SR04

Cours de l'uv SR04 - Les réseaux

Version 12

PROF. ABDELMADJID BOUABDALLAH

06/01/2020

Table des matières

Introduction

En raison des rapides progrès technologiques que nous connaissons et en raison du rapprochement du monde informatique et de celui des télécommunications, nous avons assisté à une profonde mutation de l'utilisation des systèmes informatiques. Nous sommes passés de l'informatique centralisée où le concept de « salle informatique » – une pièce abritant un gros ordinateur dans laquelle les utilisateurs apportaient leurs travaux à traiter – à une informatique distribuée utilisant un ensemble d'ordinateurs interconnectés par des liaisons de communication appelés les réseaux informatiques.

Les applications des réseaux sont nombreuses et peuvent intégrer divers équipements en plus des ordinateurs comme les capteurs de paramètres environnementaux (température, mouvement, pression, etc) et divers équipements comme les équipements biomédicaux, mécaniques, etc.

L'UV SR04 présente les architectures et technologies des réseaux et télécommunication.

Après avoir présenté les principes de fonctionnement des architectures réseaux, nous présenterons les protocoles d'Internet (TCP-IP/IPv6). Nous développerons en détails l'adressage, les protocoles de routage, les protocoles de transport dans l'Internet et d'autres briques importantes comme le DNS, le NAT, etc. Ensuite, nous aborderons les technologies réseaux locaux : architectures des réseaux locaux (LANs), les LANs fixes hauts débits, réseaux locaux sans fil (WIFI), interconnexion de réseaux, et les réseaux locaux virtuels (VLANs). les réseaux personnels et l'Internet des objets (IoT).

Dans la deuxième partie de cette UV, nous traiterons les communications longue distance.

Nous commencerons par présenter les concepts de base des transmissions de données sur support physique et aborderons ensuite les technologies pouvant servir de Backbone comme la technologie MPLS, et conclurons par une étude des critères de choix de la technologie adéquate pour l'interconnexion de plusieurs sites géographiquement éloignés.

Le modèle OSI

A. Les réseaux informatiques

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants avec un site central puis des ordinateurs entre eux et enfin de connecter des machines terminales telles que des stations de travail avec leurs serveurs. Aujourd'hui, les réseaux sont omniprésents. Leur développement a commencé dès la naissance des techniques de télécommunication.

Dans un premier temps, ces communications étaient destinées au transport de données informatiques. Aujourd'hui, ces réseaux intègrent non seulement des données mais aussi de la parole et de la vidéo. Les premiers réseaux permettaient simplement de raccorder un équipement distant à d'autres équipements d'entreprise comme un serveur par exemple. Les débits de ces connexions étaient très faibles. Parallèlement, les constructeurs informatiques (IBM, DEC, Bull, etc.) se sont lancés dans le développement de leur propre architecture réseau. Quand on dit "architecture", on fait référence à l'architecture logicielle et matérielle mais pas à la façon dont connectés les nœuds d'un réseau, comme c'est le cas de l'architecture d'un bâtiment. Quand on s'intéresse à la manière dont sont connectés les nœuds, on parle de topologie réseau que nous évoquerons plus loin dans ce cours.

À ses débuts, le développement des réseaux se faisait selon les choix des concepteurs sans prendre en compte les contraintes d'interopérabilité avec les produits développés par différents constructeurs. En effet, au début des années 1980, nous avions assisté à une croissance exceptionnelle du nombre et de la taille des réseaux. Vers le milieu des années 80, les constructeurs informatiques ont commencé à rencontrer des problèmes d'interopérabilité des réseaux vu que ces

architectures n'utilisaient pas les mêmes protocoles et que chacun souhaitait garder la main sur sa clientèle. Cela est équivalent à vouloir faire parler des gens qui ne parlent pas la même langue. Les principales architectures qui dominaient le marché des réseaux sont : le réseau SNA (Systems Network Architecture) développé par IBM, l'architecture DECnet (Digital Equipment Corporation net), et l'architecture DSA (Distributed System Architecture) développé par CII-Honeywell-Bull.

Dans le but de définir une architecture générique qui sera suivie par les constructeurs informatique pour développer des architectures réseau standards, l'organisme international de normalisation ISO (International Standardization Organization) a mis au point dans un premier temps un modèle de référence d'architecture réseau pour aider les fournisseurs à développer des réseaux compatibles avec d'autres réseaux (ou des réseaux standards). Ce modèle est appelé modèle de référence OSI (Open System Interconnection). Dans un deuxième temps, l'ISO s'est attaqué au développement de protocoles standards afin de mettre au point une architecture réseau universelle, standard, adoptée par tous les constructeurs informatiques. Le modèle OSI publié en 1984 propose aux fournisseurs un ensemble de normes permettant d'assurer une compatibilité et une interopérabilité entre divers types de technologies réseaux développées par différents constructeurs à travers le monde.

1. Fonctions des réseaux

Les réseaux informatiques assurent essentiellement le codage des informations, leur mémorisation et leur traitement, et enfin la transmission sur le support physique. Afin que l'information atteigne le nœud destinataire, les informations transmises peuvent traverser plusieurs nœuds relais. Selon que les nœuds communicants se trouvent sur un même site géographique ou sur des sites très éloignés les appellations des réseaux diffèrent. On parle alors de réseaux locaux (LANs), de réseaux metropolitains (MANs), ou de réseaux longue distance (WANs). D'autres types de réseaux existent comme les réseaux personnels, les réseaux domestiques, etc.

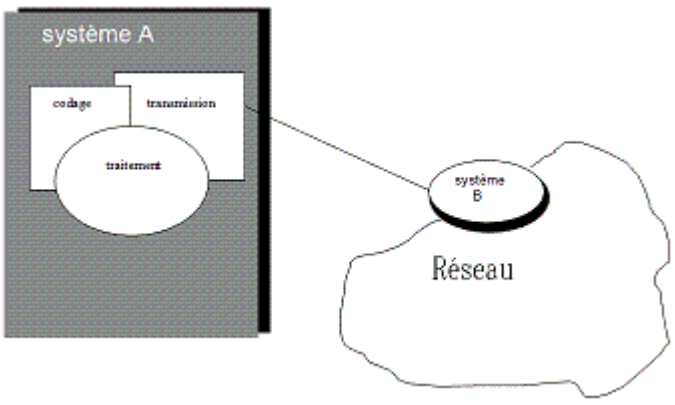


Image 1 Fonctions

2. Normalisation

Afin d'assurer une interopérabilité entre les équipements de communication soit au niveau physique ou logiciel, plusieurs organismes interviennent dans la normalisation des réseaux. Les principaux organismes de normalisation qui interviennent dans le domaine de la technologie de l'information sont :

- **ISO (International Organization for Standardization)**
  - Est une organisation destinée à coordonner et unifier au niveau

international les normes dans tous les domaines techniques à l'exclusion de l'électricité, de l'électrotechnique, et de l'électronique.

- **ITU (International Telecommunication Union)** , ex-CCITT
  - Cet organisme traite tout ce qui concerne les télécommunications.
- **Autres organismes : par exemple IEEE (Institute of Electrical and Electronics Engineers)**

3. Identification d'une norme

La dénomination d'une norme peut tenir compte d'un ensemble de critères tels que son origine (ITU, ISO,...) et son domaine d'application (réseau public, téléphone, ...).

Normes ISO

Les normes de l'ISO sont nommées avec le préfixe IS suivi d'un numéro.

Exemple

ISO/IS 8802.3

Normes ITU (ex-CCITT)

Les normes ITU sont nommées à l'aide d'une lettre suivie d'un point et d'un numéro.

La lettre précise le champ d'application.

- V : pour la transmission de données par téléphone
- X : réseaux publics de données

Exemple

V24, V28, X21, X25

B. Fonctions et organisation d'un réseau

1. Fonctions d'un réseau

Comme les réseaux ont pour objectif de transférer des informations d'un point (et éventuellement de les traiter) à un autre, une question à laquelle il n'est pas facile de répondre très rapidement est : quelles sont les briques à développer afin de réaliser cette communication?

La réponse à cette question consiste à définir et spécifier des procédures de gestion de la communication qui suppose la connaissance des tâches que le réseau doit effectuer. Par exemple, dans le cas simple d'un réseau composé de deux ordinateurs reliés par une liaison physique, le dialogue nécessite les fonctions suivantes: l'adaptation et le formatage de données, la détection et la correction des erreurs de transmission, et la régulation de flux. Alors que dans le cas d'un réseau maillé où deux entités communicantes ne sont pas forcément adjacentes, c'est à dire reliées directement par un support de communication, il est nécessaire de définir un chemin par lequel transiteront les données afin d'atteindre la destination. Lorsque les entités communicantes exigent à ce que toute donnée envoyée par l'émetteur soit reçue par l'entité réceptrice (service attendu est un service fiable), il est indispensable de mettre en place une fonction permettant de s'assurer que le

transfert de bout en bout s'est bien déroulé, et que la présentation de données s'est déroulée comme attendu.

Fondamental

Une organisation est donc nécessaire.

2. Organisation

Une fois que toutes les tâches permettant de faire fonctionner un réseau sont définies (connexion, physique, contrôle d'erreurs de transmission, contrôle de flux, routage, contrôle de bout en bout, gestion de dialogue, présentation de données, les applications), il est nécessaire de développer un module pour chaque tâche ou groupe de tâches (selon le choix décidé par les concepteurs de l'architecture), de définir un ordre d'exécution de ces tâches, et de répondre à d'autres questions comme les suivantes:

- Le contrôle de congestion avant le contrôle d'erreurs ?
- Quels sont les organes du réseau chargés de ces tâches ?
- Les solutions obtenues sont-elles indépendantes du matériel ?
- etc.

Fondamental

Deux principes sont utilisés dans la conception de réseaux : **la hiérarchie** et **la décentralisation**

La mise en œuvre d'une organisation hiérarchisée et décentralisée doit permettre de :

- Faciliter l'étude et la réalisation du réseau à partir d'éléments de base existants.
- Simplifier son fonctionnement par la donnée de règles formelles.
- Garantir une fiabilité du système.
- Assurer une facilité d'extension.
- Optimiser les performances.

Fondamental

La définition d'une **architecture** de réseau qui est un concept d'organisation de matériels et logiciels à l'aide d'une structure hiérarchisée est appelée **structure en couches**.

C. La normalisation ISO

1. Le modèle de référence OSI

Pour répondre aux questions précédentes et dans le but de définir une architecture générique qui sera suivie par les constructeurs pour développer des architectures réseau standards afin de résoudre le problème de l'incompatibilité des réseaux, l'organisme international de normalisation ISO (International Standardization Organization) a mis au point dans un premier temps un modèle de référence d'architecture réseau. Ce modèle est appelé modèle de référence OSI (Open

System Interconnection). Dans un deuxième temps, l'ISO s'est attaqué au développement de protocoles standards et obtenir ainsi une architecture réseau universelle, standard qui sera adoptée par tous les constructeurs informatiques.

Le modèle OSI, publié en 1984, propose un ensemble de normes permettant d'assurer une compatibilité et une interopérabilité entre divers types de technologies réseaux développées par différents constructeurs à travers le monde. Le modèle OSI est composé de plusieurs couches selon un modèle hiérarchique où chaque couche i assure une ou plusieurs tâches pour réaliser la communication avec l'entité homologue (couche i du site distant). La couche i échange les données avec son homologue à l'aide d'un protocole.

Un protocole est un ensemble de règles qui précisent comment doit s'effectuer la communication entre deux entités. Cette communication ne peut être réalisée qu'à l'aide de la définition des fonctions que doit réaliser ce protocole. Ces fonctions sont mises en œuvre grâce à la définition d'un format des blocs de données qui sera échangé entre les entités communicantes.

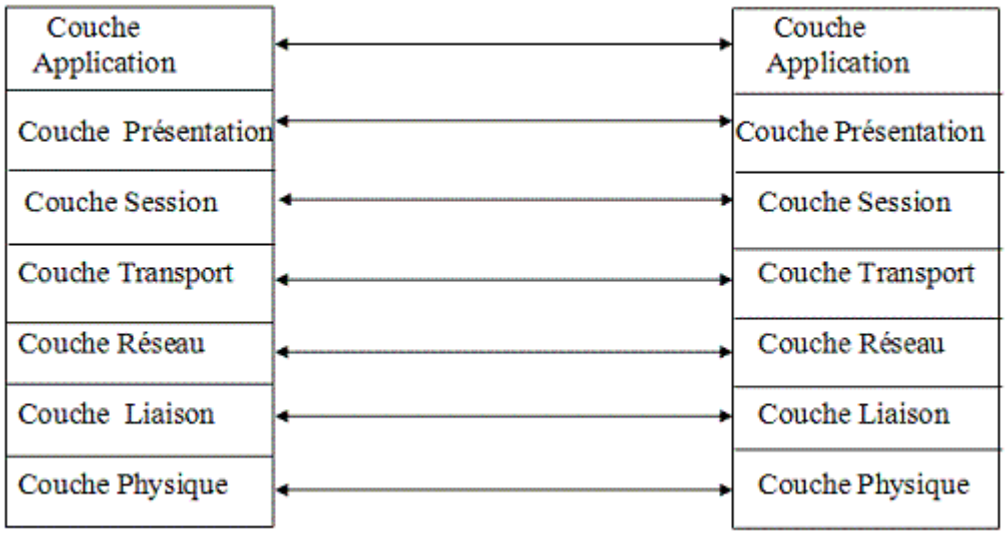


Image 2 Le modele OSI

Lorsque les données sont envoyées d'une couche i à son homologue sur un autre site, la couche i ajoute aux données à transmettre des informations de contrôle qui permettront au destinataire de comprendre ce que l'émetteur veut dire. Cette unité de données échangée par un protocole (données utile et l'en-tête) est appelée dans le vocabulaire ISO : **Protocol Data Unit ou PDU de niveau i ou i-PDU**. Une fois i-PDU construit, la couche i le soumet à la couche (i-1) pour lui demander un service de transmission. Le bloc fournit par la couche i à la couche (i-1) est appelé **Service Data Unit de niveau i ou i-SDU**.

Pour illustrer ce mécanisme, considérons par exemple un demandeur d'emploi qui prépare et envoie une lettre de demande d'emploi à un employeur. Cette lettre contient en plus du texte de la demande d'emploi, les coordonnées du demandeur, l'objet du courrier, la date, le service à qui ce courrier est adressé, éventuellement les numéros de pages si la demande tient sur plusieurs feuilles, etc. Nous constatons donc que dans cette lettre, il y a deux types d'informations: l'information utile (texte de la lettre) et l'information de contrôle qui constitue l'en-tête de la couche i. L'ensemble constitue le **i-PDU**.

Une fois que cette lettre prête (i-PDU construit), la couche i la soumet à la couche (i-1) pour lui demander un service de transmission. Le bloc fourni par la couche i à la couche (i-1) constitue le **i-SDU**. Ensuite, la couche i-1 met l'ensemble des feuilles dans une enveloppe sur laquelle figure l'adresse destinataire et l'adresse source, et d'autres informations liées au type d'envoi (lettre, express, etc). Là

aussi, nous constatons deux types d'informations : l'information utile (les feuilles contenant la demande d'emploi) et l'information de contrôle (adresse, type de courrier,etc) qui constitue l'en-tête de la couche i-1. Et ainsi de suite.

Donc, au fur et à mesure que les unités de données échangées sont traitées par une couche i, celle-ci leur ajoute un en-tête avant leur soumission à la couche (i-1). A la réception de ce bloc de données, l'entité homologue de niveau i effectue le traitement nécessaire et supprime cet en-tête avant de remettre les données restantes à la couche supérieure.

