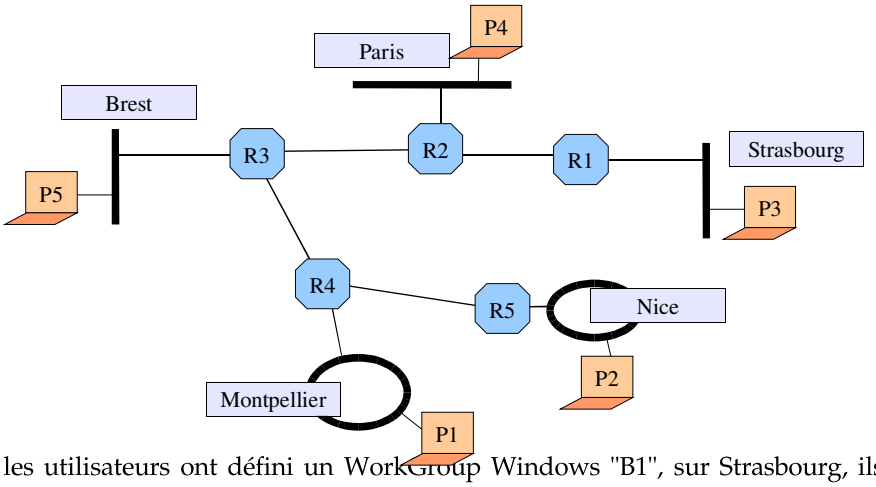
- La route par défaut correspond au panneau « Autres Directions »

Exercice



De Strasbourg, on peut se connecter sur une machine de Paris. De cette machine, on peut se connecter sur une machine de Brest. Quand on veut se connecter directement de Strasbourg à Brest, la commande " telnet " se bloque.
Que se passe-t-il?
Comment corriger le problème?

Exercice 2



Sur Brest, les utilisateurs ont défini un WorkGroup Windows "B1", sur Strasbourg, ils en ont défini un autre "Stbg".

Le ping et le telnet "passent", mais les utilisateurs ne peuvent pas s'échanger de fichiers entre les postes Windows

Que se passe-t-il?
Comment corriger le problème?

Fragmentation

MTU: Maximum Transmission Unit

La valeur de MTU indique une restriction sur la longueur maximale des trames circulant sur un réseau. (il est difficle de faire tenir un train sur un rond-point?)

Une trame de taille supérieure à la MTU sera fragmentée en plusieurs trames qui seront transmises sur le réseau.

Dans certains cas, on veut interdire la fragmentation: d'une trame.
Utilisation du bit DF de la trame IP.

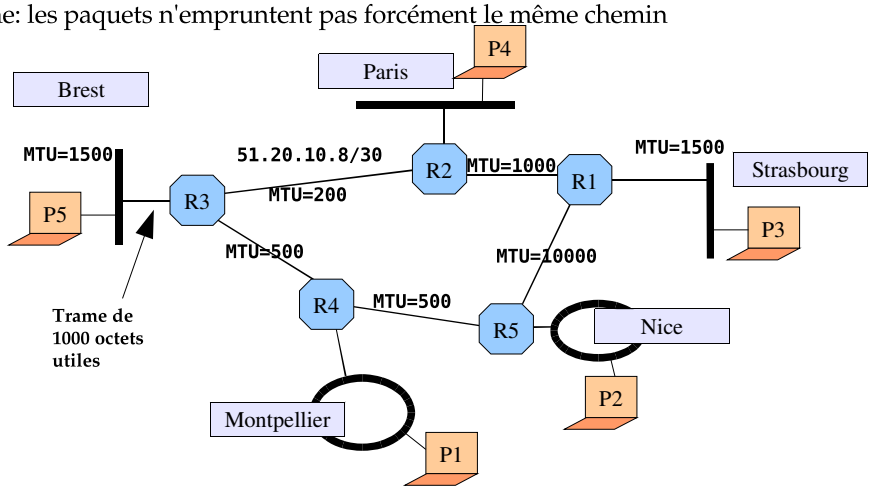
Si ce bit est à 1 alors la fragmentation interdite. La trame est détruite.

Possibilité d'envoyer une trame avec en option le bit *MTU Discovery Option* levé, ce qui permet de déterminer la plus petite taille de trame à émettre (RFC1063).

➢Le MTU peut s'apparenter à la largeur d'une route ou à la hauteur maximale sous un pont.

Exercice

Problème: les paquets n'empruntent pas forcément le même chemin



On suppose que le paquet L1000 (de longueur 1000 octets) transitera par le réseau 51.20.10.8.

Combien de paquets seront créés?

Qui fait le réassemblage ?

Exercice

Un élément intermédiaire ne fait pas de réassemblage des trames.

Seule la machine destination peut le réaliser

Pourquoi ?

Exemple

Comment est traitée une trame de 500 octets de données arrivant sur un réseau qui n'accepte que des trames de 250 octets au maximum? Donnez les valeurs de l' *offset* ,du *bit 'more'* ainsi que la taille totale des paquets?

(on suppose que la taille de l'entête IP est 20 octets)

Exemple

Réponse:

Num	entête	décalage	taille	Bit more
1	5	0	244	1
2	5	28	244	1
3	5	56	72	0

Outils de gestion du routage

Le routage complètement dynamique est complexe à calculer et les erreurs peuvent produire des trous de sécurité importants.

Le routage statique est encore plus sensible aux erreurs humaines que le routage dynamique

Les solutions doivent cumuler les avantages du routage statique (on est sûr de ce qui passe) et du routage dynamique (plus de souplesse).

Ce sont des solutions logicielles qui disposent d'un langage de haut niveau se plaçant au dessus du langage de programmation spécifique à chaque routeur.

Ce logiciel distribue ensuite la liste des routes statiques sur chaque routeur.

Ces solutions sont aussi capables de fabriquer les listes de filtres et de les distribuer.

Téléchargement de routes statiques.

Plan d'adressage

L'ensemble du réseau s'appuie sur une architecture physique (lignes spécialisées, brins Ethernet, ...) et une architecture logique (IP, applications). L'architecture physique dépend de la structure de l'entreprise et l'architecture logique dépend surtout des applications et du métier de l'entreprise.

La définition de l'architecture logique consiste principalement à définir le plan d'adressage de l'entreprise.

Le plan d'adressage est fonction de :
- origine géographique
- heures et jours
- volumes
- types de flux

Il faut donc dresser la liste des applications utilisant le réseau et obtenir les valeurs pour chacun des critères précédents. Il faut ensuite regrouper les applications par famille et construire le plan d'adressage.

Définition du plan d'adressage

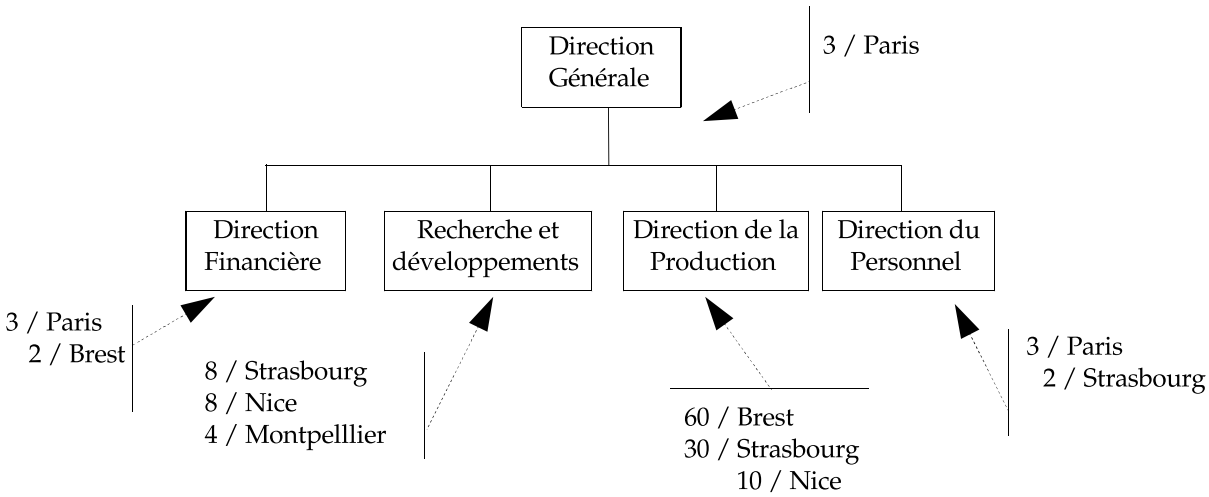
Cette opération peut être très longue et il vaut mieux prendre quelques semaines à détailler les spécifications du plan d'adressage plutôt que d'être obligé de revoir fréquemment le plan.

La moindre modification de la politique de routage ou de peering (échanges entre fournisseurs de capacités) peut avoir des conséquences très importantes pour l'utilisateur final

La somme de savoirs et savoir-faire exigés à ce poste est importante: maîtrise des protocoles et des équipements, bonne connaissance des architectures et des éventuels dysfonctionnements, parfaite compréhension des subtilités d'un plan de routage (chez un opérateur) ou d'adressage (dans une société utilisatrice).

Architecture

La société PFD est organisée de la manière suivante :



Exercice

Décomposer les types de flux en 3 niveaux de criticité

Faites une liste des différents types de flux d'informations essentiels
Classez ces types par ordre d'importance
Sélectionnez les 3 premiers

Matrice de fonctionnement

Associez à chaque direction un niveau traduisant le volume des informations
Attribuez à chaque direction un type de flux
Constituez l'architecture réseau de chaque domaine en tenant compte des débits (3 vitesses de ligne: lente, moyenne, rapide)
Comment peut-on passer d'un monde à l'autre?
Où est située la passerelle?
Comment réduire le nombre de noeuds critiques?

Comment sécuriser l'accès aux sites critiques?

X

Les réseaux virtuels

VLAN

Un LAN (Local Area Network), est normalement borné par les équipements de niveau 3 ou supérieurs qui constituent les frontières du domaine de diffusion. Il s'agit d'équipements de type routeur ou passerelle.

L'utilisation de la technologie VLAN (Virtual Local Area Network) permet de s'affranchir de ces frontières en créeant un réseau local logique au niveau 2.

Un commutateur implémentant les VLANs permet de regrouper certain de ses ports, créant ainsi des LAN virtuels.

Le Trunking permet quant à lui d'utiliser un seul support physique pour transporter le trafic de plusieurs VLANs. Il s'agit d'ajouter un champ à la trame ethernet indiquant l'identifiant du VLAN auquel correspond le paquet.

Deux implémentations existent : l'ISL de CISCO (InterSwitch Link Protocol), et standard IEEE 802.1q.

Il est ainsi possible de faire abstraction des contraintes géographiques et de privilégier les facteurs organisationnels lors de la segmentation des réseaux.

VLAN

Avantages des VLANs:

- Diminution du nombre d'équipements réseau nécessaires à la définition d'une architecture.
- Souplesse d'administration des équipements; un poste client peut être déplacé physiquement tout en restant dans le même réseau logique.
- Déploiement de réseaux locaux logiques sur des réseaux étendus physiques.
- Sécurité accrue par la segmentation qu'effectue le commutateur : le VLAN « employés » est séparé du VLAN « direction ».

Composantes des VLAN

Membership :

Definit la méthode de selection des membres

Identification :

Definit la méthode d'association des trames aux VLANs

Configuration :

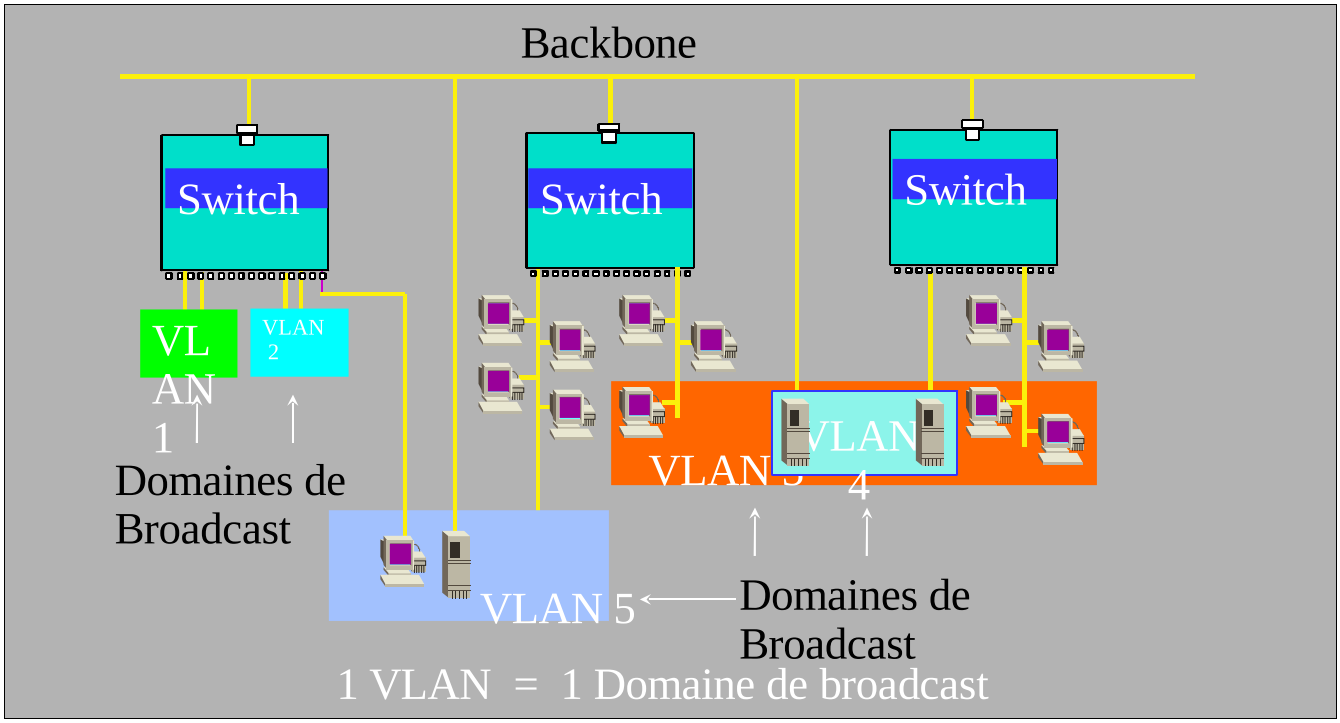
Definit la configuration des VLANs

Communication Inter-VLAN :

Definit la méthode d'interconnexion des VLANs

Architecture

Un VLAN est un domaine de collisions programmé



Fonctionnement

Les membres d'un VLAN sont regroupés dans 3 types de VLANs:

- par Port
- par Protocole
- par Réseau (IP)

Trame modifiée 802.1q

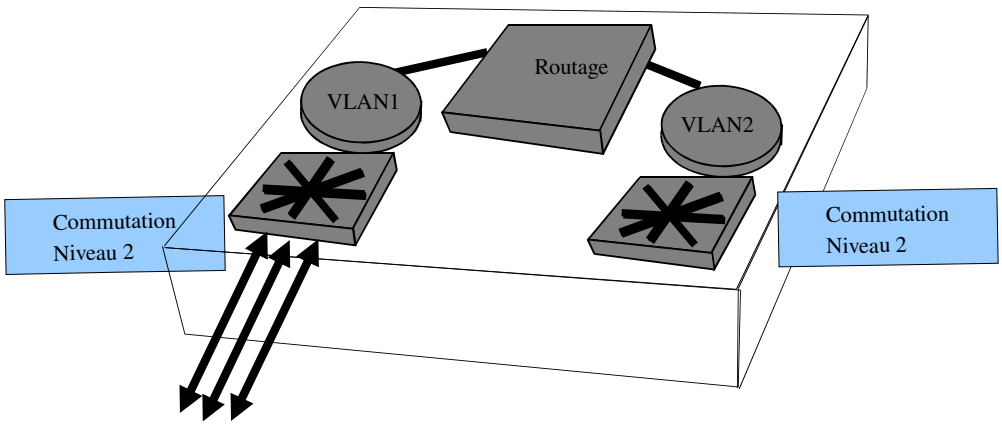
Quatre octets sont insérés dans la trame Ethernet entre les champs d'adresses et le champ longueur/type.

<table>
<tr><td>10101010</td><td>10101010</td><td>10101010</td><td>10101010</td><td>10101010</td><td>10101010</td><td>10101010</td><td>10101011</td></tr>
<tr><td colspan="6">Adresse MAC destination</td><td colspan="2">Adresse Mac source</td></tr>
<tr><td colspan="4">Adresse MAC source</td><td colspan="2">Taille des données</td><td>Données</td><td>Données</td></tr>
</table>

Champ TPI (2 octets)
Champ TAG (2 octets)

3 bits	1bit	12 bits
Priorité	CFI	Identification du VLAN (VID) 4096 VLANs possibles

Schéma de principe



XI

IPv6

Besoin

IPv6 a été lancé en 1993 par l'IETF sous le nom IPng (IPv5 a déjà servi pour des expérimentations).

Nombre d'adresses IP :

Téléphones, PDA, domotique, ...

Multimédia :

Le champ TOS est mal utilisé : utilisation d'un mode "temps-réel" difficile.

Futurs utilisateurs :

Opérateurs téléphoniques.
Pays en développement : le DoD possède les plus gros paquets d'adresses et n'a pas prévu de les libérer.
Les postes de travail deviennent mobiles => besoin d'auto-configuration.

Stocks adresses IPv4

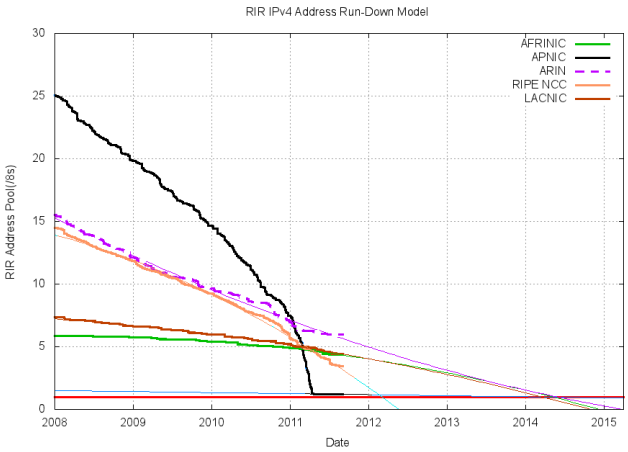
En 1998, les experts estimaient que la limite d'adressage serait en 2008 à plus ou moins 3 ans...

D'autres affirmaient que grâce aux nouvelles technologies (NAT, DHCP, protocoles de routage), l'espace d'adresses ne sera jamais saturé.

En janvier 2010, il ne restait que 10% d'adresses IPv4 disponibles et plus que 6,25% en Juin 2010.

En février 2011, le dernier bloc d'adresses IPv4 a été alloué.

source: http://www.potaroo.net/tools/ipv4



Fonctionnalités

Plage d'adresses: 2^32 en IPv4 2^128 en IPv6
667 132 135 milliards d'adresses par millimètre carré de la planète.

- Sécurité
- Qualité de service

- Mobilité
- Renumérotation

- Support pour l'auto-configuration

Utilise une double pile IPv4 et IPv6 pour faciliter la migration. IPv4 et IPv6 ne sont pas compatibles. Par contre, IPv6 est compatible avec la plupart des services de niveau supérieur : TCP, UDP, OSPF, ...

Ne gère plus la notion de broadcast
Intègre une notion any-cast et de multi-cast

En-tête simplifiée : passe de 20 octets en IPv4 à 40 octets
- Le nombre de champs a été réduit de moitié
- Les options sont placées dans des entêtes séparées
- La longueur des options n'est plus limitée à 40 octets

Taille maximum de trames à 4Go au lieu de 64k

Historique

- 1969 : création du réseau ARPANET (Advanced Research Project Agency Network)
- 1975 : définition de TCP (TCP et IP ont été développés par BBN (Bolt Beranek and Newman))

- 1980 : version d'Unix Berkeley contenant TCP/IP
- 1983 : toutes les machines du réseau ARPANET utilisent TCP/IP

- 1990 : Internet Stream Protocol (ST) qui deviendra IPv5 en 1994, puis transformé en RSVP

- 1993 : Lancement IPv6 par l'IETF sous le nom IPng
- Août 1994 : premières implémentations de test
- Décembre 1994 : soumission de ces documents comme proposition de standard
- **30 mars 1995** : premier échange de trames IPv6
- Juillet 1995 : premières versions bêta des logiciels
- Décembre 1995 : fin des tests à grande échelle et premières sorties des logiciels de production.

- 2000 : interconnexion de France Telecom aux principaux noeuds IPv6 mondiaux
- 2002 : déploiement IPv6 chez Nerim
- 2003 : déploiement IPv6 natif chez Nerim
- 2005 : déploiement IPv6 chez OVH
- **6 juin 2006** : arrêt du réseau 6bone
- 2008 : déploiement IPv6 chez Free dans son offre grand public
- 2009 : google dispose d'une entrée IPv6 : http://ipv6.google.com/ (2a00:1450:8006::93)
- **8 juin 2011** : Test grandeur nature d'IPv6 "Six Day"

Déploiement

L'IETF, avec son choix pour la technologie IPv6, désire non seulement répondre aux exigences actuelles mais surtout anticiper les besoins futurs de ces marchés.

Les marchés se développeront comme prévu ; il est donc du ressort de l'IETF d'imposer IPv6 dans le cadre d'une "immense infrastructure informatique mondiale et interopérable créée dans l'espoir d'utiliser des protocoles ouverts", à l'opposée d'un "monde de réseaux disjoints recourant à des protocoles contrôlés par des fournisseurs individuels".

En vue d'aboutir à cet objectif, l'IETF considère que le déploiement stratégique d'IPv6 doit se réaliser de la manière la plus flexible possible, à savoir grâce à une totale compatibilité avec IPv4.

Spécifications

- Être bâties autour de standards ouverts et accessibles au public.
- Définir une méthode de migration claire et réaliste.
- Permettre la gestion d'au moins un milliard de réseaux, soit mille milliards de stations, avec auto-configuration des adresses et mise en place d'un adressage global et unique de chaque équipement, même en présence d'une structuration topologique.
- Utiliser les méthodes de routage RIP, OSPF, etc.
- Être indépendantes du réseau physique, le Flow Label d'IPv6 doit même pouvoir correspondre avec les circuits virtuels ATM.
- Supporter les diverses topologies de réseaux interconnectés et un service de type datagramme (orienté sans connexion).
- Exploiter de façon optimisée les réseaux à hautes performances d'où le choix d'un en-tête sans contrôle de parité et cadré sur des multiples de 4 octets.
- Garantir la sécurité de certaines opérations, comme l'authentification ou le chiffrement spécifique du niveau 3 réseau.
- Supporter la diffusion de groupe (multicast).
- Gérer plusieurs classes de services (avec le Flow Label).
- Incorporer des protocoles de contrôle semblables à ceux de IPv4 (ping, traceroute).
- Permettre l'encapsulation de divers protocoles dans IPv6.
- Offrir un service fiable et robuste.

Disponibilité

Tous les OS récents intègrent l'IPv6 :

- Windows depuis XP SP1 (non activé par défaut mais disponible)
- Windows Server depuis 2003
- Windows Vista/Seven
- Mac OS depuis Jaguar (10.2)
- GNU/Linux depuis la version 2.6 du noyau
- AIX depuis la version 4.3
- Solaris depuis la version 8
- HPUX depuis la version 11.23

- les terminaux mobiles (téléphones, smartphones, tablettes, etc.)
- les logiciels mis à jours

Les applications spécifiques (métier)

Problèmes : parfois anciennes et rarement maintenues (développement sous-traité)
Le coût de sa mise à jour varie énormément.

XII

Entêtes IPv6

Format des trames

Les en-têtes sont simplifiées

- Le nombre de champs a été réduit de moitié
- Les options sont placées dans des entêtes séparées
- La longueur des options n'est plus limitée à 40 octets

La taille de l'entête passe de 20 octets à 40 octets

- Header checksum, checksum calculé sur les bits du Header => supprimé

- Adresses sur 32 bits => 128 bits
- Alignement sur 32 bits => 64bits

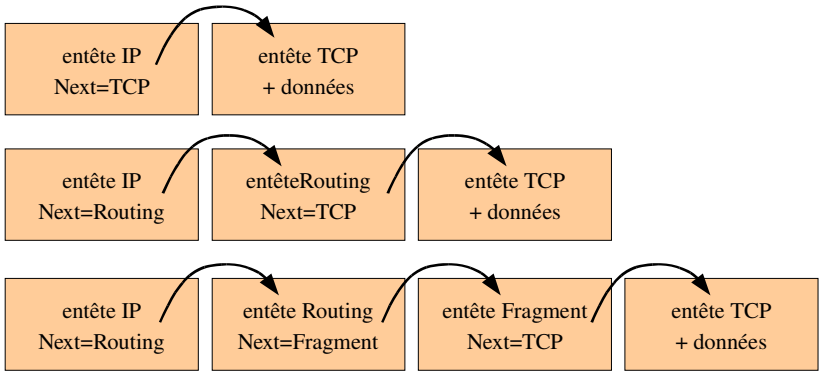
Trame IPv6

<- 64 bits ->					
< 4 > <- 8 ->	<- 20 bits ->		<- 32 bits ->		
Vers	Tr. Class	Flow Label	Payload Length	Next Header	Hop Limit
Source Address					
Destination Address					

- Traffic Class : priorités ou classes de trafic
- Flow Label : marquage des paquets spéciaux
- Payload Length : longueur en octet des paquets après entête. Autorise des paquets > 64k si Payload=0 et que l'on met la taille dans l'entête de l'option « Hop-by-hop »
- Next Header : spécifie le type de l'entête suivant. On utilise les mêmes valeurs que pour le champ proto de Ipv4 (ICMP=1, TCP=6, UDP=17)
- Hop Limit : fonctionne sur le même principe que le champ TTL : -1 à chaque traversée d'équipement
- Adresse destination : adresse de l'équipement cible. On peut aussi y mettre l'adresse d'un équipement différent si l'entête « Routing Header » est ajoutée

Entêtes supplémentaires

Principe



Règles de fonctionnement

Les en-têtes supplémentaires ne sont pas examinées ou manipulées par les noeuds intermédiaires.