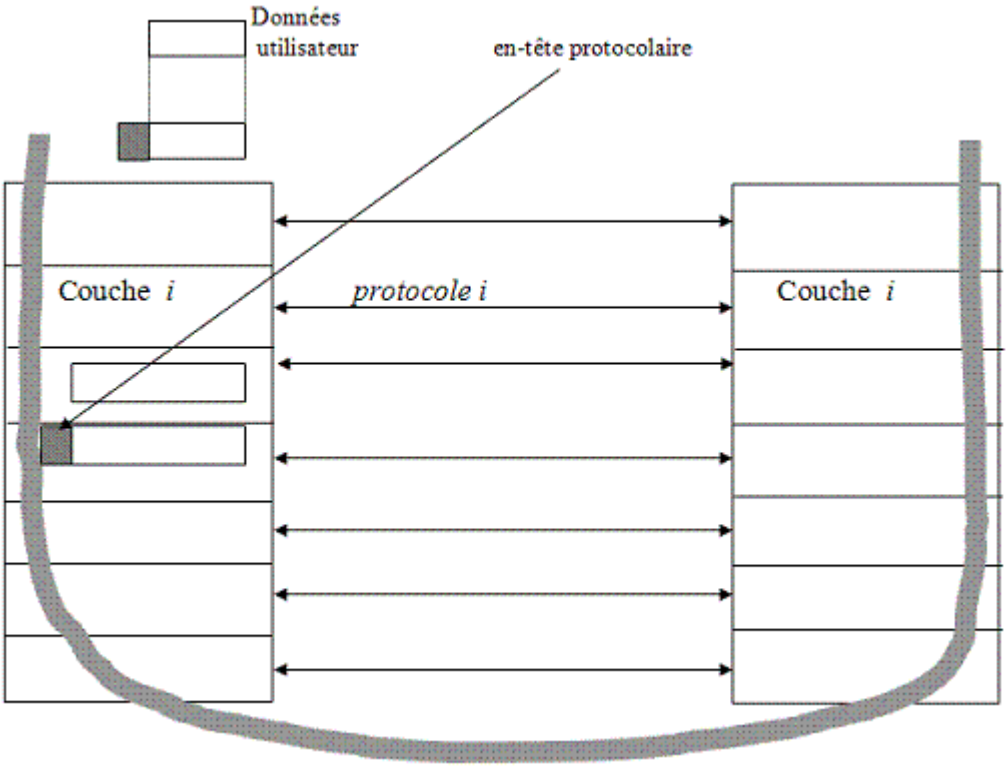


Image 3 Communication par protocole de niveau i

2. Les concepts d'une architecture en couches

De l'exemple donné dans la section précédente, nous remarquons qu'une couche i interagit avec les couches i+1 et i-1. On dit que la couche i rend service à la couche i+1 en s'appuyant sur les services de la couche i-1.

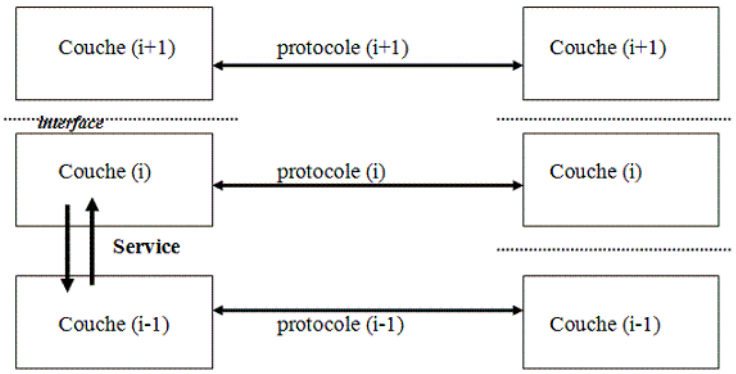


Image 4 Protocoles et interfaces entre les couches

Système N : est un composant constitué de matériels et de logiciels réseaux

comme une machine, un serveur, etc.

Pour résumer :

- Chaque couche i est composée d'une ou plusieurs **entités**.
- Les entités adjacentes communiquent à travers une frontière commune appelée **interface**.
- Les entités d'une même couche sont appelées entités **homologues**.
- Le point par lequel les couches adjacentes communiquent s'appelle **Point d'accès au service ou SAP (N-Service Access Point)**
- Deux entités homologues communiquent à l'aide d'un **protocole**
- La norme ISO a retenu une architecture en sept couches :
  - Chaque couche règle les problèmes non réglés par les couches inférieures
  - Chaque couche (N) rend des services (N) aux entités (N+1) en s'appuyant sur les services offerts par la couche (N-1).

Point d'accès au service ou SAP(N)

- Le Service Access Point ou SAP entre deux couches N et N+1 est le point où les services (N) sont fournis par une entité d'un sous-système (N) à un sous-système (N+1). Concrètement c'est l'information qui permet à une couche N d'identifier les entités de la couche (N+1) de manière à pouvoir fournir les données reçues à l'entité concernée au niveau (N+1).
- Chaque point d'accès peut être assimilé à une adresse du service.

Protocole de niveau (N)

- Comme défini précédemment, **un protocole** de niveau N est l'ensemble de règles et de formats prédéfinis déterminant les caractéristiques de communication de deux entités d'une couche (N). Sa mise en œuvre est effectuée à l'aide de l'échange d'un bloc de données appelé **PDU (Protocol Data Unit)** composé de l'en-tête protocolaire et des données soumises par le niveau N pour émission.
- La donnée remise par la couche N+1 à la couche N (et vice versa) s'appelle :

  Unité de Données du Service de niveau N : N-SDU (N-Service Data Unit)
- La donnée échangée entre deux couches N s'appelle :

  Unité de Données du Protocole de niveau N : N-PDU (N-Protocol Data Unit) .

  Nous utilisons souvent les termes : **trame** au lieu de DL-PDU (DL pour Data Link), **paquet** au lieu de N-PDU (N pour Network), et **segment** au lieu de T-PDU (T pour Transport)

3. Dialogue entre couches : la segmentation

Question : Dans le modèle décrit précédemment, est-ce que le SDU d'une couche x est le même que le PDU de cette couche. Autrement dit, est ce que x-SDU et x-PDU sont identiques ?

Réponse : la réponse est NON car :

- Il y a au moins des entêtes de protocoles qui vont être rajoutés aux x-SDU pour construire le x-PDU.
- Il y a aussi la possibilité de fragmentation du x-SDU par la couche x lorsque la couche (x-1) impose une taille maximum de données.

  Par exemple, la couche 2 d'Ethernet impose une taille maximum de données

égale à 1500 octets. Donc, toute couche 3 souhaitant soumettre un paquet à la couche Ethernet devra découper le bloc qu'elle a obtenu de la couche 4 s'il dépasse 1500 octets moins la taille de l'en-tête de niveau 3 à ajouter.

- Une couche x recevant de son niveau supérieur un x-SDU peut décider que la taille de celui-ci est trop grande pour être admise par le protocole de niveau (x-1).
- Dans ce cas, la couche x le découpe en fragments et chacun est destiné à être habillé d'un entête de protocole de façon à en faire un x-PDU.
- Les entêtes de protocole doivent contenir une information permettant de détecter si le x-PDU reçu contient un bout (début, fin, milieu) ainsi que la position de ce fragment dans le bloc total, ou bien s'il contient la totalité du x-SDU.

Fondamental

- Cette opération s'appelle **la fragmentation** ou **segmentation**.
- L'opération inverse est **le réassemblage**.

4. Dialogue entre couches : la concaténation

Question : X-PDU et (X-1)-SDU sont-ils identiques ?

Réponse : Fréquemment oui dans les couches inférieures (N-PDU et DL-SDU par exemple), théoriquement non.

Il existe une possibilité supplémentaire

- L'idée résulte du constat selon lequel il peut arriver que plusieurs X-PDU petits soient à transférer entre les deux mêmes couches X, alors que la couche X-1 est parfaitement capable d'échanger des données plus grandes.
- La couche X est alors capable de regrouper plusieurs X-PDU déjà formés dans un même (X-1)-SDU.
- La couche X-1 n'est au courant de rien et remet à la couche X distante le (X-1)-SDU complet.
- C'est cette dernière qui séparera les X-PDU les uns des autres.

Fondamental

- Cette opération est appelée **la concaténation**.
- L'opération inverse est appelée **la séparation**.

5. Dialogue entre couches : connexion et multiplexage

Mode connecté et mode non connecté

Chaque couche X peut dialoguer avec son homologue selon deux modes :

- Mode connecté : ce mode de communication se déroule en trois phases :

  (1) établissement de la connexion,

  (2) échange de données,

  (3) libération de la connexion.

  Ce mode permet en particulier d'offrir un service fiable grâce à l'implémentation de procédures de contrôle d'erreurs, de reprise sur erreurs, et de contrôle de flux. Il permet également la négociation de quelques paramètres de connexion comme la taille maximum des messages à échanger, la taille de la fenêtre (que nous expliquerons plus loin dans ce chapitre).

- Mode non connecté : dans ce mode, lorsqu'une entité souhaite envoyer des données, elle procède immédiatement à l'émission sans vérifier si le destinataire est disponible et d'accord pour recevoir les données, ni effectuer un contrôle d'erreurs et de flux.

Multiplexage

Il y a multiplexage d'un niveau X sur un niveau X-1 dès lors qu'il est possible d'avoir plusieurs connexions de niveau X empruntant la même connexion de niveau X-1.

Les entêtes protocolaires de niveau X contiennent une information permettant d'identifier la connexion de niveau X concernée parmi toutes celles qui utilisent la même connexion de niveau X-1.

D. Couche physique

1. Rôle de la couche physique

La couche physique reçoit de la couche liaison de données des trames manipulées comme une **succession de bits** et les envoie sur le support physique. Cette couche se charge donc de la transmission des signaux électriques ou optiques échangés entre deux couches liaison. Elle assure également le codage, la modulation, et dans certains cas comme le cas des réseaux locaux, on y trouve des services tels que la détection de collisions, etc.

C'est dans cette couche que sont définies les interfaces physiques, l'utilisation des câbles (type, tension, longueur ...), les communications hertziennes (fréquence, amplitude ...), les fibres optiques, etc.

Expliquer la transmission de données sur support physique nécessite la présentation de plusieurs notions, certaines théoriques comme les limites de la capacité d'un canal, le débit, la numérisation, etc. Nous présenterons ces principes et notions dans le chapitre "Transmission de données".

Nous reviendrons plus loin sur la couche physique dans les cas particuliers des réseaux locaux filaires et sans fil.

Dans cette couche on trouve : les interfaces de connexion ou jonctions, les modems, les multiplexeurs,...

E. Couche liaison de données

1. Fonction de la couche liaison de données

La couche liaison formate les données soumises par la couche supérieure, généralement la couche réseau, en trames. Elle s'appuie sur la couche physique pour émettre et récupérer (de la couche physique) les bits constituant la trame. La couche liaison gère l'échange de trames entre deux systèmes ou relais adjacents en assurant essentiellement **le contrôle d'erreurs** qui peuvent se produire lors de leurs transit dans le support physique. Éventuellement, la couche liaison peut assurer la reprise sur erreur par correction d'erreur ou par demande de retransmission de la trame erronée ainsi que le **contrôle de flux** afin d'offrir un service fiable.

La couche liaison formate les données en **trames** et calcul **l'information de contrôle** avant la transmission. A la réception, elle effectue une vérification si la trame reçue est correcte ou non. Dans certaines architectures, la couche liaison ignore les trames erronées et attend les suivantes et dans d'autres, la couche 2 réceptrice demande la retransmission de la trame erronée ou corrige les erreurs.

- Le découpage en trames peut être réalisé par :
  - insertion de silences
  - ajout d'un compteur d'octets
  - utilisation de caractères de début et de fin de trames

Les services offerts par la couche liaison peuvent être :

- sans connexion et sans acquittements : la couche 2 envoie les trames indépendamment les unes des autres vers la couche 2 homologue sans avoir établit préalablement une connexion. Si la couche 2 reçoit des trames correctes ou détecte des erreurs de transmission, elle ne donne aucune information au récepteur. En cas d'erreur, la trame est rejetée et se met en attente de recevoir la suivante. La couche 2 d'Ethernet en est un exemple.
- sans connexion et avec acquittements : ce service permet à l'émetteur de savoir si la trame qu'il a envoyé a bien été reçue ou non. Il s'agit donc d'un service plus fiable. Ce service est très utile dans les réseaux où les canaux sont peu fiables comme les liaisons sans fil. Le WIFI en est un exemple.
- avec connexion : il se déroule en trois phases (établissement de la connexion, échange de données, et libération de la connexion) et permet de garantir que chaque trame envoyée est reçue une seule fois, cela ne veut pas dire que les trames ne se perdent pas ou ne subissent pas des erreurs mais si un tel problème se produit, la couche liaison du récepteur le notifie à l'émetteur pour retransmettre la ou les trames ayant subit des erreurs (tout dépend du protocole conçu).

2. Contrôle d'erreurs

Lorsque la couche liaison aura formaté une trame, elle la soumet à la couche physique pour émission via le support physique. Lors du transit du signal correspondant au train de bits dans le support physique, des erreurs de transmission peuvent se produire à cause de différents phénomènes physiques comme le bruit, la diaphonie, etc. De plus, des situations de perte de trames peuvent se produire à cause du débordement du buffer de réception, ou autre raison.

Dans ce qui suit, nous présenterons les méthodes permettant de résoudre ces problèmes.

Coté émetteur

- Comment s'assurer que le récepteur a reçu correctement les trames ?

  Réponse : utilisation des acquittements (ACK) qui sont des messages envoyés par le récepteur pour notifier à l'émetteur la bonne réception de la trame
- Et si la trame n'est pas arrivée à destination ?

  - Utilisation de timer au bout duquel l'émetteur considère que la trame a été perdue

  - A l'expiration de ce timer, l'émetteur réémet la trame
- Et si la trame est bien arrivée à destination et l'acquittement n'est pas arrivé à l'émetteur?

  Réponse : comme l'émetteur considère que la trame a été perdue, il renvoie la même trame qui a déjà été bien reçue par le récepteur. En conséquence,

il y a donc réception de la trame en plusieurs exemplaires. Il est donc nécessaire d'ajouter un numéro aux trames.

Coté récepteur

La couche liaison applique un algorithme pour vérifier si la trame reçue est correcte ou non. Dans le cas où la trame reçue est erronée, deux solutions sont possibles :

a) correction d'erreurs de transmission : utilisation des codes correcteurs d'erreurs

b) demande de retransmission des trames erronées

Comme la correction d'erreurs nécessite d'importantes informations de contrôle et un traitement non négligeable, il est plus simple de demander à l'émetteur la retransmission de la trame erronée.

Pour effectuer le contrôle d'erreurs, la couche liaison génère, selon une méthode donnée, une information de contrôle appelée FCS (Frame Check sequence), ce qui permet au récepteur de vérifier si la trame reçue est correcte ou non.

Image 5 Une trame contient des bits de contrôle

3. Méthodes de détection d'erreurs (CRC)

Problématique

- Etant donné un train de bits à transmettre (coefficients d'un polynôme P)
- L'arithmétique utilisée dans cette méthode est faite modulo 2, c'est à dire :
  - Il n'y a pas de retenue dans l'addition et la soustraction
  - L'addition et la soustraction sont équivalentes à un OU EXCLUSIF.
- L'émetteur et le récepteur utilisent un même polynôme générateur G.
- Les bits de poids faible et de poids fort de G doivent être à 1.

Idée de l'algorithme

Coller à la fin de la trame des bits de contrôle de manière à ce que le polynôme P obtenu soit divisible (division modulo 2) par le polynôme G.

Quand le récepteur reçoit la trame, il divise le polynôme correspondant par G.

Si le reste de la division est non nul alors il y a erreur de transmission.

Algorithme

1. Soit r le degré du polynôme générateur G, ajouter r zéros après le bit de poids faible du bloc.
   Il contient ainsi m+r bits (correspondant au polynôme $x^rP(x)$)
2. Effectuer la division modulo 2 de la chaîne de bits correspondants au polynôme $x^rP(x)$ par la chaîne de bits correspondant au polynôme G(x)
3. Soustraire (modulo 2) le reste de la division de la chaîne de bits correspondant au polynôme $x^rP(x)$.

Le résultat de cette opération est la trame transmise au destinataire. Soit T(x) le polynôme correspondant.

Exemple de CRC normalisé (ISO)

CRC	C(x P(x)
CRC-8	$x^8 + x^2 + x^1 + 1$
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^1 + 1$
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + 1$
CRC-16	$x^{16} + x^{15} + x^2 + 1$
CRC-CCITT	$x^{16} + x^{12} + x^5 + 1$
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Image 6 CRC normalisé

4. Contrôle de flux

Problème

Nous allons étudier ce problème en considérant la couche liaison mais il est important de noter qu'un mécanisme de contrôle de flux peut être mis en place dans la couche réseau et la couche transport.

Lorsqu'un émetteur envoie de façon systématique plus de trames que le récepteur ne peut en accepter, cela peut produire des situations de perte de trames. Il est donc nécessaire de mettre en place un mécanisme permettant d'adapter le débit d'émission afin que le récepteur puisse traiter toutes les données reçues sans en perdre.

Solution

Pour mettre en place un contrôle de flux, deux approches sont possibles :

- **envoyer et attendre :** avec cette technique, l'émetteur ne peut procéder à l'émission de la trame suivante qu'après la réception d'une permission envoyée par le récepteur.
- **Fenêtre à anticipation (Crédit) :** cette méthode permet à un émetteur d'envoyer une quantité donnée d'octets ou un nombre donné de trames (selon le protocole) sans être obligé d'attendre un accusé de réception pour chaque trame. Ce nombre est défini soit de manière statique par configuration ou négocié lors de l'établissement de la connexion si le protocole fonctionne en mode connecté.

Définition

On appelle **crédit** le nombre maximum k de messages qui, vu de l'émetteur, peuvent être en cours d'acheminement à un instant donné. Dans certains protocoles, le crédit peut être une quantité d'information (en octets).

Définition

On appelle **fenêtre** l'intervalle des numéros de messages en cours

d'acheminement, c'est à dire l'intervalle des No de messages envoyés et pour lesquels un accusé de réception n'a pas été encore reçu.

F. Couche réseau

La couche réseau assure l'acheminement des paquets et la détermination d'un chemin entre des systèmes relais. Cette fonction se base sur le fait qu'à chaque machine du réseau est associée une **adresse**, qui est généralement unique. Nous verrons dans le chapitre "adressage IP" le cas particulier où une adresse peut ne pas être unique (adressage privé).

L'acheminement des paquets se fait à l'aide d'une table de routage qui indique l'adresse du prochain nœud vers lequel le paquet devra être relayé afin d'atteindre le nœud destinataire.

Il existe deux principales méthodes de routage : le mode **circuit virtuel** qui est basé sur un mode connecté et le **mode datagramme** ou mode non connecté

1. Modes utilisés

Mode circuit virtuel

- Dans le mode de communication par circuit virtuel, un chemin logique ou circuit virtuel est une **connexion logique** établie entre deux sites à travers le réseau. Tous les paquets envoyés de la source vers le destinataire empruntent ce chemin, en conséquence, les paquets arrivent dans l'ordre de leur émission.
- Généralement, avec ce mode circuit virtuel, des mécanismes permettant d'assurer la fiabilité des échanges sont implémentés. Le circuit virtuel procure donc à la couche transport un canal où il n'y a ni erreur, ni duplication.
- Le circuit virtuel est établi pour toute la durée de transfert sauf si des problèmes de déconnexion apparaissent. Dans ce cas, il est nécessaire de relancer la connexion.
- Trois étapes interviennent dans une communication par circuit virtuel :
  a. **Etablissement du CV :** un paquet d'appel, contenant l'adresse de l'émetteur et celle du destinataire, envoyé de l'émetteur vers le destinataire trace le circuit virtuel en générant des **No. de voie logique** sur les liens physiques traversés.
  b. **Transfert des paquets de données :** tous les paquets de données passent par le chemin tracé. Les paquets de données ne contiennent pas les adresses source et destination complètes mais seulement le n°. de voie logique.
  c. **Libération du CV :** un des deux interlocuteurs demande à l'autre de mettre fin à cette communication, ce qui induit la fermeture du circuit virtuel.

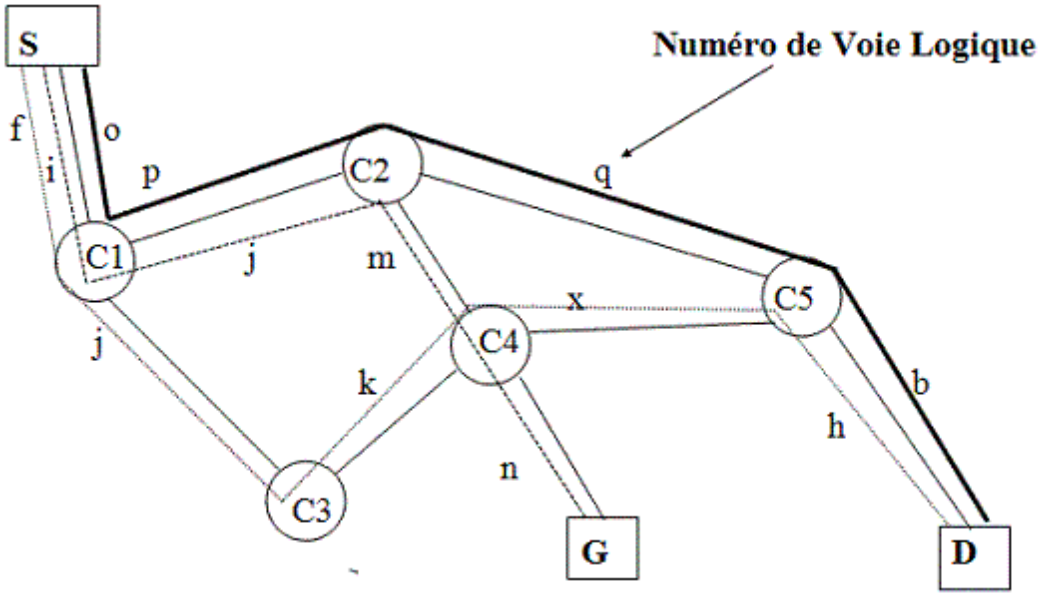


Image 7 Circuit virtuel

Un circuit virtuel est une cascade de voies logiques

Mode non connecté ou Datagramme

Dans la communication en mode datagramme, les paquets portent l'adresse source et l'adresse destination. Ils sont transmis indépendamment les uns des autres et sont envoyés de façon isolée de la source vers le destinataire en se basant sur les informations indiquées dans la table de routage. Lorsque la couche réseau reçoit un paquet, elle examine l'adresse destinataire se trouvant dans l'en-tête du paquet. Si l'adresse de destination n'est pas celle de ce nœud, alors la table de routage est consultée afin de déterminer par quelle interface de sortie ce paquet devra être envoyé au prochain nœud se trouvant sur le chemin qui mène vers le nœud destinataire. Ensuite ce paquet est soumis à la couche liaison qui se charge de sa transmission. Les méthodes de construction et de maintien des tables de routage sont présentées dans la section suivante.

Dans une communication en mode datagramme, les paquets d'un même message peuvent arriver dans le désordre et sont parfois perdus. De plus ce mode n'intègre pas de mécanisme de contrôle de flux. En conséquence il n'y a pas de garantie sur le transfert des paquets.

2. Le routage

Dans le routage on distingue deux opérations :

Détermination du chemin ou algorithme de routage

Cette opération consiste à calculer les chemins dans le réseau. Elle est réalisée à l'aide d'algorithmes de routage qui peuvent être statiques ou dynamiques.

Avec le routage statique, les routes sont définies manuellement et ne pourront pas changer sans intervention humaine. Ce mode n'est pas adapté aux grands réseaux car une panne d'un lien ne permet pas de rerouter les paquets par un autre chemin disponible. Quant au routage dynamique, celui-ci est mis en œuvre grâce à des algorithmes distribués exécutés sur l'ensemble des nœuds. Les échanges d'information d'accessibilité permettent aux nœuds de mettre à jour leur table suite à la découverte d'une route plus intéressante (en terme de la métrique utilisée qui

est généralement le nombre de sauts) ou à la détection de panne d'un voisin.

Acheminement

Cette opération est déclenchée lors de la réception d'un paquet par un nœud.

Elle consiste à examiner l'en-tête du paquet (pour obtenir l'adresse destination), consulter la table de routage pour obtenir le canal de sortie par lequel il faudra envoyer le paquet, et mettre le paquet dans la file d'attente de sortie du canal.

3. La congestion

Lorsque les échanges de paquets s'intensifient, on peut constater une dégradation des performances globales suite à l'incapacité des nœuds relais à gérer un trop grand nombre de paquets entrants. Des paquets seront donc rejetés, et en conséquence, ne seront pas délivrés à destination. On parle alors de situation de congestion. Ces congestions peuvent se produire également car les équipements intermédiaires sont lents ou leurs mémoires tampons sont saturées.

Pour y remédier, des mécanismes de contrôle de congestion doivent être mis en place. Pour plus d'efficacité, il sont implémentés dans la couche transport.

G. Couche transport

1. Fonctions

La couche transport s'appuie sur la couche réseau pour offrir un service de transport de bout en bout entre deux machines. Ce service fourni aux applications à l'aide d'interfaces (APIs) est indépendant du réseau mis en place. La couche transport peut offrir un service qui peut être en mode connecté ou en mode non connecté.

2. Sockets de Berkeley

L'interface de programmation entre les applications (communication inter-processus) via la couche transport de l'Internet (protocoles TCP et UDP) est appelée socket. Pour créer une connexion entre deux processus s'exécutant sur deux machines connectées via un réseau (un client et un serveur), les sockets réseau permettent de gérer les flux échangés entre processus à l'aide d'APIs (Application Programming Interface). Le rôle d'API est de contrôler et d'utiliser les sockets réseau.

La socket de Berkeley (BSD, Berkeley Software Distribution), créée dans les années 80, est une interface du système UNIX. D'autres APIs existent comme :

- L'API sockets sous Windows est baptisée WinSock.
- TLI - Transport Layer Interface : est une interface créée par AT&T standardisée comme XTI (X/Open Transport Interface)

peut fonctionner avec la pile TCP/IP

H. Couche session

1. Fonctions

- Spécifie les règles et la synchronisation du dialogue entre deux processus d'application.
- Assure la négociation du protocole d'échange
- Assure l'établissement, le maintien, la rupture de liens logiques de communication.
- Le protocole de session doit fournir des mécanismes qui permettent la détection d'erreurs et d'incidents même si le réseau est fiable.

2. Services fournis par la couche session

Les principaux services susceptibles d'être offerts par la couche session à la couche présentation dans un modèle avec connexion sont :

Gestion de la connexion

Réalise l'établissement, le maintien, et la libération des connexions de session. Au moment de l'établissement de la connexion, il y a négociation pour fixer les paramètres. Par exemple :

- Sélectionner les unités fonctionnelles mises en œuvre sur la connexion
- Les paramètres de qualité de service.

La libération de la connexion peut être normale ou anormale.

3. Etablissement des connexions de session

Permet aux correspondants de s'assurer de leur existence mutuelle et comprend :

- **L'affectation d'une connexion de transport** à une connexion de session est effectuée par réutilisation d'une connexion de transport existante ou par établissement d'une nouvelle connexion de transport.
- **La mise en correspondance des adresses de transport et de session** : concerne l'adressage au niveau session. Elle est effectuée uniquement lorsque la correspondance entre les connexions de session et de présentation n'est pas biunivoque.
- **L'identification de la connexion** : consiste à affecter à la connexion un paramètre qui la désigne de façon unique.
- **le transfert éventuel des identificateurs de SSAP** de l'appelant et de l'appelé est effectué lorsque les adresses de session et de transport sont distinctes.
- **choix des paramètres de qualité de service**.
- **la négociation des paramètres de session** est effectuée pour déterminer les modes d'exploitation et les facilités offertes aux utilisateurs sur la connexion. La négociation porte sur les points suivants :
  - numéro de version du protocole de session
  - unités fonctionnelles
  - attribution initiale des jetons
  - taille maximum de TSDU
- **transfert de données liées à l'initialisation** concerne le transfert des identificateurs de SSAP de l'appelant et de l'appelé au moment de l'établissement de la connexion.

I. Couche présentation

1. Fonctions

La couche présentation fournit les "**représentations syntaxiques**" de référence communes à deux applications pour qu'elles puissent communiquer. Elle permet de résoudre les problèmes des différences de représentation des données.

Il est possible aussi que des applications utilisent un véritable langage de description de données à l'aide de règles de représentation des données pour le transfert entre applications en réseau. Le standard ISO ASN.1 est un exemple utilisé dans le cadre des applications de gestion de réseau. De plus, la couche présentation pourrait aussi fournir des services de chiffrement de l'information.

Il est important de noter que souvent (dans les architectures d'aujourd'hui), les fonctionnalités de cette couche sont souvent intégrées directement dans les logiciels d'application.

Normes et recommandation

- ISO 8859, également appelée plus formellement ISO/CEI 8859, est une norme commune de l'ISO et de la CEI de codage de caractères sur 8 bits pour le traitement informatique du texte.

  ISO 8823 - Protocole de présentation.
- X400 - Transfert fiable pour messagerie.

  Une messagerie électronique consiste en une distribution de messages entre des utilisateurs reliés entre eux et à partir de leurs postes de travail informatique. L'Echange de Données Informatisé (EDI) peut être défini comme l'échange d'ordinateur à ordinateur de données concernant des transactions commerciales en utilisant des réseaux et des formats agréés.

  Les recommandations X400 peuvent être choisies comme mécanisme de transmission de données pour l'EDI, la taille des fichiers EDI échangés étant de l'ordre de grandeur, de celle des messages échangés entre humains.

  La série de recommandations X400 définit une norme internationale pour la structure et la transmission de messages de courrier électronique.

J. Couche application

La couche application fournit les services et les protocoles nécessaires aux applications qui souhaitent communiquer/utiliser le réseau. A noter que ces applications elles-mêmes ne font pas partie de la couche application.

Les exemples de protocoles de la couche application les plus connus sont HTTP(pour naviguer sur le web), FTP (pour le transfert des fichiers) et SMTP (pour le transfert de messages électroniques).

1. Protocoles de transfert de fichiers

- Le protocole de transfert de fichiers FTP permet le transfert d'un fichier d'un système à un autre.
- FTP peut être une application "pure" du modèle OSI comme elle peut contenir des fonctionnalités de présentation et parfois des éléments de la

couche session.