La seule exception est l'en-tête de l'option noeud par noeud ("Hop-by-hop") : elle porte des informations qui doivent être examinées par les noeuds du réseau.

L'en-tête "Hop-by-Hop" doit suivre immédiatement l'en-tête IPv6.

Lorsqu'une trame arrive à destination, le premier en-tête supplémentaire, ou l'en-tête transport dans le cas d'absence d'en-tête supplémentaire, est traité.
Le contenu de chaque en-tête déterminera s'il faut, ou pas, traiter l'en-tête suivant.

Chaque en-tête supplémentaire est d'une longueur d'un multiple de 8 octets, afin de conserver un alignement de 8 octets pour les en-têtes suivants.

Ordre des en-têtes supplémentaires

Lorsqu'il y a plus d'une en-tête supplémentaire utilisée dans le même paquet, les en-têtes doivent apparaître dans l'ordre suivant:

Entêtes de services		**Entêtes de protocoles**	
Hop-by-Hop	0	IPv4	4
Routage	43	TCP	6
Fragmentation	44	UDP	17
Confidentialité	50	IPv6	41
Authentification	51	ICMPv6	58
Fin des entêtes	59	SCTP	132
Destination (routé par)	60	Mobilité	135
		Shim6	140

Chaque type d'en-tête ne doit apparaître qu'une seule fois dans le paquet (excepté dans le cas d'une encapsulation IPv6 dans IPv6, où chaque en-tête IPv6 encapsulée doit être suivie par son propre en-tête supplémentaire).

En-têtes "standards"

En-tête de routage

Utilisée par une source pour établir une table de noeuds intermédiaires (ou ensemble de groupes) que doit emprunter le paquet pour arriver à destination.

En-tête de fragmentation

Dans IPv6, la fragmentation n'est réalisée que par la source et plus par les routeurs intermédiaires.

En-tête d'authentification

Utilisé pour authentifier et assurer l'intégrité des paquets. La non-répudiation est obtenue par un algorithme d'authentification exécuté sur l'en-tête d'authentification. L'uthentification est obtenue par certificat.

En-tête de confidentialité

Cherche à donner une confidentialité et une intégrité en chiffrant les données à protéger et en les plaçant dans la section données de l'en-tête de confidentialité (Privacy Header).

Suivant les exigences de sécurité de l'utilisateur, soit la trame de couche transport (e.g. UDP ou TCP) est chiffrée, soit le datagramme entier d'IPv6 l'est.

XIII

Adressage IPv6

Adressage

Les adresses IPv6 sont des identifiants de 128 bits (16 octets) pour des noeuds ou un ensemble de noeuds.

Il y a trois types d'adresses:

- Unicast: employé pour envoyer un datagramme à un unique noeud.
- Cluster: employé pour identifier un groupe de nœuds qui ont en commun un préfixe d'adresse. Un datagramme envoyé à une adresse cluster sera délivré à un membre du groupe.
- Multicast: employé pour envoyer un datagramme à tous les membres d'un groupe de noeuds.

Il n'y a pas d'adresses de broadcast dans la version d'IPv6, les adresses multicast assurent leurs fonctions.

Comme dans IPv4, un sous-réseau IPv6 est associé à une seule liaison. Mais IPv6 permet aussi d'associer plusieurs sous-réseaux à une même liaison.

Représentation des adresses

Il y a trois formes conventionnelles de représentation d'adresses IPv6:

- x:x:x:x:x:x:x:x, huit blocs, où les 'x' sont les valeurs hexadécimales de 2 octets chacun.
  Exemples:
  `FEDC:BA98:7654:3210:FEDC:BA98:7654:3210`
  `1080:0:0:8:800:200C:417A`

Il n'est pas nécessaire d'écrire tous les zéros devant un chiffre hexadécimal dans un champ individuel, mais il doit y avoir au moins un chiffre dans chaque champ.

- Pour avoir une écriture facilitée, on peut supprimer les zéros. "::" indiquera un ou de multiple groupes de 16 bits à 0.
  Par exemple l'adresse multicast suivante:
  `FF01:0:0:0:0:0:43`
  sera représentée de la manière suivante:
  `FF01::43`
  les "::" ne peuvent apparaître qu'une seule fois dans l'adresse.

- dans un environnement mixte de noeuds IPv6 et IPv4: x:x:x:x:x:x:d.d.d.d, 6 groupements de 16 bits et 4 groupements de 8 bits de la représentation standard d'IPv4.

  Exemples:
  `0:0:0:0:0:0:13.1.68.3`
  `0:0:0:0:0:1:129.144.52.38`

  `::13.1.68.3`
  `::1:129.144.52.38`

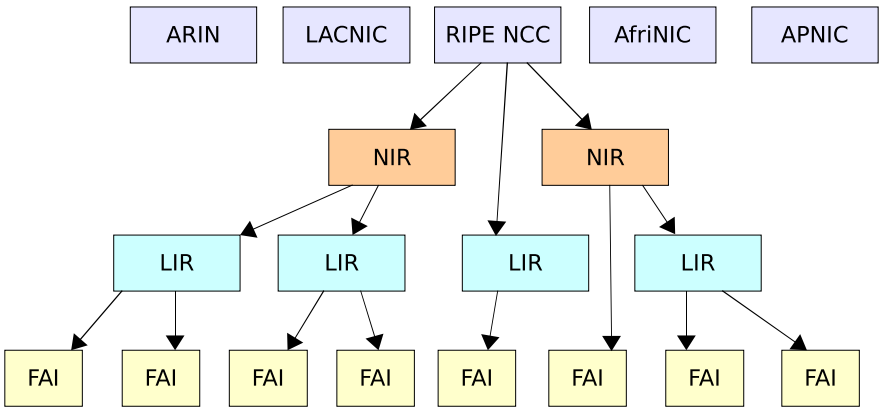
Plans d'adressage

Les types d'adresses d'IPv6 sont décrites par les bits de poids fort de l'adresse.

Adresse	Préfixe	Espace alloué
Réservé	0::/8	1/256
non attribué	100::/8	1/256
NSAP	200::/7	1/128
IPX	400::/7	1/128
non attribué	600::/7	1/128
non attribué	800::/5	1/32
non attribué	1000::/4	1/16
Plan d'adressage agrégé	2000::/3	1/8
Adresse Unicast par fournisseur de service (obsolète)	4000::/3	1/8
non attribué	6000::/3	1/8
Réservé pour les adresses géographiques (obsolète)	8000::/3	1/8
non attribué	A000::/3-FE00::/9	~ 1/4+15/16
Adresses locales de liens	FE80::/10	1/1024
Adresses locales de site	FEC0::/10	1/1024
Adresses privées	FC00::/7	1/128
Adresses Multicast	FF00::/8	1/256

Attribution

Les adresses IPv6 sont attribuées suivant un schéma similaire à celui d'IPv4



whois

IANA	whois.iana.org
ARIN	whois.arin.net
LACNIC	whois.lacnic.net
RIPE-NCC	whois.ripe.net
AfriNic	whois.afrinic.net
APNIC	whois.apnic.net

Répartition du plan global

2001:0000::/23	IANA	07/99	2001:1800::/23	ARIN	04/03	2001:4800::/23	ARIN	08/04	2610:0000::/23	ARIN	11/05
2001:0200::/23	APNIC	07/99	2001:1A00::/23	RIPE NCC	01/04	2001:4A00::/23	RIPE NCC	10/04	2620:0000::/23	ARIN	09/06
2001:0400::/23	ARIN	07/99	2001:1C00::/22	RIPE NCC	05/01	2001:4C00::/23	RIPE NCC	12/04	2800:0000::/12	LACNIC	10/06
2001:0600::/23	RIPE NCC	07/99	2001:2000::/20	RIPE NCC	05/01	2001:5000::/20	RIPE NCC	09/04	2A00:0000::/12	RIPE NCC	10/06
2001:0800::/23	RIPE NCC	05/02	2001:3000::/21	RIPE NCC	05/01	2001:8000::/19	APNIC	11/04	2C00:0000::/12	AfriNIC	10/06
2001:0A00::/23	RIPE NCC	11/02	2001:3800::/22	RIPE NCC	05/01	2001:A000::/20	APNIC	11/04	**2D00:0000::/8**	**IANA**	**07/99**
2001:0C00::/23	APNIC	05/02	**2001:3C00::/22**	**IANA**		2001:B000::/20	APNIC	03/06	**2E00:0000::/7**	**IANA**	**07/99**
2001:0E00::/23	APNIC	01/03	2001:4000::/23	RIPE NCC	06/04	2002:0000::/16	6to4	02/01	**3000:0000::/4**	**IANA**	**07/99**
2001:1200::/23	LACNIC	11/02	2001:4200::/23	AfriNIC	06/04	2003:0000::/18	RIPE NCC	01/05			
2001:1400::/23	RIPE NCC	02/03	2001:4400::/23	APNIC	06/04	2400:0000::/12	APNIC	10/06			
2001:1600::/23	RIPE NCC	07/03	2001:4600::/23	RIPE NCC	08/04	2600:0000::/12	ARIN	10/06			

`http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml`

Ces zones sont souvent sous-découpées. Par exemple, le protocole Teredo utilise le plan 2001:0000::/32

Les types d'adresses

Pour les noeuds utilisant le protocole IPv4, les adresses unicast IPv6 ont pour préfixe 0000 0000.

Cette allocation supporte l'allocation directe des adresses fournisseurs (provider), adresses NSAP [NSAP-USE], adresses IPX, adresses d'usage local, et les adresses multicast.

De l'espace est réservé pour les adresses géographiques. Les espaces adresses "Réservé" (85% du total adressable) seront attribués pour de futures utilisations.

Elles pourront être utilisées pour étendre les adresses existantes (e.g. adresses de fournisseurs supplémentaires, adresses IPX, etc.) ou pour de nouveaux emplois.

On distingue les adresses unicast des adresses multicast par la valeur des octets de poids fort de ces adresses. Une valeur de FF (1111 1111) identifie une adresse multicast, toutes les autres sont des adresses unicast.

Adressage fournisseur (obsolète)

Entête: 010 4000::/3

register ID	provider ID	subscriber ID	subnet ID	node ID

register ID :

010	RIPE NCC
100	IANA
101	APNIC
110	InetNIC

provider ID : fournisseurs qui attribuent des portions d'espace d'adresses aux abonnés (subscribers).
subscriber ID : permet de distinguer un abonné parmi d'autres attachés au même provider ID.
subnet ID : identifie une liaison physique spécifique.
node ID : identifie un noeud parmi le groupe de noeuds déterminé par un préfixe de sous-réseau.

NSAP 200::/7

7	1	4	12	32	16	48
000001	G	AFC	IDI	Prefix	Area	ID

IPv6 supporte les adresses NSAP (Network Service Access Point) d'une manière transparente (sans conversion) et celles-ci sont totalement compatibles avec l'en-tête étendue de noeud-par-noeud.
Abandonné fin 2004.

IPX 400::/7

Novell a abandonné IPX en 1996

Adresses individuelles ou unicast

L'adresse unicast d'IPv6 est basée sur le même principe de l'adresse IPv4 en CIDR (Classless Internet Domain Routing).

Les adresses sont allouées de manière contiguë et ont en commun les mêmes bits de poids fort, les mêmes préfixes.

Adresse indéterminée

L'adresse 0:0:0:0:0:0:0:0(::) est appelée adresse unspecified.

- Ne doit être affectée à aucun noeud
- Indique l'absence d'adresse

On peut la trouver dans le champ d'une adresse source de n'importe quel datagramme envoyé par une station "initialisée" avant que cette dernière n'est réussie à constituer sa propre adresse.

L'adresse unspecified ne doit pas être employée comme adresse destination des datagrammes ou dans les en-têtes de routage d'IPv6.

Adresses encapsulant IPv4

La transition simple à IPv6 (Simple IPv6 Transition - SIT) utilise deux formes d'adresses unicast IPv6, conçus spécialement pour faciliter l'évolution de l'Internet passant d'IPv4 à IPv6.

Dans les deux cas, l'adresse IPv4 est incluse dans la partie basse de l'adresse IPv6 (32 derniers bits).

La première forme d'adresse est conçue pour représenter les adresses IPv4 des nœuds IPv4 (les nœuds ne peuvent pas comprendre le protocole IPv6) en adresses IPv6.

La seconde forme d'adresse est conçue pour être utilisée par les nœuds IPv6 qui ont besoin de "dialoguer" avec des nœuds IPv4. On dira que ces adresses IPv4 sont compatibles IPv6.