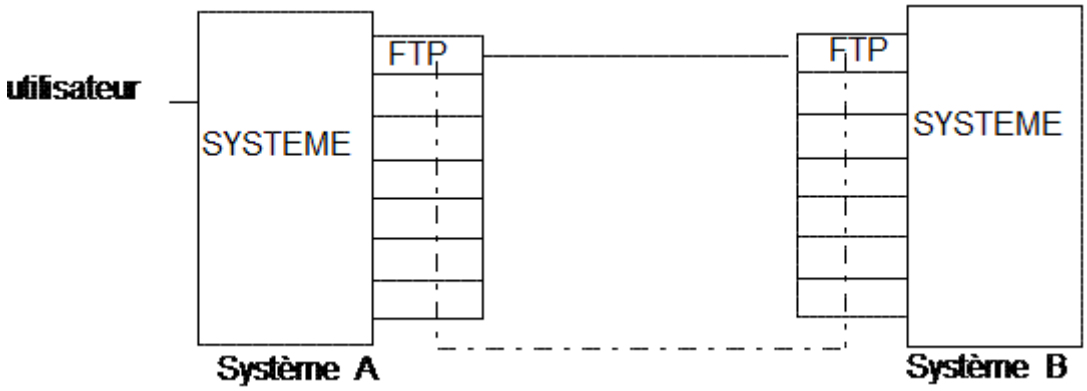


Image 8 Ici FTP est une application purement OSI

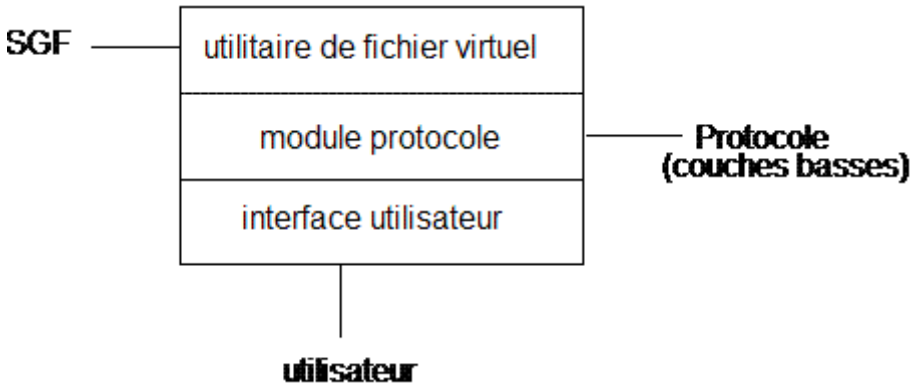


Image 9 Relation entre utilisateur, protocoles et SGF

Un utilisateur sur la machine A peut demander le transfert de fichier de :

- la machine A vers la machine B.
- la machine B vers la machine A.
- la machine B vers une autre machine C.

FTP permet de transférer des fichiers entre systèmes hétérogènes.

La représentation (ou le format) des fichiers est souvent différente d'un système à un autre. La structure des fichiers doit être donc connue par FTP.

Afin d'éviter de connaître les M*N structures, une structure générale appelée **fichier virtuel** est définie. La conversion d'un fichier local en un fichier virtuel est faite soit par FTP soit par un module de présentation.

2. Messagerie X400

- X400 est un standard de messagerie électronique.
- X400 intervient dans toutes les phases
  - de la vie d'un message.
  - de la décision d'envoi par l'émetteur à la mise à la corbeille du message reçu par le destinataire.

Phases d'un système de messagerie

1. La composition : la construction des messages et des réponses.
2. Le transfert : l'acheminement de l'information de l'émetteur vers le récepteur.
3. La phase d'information : informer l'émetteur si son message a été remis, rejeté, ou perdu.

4. La conversion : permet l'affichage correcte des informations.
5. La mise en page.
6. La remise.

Modèle fonctionnel de X400

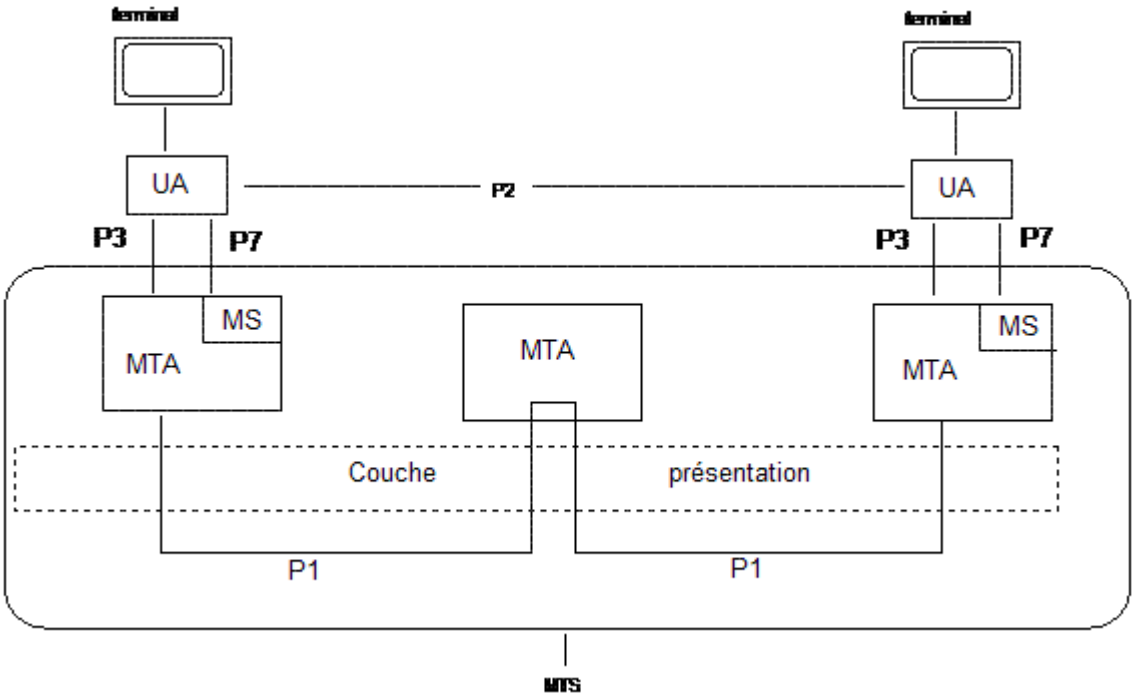


Image 10 X400

Terminologie

- **UA** : Agent utilisateur
- **MS** : Mémoire de stockage des messages
- **MTA** : Agent de transfert de messages
- **MTS** : Système de transfert de messages
- **Agent utilisateur** : est un programme qui fournit une interface avec le système de messagerie. il permet :
  - La composition des messages
  - L'envoi et la réception de messages
  - La gestion des boites aux lettres
- **Agent de transfert de messages** : reçoit le courrier préparé par l'agent utilisateur et se charge de son acheminement. C'est un centre de tri électronique.

  Les boites aux lettres sont gérées par les **mémoires de stockage**. Les messages entrants sont stockés dans les boites aux lettres en attente de lecture, de destruction, de renvoi, de chargement lors de la connexion de l'agent utilisateur.

Exemple

P1, P3 et P7 sont des protocoles d'échange.

3. Administration des réseaux

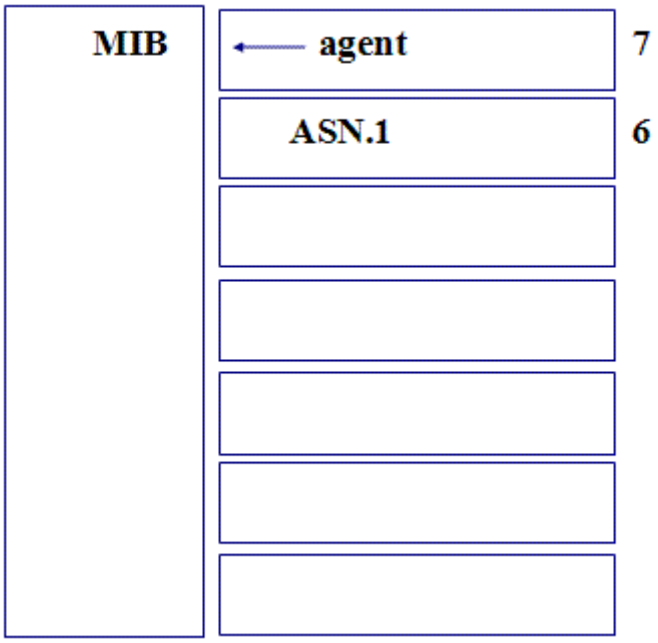


Image 11 Management Information Base

Principe

Le terme **administration de réseaux** recouvre l'ensemble des fonctions qui sont nécessaires pour :

- L'exploitation
- La sécurité
- Le suivi et l'entretien du réseau

Les actions de l'administrateur réseau

Il réalise trois grands types d'actions :

- **Des actions temps réel** pour connaître l'état de son réseau (charge,...) et agir sur celui-ci, assurer la sécurité.
- **Des actions différées** pour planifier, optimiser, quantifier et gérer les évolutions du réseau (statistiques, comptabilité,...)
- **Des actions prévisionnelles** qui lui permettent d'avoir une vision à moyen et long terme et d'évaluer des solutions alternatives.

Vocabulaire et concepts

Agent : est un programme exécuté sur un équipement que l'on veut administrer. Il est interrogé à distance et fournit les informations ou exécute les instructions demandées.

Plate-forme d'administration : ce logiciel, souvent graphique, interroge, via un protocole d'administration les agents et présente les résultats à l'administrateur.
Bases de données : toutes les informations concernant le réseau à gérer sont stockées dans des bases de données qui peuvent être :

- **MIB (Management Information Base)** : décrit les objets gérés dans les équipements. Cette description donne le type, le format, et la taille des objets. Les valeurs de ces objets sont stockées dans les registres internes de l'équipement.

Bases de données de la plate-forme : contiennent par exemple la topologie et la description des équipements du réseau. Elle peuvent contenir aussi les valeurs qui viennent d'être calculées ou un historique pour des études statistiques.

Protocole SNMP (Simple Network Management Protocol)

- Conçu pour être simple.
- Prévu pour des petits sites (SNMPv2 ou CMIP pour des sites plus importants).
- Permet d'ajouter, de modifier ou d'effacer des paramètres dans les équipements réseaux.
- Trois types d'interactions sont définis :
  a. **Interrogations** : produites par la plate-forme, permettent de demander la valeur d'un paramètre ou de plusieurs éléments dans la base de données de l'agent.
  b. **Mises à jour** : produites par la plate-forme, permettent d'affecter une nouvelle valeur dans les objets gérés par un agent.
  c. **Les alarmes** : initiées par l'agent, elles indiquent aux plates-formes l'occurrence d'un événement exceptionnel. L'agent doit être au préalable configuré avec la liste des plates-formes à contacter

Différentes catégories de réseaux peuvent être dénombrées.

On en compte généralement cinq, différenciées par la distance maximale entre les deux points les plus éloignés.

Internet, Intranet, TCP-IP et IPv6

II

A. Introduction

1. Historique

Les grandes dates

L'objectif principal de la famille TCP-IP est la construction d'une interconnexion de réseaux ou bien la construction d'un réseau de réseaux, d'où le terme Internet pour Internetworking. Ce réseau permet à des équipements interconnectés par des réseaux physiques hétérogènes de communiquer de manière transparente.

Quelques dates importantes :

- 1970 : Début des travaux.
- 1977-1979 : Les protocoles ont pris forme.

- 1980 : Apparition de l'Internet.

2. Les instances de régulation de l'Internet

Contrairement aux réseaux propriétaires,TCP-IP est devenu populaire auprès des développeur et des utilisateurs grâce à son ouverture et son évolution perpétuelle. N'importe qui peut commenter ou proposer un standard, connu sous le nom de RFC. Pour devenir un standard officiel Internet, un document définissant un protocole ou un aspect quelconque de TCP-IP doit subir une procédure d'évaluation et de ratification.

Quiconque désirant contribuer à l'effort de recherche peut tester et commenter les documents. Les instances de régulation de l'Internet sont les suivantes :

- **Internet Society** : A pour but de promouvoir l'évolution et la croissance de l'Internet en tant qu'infrastructure globale de recherche.

  Ce consortium est composé de plusieurs groupes : IAB, IETF, IESG, IRTF, IANA.
- **Commission d'activité Internet** (**IAB : Internet Activity Board**), créée en 1983.

  Elle assure l'orientation de la coordination de la plus grande partie de la recherche et des développements relatifs aux protocoles TCP/IP.
- **Internet Engineering Task Force** (**IETF**) : Est le groupe de standardisation à court terme, divisé en 9 zones (application, routage et adressage, sécurité,...). Il fut gouverné par l'IESG

  Chaque zone est formée de groupes de travail qui étudient des sujets techniques et discutent de nouvelles spécifications, et la proposition de nouveaux standards.
- **Internet Steering Group** (**IESG**) : il fut constitué afin d'aider la direction de l'IETF. Il est composé de responsables de l'IETF et de directeurs de zones de tous les groupes de travail. C'est après ses recommandations que l'IAB ratifie un standard.
- **Internet Research Task Force** (**IRTF**) : effectue les investigations à long terme sur les publications techniques qui ne sont pas nécessairement évoquées dans les documents devant être ratifiés.

3. Internet Request For Comment (RFC)

Le processus de standardisation de l'Internet (RFC 2026) concerne tous les protocoles, les procédures et les conventions utilisées dans et par l'Internet quoi qu'ils fasse partie ou non de la famille TCP-IP.

- Les RFC constituent les standards officiels de la communauté Internet
- Beaucoup de RFC ne sont pas des standards
- Toutes les RFC sont disponibles gratuitement.

Les spécifications de standards Internet

Les spécifications soumises au processus de standardisation Internet peuvent être des spécifications technique (TS : Technical Specification) ou des déclarations d'applicabilité (AS : Applicability Statement).

Une spécification technique est la description d'un protocole, d'un service, d'une procédure, d'une convention ou d'un format. Elle peut décrire la totalité des aspects pertinents de son sujet ou laisser un ou plusieurs paramètres ou options non définis.

Une déclaration d'applicabilité définit comment et dans quelles circonstances une ou plusieurs spécifications techniques sont appliquées pour soutenir une capacité

Internet particulière. Une déclaration d'applicabilité peut définir des utilisations pour des spécifications techniques qui ne sont pas des standards Internet,

Une déclaration d'applicabilité appliquera l'un des « niveaux d'exigence » (requirement levels) suivants à chaque spécification technique à laquelle elle se rapporte :

(a) Obligatoire (Required) : une mise en œuvre de la spécification technique référencée, comme défini par la déclaration d'applicabilité, est tenue d'atteindre une conformité minimale. Exemple, tous les systèmes Internet utilisant la suite de protocoles TCP/IP doivent mettre en œuvre les protocoles IP et ICMP.

(b) Recommandé (Recommended) : Les vendeurs sont vivement encouragés à inclure dans leurs produits les fonctions, les caractéristiques et les protocoles des spécifications techniques recommandées, et ils ne devraient les omettre que si cela est justifié par des circonstances particulières. Par exemple, tous les systèmes utilisant un accès distant devraient mettre en œuvre le protocole TELNET.

(c) Électif (Elective) : une mise en œuvre de la spécification technique référencée est optionnelle dans le domaine d'application de la déclaration d'applicabilité, c'est-à-dire que la déclaration d'applicabilité n'établit aucune nécessité explicite d'appliquer la spécification technique. Toutefois, un vendeur particulier peut décider de la mettre en œuvre, ou un utilisateur particulier peut décider qu'elle est nécessaire dans un environnement spécifique.

Il y a des spécifications techniques qui sont hors du circuit des standards ou qui en ont été retirées, et qui ne sont donc pas obligatoires ni recommandées ni électives. Deux autres appellations de niveau d'exigence sont disponibles pour ces spécifications techniques :

(d) Utilisation limitée (Limited Use) : l'utilisation de la spécification technique est considérée comme appropriée uniquement dans des circonstances limitées ou uniques. Par exemple, l'utilisation d'un protocole avec l'appellation Experimental devrait généralement se limiter à ceux impliqués activement dans l'expérience.

(e) Non recommandé (Not Recommended) : une spécification technique considérée comme inappropriée pour une utilisation générale est étiquetée « Non recommandée ». Cela peut être à cause de sa fonctionnalité limitée, de sa nature spécialisée ou de son statut historique.