80 bits	16 bits	32 bits
00000...0000	FFFF	adresse IPv4

Adressage agrégé

2000::/3

3			13	8	24	16	64
0	0	1	TLA	reservé	NLA	SLA	Id
Partie publique						Partie privée	

TLA: Top Level Aggregator opérateur internationaux
NLA: Next Level Aggregator opérateur intermédiaires reliés aux TLA
Attribués par IANA/RIR/LIR
SLA: Site Level Aggregator sous réseaux locaux

Id: identifiant d'interface

<- 24 ->				<- 40 ->
<- 6 ->	1	1	<- 16 ->	
	u	g	constructeur	identifiant physique

(u)niversel: à 1 si l'adresse est mondiale
(g)roupe: 1 si multicast

Construction de l'Id

L'Id peut être construit en fonction de l'adresse MAC

L'adresse MAC est codée sur 48 bits

Le code 0xFFFE est inséré au milieu de l'adresse MAC et on fixe u à 1 et g à 0.

Dans d'autres environnements, où les adresses IEEE-802 ne sont pas disponibles, d'autres adresses de la couche liaison peuvent être utilisées, comme les adresses E.164.

Si l'interface ne possède pas d'adresse MAC, il faut prendre une adresse au hasard avec u à 0

L'utilisation d'un unique identifiant de noeud rend possible et de manière assez simple l'autoconfiguration des adresses.

Répartition du 2000::/3

La plage d'adresse 2000::/3 est découpée en sous plages :

2000::/16	2000:xxxx	adresses allouées provisoirement avant l'ouverture du registre officiel
2001::/16	2001:xxxx	adresses ouvertes à la réservation depuis 2001
2002::/16	2002:xxxx	adresses 6to4 permettant d'acheminer le trafic IPv6 via un ou plusieurs réseaux IPv4
2003::/16 3ffd::/16	2003:xxxx 3ffd:xxxx	réservées pour usage ultérieur
3ffe::/16	3ffe:xxxx	adresses du 6bone pour l'expérimentation des interconnexions de réseaux IPv6. Aujourd'hui terminé

Adresses locales

Ce sont des adresses utilisées à l'intérieur d'un site d'un abonné, qui n'est pas connecté au monde Internet. Lorsque le site veut se connecter au monde Internet, il forme ses adresses globales en remplaçant le préfixe local par un préfixe souscripteur.

Un routeur ne doit pas retransmettre un paquet ayant une adresse source de type unicast local.

bouclage ::1/128

- utilisée par un noeud pour envoyer un datagramme à lui-même
- n'est affectée à aucune interface
- ne doit pas être utilisée comme adresse source de datagrammes envoyés à l'extérieur du noeud

Unicast FE80::/64

8	2	54	64
11111110	10	0	IDentifiant de machine

Correspond à l'adresse 169.254/16 en IPv4

Adresses locales de sites

site FEC0::/48

8	2	38	16	64
11111110	11	0	subnet Id	Node ID

Les adresses en FEC0 sont réservées pour un site donné. Malheureusement, cette notion n'a pas été clairement définie et cette plage d'adresse est devenue obsolète.

privées FC00::/7

Cette plage remplace la zone précédente. Les adresses de cette zone ne sont pas routables. Elles sont similaires aux réservations de la RFC 1918 (172.16/12, 10/8 et 192.168/16).

Elle est découpée en deux classes:

- FC00::/8 pilotée en central.
- FD00::/8 gérée par des adresses aléatoires

Algorithme pour la génération d'adresse aléatoire :

- Récupérez l'heure au format 64 bits NTP -> v1
- Trouvez un identifiant local de 64 bits (prenez l'adresse MAC/48 ou un numéro de série) -> v2
- Cela donne une cle=v1 & v2
- Calculez un SHA-1 digest (sha1sum sur la clé précédente) et ne gardez que les 40 derniers bits -> identifiant
- Mettez bout-à-bout FC00::/7 avec les bits de gauche à 1 et l'identifiant précédent

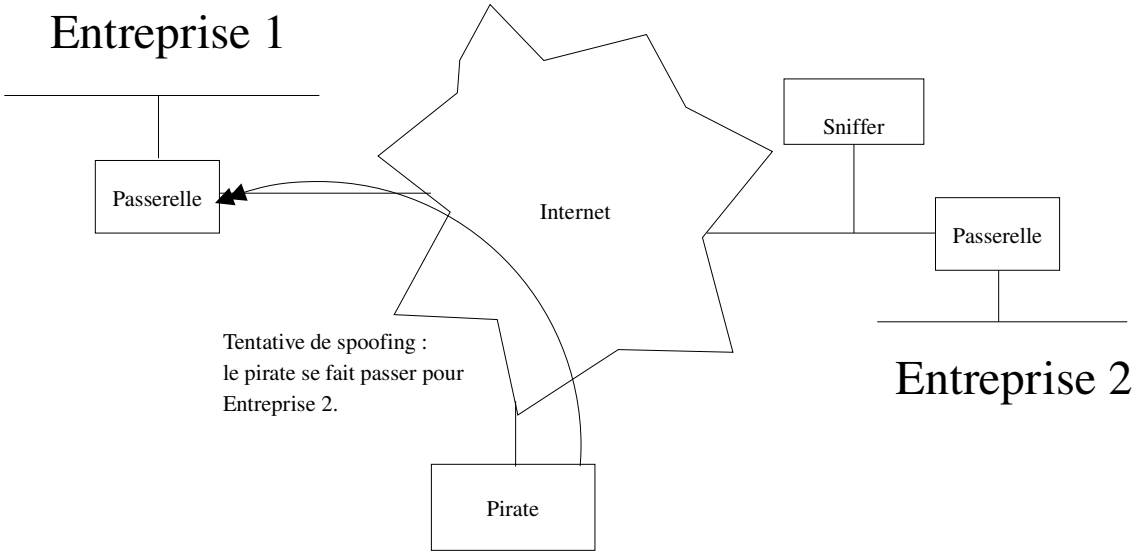
XIV

VPN et tunnels

Objectif

Le but du VPN (Virtual Private Network) est de créer une liaison sécurisée entre deux parties en se servant d'un réseau public (en général Internet).

Le VPN permet de s'assurer que l'émetteur est bien le bon et donc d'éviter le spoofing.
De plus, le VPN en chiffrant les données protège dans une certaine mesure des analyseurs de trames.

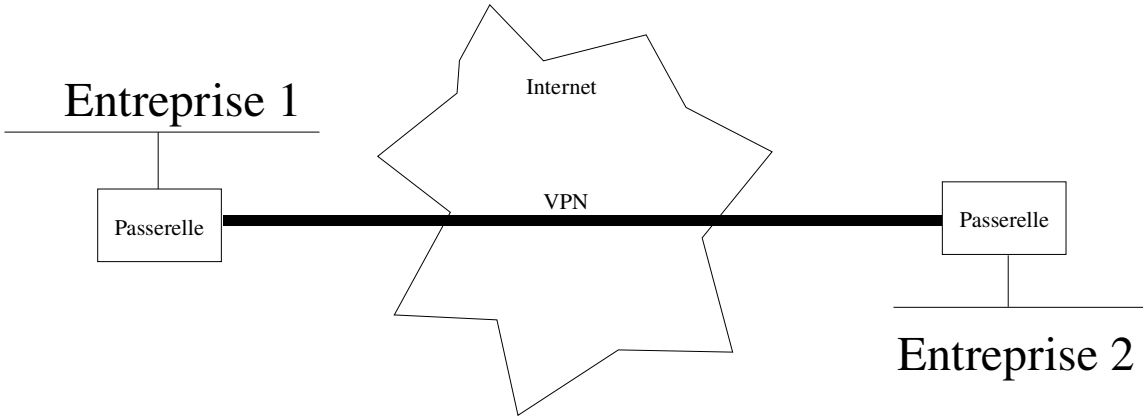


Fonctionnement

Un VPN est composée d'un serveur VPN et d'un Client VPN qui forment entre eux un tunnel.

Les deux parties étant identifiées de manière sûre par un système de clef, les données transitent chiffrées sur le tunnel.

L'intérêt est de se créer ainsi un réseau qui semble en dehors d'Internet mais qui s'appuie sur sa structure.
Cela réduit les coûts puisqu'il suffit d'avoir un simple accès à Internet pour que cela devienne possible.



Fonctionnement

L'intérêt du VPN est donc de permettre des échanges sécurisées entre 2 tiers.
Cela peut permettre par exemple à des postes itinérants (ie des commerciaux) d'accéder depuis n'importe quel endroit aux ressources de l'Intranet et ce de manière sécurisée.

L'inconvénient est que le VPN s'appuyant généralement sur un réseau public (Internet), aucune garantie de services n'est possible. La ligne peut être coupée ou saturée sans qu'aucun des deux parties ne puissent agir pour restaurer le service.

XV

openVPN

openVPN

Les exemples précédents mettent en place un système de tunnel entre deux postes.

On peut constater deux inconvénients majeurs:
- prévu pour un service réseau : on est limité à un seul service UDP
- utilisation de TCP

Autre méthode, utilisation d'un outil dédié : OpenVPN (basé sur SSL) ou openSWAN (anciennement freeSWAN et implémenté sur IPSEC)

Le principe global reste le même mais un VPN relie les machines comme si elles étaient sur un même réseau local. Tous les services sont donc accessibles.

OpenVPN travaille habituellement sur udp. Dans cet exemple, nous utiliserons le port 1234, mais nous aurions pu garder le numéro port udp officiel utilisé par OpenVPN :1194.

Prérequis pour l'installation OpenVPN
Vérifier que sur votre système vous disposez de :
- la librairie OpenSSL (http://www.openssl.org)
- la librairie Lzo (http://www.oberhumer.com/opensource/lzo)
- les pilotes TUN/TAP (http://vtun.sourceforge.net/tun/)

Téléchargez la dernière version de OpenVPN sur:
http://prdownloads.sourceforge.net/openvpn/openvpn-xxxxx.tar.gz

OpenVPN

OpenVPN est Open Source sous licence GPL. Il permet de mettre en place des VPN (Virtual Private Network) sécurisés pour rélier deux machines, deux ou plus réseaux privés, en utilisant un tunnel chiffré traversant Internet.

Fonctionnalités:
- encapsuler dans un tunnel n'importe quel sous-réseau IP dans un unique port TCP ou UDP,
- créer une infrastructure de tunnels sous Linux, Solaris, Mac OS X et Windows 2000/XP,...
- fonctionnalités de chiffrement,
- fonctionnalités d'authentification et de certification via OpenSSL,
- utiliser une compression des flux,
- créer des ponts ethernets sécurisés avec les périphériques tap.

Installation

Depuis les sources

Décompresser la distribution :

```
tar xzf openvpn-xxx.tar.gz
```

Compilez OpenVPN :

```
cd openvpn-xxx
./configure --disable-lzo
 make
 make install
```

LZO est une bibliothèque de compression de données en temps réel, sans perte de données. Elle est portable à travers des plateformes et écrite en C.

Depuis une version compilée

Exemple pour la Redhat 4 ES :

Dépendances requise si vous utilisez la compression (librairie LZO):

```
ftp://rpmfind.net/linux/dag/redhat/el4/en/i386/dag/RPMS/lzo-xxx.xx.i386.rpm
```

puis

```
rpm -i lzo-xxx.xx.i386.rpm
```

Installation des exécutables

```
ftp://rpmfind.net/linux/dag/redhat/el4/en/i386/dag/RPMS/openvpn-xxx.xx.rf.i386.rpm
```

puis

```
rpm -i openvpn-xxx.xx.rf.i386.rpm
```


Configuration de base

Sur chaque poste, il faut vérifier qu'il est possible de déclarer des pilotes réseaux virtuels.
On utilise TUN est un périphérique virtuel point à point conçu pour gérer le tunnel IP.

```
modprobe tun
```

Il existe aussi le périphérique Ethernet virtuel TAP qui est conçu pour gérer le tunnel Ethernet et qui utilise les adresses MAC.

Sur le poste « serveur » 10.21.100.101

Fichier de configuration serveur

```
ifconfig 12.0.0.1 12.1.0.1
dev tun
port 1234
proto udp
user body
group body
```

Utilisateur et groupe autorisés pour excuter le VPN

Fichier de configuration client

```
ifconfig 12.1.0.1 12.0.0.1
remote 10.21.100.101 1234
dev tun
port 1234
proto udp
user body
group body
```

Périphérique point à point virtuel utlisé

Lancez le serveur

```
openvpn --config /etc/openvpn/openvpn-serveur.conf
```

Lancez le client

```
openvpn --config /etc/openvpn/openvpn-client.conf
```

Test de connexion

Sur les postes clients et serveurs, lancez les commandes suivantes:

```
ifconfig
```
Que constatez vous?

```
route
```
Que constatez vous?

On vérifie que les postes serveurs et le clients communiquent bien ensemble

```
ping  -c 4 12.1.0.1      //serveur
ping  -c 4 12.0.0.1      //client
```

Autre test

On lance un `tcpdump` sur le serveur

```
tcpdump -i tun1
```

Au même moment, on fait un `ping` vers le serveur, depuis le client

```
ping  -c 10 12.1.0.1
```
Que constatez vous?