Au fur et à mesure, quelques protocoles sont dépassés par d'autres. Ils deviennent historiques.

4. Modèle en couches

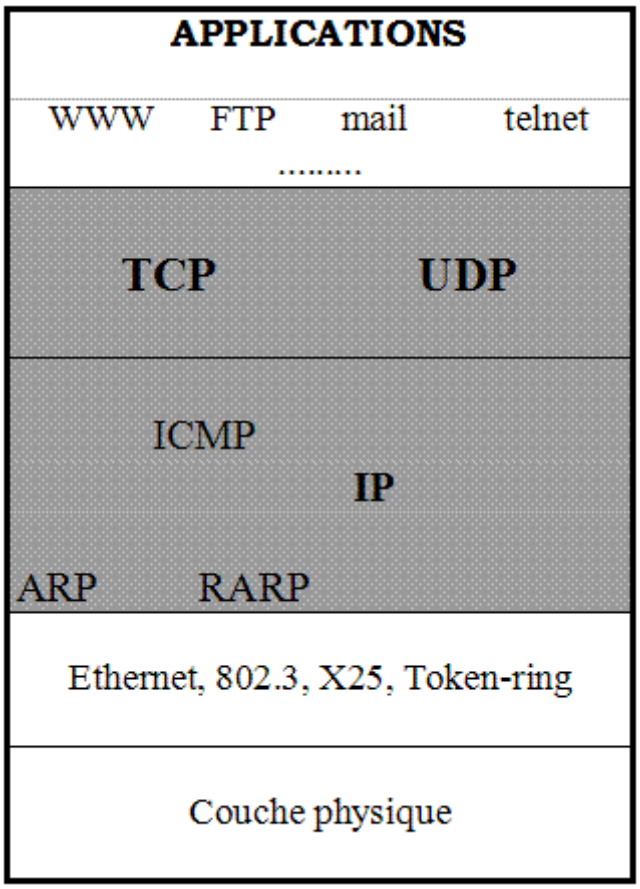


Image 12 Modele en couches

B. Adressage

1. Classes d'adresses IP

L'adressage IP est décrit dans la RFC 1166. Pour pouvoir identifier un nœud du réseau Internet, il est necessaire de lui attribuer une adresse réseaux ou adresse IP

Une adresse IP (sur 32 bits) comprend un identificateur de réseau et un identificateur de machine dans ce réseau.

nom_réseau	*id_machine.*

Image 13 Composition d'une adresse IP sur 32 bits

Les adresses IP sont représentées sous forme de quatre entiers décimaux séparés par un point décimal.

- Adresse IP : 10000000 00001010 00000010 00011110
- Adresse en décimal : 128.10.2.30

Une adresse IP peut être de classe A, B ou C.

- Adresse classe A (1.x.x.x à 127.x.x.x)

0	*id_réseau (7 bits)*	*id_machine(24 bits)*

- Adresse classe B (128.0.x.x à 191.255.x.x)

1	0	*id_réseau (14 bits)*	*id_machine (16 bits)*

- Adresse classe C (192.0.0.x à 223.255.255.x)

1	1	0	*id_réseau (21 bits)*	*id_machine (8 bits)*

- Adresse classe D

1	1	1	0	*Adresse multicast*

- Adresse classe E

1	1	1	1	*Réservée*

Image 14 Classes d'adresses IP

2. Adresse de réseau et adresse de diffusion

Convention 1

Un identificateur de machine égale à zéro :

- n'est jamais affecté à une machine
- sert à référencer le réseau lui même
- utilisé comme adresse source lors du démarrage

Convention 2

Une adresse de diffusion :

- identifie toutes les machines du réseau
- tous les bits de id_machine sont à 1

Diffusion dirigée

Pour effectuer des diffusions dirigées, il faut que les routeurs soient configurés pour transmettre les diffusions dirigées.

Broadcasting

- L'adresse broadcast 255.255.255.255 est utilisée dans les réseaux à diffusion (Ethernet, Token-Ring)
- Les routeurs ne font pas suivre le paquet (sauf avec l'option BOOTP forwarding)

Multicasting

- Chaque groupe a une adresse de groupe sur 28 bits
- Plage d'adresses de groupe : 224.0.0.0 à 239.255.255.255

3. Gestion des adresses Internet

- Toutes les adresses de réseau sont affectées par une autorité centrale.
  - Centre d'information du réseau Internet (InterNIC : Network Information Center).
- L'autorité n'affecte que l'adresse réseau de l'adresse IP et délègue l'affectation des adresses machines à l'organisation concernée.

4. Internet privé

Une des solutions permettant de résoudre le problème de pénurie d'adresses est la définition d'un adressage privé.

La RFC 1597- Address allocation for private Internets- relaxe la contrainte de l'unicité de l'adresse.

L'utilisation de l'adressage privé se limite au sein d'une institution qui ne nécessite pas forcément une connexion à l'Internet.

Les nœuds ayant uniquement des adresses privé n'ont pas une connectivité IP directe à l'Internet. Il communiquent, via un une passerelle (proxy) ou une opération de translation d'adresse appelée NAT (Network Address Translation). Le NAT permet de réaliser une mise en correspondance entre une adresse privée et une adresse publique (routeur de connexion avec l'internet).

Trois plages d'adresses ont été réservées par l'IANA à cet effet :

- 10 : un réseau de classe A
- 172.16 à 172.31 : 16 réseaux classe B
- 192.168.0 à 192.168.255 : 256 réseaux de classe C

Ces plages d'adresse ne sont pas routable.

5. Sous adressage

Le processus de segmentation d'un réseau IP en sous-réseaux de plus petites taille consiste à définir un sous-adressage. Cela permet :

- la réduction de la taille des tables de routage,
- de faciliter l'administration du réseau,
- de définir un autre niveau d'hiérarchie

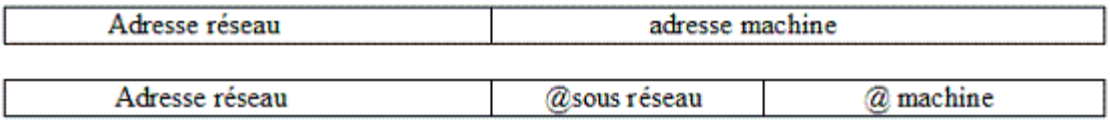


Image 15 ajout d'un niveau de hierarchie

- Pas de visibilité de l'extérieur.

Exemple

Considérons un réseau comprenant deux réseaux physiques.

- Seuls les routeurs savent qu'il existe deux réseaux physiques.
- Les routeurs des autres systèmes routent le trafic comme s'il n'y avait qu'un seul réseau physique.

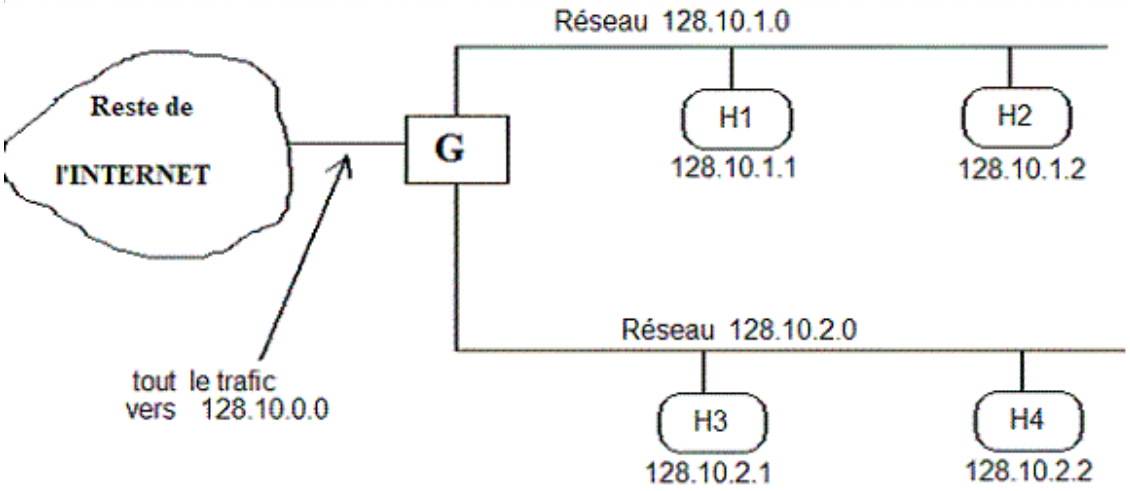


Image 16 Sous-adressage

- Tous les routeurs de l'Internet (sauf G) routent les datagrammes vers ce sous-réseau de la même façon
- L'administrateur affecte une adresse de la forme 128.10.1.x aux machines du premier sous-réseau, et 128.10.2.x aux machines du second sous-réseau.
- Pour sélectionner le sous-réseau, G examine le troisième octet de l'adresse destination et route les datagrammes contenant la valeur 1 vers le réseau 128.10.1.0

6. Réalisation du sous-adressage avec les masques

- Les bits du masque de sous-réseau sont à :
  - '1' si le réseau traite les bits correspondants de l'adresse IP comme faisant partie de l'adresse réseau.
  - '0' si le réseau les traite comme un identificateur de machine.
- Le masque de réseau 11111111 11111111 11111111 00000000 indique que :
  - **les trois premiers octets identifient le réseau** y compris le sous-réseau
  - **le quatrième octet identifie une machine sur ce réseau.**

Cette méthode permet de définir des masques réseaux statiques, c'est à dire le nombre de machines adressables par sous-réseau est le même.

Variable Length Subnet Masks (VLSM)

Lorsque la taille des sous-réseaux composant le réseau IP diffère d'un sous-réseau à un autre, il est possible de définir différents masques : un sous réseau peut être éclaté en deux parties en ajoutant un autre bit (de la partie Id_machine) à la partie sous-réseau. Cela permet ainsi de construire des sous réseaux de plus petite taille si besoin, ce qui éviterait le gaspillage d'adresses.

Exemple d'adressage VLSM

Considérons une entreprise ayant une adresse de classe C. Cette entreprise a besoin de définir cinq sous-réseaux dont les tailles sont les suivantes (en nombre de machines par sous-réseau) :

Sous-réseau 1 : 50 nœuds

Sous-réseau 2 : 50 nœuds

Sous-réseau 3 : 50 nœuds

Sous-réseau 4 : 30 nœuds

Sous-réseau 5 : 30 nœuds

Problème : Avec un sous-adressage statique, il n'est pas possible de répondre à ce besoin car :

- si on utilise 2 bits pour coder les sous-réseaux afin de pouvoir définir 50 adresses de machines dans chacun (6 bits ID_machine sont nécessaires), cela ne nous permettra pas de définir 5 sous-réseaux.

- si on prends 3 bits pour coder les 5 sous réseaux (il en restera 3 bits), chaque sous-réseau pourra adresser 30 machines maximum, ce qui ne répond pas au besoin définit plus haut.

Solution : Définir plusieurs masques

- En utilisant le masque 255.255.255.192 (2 bits sont utilisés pour le sous-réseau), le réseau pourra être organisé en quatre sous-réseaux et chacun peut accueillir 62 nœuds.

- Le quatrième sous-réseau, peut ensuite être divisé en deux sous-réseaux et chacun peut accueillir 30 hosts en utilisant le masque 255.255.255.224 (en prenant un bit supplémentaire de la partie Id_machine).

Ainsi, il y aura donc trois sous-réseaux ayant chacun 62 machines et deux sous-réseaux ayant chacun 30 machines. Cela satisfait bien les exigences de l'énoncé et évite le gaspillage d'adresses.

7. Adressage CIDR

Constat :

- Les adresses de classe A et B viennent à manquer.
- Les adresses de classe C disponibles sont en nombre appréciable.
- Les organisations de grande taille ayant plus de 254 machines se voient forcées d'utiliser plusieurs adresses de classe C.

Solution : définir un adressage de surréseau, appelé CIDR (RFCs 1518 à 1520), qui consiste à affecter un bloc d'adresses de classe C plutôt qu'une adresse de classe B.

----> Utilisation plus rationnelle des adresses.

- L'adressage surréseau ou CIDR est conçu pour les fournisseur d'accès.
- L'adressage sur-réseau réduit la taille des tables de routage
- CIDR permet de résumer un bloc d'adresses de classe C en une seule entrée dans la table de routage.
  - <adresse de base du bloc, masque de surréseau>
  - **Adresse de base du bloc** : adresse de départ du bloc
  - **Masque de surréseau** : C'est le nombre d'adresses de classe C dans ce bloc. Il contient des "1" pour le préfix commun à toutes les adresses de classe C et des "0" pour les parties propres à chacune des classes. : adresse de départ du bloc

  Autre notation : une adresse CIDR peut être écrite aussi sous le format <adresse de base du bloc>/x, où x est le nombre de bits à 1 dans le masque de surréseau.

Exemple

Soit l'entrée de la table de routage <200.1.160.0, 255.255.224.0> ou 200.1.160.0/19

Adresse de base : 200.1.160.0

Masque CIDR : 255.255.224.0

@ : **11001000.00000001.101**00000.00000000
masque : 11111111.11111111.11100000.00000000
L'intervalle d'adresses de classe C est donc :
a1 : **11001000.00000001.10**100000.00000000 = 200.1.160.0
...
af : **11001000.00000001.10111111**.00000000 = 200.1.191.0

C. IP sur LAN

1. ARP : Address Resolution Protocol

Lorsque des machines sont connectées sur un réseau local ou LAN, celles-ci sont identifiées par des adresses physiques, appelées aussi adresses MAC. Si une machine A s'apprête à envoyer un paquet IP à une machine B, connectée sur le même LAN, dont elle connaît l'adresse IP, la machine A doit obtenir l'adresse MAC de la machine B pour qu'elle puisse solliciter sa couche 2 pour transmettre le paquet. Il est donc nécessaire de déterminer un moyen permettant la mise en correspondance d'une adresse IP avec la bonne adresse physique (adresse MAC).

Solution : résoudre les adresses dynamiquement à l'aide d'un protocole de bas niveau appelé Address Resolution Protocol. (ARP)

a) Principe

Lorsqu'une machine A veut déterminer l'adresse physique d'une machine B dont l'adresse IP est IB, elle diffuse un paquet spécial qui demande, à la machine dont l'adresse IP est IB, de répondre en indiquant son adresse physique PB.

- Toutes les machines, B incluse, reçoivent ce paquet.
- Seule la machine B reconnaît son adresse IP et renvoie donc son adresse physique.
- Lorsque A reçoit la réponse, elle envoie le paquet IP à B.

b) Mémoire Cache de résolution d'adresse

Pour réduire le coût de communication (diffusion coûteuse), les machines qui utilisent ARP gèrent un cache dans lequel elles enregistrent les associations d'adresses physiques et d'adresses IP les plus récentes.

c) Réalisation des ARP

Avant l'envoi d'un paquet (Etant donné l'adresse IP) :

- La machine consulte la mémoire cache pour voir si elle connaît l'association adresse physique-adresse IP.
  - Si c'est le cas, elle extrait l'adresse et prépare la trame
  - sinon envoi un paquet ARP et attend la réponse.

2. Format ARP

<table>
<tr><td colspan="2">ident. Espace adressage phys.</td><td>Identification espace adressage logique</td></tr>
<tr><td>lg @phys</td><td>lg @protocole</td><td>code</td></tr>
<tr><td colspan="3">adresse physique de l'émetteur de la trame</td></tr>
<tr><td colspan="2">adresse phys. (suite)</td><td>adresse du protocole de ...</td></tr>
<tr><td colspan="2">l'émetteur de la trame</td><td>adresse physique du récepteur ...</td></tr>
<tr><td colspan="3">... de la trame (inconnue)</td></tr>
<tr><td colspan="3">adresse du protocole récepteur du paquet</td></tr>
</table>

Image 17 Format ARP

3. Protocoles de recherche d'une adresse IP

Les protocoles de recherche d'adresse permettent à une machine n'ayant pas d'adresse IP et d'autres informations de configuration de les obtenir.