Un tunnel sécurisé par clé statique

La configuration du base n'était pas sécurisé. Maintenant, nous allons mettre en place une solution simple sécurisée. Pour cela, nous allons créer une clé statique aléatoire dans un fichier nommé macle sur le serveur.

```
openvpn --genkey --secret macle
```

Ensuite copiez le fichier macle vers le client en utilisant la commande sécurisé scp

```
scp macle 10.21.100.102:/etc/openvpn
```

En ligne de commande

Sur le serveur

```
openvpn --dev tun1 --ifconfig 12.0.0.1 12.1.0.1 --verb 5 --secret macle
```

Sur le client

```
openvpn --remote 10.21.100.102 --dev tun1 --ifconfig 12.1.0.1 12.0.0.1 --verb 5 --secret macle
```

Par fichier de configuration

Fichier de configuration serveur

```
ifconfig 12.0.0.1 12.1.0.1
dev tun
secret /etc/openvpn/macle
proto udp
user body
group body
```

Utilisateur et groupe autorisés pour excuter le VPN

Fichier de configuration client

```
ifconfig 12.1.0.1 12.0.0.1
remote 10.21.100.101 1234
secret /etc/openvpn/macle
dev tun
proto udp
user body
group body
```

Clé statique partagée

Périphérique point à point virtuel utlisé

N'ayant pas définit les ports dans les deux méthodes, openvpn utilise le port par défaut.

Chiffrement du VPN

Nous allons mettre en oeuvre SSL dans le but d'authentifier les deux extrémités.
Pour cela nous utiliserons deux postes : SERV et CLT
Cette méthode supporte aussi une topologie avec un serveur et plusieurs clients.

Sur SERV

Création d'un certificat d'autorité

```
openssl req -nodes -new -x509 -keyout SERV-ca.key -out SERV-ca.crt
```

Nous allons générer les certificats pour SERV et CLT et les signer à l'aide du certificat d'autorité

Récréez l'environnement de configuration d' openssl.cnf

```
cd /usr/share/ssl/
éditez openssl.cnf
```

Placez vous dans le répertoire /etc/openvpn pour effectuer les manipulations

```
cd /etc/openvpn
mkdir demoCA
cd demoCA
touch index.txt
mkdir newcerts
echo "01" > serial
```


Certificats SERV et CLT

Certificat le serveur

Construction d'une clé privée et d'une demande de certificat

```
openssl req -nodes -new -keyout SERV.key -out SERV.csr
```

Avec le certificat d'autorité (SERV-ca.crt) et la clé privée d'autorité (SERV-ca.key), on va obtenir un certificat approuvé SERV.crt

```
openssl ca -cert SERV-ca.crt -keyfile SERV-ca.key -out SERV.crt -in SERV.csr
```

Certificat sur le client

Création de la clé privée et de la demande de certificat sur CLT

```
openssl req -nodes -new -keyout clt.key -out clt.csr
```

Envoi le fichier généré à SERV pour validation

```
scp clt.csr 10.21.106.56:/etc/openvpn
```

Sur le SERV, nous validons le certificat de CLT

```
openssl ca -cert SERV-ca.crt -keyfile SERV-ca.key -out clt.crt -in clt.csr
```

Une fois le certificat validé, nous le renvoyons à CLT

```
scp clt.crt 10.21.106.7:/etc/openvpn
```

Il faut aussi renvoyer le certificat de l'autorité à CLT

```
scp SERV-ca.crt 10.21.106.7:/etc/openvpn
```

Génération du fichier DH

Génération d'un fichier `DH` de `1024` bits sur `SERV`.

Placez vous dans le répertoire `/etc/openvpn` pour effectuer les manipulations:

```
openssl dhparam -out dh1024.pem 1024
```

Nous allons passer à la configuration de `openvpn`.

Sur SERV

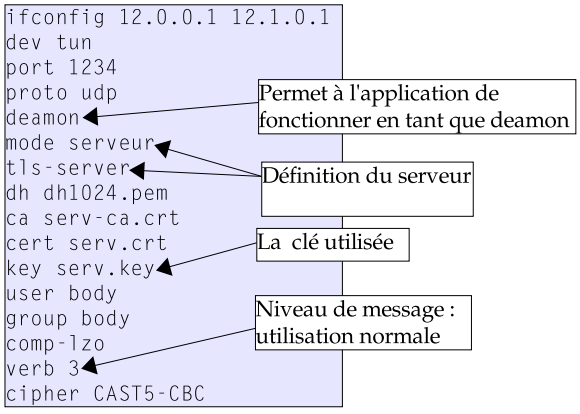
Editez le fichier exemple `/usr/share/doc/openvpn-xx.xx/sample-config-files` et renommez le en `serveur.conf` pour `SERV`.
Copiez le dans le répertoire `/etc/openvpn`

Sur CLT

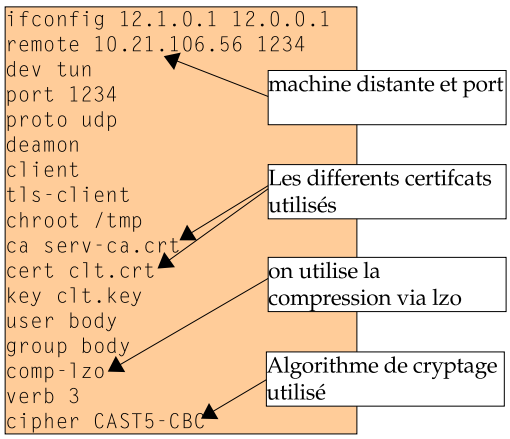
Editez le fichier exemple `/usr/share/doc/openvpn-xx.xx/sample-config-files` et renommez le en `client.conf` pour `CLT`
Copiez le dans le répertoire `/etc/openvpn`

Fichier de configuration

Fichier de configuration serveur



Fichier de configuration client



Lancement

Lancez le serveur

```
openvpn --config /etc/openvpn/openvpn-serveur.conf
```

Lancez le client

```
openvpn --config /etc/openvpn/openvpn-client.conf
```

Vérifiez que la liaison est opérationnelle avec la commande `ping`

- sur `SERV`
  ```
  ping 12.1.0.1
  ```
- sur `CLT`
  ```
  ping 12.0.0.1
  ```


XVI

DMZ

Définition

Pour les entreprises souhaitant être connectées à Internet et administrer un site Web avec de grands volumes de trafic, il est recommandé d'intégrer à leur configuration de réseau une structure de zone démilitarisée (DMZ) protégée par un pare-feu.

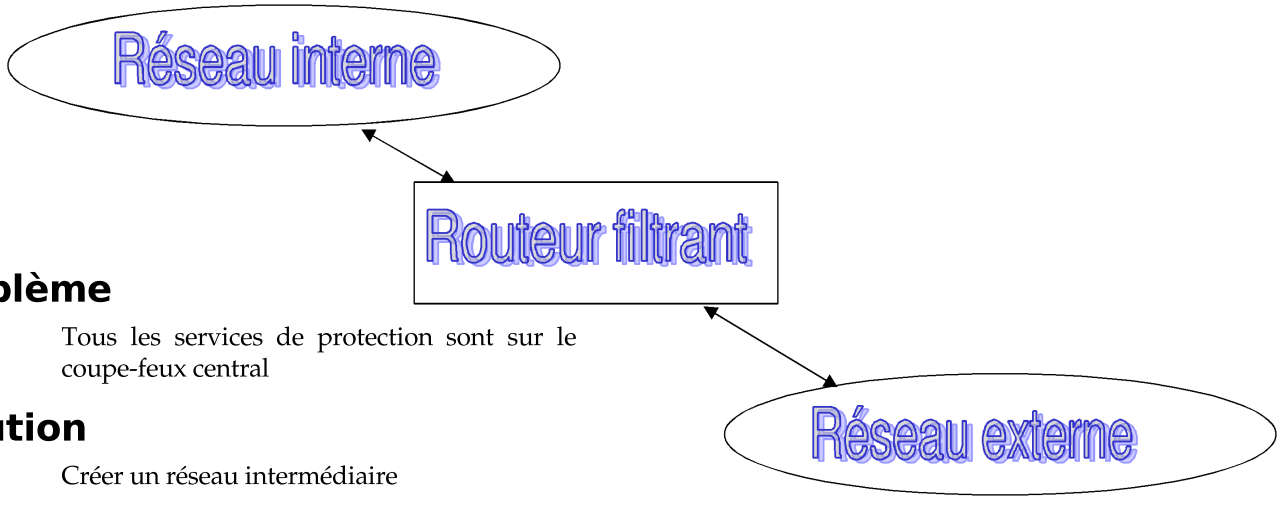
Un coupe-feux de type "passerelle d'applications" autorise également des filtres en fonction d'adresses IP afin de laisser passer les flux de données d'un utilisateur ou d'un groupe d'utilisateurs

Il possède des caractéristiques similaires à un coupe-feux:

- Translation d'adresses
  Masque le réseau extérieur du réseau interne
- Filtrage sécurité
  Une liste de sites interdits permet facilement de filtrer les accès clients

Du routeur filtrant à l'architecture des coupe-feux

Architecture de base



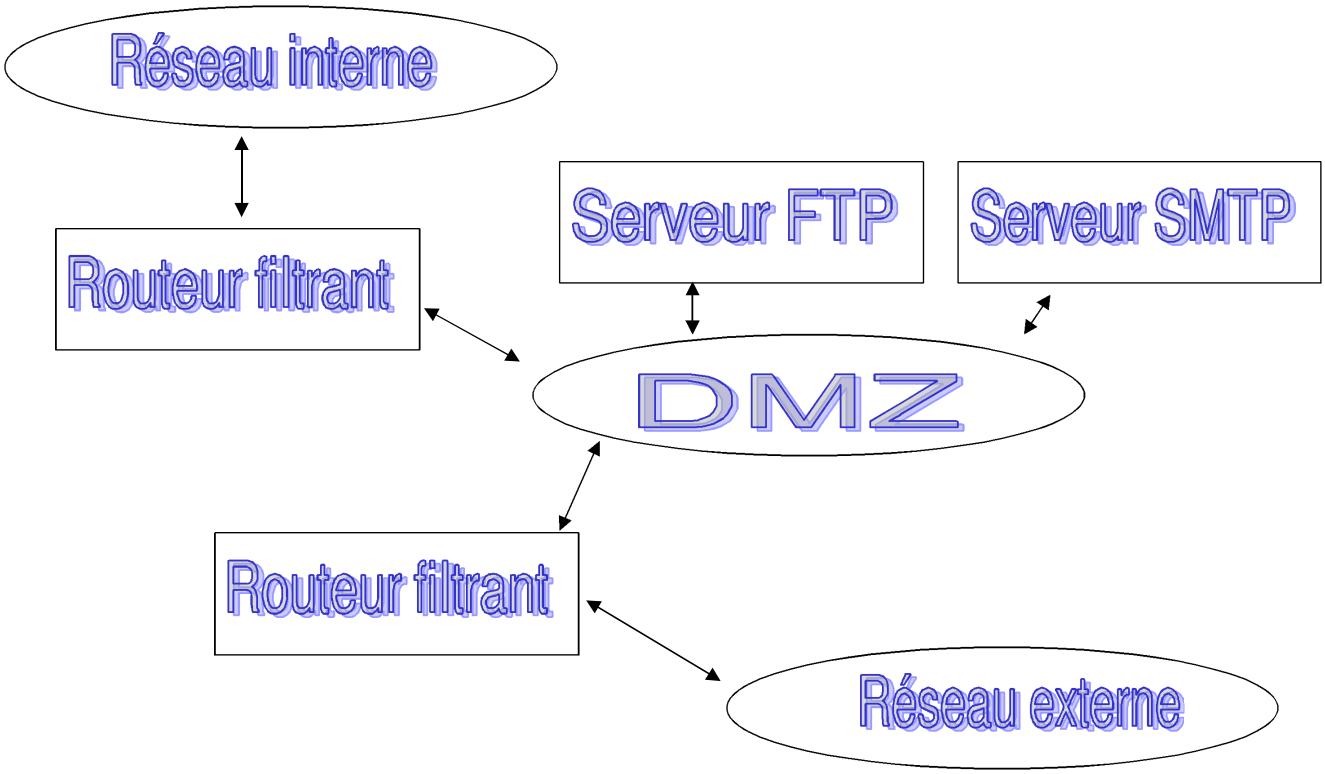
Problème

Tous les services de protection sont sur le coupe-feux central

Solution

Créer un réseau intermédiaire

DMZ



DMZ

Le trafic sur la DMZ n'est que du trafic intérieur <-> extérieur.

Un analyseur de trames ne voit pas les trames internes.

DMZ protégée par coupe-feux

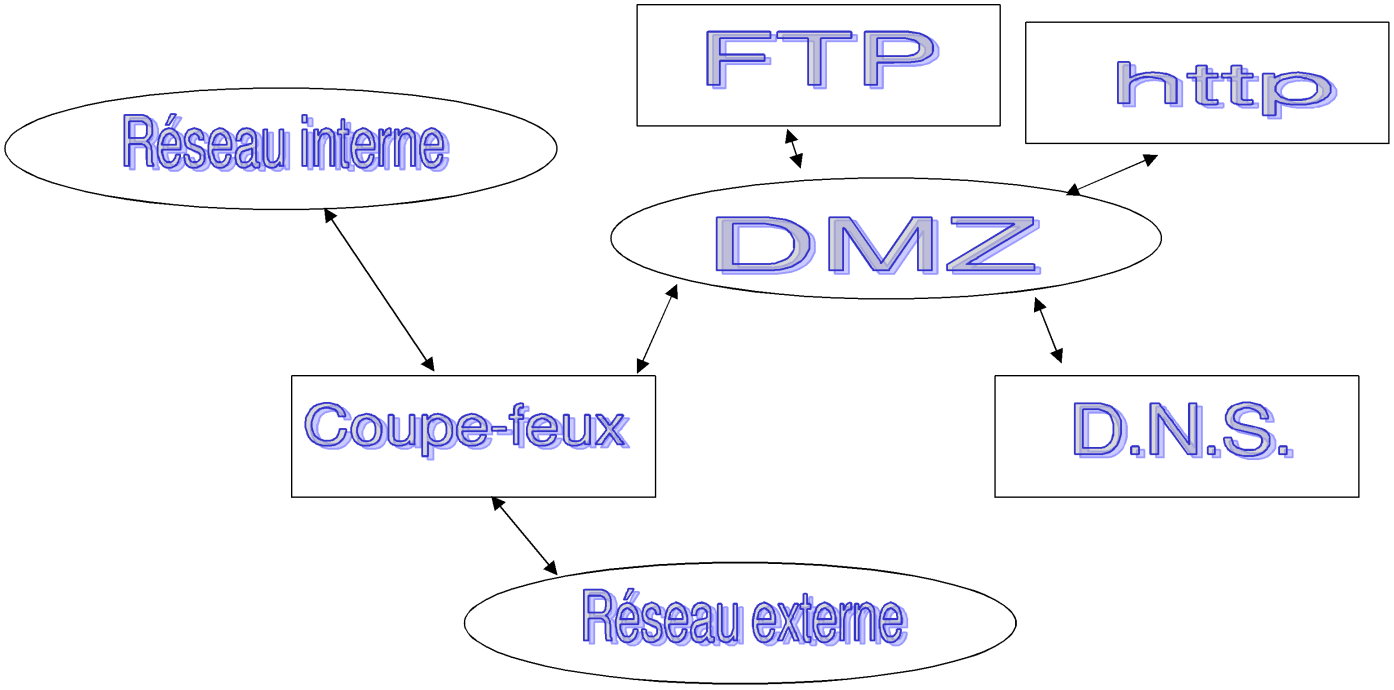
On peut réduire la configuration « deux routeurs » dans un seul serveur appelé coupe-feux

Cette configuration dispose d'un système serveur avec trois interfaces réseau :

- Internet
- réseau privé
- DMZ protégée.

Le Web public, FTP (File Transfer Protocol), la messagerie électronique et les serveurs DNS sont regroupés dans le réseau de DMZ protégée.

DMZ protégée par coupe-feux



Serveur Proxy

Apporte un service **"mandataire"** pour l'accès Internet

Ce mandataire peut agir sur de nombreux services: proxy ftp, proxy smtp, proxy web, ...

Agit par redirection des ports et filtrage des requêtes

- Le client accède au Web via le serveur proxy référencé par son adresse IP et son numéro de port.
- Le site distant renvoie ses réponses au serveur proxy.
- Le WEB ne voit que le serveur proxy

Exemple de fonctionnement d'un serveur Proxy Web

- Le client envoie la requête au proxy
- Le proxy vérifie son cache
- Le proxy transmet la requête au serveur WEB
- Le serveur renvoie le document demandé
- Le proxy délivre le document au client
- Le proxy met le document dans le cache

Serveur proxy

Habituellement, les serveurs proxy se trouvent

- Entre le coupe-feux et le réseau interne
- Entre le réseau interne et des serveurs critiques

Apports

- Economie de bande passante sur le lien WAN réseau interne/Internet.
- Gain de performances car cache disque du proxy
- Gain compensé par les performances réelles du proxy

XVII

Pare-feux

Définition

Un pare-feu (appelé aussi *firewall* en anglais) est une architecture qui permet de protéger un ordinateur ou un réseau d'ordinateurs des attaques provenant d'un réseau externe (notamment d'internet).

Une architecture pare-feu est constituée de routeurs filtrants permettant un accès à la DMZ. Par abus de langage et par simplification, on nomme aujourd'hui "pare-feux" les routeurs filtrants. Dans la suite, nous utiliserons le terme "pare-feux" avec cette définition de routeur filtrant.

Le filtre s'appuie sur le contenu des trames, par exemple sur les adresses IP source et destination, et/ou les ports source ou destination pour définir des règles de filtrage. Il peut aussi s'appliquer à un enchaînement de trames, une séquence particulière, etc,...

Fonctionnement

Un système pare-feu définit un ensemble de règles permettant :

- d'autoriser la connexion (*accept*) ,
- de bloquer la connexion (*drop*) ,
- de rejeter la demande de connexion (*reject*).

L'ensemble de ces règles constitue une **politique de sécurité** pour son réseau.

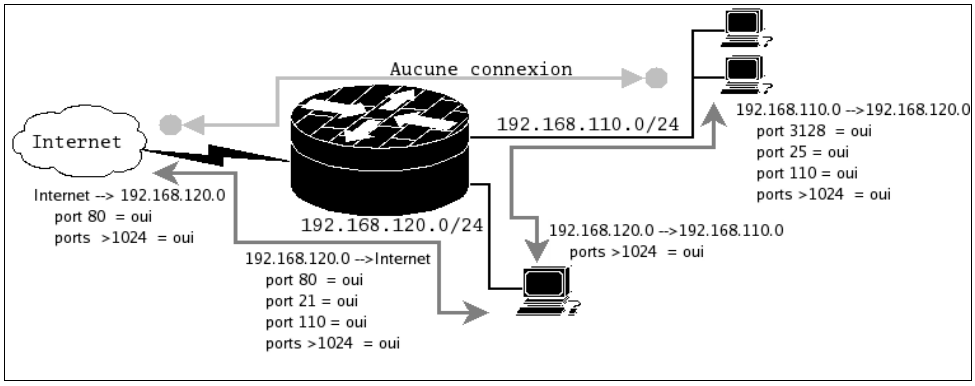
Une politique de sécurité parmi d'autres stipule :

On ferme tout et on ouvre au fur et à mesure en fonction de ses besoins.

Si cette politique est la plus sûre, elle demande beaucoup de travail car il faut analyser au préalable les types de connexions et de paquets qui circulent sur le réseau.

Fonctionnement

Politique de sécurité d'une DMZ :



Le filtrage

Filtrage de paquets

Le pare-feu effectue le filtrage de paquets IP, c'est-à-dire qu'il analyse les entêtes des paquets IP échangés entre deux machines.
Quand il y a une communication avec une machine de l'extérieur et une machine du réseau local, et inversement, les entêtes des paquets IP sont analysées par le firewall.
On y retrouve les informations suivantes :

- l'adresse IP de la machine émettrice,
- l'adresse IP de la machine réceptrice,
- le type de paquet (TCP, UDP,...),
- le numéro de port (généralement associé à un service).

Lorsque le filtrage est basé :

- sur les adresses IP, on parle de filtrage par adresse (*adress filtering*),
- sur le type de paquets et le port, on parle de filtrage par protocole (*protocol filtering*)

Filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application, et travaille au niveau des couches 5 à 7 du modèle OSI.
Le filtrage applicatif suppose donc une connaissance de l'application, et notamment de la manière utilisée pour structurer les données échangées.

Problèmes

Toute la difficulté réside dans l'établissement des règles :

- *des règles trop permissives* ne garantiront pas une protection adéquate,
- *des règles trop strictes* entraîneront une perte de service pour les utilisateurs.

Par exemple :

L'accès à un serveur Web se fait en général sur le port 80 mais la réponse se fait sur un port supérieur ou égal à 1024 qu'il est impossible de connaître à l'avance.

Ce n'est pas forcément pour autant qu'il faudra "ouvrir" tous les ports supérieurs ou égaux à 1024.

XVIII

QOS

Présentation

Disciplines de files d'attentes (qdisc)

Détermine comment les paquets sont envoyés.

Classes

Elles sont attachées aux qdiscs et en déterminent l'organisation. On distingue les classes filles des classes intermédiaires. Chaque classe dispose d'un qdisc qui en gère le flux.

Filtres

Sélection d'une discipline pour un paquet. Les filtres sont attachés aux qdiscs et aux classes. Ils permettent d'orienter le flux dans les différentes classes filles.

Organisation

Classe racine

Chaque interface physique dispose d'une classe racine: la qdisc root

Elle est déclarée par « `tc qdisc` »:

```
tc qdisc add dev eth0 root handle 10: cbq
```

Le numéro 10 est choisi unique et permet de nommer cette racine dans les classes attachées.
CBQ est un algorithme de pilotage de la qdisc.

Classes intermédiaires

L'ajout de classes intermédiaires se fait par « `tc class` »

```
tc class add dev eth0 parent 10:0 classid 10:1 cbq bandwidth 100Mbit rate 10Mbit
```

Algorithmes

Ordonnanceurs de paquets:

CBQ	Class-Based Queueing, ordonnanceur de paquets couramment utilisé. CBQ distribue les paquets en attente en un arbre hiérarchique de classes. Les feuilles de cet arbre sont ensuite gérées par des algorithmes spécifiques (les "disciplines")
HTB	Hierarchical Token Buckets. Mêmes objectifs que CBQ mais en utilisant sur des algorithmes différents.
SFQ	Stochastic Fairness Queuing. Peu consommateur en ressources, il ne gère pas finement les surcharges.
CSZ	Clark-Shenker-Zhang. Garantie de service.
TBF	Sans classes. Fondé sur le débit. Peu consommateur en ressources.
RED	Random Early Detect. Supprime des paquets pour éviter la congestion.

Paramètres des classes

Suivant l'algorithme choisi, il est possible de préciser les paramètres d'utilisation

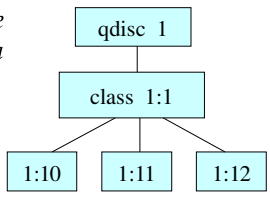
Pour HTB

- rate : bande passante minimale garantie
- ceil : bande passante maximale autorisée
- prio : valeur indiquant l'ordre de passage lors d'une demande de bande passante supplémentaire. Plus la valeur est faible, plus la priorité est grande.

Exemples

```
tc class add dev eth0 parent 1: classid 1:1 htb rate 100Mbps
tc class add dev eth0 parent 1:1 classid 1:10 htb rate 20Mbps ceil 100Mbps
tc class add dev eth0 parent 1:1 classid 1:11 htb rate 30Mbps ceil 100Mbps prio 1
tc class add dev eth0 parent 1:1 classid 1:12 htb rate 50Mbps ceil 100Mbps prio 10
```

Si la classe 10 est vide mais que la 11 et la 12 sont occupées, la 11 disposera de 30Mbps minimum et la 12 de 50Mbps. Les 20Mbps restant seront alloués à la 11 de plus haute priorité.



Pour CBQ

- bandwidth : indique la bande passante
- bounded : ne peut pas déborder vers d'autres classes
- isolated : bande passante inutilisable par d'autres classes

Filtrage

Afin de pouvoir distribuer les trames dans les classes, il faut pouvoir les identifier.
Utilisation du marquage de trame avec iptables ou bien par filtre direct.

La pose d'un filtre se fait avec « `tc filter` »

Marquage de trame

```
iptables -t mangle -A OUTPUT -p tcp -j MARK --set-mark 3
```

Toutes les trames tcp seront marquées avec le numéro 3

```
tc filter add dev eth0 parent 10:0 protocol ip handle 3 fw flowid 10:1
```

Filtrage direct

```
tc filter add dev eth0 parent 10:0 protocol ip prio 100 u32 match ip dst 10.32.0.2 match ip
dport 8080 0xffff flowid 10:2
```


Exemple CBQ

```
#!/bin/sh

iptables -t mangle -F

iptables -t mangle -A OUTPUT -p tcp -j MARK --set-mark 3
iptables -t mangle -A OUTPUT -p udp -j MARK --set-mark 4



tc qdisc del dev eth0 root handle 10: 2>/dev/null
tc qdisc add dev eth0 root handle 10: cbq bandwidth 100Mbit avpkt 1000 mpu 64



tc class add dev eth0 parent 10:0 classid 10:1 cbq bandwidth 100Mbit rate 10Mbit allot 1514
prio 1 maxburst 10 avpkt 100 bounded
tc class add dev eth0 parent 10:0 classid 10:2 cbq bandwidth 100Mbit rate 100kbit allot 1514
prio 1 maxburst 10 avpkt 100 bounded


tc filter add dev eth0 parent 10:0 protocol ip handle 3 fw flowid 10:1
tc filter add dev eth0 parent 10:0 protocol ip handle 4 fw flowid 10:2
```

Exemple HTB

```
#!/bin/sh

iptables -t mangle -F

iptables -t mangle -A OUTPUT -p tcp -j MARK --set-mark 3
iptables -t mangle -A OUTPUT -p udp -j MARK --set-mark 4

tc qdisc del dev eth0 root 2>/dev/null
tc qdisc add dev eth0 root handle 10: htb



tc class add dev eth0 parent 10: classid 10:1 htb rate 100Mbps ceil 100Mbps burst 2k
tc class add dev eth0 parent 10:1 classid 10:11 htb rate 40Mbps ceil 100Mbps burst 2k prio 1
tc class add dev eth0 parent 10:1 classid 10:12 htb rate 60Mbps ceil 100Mbps burst 2k prio 1


tc filter add dev eth0 parent 10:0 protocol ip handle 3 fw flowid 10:11
tc filter add dev eth0 parent 10:0 protocol ip handle 4 fw flowid 10:12
```


XIX

Voix sur IP

RTC

Historiquement, le réseau utilisé pour la téléphonie est le réseau RTC (réseau téléphonique commuté).