Les protocoles BOOTP et DHCP permettent à une machine n'ayant pas d'adresse IP et d'autres informations de configuration de les obtenir.

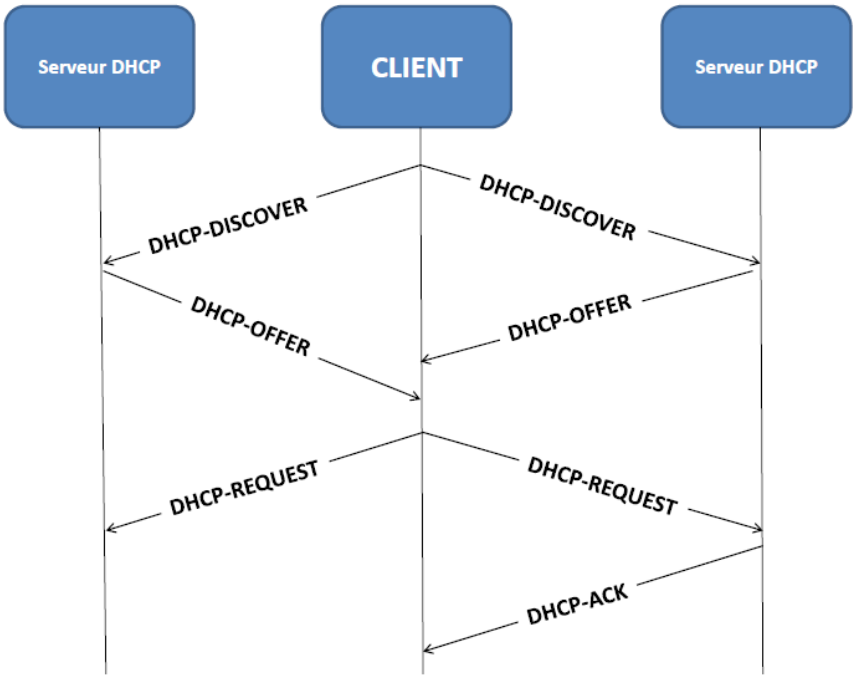
BOOTP (RFC 951, 1533,1542)

- permet le téléchargement d'un fichier de configuration (adresse IP, adresse de la passerelle, adresse du serveur de noms,etc) depuis un serveur à l'aide du protocole de transfert de fichiers TFTP. A l'origine, BOOTP a été développé pour permettre aux machines sans disque de démarrer à distance sur un réseau.
- RFC 2132 définit une série de paramètres de configuration
- BOOTP utilise le protocole UDP, ce qui le rend portable sur toute la machine supportant la pile TCP/IP

DHCP (Dynamic Host Configuration Protocol)

- DHCP est une extension du protocole BOOTP
- Avec BOOTP, l'administrateur est obligé d'attribuer une adresse IP à chaque machine même si elle ne se connecte que rarement

  ----> gaspillage d'adresses
- Avec DHCP, l'adresse est affectée dynamiquement par un serveur au démarrage.
  - Dans le temps, une adresse IP peut servir pour désigner différents équipements.
- DHCP offre une compatibilité avec BOOTP dont il garde le format des messages : Un client implémentant DHCP peut obtenir des informations d'un serveur BOOTP.
- Pour obtenir une adresse IP valide de manière dynamique, un client DHCP échange différents messages avec un serveur DHCP. La figure suivante montre comment un client, qui se connecte à un réseau pour la première fois, obtient une adresse IP à partir d'un serveur DHCP.



1) Le client DHCP diffuse sur le segment local un message DHCP-DISCOVER pour localiser un serveur DHCP. Tous les hôtes reçoivent ce message, mais seulement les serveurs DHCP envoient des messages réponses au client. Le client peut suggérer son adresse IP et la durée du bail (lease),

(2) Un serveur qui a reçu le message DHCP-DISCOVER offre une adresse IP appropriée et d'autres paramètres de configuration au client en répondant par un message DHCP-OFFER,

3) Si plusieurs serveurs DHCP envoient un message DHCP-OFFER au client, celui-ci accepte la première offre reçue et diffuse un message DHCP-REQUEST pour informer tous les serveurs DHCP qu'il utilisera l'adresse IP retenue. Ce message inclut une valeur identifiant le serveur (pour le cas où il y en aurait plusieurs) et décline implicitement les offres des autres serveurs,

(4) Lors de la réception du message DHCP-REQUEST du client DHCP, le serveur DHCP répond avec les paramètres définitifs de configuration par message DHCP-ACK confirmant que l'adresse IP a été attribué au client (si le serveur a déjà assigné l'adresse IP, il envoie un DHCPNACK). A l'exception du serveur sélectionné par le client, les autres serveurs DHCP récupèrent les adresses IP offertes au client,

- Si le client détecte que l'adresse IP est déjà utilisée sur le segment, il envoie un DHCPDECLINE au serveur et le processus recommence

- Si le client n'a plus besoin d'une adresse IP, il envoie un message DHCP-RELEASE au serveur.

D. Le protocole IP

Le protocole IP achemine les datagrammes (paquets dans le monde IP) de bout en bout entre une source et une destination,. Il fonctionne en mode non connecté et ne garantit pas la remise des datagrammes à leur destination (pas de recouvrement d'erreurs, pas de contrôle de flux)

- Chaque datagramme porte l'adresse source et l'adresse destination
- Chaque interface d'un équipement a une adresse IP
- Il est nécessaire de connaître l'adresse IP d'un équipement pour communiquer avec lui
- Le protocole IP peut utiliser n'importe quel type de liaison de données (Ethernet, Ethernet 100Mbits/s, Token-ring, FDDI, ATM, Liaison série (SLIP, PPP), X25...). On parle d'"IP over Everything"

1. Format d'un datagramme IP

Les paquets de données d'IP, appelés aussi datagramme IP, sont alignés sur des mots de 32 bits. Ils sont composé de l'en-tête (partie fixe et partie de taille variable) ainsi que le champs données qui est de longueur variable. Le format du datagramme IP est le suivant :

Format d'un datagramme IP

32 bits

Version	longueur header	type de service	longueur totale
Identificateur		flag	offset fragment
durée de vie	protocole	checksum header	
adresse source			
adresse destination			
options			Padding
Données			

- **Version** : Est utilisé pour vérifier que l'émetteur, le récepteur, et tous les routeurs intermédiaires les reliant sont d'accord sur la structure du datagramme . IP rejette des datagrammes ayant un numéro de version différent de la sienne pour éviter une interprétation erronée.
- **Longueur du header** : Longueur de l'en-tête en mots de 32 bits.
- **Type de service** : Indique comment le datagramme doit être géré.

Priorité			D	T	R	inutilisé	
0	1	2	3	4	5	6	7

Image 18 Structure du champ type de service

2. Encapsulation des datagrammes

- La taille maximal d'un datagramme est de 65535 octets.
- L'encapsulation est le transport d'un datagramme IP dans une trame physique.
- Le matériel ignore la structure des datagramme et n'interprète pas l'adresse IP destinataire.
- Comme chaque technologie définit une limite supérieure à la quantité d'informations qui peut être transmise dans une trame physique (MTU : Maximum Transmission Unit). Par Exemple le MTU d'Ethernet est de 1500 octets
- IP découpe les grandes datagrammes en morceaux plus petits (fragments) lorsqu'ils doivent traverser des réseau physiques ayant un MTU plus petit.

Remarque : Une fragmentation peut se produire n'importe où sur le chemin reliant la source et la destination.

3. Réassemblage des fragments

Les différents fragments sont acheminés comme des datagrammes indépendants jusqu'à leur destination finale où ils doivent être réassemblés.

Champs IDENTIFICATEUR

- Contient un entier unique qui identifie le datagramme.
- Les machines qui emettent les datagrammes doivent générer une valeur de champs identificateur unique pour chaque fragment (gestion d'un compteur en MC)

Champs OFFSET FRAGMENT

- Exprimé en multiple de 8 octets et commence à partir d'une valeur de zéro.
- Indique le déplacement des données transportées dans le fragment courant, par rapport au datagramme initial.

Champs FLAGS

- Les deux bits de poids faible du champs flag contrôlent la fragmentation.
- Si le premier bit est égal à '1' alors le datagramme ne doit pas être fragmenté.
- Si un routeur reçoit un datagramme avec ce bit à "1" et il a besoin de fragmenter le datagramme, il le détruit et renvoie un message d'erreur à l'émetteur.

Bit de poids faible de FLAGS

- Le bit "fragment à suivre" permet à la destination de déterminer si elle a reçue tous les fragments ou non.
- Une fois que la destination a reçu un fragment où le bit "fragment à suivre" est à "0", elle sait que le fragment transporte la fin du datagramme.
- A partir des champs OFFSET FRAGMENT et LONGUEUR TOTALE, de chacun des fragments reçu, une station destination peut déterminer si les fragments disponibles contiennent les données nécessaires au réassemblage du datagramme initial.

Champs DUREE DE VIE

- La machine émettrice définie la durée de vie (TTL) maximale.

- Les machines et les routeurs doivent décrémenter la durée de vie du datagramme au fur et à mesure que le temps s'écoule. Le datagramme est détruit lorsque TTL=0.

4. Options du datagramme IP

Le champs option n'est pas obligatoire, les options sont utilisée à des fins de test ou de mise au point.

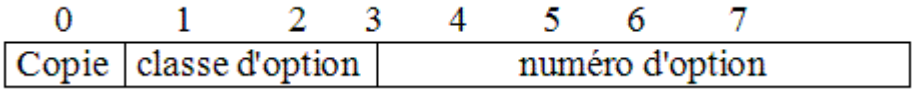


Image 19 Options du datagramme IP

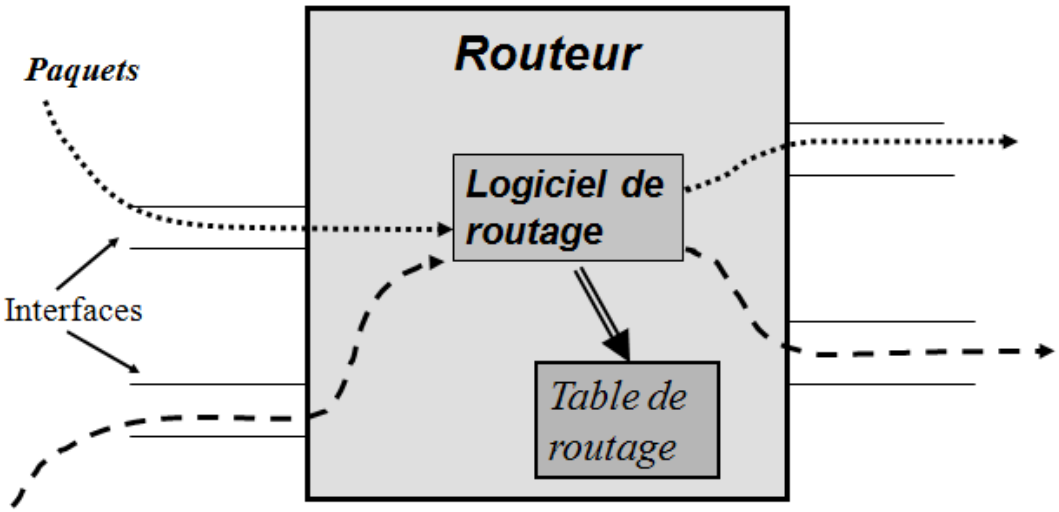
- **Copie** : Ce bit indique comment le routeur traite les options pendant la fragmentation.
  - Copie = 1 : l'option doit être recopiée dans tous les fragments.
  - Copie = 0 => l'option ne doit être recopiée que dans le premier fragment (et non dans les autres)
- Les bits **classe d'option** et **numéro d'option** indiquent le type d'option et une option particulière.
  - **L'option enregistrement de route** : Permet à la source de créer une liste 'adresses IP vide et demander à chaque routeur qui gère un datagramme d'ajouter sa propre adresse IP à la liste.
  - **L'option routage par la source** : Dans le routage par la source, l'émetteur impose un chemin au sein de l'internet.
  - **Routage strict défini par la source** : Indique le chemin précis que doit emprunter un datagramme pour atteindre sa destination.
  - **Routage lâche défini par la source** : Inclut également une suite d'adresse IP. Il indique que le datagramme doit transiter par les adresses IP de la liste mais autorise, pour deux adresses consécutives de la liste, le transit par plusieurs intermédiaires d'un réseau donné.

E. Routage des datagrammes IP

- Le protocole IP offre un mécanisme d'adressage "unique" permettent de construire un réseau ayant une couverture mondiale.
- Toute machine disposant d'accès à plusieurs réseaux physiques peut se comporter comme un routeur.
- Un datagramme transite de routeur en routeur jusqu'à ce que l'un d'entre eux puisse le remettre directement au destinataire.
- Le routage se base sur une métrique (coût du chemin) qui sert aux équipements d'effectuer un choix quand deux ou plusieurs routes conduisent à la même destination.
- La métrique utilisée peut être le nombre de routeurs traversés, le débit, fiabilité.
- Pour connecter une station (équipement ayant un seul attachement au réseau), il faut préciser : son adresse IP, le masque réseau associé, le routeur par défaut, au moins un serveur de noms.
- Ces valeurs peuvent être apprises par une station grâce aux protocoles

DHCP, BOOTP, ou ICMP route discovery.

- S'il existe des routes plus adaptées, elles seront apprises grâce à ICMP redirect.
- Un routeur maintient des tables de routage qui indiquent les interfaces de sortie permettant d'atteindre une destination donnée.



1. Routage IP utilisant des tables

Le routage des datagrammes IP se base, sur chaque machine, sur une "**table de routage Internet**" (INTERNET ROUTING TABLE). Cette table de routage contient des information d'accessibilité composé principalement des paires (N,G) où N est l'adresse IP d'un réseau destinataire et G: est l'adresse du routeur suivant sur le chemin qui mène au réseau N.

- Les tables de routage ne mentionnent que les routeurs directement accessibles sur un réseau physique donné.
- Lorsqu'un datagramme est prêt à quitter la machine M :
  - IP localise l'adresse de destination et extrait la partie réseau,
  - puis, en utilisant cet identificateur de réseau, la machine M consulte sa table de routage qui indique le routeur directement accessible auquel elle devra envoyer le paquet pour qu'il puisse atteindre la destination.

2. Les routes par défaut

A la réception d'un paquet par un routeur, celui-ci recherche d'abord l'identificateur de réseau (de la machine destinataire) dans la table.

Si aucune route n'apparaît dans la table, le datagramme est envoyé à un "routeur par défaut".

L'adresse par défaut est 0.0.0.0

F. ICMP (Internet Control and error messages)

- Le protocole ICMP permet aux routeurs d'envoyer des messages d'erreurs ou de contrôle à d'autres routeurs ou machine.
- Les messages ICMP sont acheminés dans la partie données des datagrammes IP.
- Les messages ICMP sont destinés au logiciel IP de cette machine.

1. Compte rendu d'erreurs

- ICMP est un mécanisme de compte rendu des erreurs (Error Reporting Mecanism).
- ICMP ne peut servir à informer les routeurs intermédiaires des problèmes rencontrés, il rend compte à l'émetteur initial.
- Le routage des datagrammes qui transportent des messages ICMP se fait sans sécurité ni priorité supplémentaire.
- Des messages ICMP ne sont pas générés dans le cas de datagramme IP contenant des messages ICMP.