Caractéristiques

- Réseau à *commutation de circuits*: mise en relation des correspondants et mantien de cette liaison dédiée pendant la transmission de l'information.
- *Coeur de réseau numérique* sur fibre optique; *réseau capillaire analogique* (terminaison des abonnés sur paire de cuivre).
- *Distribution* (liaison abonné/centrale), *commutation* (mise en relation) et *transmission* de l'information.

Limitations

- Gestion de plusieurs milliers d'abonnés, mais ceux-ci ne communiquent pas tous simultanément.
- Transmission de données numériques possible à des débits relativement bas – 120kbs maximum.
- Débits plus élévés sur la boucle locale (ex. ADSL), mais les données sont relayées par des commutateurs et routeurs numériques dès la centrale, et ne transitent pas par le coeur du réseau RTC.
- Réseau redondant car parallèle aux réseaux de données, tels que les réseaux IP.

Comparaison RTC/VoIP

Type de réseau	**RTC**	**VoIP (réseau IP)**
Commutation	de circuits: chemin unique vers un abonné, liaison maintenue	par paquets: chemins multiples pour un même abonné, découpage des données et routage
Caractéristique de la liaison	Fixe, donc peu sûre	Flexible et multiple, difficile à écouter
Données	Arrivée dans l'ordre, retard faible, pas de gigue	Reconstitution de l'ordre d'arrivée, perte de paquets, retard, induction de gigue
Qualité de service (QoS)	Excellente: réseau spécifique au transport de la voix	"Best Effort": pas de maîtrise de la QoS des équipements sur internet

Malgré la flexibilité qu'elle offre, la commutation de paquets pose problème lors du transfert de flux temps réel tels que la voix.

Les données ne transitent plus par un circuit dédié et peuvent de ce fait arriver dans le désordre, voire être perdues en route.

Les protocoles mis en oeuvre dans les technologies de VoIP tentent de répondre à ce problème.

Avantages de la VoIP

Le principal enjeu de la voix sur IP est la convergence.

Les réseaux IP sont aujourd'hui largement déployés, et leur réutilisation pour transporter la voix permet une simplification architecturelle et une réduction des coûts, tant au niveau de l'investissement en équipement et câblage qu'en coût d'administration du réseau.

La voix sur IP favorise également la productivité, en introduisant une notion de mobilité (utilisation d'assistants personnels, création de centres d'appel virtualisés).

La convergence des données, de la voix et de la vidéo facilite par ailleurs le développement de nouvelles applications (ex: e-learning).

VoIP

Architecture

L'architecture d'un réseau VoIP met en oeuvre des éléments fonctionnellement similaires à ceux que l'on retrouve dans le réseau téléphonique commuté: il s'agit de terminaux, de routeurs et de passerelles.

Le routeur

remplace le commutateur RTC. Il aiguille les données lors de leur transmission dans le réseau IP.

La passerelle

assure la convergence et l'interconnexion entre le réseau RTC et le réseau IP.

Les terminaux

sont des téléphones IP ou des postes de travail.

Protocoles de VoIP

La VoIP étant en phase de convergence technique, plusieurs visions de la place de l'intelligence dans le réseau coexistent actuellement.

Le protocole H323 introduit, par exemple, des équipements de contrôle appelés "gatekeepers", qui ont pour rôle de maintenir une correspondance au niveau de l'adressage entre numéros de téléphone et adresses IP, ainsi que de gérer les autorisations d'accès au réseau.

A contrario, l'utilisation du protocole SIP déporte l'intelligence vers les terminaux, qui implémentent alors des fonctionnalités de signalisation et d'adressage.

Matériels

	H323	MGCP et MeGaCo	SIP
Gestion des accès	GateKeeper H323 (GK)	MGC (Media Gateway Controler)	Registrar (proxy SIP)
Mixage A/V (conférence)	MCU (Multipoint Conferencing Unit)	MG (Media Gateway)	Pont de conférence (RTPproxy, asterisk, matériel dédié)

Protocoles de VoIP

Structure

Les protocoles de voix sur IP sont un regroupement de protocoles assumant des rôles différents:

- *signalisation*: établissement, contrôle et fin d'appel; enregistrement, admission et statut. Le protocole de signalisation donne généralement son nom au protocole de VoIP.
- *session*: gestion des flux média par négociation des codecs et des ports RTP/RTCP.
- *transport/média*: protocole de transport temps réel, généralement RTP/RTCP, encapsulant le média en lui-même (la voix enocdée par un codec G711, par exemple).

Médias rencontrés: voix, vidéo, fax, données (SMS, messagerie instantanée IM, partage d'application).

Protocoles de VoIP

Caractéristiques réseau

<table>
<tr><th></th><th colspan="2">H323</th><th colspan="2">MGCP et H248/MeGaCo</th><th colspan="2">SIP</th></tr>
<tr><td rowspan="2">Signalisation</td><td rowspan="2">H225:</td><td>Q931: établissement, contrôle et fin d'appel; TCP/1720 et suivants</td><td rowspan="2">MGCP:</td><td rowspan="2">le MGC attaque sur UDP/2427,
la MG répond sur UDP/2727</td><td rowspan="2">SIP:</td><td rowspan="2">Session Initiation Protocol, UDP/5060</td></tr>
<tr><td>RAS: registration, admission, status; UDP/1719 (gatekeeper H323)</td></tr>
<tr><td>Session</td><td>H245:</td><td>gestion des flux media, négociation des codecs et des ports; TCP/1024 et suivants</td><td>SDP:</td><td>Session Description Protocol; encapsulé dans MGCP</td><td>SDP:</td><td>Session Description Protocol; encapsulé dans SIP</td></tr>
<tr><td rowspan="2">Transport</td><td rowspan="2">RTP et RTCP:</td><td colspan="5">RTP: 1 port UDP pair pour le transport (entre 16000 et 32000 par défaut)</td></tr>
<tr><td colspan="5">RTCP: port UDP suivant pour le contrôle (5% du volume RTP pour RTCP).</td></tr>
</table>

- H323 (1997): consommateur de ressources réseau. Issu de l'UIT-T, il reproduit les échanges RNIS (complexes), simplifiés dans la version 4.
- MGCP (1998) devenu MeGaCo (1999): pour les réseaux d'opérateurs, clients multi-protocoles.
- SIP (2003): le plus simple et répandu, il imite HTTP et tend à supplanter H323.

SIP

L'autre grand acteur du monde de la voix sur IP est le protocole SIP (Session Initiation Protocol).

Normalisé par l'IETF (rfc. 3261 et 2543), il opère des simplifications importantes par rapport à H323, notamment parce qu'il s'inspire moins du modèle de la téléphonie existante, et plus des protocoles applicatifs non liés au transport de la voix, tel que HTTP, qui est son plus proche parent.

C'est un protocole de signalisation dissocié des flux de données.
Cette indépendance lui confère de la flexibilité.

> *A titre d'exemple, il autorise plus facilement la redirection d'un flux audio ou l'adjonction d'un correspondant supplémentaire en cours de conversation.*

Si le protocole H323 jouit de par son ancienneté d'une certaine notoriété, il est aujourd'hui évident que la souplesse et la simplicité de SIP le rendent incontournable.

C'est sur ce protocole que la suite de ce document s'appuiera.

SIP

SIP fournit à la fois des fonctionnalités de signalisation et avec l'aide du protocole SDP (Session Description Protocol), de négociation des paramètres de la session.

La signalisation comprend la localisation des terminaux, la recherche de leur disponibilité, ainsi que les autorisations d'accès.

La négociation des paramètres permet d'établir les capacités des parties, en termes de type de média (voix, vidéo, données, etc...),

Lorsque l'appel est établi, SIP va suivre la communication et coordonnera toute modification des paramètres de la session, ainsi que sa terminaison.

Il peut également implémenter des fonctionnalités avancées telles que le cryptage des données transférées.

Le flux de signalisation étant indépendant du flux média, la communication est maintenue en cas d'interruption du contrôle de la communication (le 'Registrar' est tombé). En revanche, les services ne sont évidemment plus assurés.

Registrar SIP

Les entités qui interviennent dans une session SIP sont identifiées par une uri du type:

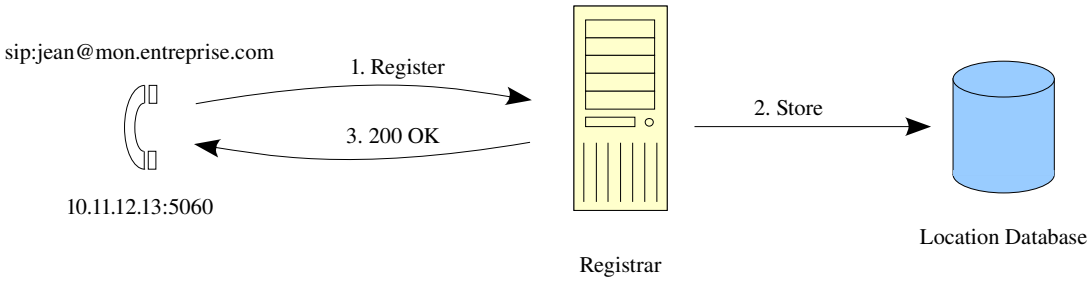
sip:user@domain.tld

Un client SIP s'enregistre (éventuellement en s'authentifiant) auprès d'un registrar SIP, désigné ici par *domain.tld*. Cet enregistrement permet par la suite la localisation des utilisateurs, et se fait au moyen de la requête REGISTER.

Exemple de requête d'enregistrement SIP:

```
REGISTER sip:domain.tld SIP/2.0
Via: SIP/2.0/UDP 192.168.1.1:5060;branch=z9hG4bK3641ce7c;rport
From: <sip:0123456789@freephonie.net>;tag=as6bd3ddf6
To: <sip:0123456789@freephonie.net>
Call-ID: 1f335cb17d272e3e01a928a231e4a179@192.168.1.1
CSeq: 102 REGISTER
User-Agent: Asterisk PBX
Max-Forwards: 70
Expires: 1800
Contact: <sip:s@0123456789>
Event: registration
Content-Length: 0
```

Registrar SIP



L'enregistrement dans la base de données (ou dans un simple fichier) spécifie que l'utilisateur *sip:jean@mon.entreprise.com* est accessible à *sip:jean@10.11.12.13:5060*.

Requêtes SIP

Les autres requêtes SIP les plus utilisées sont :

- INVITE permet d'inviter un correspondant à se joindre à une session. Cela revient à "appeler" un correspondant.
- ACK sera envoyé par l'appelant pour confirmer le résultat d'une requête INVITE.
- OPTIONS sert à déterminer les capacités d'une entité SIP.
- BYE est utilisé pour mettre fin à une session.

Réponses SIP

Les résultats des différentes requêtes SIP sont déterminés au moyen de codes d'erreurs à trois chiffres, similaires à ceux qui sont utilisés par le protocole HTTP.

Un code 2XX indique un succès, et un code 4XX une erreur du client. Les codes 1XX, 3XX, 5XX et 6XX existent également, et signifient respectivement information, redirection, erreur du serveur, et échec général.

Exemple
un serveur SIP qui n'implémente pas la requête OPTIONS répond par un code 501:

```
SIP/2.0 501 not implemented yet
Call-ID: 4b7aa10627a8af8d586b0d5148895a24@192.168.1.1
CSeq: 102 OPTIONS
From: "asterisk" <sip:asterisk@192.168.1.1>;tag=as3f8529f2
To: <sip:domain.tld>;tag=01-08061-01ed4ea1-7817bcda6
Via: SIP/2.0/UDP 192.168.1.2:5060;received=192.168.1.2;rport=5060;branch=z9hG4bK617f0112
```


Proxy SIP

Il est possible avec SIP de créer une infrastructure d'hôtes réseau appelés serveurs proxy.

Bien qu'optionnels, ils jouent un rôle très important dans une architecture SIP, permettant de router les appels en fonction de la localisation de l'appelant, de la facturation ou encore de l'authentification.

Lorsqu'une entité SIP s'enregistre auprès d'un registrar, celui-ci inscrit cette information dans une base de données.

Quand deux entités qui ignorent leurs adresses IP respectives veulent établir une session, elles font appel à un ou plusieurs serveurs proxy qui interrogent à leur tour les registrars.

Un proxy SIP n'intervient pas dans le routage des flux audio: dès lors que les correspondants ont établi une session, la voix passe directement entre eux, en fonction du routage de la couche réseau.

Proxy SIP

Les proxy SIP peuvent être de type "stateful" ou "stateless".

Cette terminologie décrit la capacité d'un serveur proxy à mémoriser l'état d'une transaction SIP.

Un proxy "stateless" n'est pas capable de mettre en correspondance le début d'un appel et sa fin.

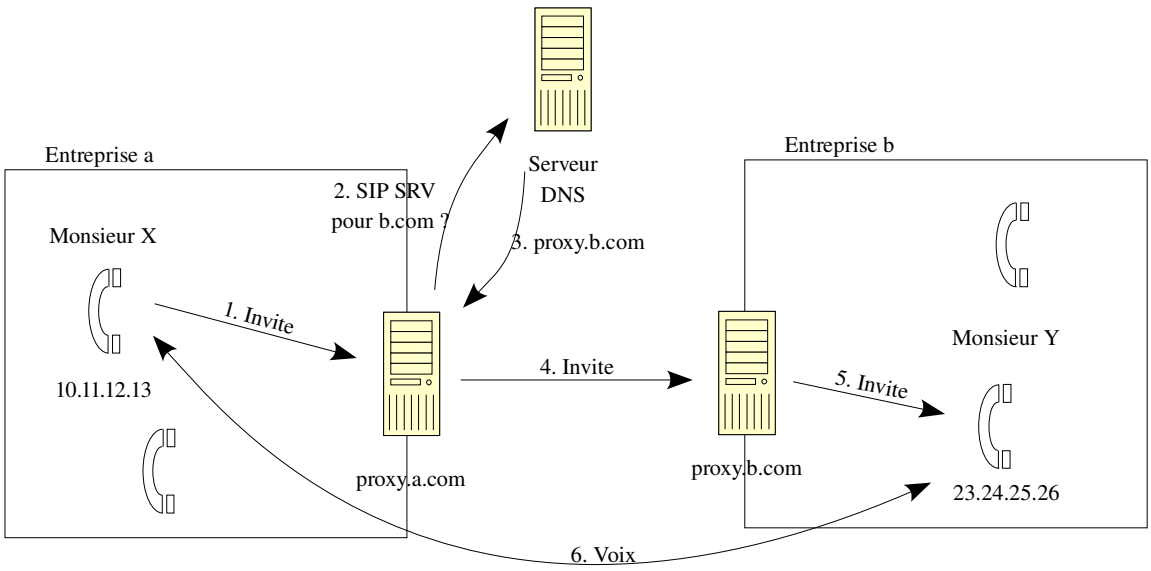
Il faudra recourir aux services d'un proxy "stateful" dès lors que l'on voudra implémenter les fonctionnalités suivantes:

- Facturation des appels au temps écoulé
- Essayer successivement plusieurs localisations pour tenter de joindre un utilisateur
- "Forker" un appel, c'est-à-dire le dupliquer.

SER (Sip Express Router) est un des serveurs proxy applicatifs les plus utilisés.

Proxy SIP

Exemple de déploiement SIP entre deux entreprises



SDP

En plus de la signalisation, SIP s'appuie sur le protocole SDP pour négocier les paramètres de la session lors de son initialisation.

Cela passe par une analyse des capacités des intervenants, et la détermination de l'intersection de celles-ci.

Ici, l'application *asterisk* (qui implémente entre autres fonctionnalités celle de registrar SIP) détermine les codecs audio communs à deux intervenants:

```
Using INVITE request as basis request - 18746-QX-01ee2e1e-2af843cb3@domain.tld
Sending to 192.168.1.1 : 5060 (non-NAT)
Found peer 'domain.tld'
Found RTP audio format 8
Peer audio RTP is at port 192.168.1.1:31050
Found description format PCMA
Capabilities: us - 0x1f07ff (g723|gsm|ulaw|alaw|g726|adpcm|slin|lpc10|g729|speex|ilbc|jpeg|png|
h261|h263|h263p), peer - audio=0x8 (alaw)/video=0x0 (nothing), combined - 0x8 (alaw)
```


RTP

De par leur nature, les réseaux IP sont mal adaptés au transfert de la voix.

Les réseaux IP sont en général conçus pour fournir une qualité de service moyenne, et la commutation des paquets peut influer sur l'ordre de leur arrivée.

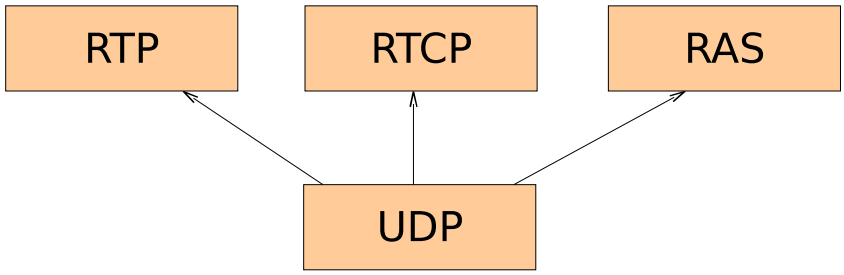
Il revient donc aux protocoles affectés au transport des données de combler ces lacunes. C'est le protocole RTP (Real Time Protocol) qui est le plus utilisé dans le cadre de la VoIP.RTP

Né en janvier 1996, son objectif est de rendre possible la mise en oeuvre d'applications audio et vidéo sur IP.

RTP est un protocole qui s'appuie sur UDP. Il intègre le protocole RTCP pour son contrôle, un peu comme ICMP vis-à-vis d'IP.

Il est décrit dans la RFC 1889.

Fonctionnement



RTP

Transport de données en temps réel. Pas de garantie sur la qualité de service.

RTCP

Transmettre périodiquement des paquets de contrôle à tous les participants d'une session.

RAS

Admission et état des communications.

Fonctionnement

RTP utilise un couple de ports UDP pour son service:

- un port pour les flux audio (de numéro pair),
- un port pour les flux de contrôle RTCP (le numéro impair suivant).

Les ports sont choisis dynamiquement dans la fourchette 16k-32k.

Chaque trame RTP transporte l'équivalent de 20ms de flux audio.

RTP peut utiliser, soit du flux unicast soit du multicast (sa vocation première). Dans le cas du multicast, il utilise RTCP pour envoyer à intervalles réguliers des trames indiquant qui rejoint ou quitte le groupe.

Pour réaliser l'envoi de flux audio et de flux vidéo simultanément (vidéo conférence), il faut définir deux couples de ports UDP. L'un pour la voix, l'autre pour l'image. RTP ne réalise pas le couplage: la synchronisation entre ces couples sera réalisée par RTCP.

RTCP

RTCP réalise quatre fonctions:

- Fournir des informations sur la qualité de la session.
- Garder une trace de tous les participants une session. Attribution d'un CNAME unique pour chaque participant.
- Contrôle du débit pris par RTCP pour une session RTP: plus il y a de participants, plus la fréquence d'envoi des paquets RTCP est faible. Le débit RTCP doit rester inférieur à 5% du débit de la session.
- Transmettre des informations utilisateurs sur la session, comme par exemple transmettre le nom d'un participant sur les autres postes.

RTP et NAT

Choix dynamique des ports

Les ports de niveau 4 utilisés par RTP sont choisis dynamiquement. Par ailleurs, lors d'une utilisation combinée de RTP avec un protocole d'établissement de session tel que SIP, c'est celui-ci qui indiquera les adresses IP des équipements RTP à mettre en relation.

Ces adresses IP seront alors contenues dans le payload des messages SIP, ce qui empêchera les mécanismes classiques de la translation d'adresses de remplacer par des adresses IP publiques d'éventuelles adresses IP réservées à une utilisation privée (cf. RFC 1918).

Il existe plusieurs solutions pour remédier à cette situation:

- Utiliser des adresses IP publiques
- Mettre à profit les réseaux privés virtuels pour garantir la connectivité,
- Exploiter des firewalls applicatifs capables de lire et d'interpréter le payload SIP.

Codecs voix

Les codecs, pour Codeur/DECodeur, numérise les données selon un format propre. Les données sont ensuite encapsulées dans RTP, qui les transporte.

Certains codecs sont devenus standards, et sont disponibles sur tous les équipements de VoIP. D'autres ne sont disponibles que sur des équipements plus récents. Les codecs les plus utilisés sont:

G711u et G711a

Egalement connus sous la dénomination ulaw/alaw. Nécessitent 64Kbps mais garantissent une bonne qualité de voix.
La version "u" est utilisée en Amérique du Nord et au Japon, la version "a" dans le reste du monde. Inventés par Bell, ces codecs ont été standardisés par l'ITU en 1988 et sont maintenant utilisés dans tous les réseaux téléphoniques numériques modernes.
La plupart des équipements de VoIP implémente G711.

G726

Ce codec trouve également son origine dans les réseaux téléphoniques classiques. Il utilise 32Kbps pour fournir une qualité approchant celle de G711.
C'est pour cette raison qu'il est souvent utilisé dans les "trunks" internationaux.
C'est également le codec utilisé par les téléphones DECT (Digital Enhanced Cordless Telephony).

Codecs voix

G729

Standardisé par l'ITU, ce codec ne nécessite que 8Kps pour fournir une qualité respectable.
Il faudra cependant s'affranchir d'un reversement financier pour acquérir les droits d'utilisation dans un cadre commercial. Il utilise fortement le processeur de la machine.

GSM

Le réseau GSM (Global System for Mobile communications) utilise un codec dénommé RPE-LTP (Regular Pulse Excitation Long-Term Prediction).
Ce codec, couramment appelé GSM, utilise 13Kbps et exploite la prédiction temporelle. Ses variantes modernes font l'objet de nombreux brevets.

Autres codecs voix

- G727/G727.1: 16, 24, 32 ou 40kbps
- G728: 16kbps
- G723: 5.3 et 6.3kbps
- Speex: VBR (Variable Bit Rate): adaptation dynamique de la compression en fonction de la bande passante disponible

Autres codecs

Selon le type de media transporté, différents codecs sont utilisés.

Codecs vidéo

H261, H263, H263+, H264 (MPEG-4, audio ET vidéo). Utilisent UDP.

applications partagées

Ensemble de protocoles T120 regroupant T123, T124, T125. Utilisent TCP.

"Instant Messaging" et SMS

Jabber et SM-PPP, qui utilisent TCP. Jabber sera prochainement inclus dans SIP

Télécopie ou FoIP (Fax over IP)

- G711 pass-through: Il s'agit d'encoder les signaux T30 comme de l'audio et transporter le media T38
- T37: fax-image file via e-mail. Envoi par message électronique d'un fichier à un télécopieur.

Qualité de service (QOS)

QOS et IP

Afin de garantir une qualité d'écoute correcte lors du transfert de la voix sur IP, il sera obligatoire d'implémenter un mécanisme de QOS.
Ce mécanisme devra réserver une bande passante suffisante pour les flux audio et garantir une latence suffisament faible.

La qualité téléphone normalise le retard à 150ms par trajet. En pratique, 400ms sont un seuil plafond.

Le protocole IP lui-même ne fournit pas les fonctionnalités nécessaires: l'entête IP contient bien un champ "type de service" (TOS) mais celui-ci est mal exploité et parfois même utilisé à d'autres fins, tels que la détection de congestion.

Il sera donc nécessaire d'exploiter une technologie externe.

En production, il est courant de réservé un VLAN dédié à la voix, avec une garantie de bande passante et une priorisation de paquets.

Qualité de service (QOS)

Exemple

Le noyau linux permet, par exemple, de définir des classes de trafic auxquelles on pourra affecter une bande passante garantie et des priorités:

```
modprobe ip_nat_sip
modprobe ip_conntrack_sip
iptables -t mangle -A POSTROUTING -o eth0 -m helper --helper sip -m state --state
ESTABLISHED,RELATED -j CLASSIFY --set-class 1:10

tc qdisc add dev eth0 root handle 1: htb default 20
tc class add dev eth0 parent 1: classid 1:1 htb rate 1000kbps
tc class add dev eth0 parent 1:1 classid 1:10 htb rate 200kbps ceil 1000kbps prio 0
tc class add dev eth0 parent 1:1 classid 1:20 htb rate 800kbps ceil 1000kbps prio 1
```

Ici, tout trafic lié à une communication SIP sortant par l'interface ethernet eth0 sera affecté à la classe 1:10. L'algorithme d'ordonnancement de paquets "htb" (Hierarchal Token Bucket) est ensuite utilisé pour affecter à cette classe de traffic une bande passante minimale garantie de 200kbps, avec une priorité haute.