2. Structure des messages ICMP

Tous les messages ICMP commencent par trois champs identiques qui sont les suivants :

1. **Type de message (8 bits)**
   - Identifie le type de message.
2. **Code (8 bits)**
   - Fournit des informations supplémentaires sur le type de message
3. **Champs de contrôle (16 bits)**
   - Même que IP, mais le contrôle porte uniquement sur le message ICMP.

Les messages ICMP qui rendent des comptes d'erreurs incluent toujours les 64 premiers bits du datagramme à l'origine de l'erreur.

Ceci permet à l'émetteur de localiser l'erreur.

Quelques valeurs du champs type

- 0 : réponse à une demande d'écho
- 3 : destination inaccessible
  - code :
    - 0 : le réseau ne peut être atteint
    - 1 : la station ne peut être atteinte
    - 2 : le protocole ne peut être atteint
    - ...
- 4 : réduction du débit d'émission
- 5 : redirection
- 8 : demande d'écho
- 9 : information sur les routeurs
- 10 : selection du routeur
- 11 : la durée de vie a atteint 0
- 12 : problème de paramètrage
- 13 : estampille temporelle
- 14 : réponse à l'estampille temporelle

- 15 : demande d'informations
- 16 : réponse à demande d'informations
- 17 : demande de netmask
- 18 : réponse à demande de netmask
- 30 : traceroute

3. Test de l'accessibilité et de l'état

- Une machine ou un routeur peut envoyer des messages ICMP de demande d'ECHO ICMP vers une destination particulière.
- La station réceptrice de la demande d'ECHO, répond en envoyant une REPONSE ECHO à l'émetteur.

Cette commande permet de tester le bon fonctionnement du système de transport.

Important : Sur de nombreux systèmes, la commande invoquée pour émettre des demandes d'ECHO ICMP est PING.

4. Compte rendu de destination inaccessible

Lorsqu'un routeur ne peut remettre un datagramme, il renvoie un message ICMP de "**destination inaccessible**" à l'émetteur initial.

Exemples :

- si un routeur reçoit un datagramme ayant l'option ROUTAGE PAR LA SOURCE, comportant une route incorrecte, alors ICMP génère un message d'échec d'option routage par la source (source route failure).
- si le routeur reçoit un datagramme et se retrouve dans l'obligation de le fragmenter mais le bit non fragmentation (bit DF de l'en-tête IP) est à '1', alors le routeur rejette le paquet et renvoie un message FRAGMENTATION NEEDED à l'émetteur.

5. Congestion et datagramme de contrôle de flux

- Une congestion se produit lorsque les routeurs sont submergés de trafic.
- Une machine utilise le message ICMP (**SOURCE QUENCH**) pour remédier à la congestion.
- Lorsqu'il y a saturation de la mémoire du routeur, des datagrammes sont détruits.
- Le message "**Source Quench**" est une demande adressée à la source, à qui il est demandé de réduire son débit d'émission.

6. Demande de réduction ou de modification de route

- Lorsqu'un routeur détecte qu'une machine utilise une route non optimale, il lui envoie un message **ICMP REDIRECT** pour lui demander de modifier ses routes.
- Le routeur transmet également le datagramme original à sa destination.

7. Détection des boucles de routage

Le compteur **durée de vie** (**TTL**) est utilisé pour éviter qu'un datagramme entre dans une boucle infinie.

- Un routeur diminue de "1" le champs TTL lorsqu'il traite un datagramme.
- Un routeur détruit le datagramme lorsque le champs TTL est égal à 0.

Il y a destruction d'un datagramme lorsque le TTL est égal à 0 ou quand le délai de réassemblage des fragments du datagramme a expiré.

- Emission d'un message **ICMP DELAI EXCESSIF** à l'émetteur initial.
  - Le champs **code** = 0 : Durée de vie expirée.
  - Le champs **code** = 1 : Délai de réassemblage expiré.

Lorsque le premier fragment arrive, la machine réceptrice active un temporisateur, et considère qu'une erreur s'est produite si le temporisateur expire avant que tous les fragments du datagramme ne soient reçu.

G. Couche transport

Dans les réseaux orienté mode connecté (ATM ou X25), les pannes (pannes d'équipement ou de liaison) qui se produisent ne sont pas notifiées aux nœuds en communication, en conséquence la connexion devra être réinitialisée suite à cette coupure. Avec le protocole IP, le nœuds terminaux ne sont pas affectés par les pannes de routeurs ou de liaisons physiques car le re-routage des paquets se fait de manière automatique (suite à une reconfiguration automatique des routes). Ce qui risque de se produire donc est simplement la perte momentanées de paquets. Cette perte de paquets peut être gênante pour certaines applications mais pas pour d'autres (comme les application audio par exemple). Pour cela il été définit deux protocoles de transport : TCP et UDP.

- TCP (TRANSPORT CONTROL PROTOCOL) : protocole en mode connecté offrant un service fiable
- UDP (USER DATAGRAMME PROTOCOL) : protocole en mode non connecté
- TCP et UDP identifient une application par numéro de port
- Adresse IP +No. de port identifient une socket
- Une connexion TCP ou un échange UDP sont définis par une association de deux sockets

1. UDP

- Protocole non fiable : pas de retransmission en cas de perte ou d'erreur, par de contrôle de séquencement, pas de contrôle de flux
- Pour UDP, chaque bloc généré par l'application donne lieu à un segment UDP.
- Utilisé par NFS
- utilisé pour la diffusion

Format d'un datagramme UDP

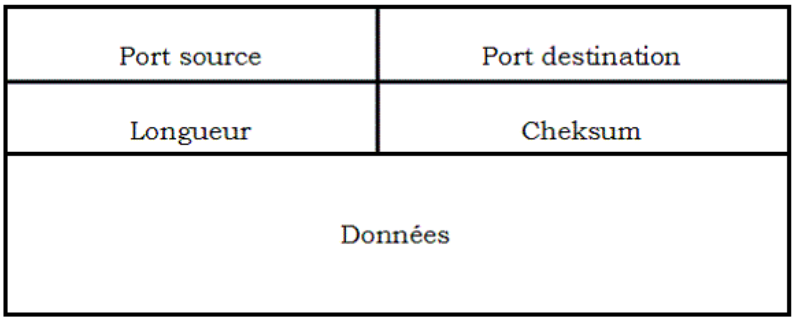


Image 20 Datagramme UDP

2. Le protocole de contrôle de transmission de TCP

Le transfert d'un flot d'octets entre deux process d'application TCP est mis en œuvre par des modules appelés « entités du protocole TCP ».

Deux entités TCP dialoguent entre elles pour rendre un service de transfert de données à deux process d'application.

L'interface entre process et entité est un buffer : le process dépose des octets dans ce buffer et l'entité TCP prélève des octets de ce buffer pour fabriquer des « segments » qui sont envoyés, via à l'entité IP, au destinataire distant.

- TCP est un protocole qui apporte la fiabilité
- TCP fonctionne en mode connecté : Phase ouverture de la connexion, échange de segments, libération de la connexion,
- les données applicatives sont fragmentées en segments dont la taille est jugée la meilleure par TCP pour transmission
- Lorsque TCP émet un segment, il arme un timer (attente d'acquittement)
- Lorsque TCP reçoit un segment, il émet un acquittement (pas immédiatement, mais au bout d'un délai)
- TCP rejette les segments erronés, et réordonne les segments
- TCP fournit un contrôle de flux.
- TCP n'interprète pas le contenu des octets (ASCII, EBCEDIC,...)
- TCP démultiplexe les informations reçues vers les différents programmes utilisateur. Il utilise les numéro de port.
- TCP utilise la connexion et non le port de protocole comme concept principal.
- TCP définit une extrémité de connexion comme une paire de différents entiers (machine, port).

Exemple : le couple (18.26.0.36, 1069) et (128.10.2.3, 25) définit une connexion

3. Format d'un segment TCP

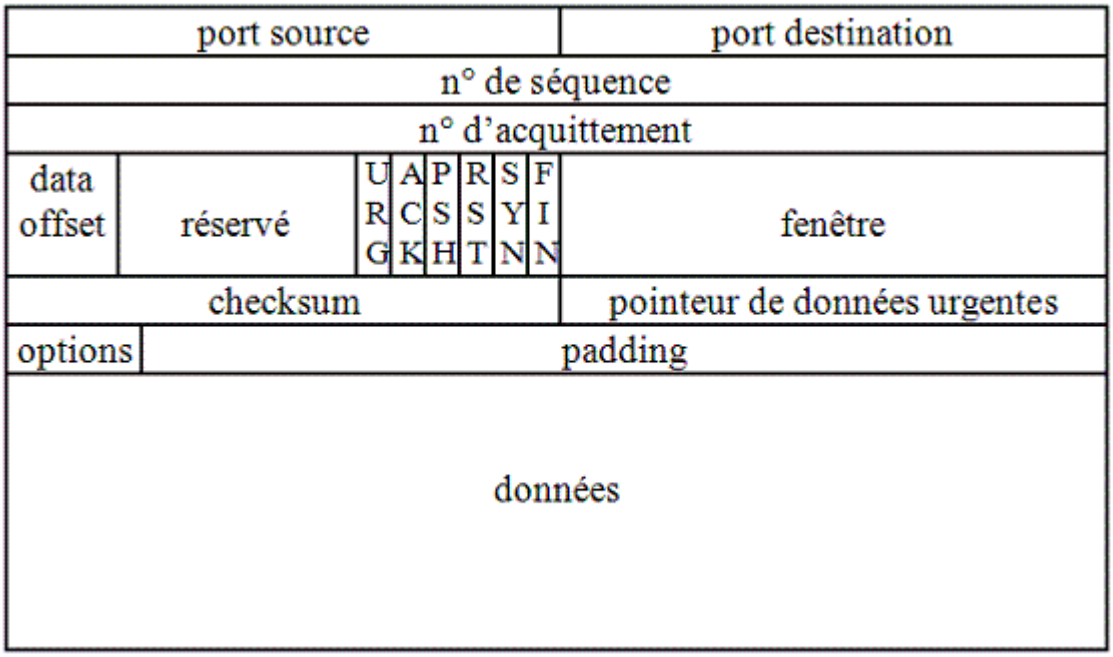


Image 21 Segment TCP

- port source et port destination : permettent de référencer les applications.
- séquence : numéro de séquence du premier octet transmis dans le segment.
- acquittement : numéro de séquence du prochain octet attendu.
- data offset (4bits) : taille en mots d e 32 de l'en-tête.
- réservé (6bits) : usage futur
- URG : pointeur message urgent
- ACK : la valeur du champs acquittement peut être prise en compte
- PSH : les données reçues doivent être immédiatement fournies à la couche supérieure
- RST : fermeture de la connexion à cause d'erreur irrécupérable
- SYN : ouverture de la connexion
- Fin : fin de la connexion
- fenêtre : nombre d'octets que le récepteur peut accepter
- checksum : de l'en-tête du message
- pointeur de données urgentes : indique les octets qui doivent être traités en priorité
- options : permet de définir par exemple la taille max. d'un segment (MSS)

4. Ouverture de connexion

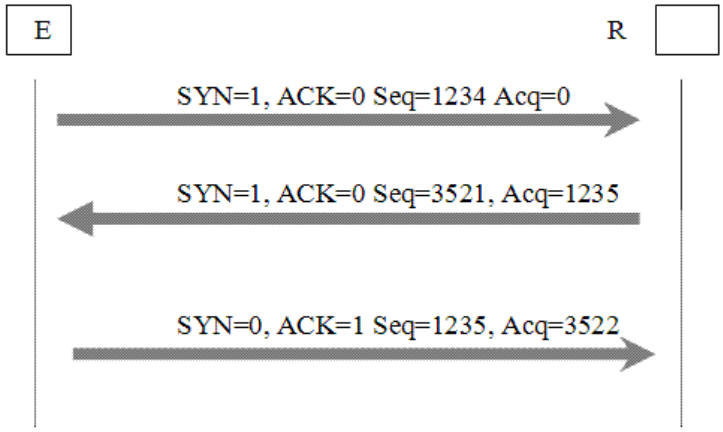


Image 22 Ouverture de connexion

5. Transfert de segments TCP

Principes du transfert de segments TCP :

• les octets sont envoyés dans des segments de taille maximale MSS

• chaque segment porte un numéro de séquence qui est celui du 1er de ses octets de données. Par exemple si le MSS est 2000, alors le No. de séquence du premier segment serait 0, le numéro du 2ème segment serait 2000, le numéro du 3ème segment serait 4000, etc.

• le récepteur acquitte les segments reçus. Ces acquittements peuvent être transportés dans des segments de données ou dans des segments spécifiques

• par convention, le numéro porté dans l'acquittement est celui du prochain octet à recevoir

• L'acquittement est cumulatif, c-a-d que la réception d'un segment portant un numéro d 'acquittement n indique que tous les octets de rang strictement inférieur ont été bien reçus par le récepteur

• Le récepteur stocke les segments reçus, y compris hors séquence, dans son buffer de réception, mais ne délivre à l'application que les octets en séquence.

Détection de pertes de segments TCP

TCP utilise deux méthodes de détection des pertes :

1- détection de perte suite à la réception de plusieurs duplicata d'un même acquittement :

cette méthode est déclenchée en cas de perte suite à une congestion ponctuelle du réseau (perte d 'un segment parmi n envoyés).

Dans le cas d'une perte ponctuelle d'un segment parmi plusieurs, la détection de cette perte peut se faire, de façon précoce, et ce avant l'attente de l'expiration du timer de retransmission. Cette détection est basée sur la réception de plusieurs acquittements successifs pour un même segment. Si un seul segment est perdu alors que d'autres, émis postérieurement, ont pu être délivrés, alors le comportement de TCP est tel que la réception d'un segment hors séquence provoque l'émission par l'entité TCP réceptrice d'un acquittement qui réclame le segment en séquence manquant. La source recevra donc plusieurs acquittements et pourra en déduire une perte ponctuelle.

Si la source reçoit 3 acquittements dupliqués pour un ancien segment (alors qu'elle en a transmis d'autres après), elle conclut la perte de ce segment.

2- détection suite au non retour de l'acquittement avant un certain délai :

cette méthode est déclenchée lorsque la congestion a impacté plusieurs segments. La source détecte la présence d'une perte quand elle estime que le délai d'attente de l'acquittement d'un segment envoyé est supérieur au délai d'aller/retour entre la source et le destinataire et cela à l'aide de l'utilisation d'un temporisateur de retransmission. Les implémentations de TCP n'associent pas un temporisateur par segment mais examinent globalement les retours des acquittements, pour tous les segments en attente d'acquittement, et ce une fois toutes les 500ms.

Retransmission des segments perdus

Il existe deux modes de retransmission des segments perdus :

- **"selective repeat " ou retransmission sélective** :

Ce type de retransmission est mis en œuvre lorsque la perte a été détectée par la réception de 3 acquittements dupliqués. Dans ce cas, seulement le segment perdu est retransmis. Après cette retransmission, l'entité TCP reprend ses transmissions normalement, à partir du prochain segment (octet) à transmettre.

- **"Go back N" ou retransmission globale** (renvoie de tous les segments non acquitté) :

• ce type de retransmission est effectué lorsque la perte de segment a été détectée par temporisateur. En effet, si l'émetteur n'a pas reçu d'acquittements dupliqués avant que le temporisateur ne soit arrivé à échéance, la probabilité est forte d'une perte globale de tous les segments émis (sinon, l'émetteur aurait reçu des acquittements dupliqués correspondant aux segments délivrés),

• L'émetteur renvoie l'ensemble des octets correspondant aux segments non acquittés,

• comme la transmission est globale et que peut-être certains segments ont été bien reçu lors de l 'envoi précédent, alors il y a un risque que le récepteur reçoive des segments dupliqués. Les segments dupliqués (les numéros de séquence permettent de détecter les doublons) sont alors ignorées,

mesure le délai aller retour (RTT) en permanence contrôle de flux par annonce de fenêtres contrôle de congestion sans signalisation réseau

6. Fermeture de connexion

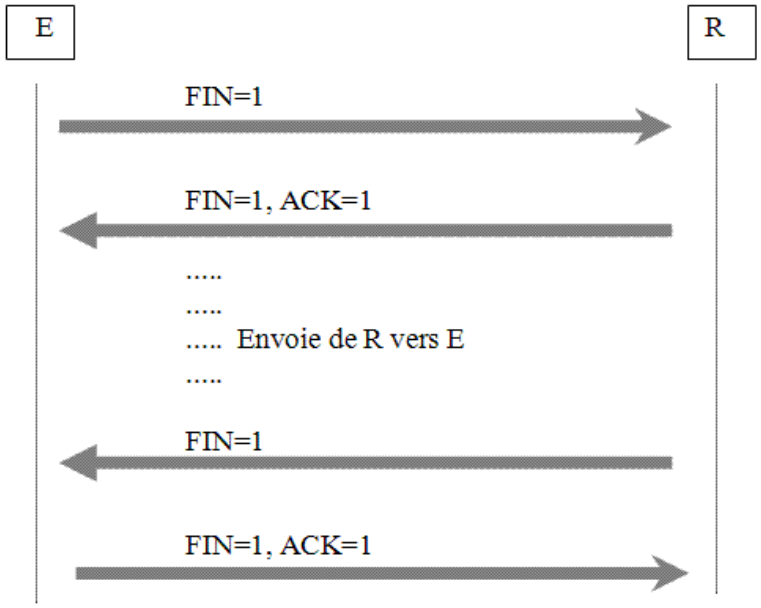


Image 23 Fermeture de connexion

7. Taille maximum des segments

- La taille maximum d'un segment (MSS) est le plus grand morceau de données que TCP enverra à l'autre extremité.
- Le MSS est annoncé lors de l'établissement de la connexion.
- Chaque extrémité a l'option d'annoncer le MSS qu'elle attend recevoir.
- Lors de l'absence d'un MSS, la valeur par défaut est égale à 536 octets.
- Beaucoup d'implémentations BSD requièrent un MSS multiple de 512.
- SunOS 4.1.3, Solaris 2.2, AIX 3.2.2 utilisent MSS=1460 lorsque le réseau est un Ethernet.

H. Algorithmes de routage

1. Introduction

Le routage est une des fonctions les plus importantes de l'architecture des réseaux IP. Lorsqu'un paquet IP est reçu via une interface de communication d'un nœud x, celui-ci est routé vers le prochain nœud se trouvant sur le meilleur chemin permettant d'atteindre le nœud destinataire si x n'est pas le destinataire du paquet.

Le protocole IP s'appuie sur une **table de routage** qui indique l'adresse du prochain nœud, l'interface de sortie, et d'autres informations. Cette table de routage peut être construite et maintenu soit de manière statique (création et mise jour par l'administrateur réseau) ou bien de manière dynamique sans intervention humaine. La mise à jours dynamique des tables de routage se base sur des échanges d'information d'accessibilité entre les routeurs.

Au début, l'Arpanet était un seul réseau géré de manière homogène, du moins par un ensemble de personnes dépendantes de la même entité administrative, ce qui

permettait d'en orienter le développement de la même manière partout.

Le protocole de routage utilisé à l'époque (routage dynamique) implique que les routeurs s'échangent continuellement des informations sur les meilleures routes à utiliser. Chaque routeur finit par avoir une route pour atteindre tout le monde, partout !

L'extension de ce réseau à des entités très différentes entres elles a conduit les architectes réseaux de l'époque à créer la notion de système autonomes (Autonomous Systems ou AS), afin de permettre à chacun de développer son réseau interne sans risque d'en diffuser le contenu à l'extérieur.

Cette nouvelle architecture entraine des changements dans l'usage des protocoles de routage. Certains sont plus adaptés que d'autres à router des blocs d'adresses IP conformément à des politiques de routage (routing policy) internationales, ce sont les protocoles externes ou EGP (Eexternal Gateway Protocol) qui est remplacé aujourd'hui par BGP (Border Gateway Protocol).

A l'intérieur du système autonome, les protocoles de routages sont des IGP (Interior Gateway Protocol).

2. Routage statique

- Configuration manuelle
- Simple à mettre en oeuvre
- Convient aux petits réseaux
- Inadapté :
  - Aux grands réseaux
  - Aux réseaux qui évoluent
  - Quand les routeurs sont éloignés

3. Routage dynamique

Les équipements échangent des informations de configurations pour construire de manière automatique les tables de routage. Cela permet d'apporter une robustesse au réseau IP.

Motivation du routage dynamique :

- Dans un environnement complexe, la mise en œuvre du routage statique est souvent difficile `a maintenir

- La mise en place d'un mécanisme de routage dynamique permet de faciliter les mises à jour,

Principe de fonctionnement général du routage dynamique :

- Chaque routeur diffuse la liste des réseaux auxquels il est connecté

- Chaque routeur met à jour sa table de routage à partir des informations reçues depuis les autres

Le routage dynamique est mis en œuvre à l'aide de démons (processus qui tourne en arrière plan) de routage : routed, gated, ripd, ospfd

4. Système autonome

- Est un ensemble de réseaux et de routeurs relevant d'une même responsabilité administrative pour des considérations de routage.
- Dans un système autonome, les protocoles de routage sont relativement homogènes.
- Les systèmes autonomes peuvent être regroupés dans des domaines

administratifs s'ils sont gérés par une même autorité administrative.

- Les organismes attribuant les adresses IP affectent aussi les n° des systèmes autonome (16 bits).

Deux catégories de systèmes autonomes

- Le réseau comme outil d'interconnexion d'applications (producteur & consommateur de l'information)
- Le réseau comme outil de transport (fournisseur d'accès à l'Internet)

Deux familles de protocoles sont associés à chacune des catégories

- **Protocoles de routage intra-domaine (intérieurs)** : permettent la construction et le maintien des tables de routage a l'intérieur d'un domaine. Il existe deux familles d'algorithmes :
  - Algorithmes à vecteur distance ou DVA (pour Distance Vector Algorithm). RIP (Routing Information Protocol) est un protocole qui implémente l'algorithme DVA
  - Algorithmes à états de liaisons ou LSA (pour Link State Algorithm). OSPF (Open Shortest Path First) est un protocole qui implémente l'algorithme LSA
- **Protocoles de routage inter-domaines (extérieurs)** : sont utilisé pour la communication avec les autres domaines. BGP est un exemple de protocole de routage inter-domaines

I. Routage intradomaine

1. Routage à vecteur de distance

Algorithme basé sur l'échange d'informations entre routeurs adjacents

- Un routeur ne connaît initialement que le coût de ses propres liaisons
- Chaque entrée de la table de routage contient un couple (**destination, distance**), la distance est mesurée en sauts.
- Périodiquement, chaque routeur diffuse sa table à tous les routeurs qu'il est capable d'atteindre directement.
- Un routeur qui reçoit une table de routage effectue un traitement à chaque entrée de la table :
  - si l'entrée n'est pas dans la table, il la rajoute
  - si le coût de la route proposée plus le coût de la route pour venir est plus petit que celui de la route stockée, il prend en compte la nouvelle route
  - sinon, il n'y a pas de changement

Exemple

Dest.	Distance	Route
rés-1	0	direct
rés-2	0	direct
rés-4	8	Pass. L
rés-17	5	Pass. M
rés-24	6	Pass. J
rés-30	2	Pass. Q
rés-42	2	Pass. J

Table de routage d'un routeur K

Image 24 Table de routage d'un routeur K

Destination	Distance
rés-1	2
rés-4	3
rés-17	6
rés-21	4
rés-24	5
rés-30	10
rés-42	3

Image 25 Table de routage reçue d'un routeur J

La modification d'une entrée dans la table de routage engendre l'émission de la nouvelle table vers tous les routeurs adjacents.

Les échanges entre les routeurs continue jusqu'à ce que l'algorithme converge.

2. Routing Infomation Protocol (RIP)

- Est conçu pour des réseaux de petites taille, il est connu sous le nom d'un programme qui met en œuvre "**routed**" (daemon).
- Est une application directe du routage à vecteur distance.
- Classe les participants en machines **actives** (routeurs qui émettent périodiquement les tables de routage) et **passives** (stations qui écoutent uniquement les messages qui circulent sur le réseau).
- Utilise le protocole UDP pour transporter ses données (port 520).

Routeurs actifs

- Diffusent un message (contenant des information de routage) toute les 30 seconde en régime stable.
- Chaque message est de type (N,D)
  - N : adresse d'un réseau
  - D : distance du routeur à ce réseau (en sauts)

- En cas de changement dans les tables de routage, l'envoie des nouvelles tables n'est pas instantané : quand un routeur a émis sa table, il doit attendre un temps aléatoire entre 1 et 5 secondes avant de réémettre sa nouvelle table.
- Un routeur déclare qu'une route n'est plus valide quand il n'a pas reçu pendant une période de 180 secondes de table d'un routeur.

Machines passives

Elles écoutent les routeurs et mettent à jour les routes en fonction des informations reçues, mais n'en diffusent pas elles-même.

RIP v2 (RFC 1387, 1388)

- Permet le routage des sous-réseaux (véhicule le netmask)
- Identifie les routes externes utilisées par un EGP
- Interopère avec RIPv1
- Diffusion muticast (224.0.0.9) plutôt que broadcast
- Autentification

3. Routage a états de liaisons

- Chaque routeur
  - Surveille activement l'état de ses liaisons
  - Diffuse cet état à tous les autres routeurs
  - Construit à partir de ces informations une carte topologique complète du réseau
  - Calcule les routes de plus courts chemin (algorithme de Dijkstra)

Le protocole OSPF (Open Shortest Path First) : RFC 1583

- Le routage est hiérarchisé pour simplifier le calcul des routes : le système autonome est découpé en zones (areas)
- Une zone est un ensemble de réseaux contigus représentée par un n° codé sur 32 bits
- Deux zones peuvent être contiguës ou connectées à un backbone par un ou plusieurs routeurs
- Deux niveaux de routage : routage intra-area et routage inter-area
- Il se place au dessus du protocole IP (port 89)

Les aires OSPF

On distingue trois classes d'aires :

- l'Aire Backbone :
  - Chemin obligatoire pour passer d'une aire à une autre
- Les Aires secondaires :
  - Tous les noeuds de routage ont une vue globale de la carte du réseau
  - Ils calculent localement la meilleure route entre une source et une destination
- Les Aires terminales (stub area) :
  - Même comportement que les aires secondaires
  - sauf qu'elles ne mémorisent pas les informations sur les routes externes
  - Toutes les routes externes sont récapitulées dans une route par défaut

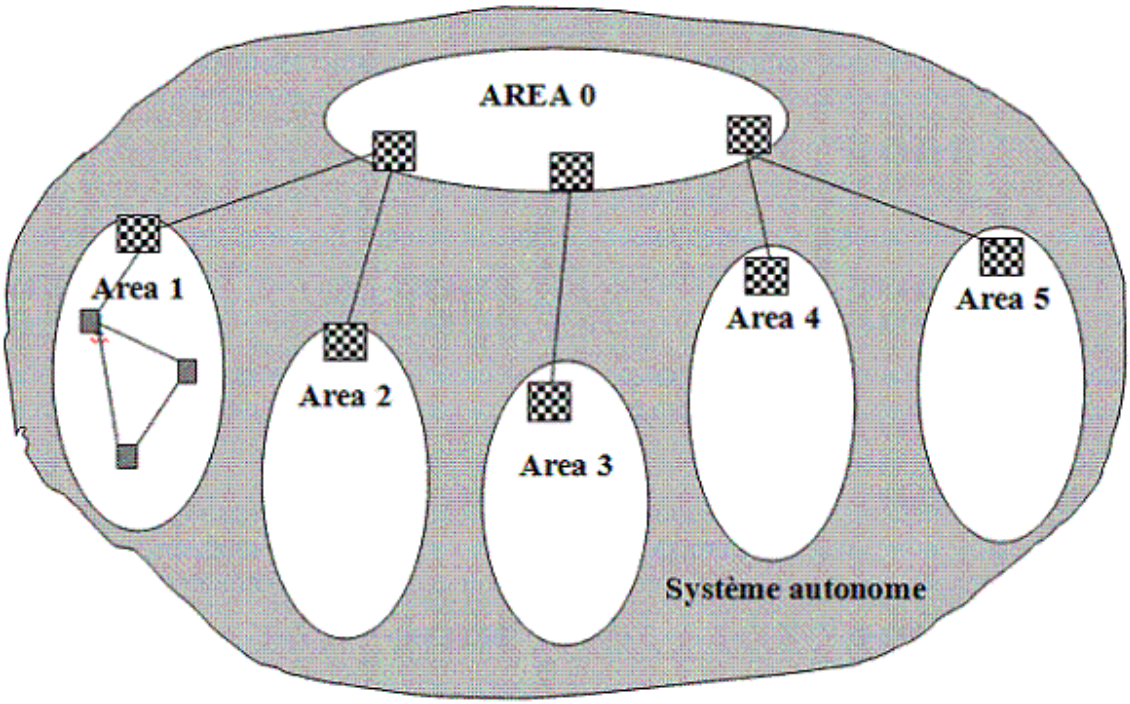


Image 26 Aires OSPF

J. Routage interdomaine

L'utilisation d'un protocole de routage interdomaines différent du routage intradomaine est nécessaire car leurs objectifs ne sont pas les mêmes :

- Les protocoles de routage intradomaine doivent acheminer les datagrammes aussi efficacement que possible vers leur destination
- Les protocoles de routage interdomaine obligent les routeurs à se préoccuper de la stratégie. Par exemple, un système autonome ne souhaite pas servir de réseau de transit

1. Annonce des routes

Annoncer une route par un protocole de routage externe implique que le système autonome accepte de véhiculer les informations vers cette destination mais aussi il est capable de joindre la destination annoncée.

L'annonce des routes doit être faite méticuleusement car elle influe énormément sur la répartition du trafic

Border Gateway Protocol (BGP) : RFC 1105

- Transmet le "chemin d'AS" entre la source et la destination (ni vraiment vecteur distance ni vraiment link state)
- Echange des informations de routage via une connexion TCP (port 179)
- Inclut un système d'authentification des messages échangés
- Peut être utilisé comme protocole interne

K. Le système de nom de domaine : DNS

1. Introduction

Les premières configurations Internet nécessitaient l'utilisation uniquement des adresses IP numériques, adresses plus difficile à retenir que des noms. Il était donc nécessaire d'évoluer vers l'utilisation de noms d'hôtes symboliques.

Par exemple, au lieu de taper " TELNET 10.12.7.14", il est plus simple de taper taper "TELNET MyHost". MyHost est ensuite traduit d'une manière ou d'une autre en adresse IP 10.12.7.14.

Bien que l'utilisation de noms d'hôtes facilite la procédure d'accès à une ressource, elle introduit le problème de maintenance et de mise en correspondance entre les adresses IP et les noms de machines de manière centralisée. En effet, utiliser une table de correspondance sur plusieurs millions de machines pose un problème de maintenance de la table de correspondance contenant plusieurs millions d'entrées sur chacune des machines, ce qui est impossible. De plus, lors d'un changement d'une entrée dans une table de correspondance, il est nécessaire de faire le changement dans les tables de toutes les machines. Par ailleurs, il y a un risque de créer des ambiguïtés de noms.

Au début de l'Internet, dans ARPANET les noms d'hôtes à mettre en correspondance avec une adresse IP étaient maintenus par le Centre d'information réseau (NIC) dans un seul fichier (HOSTS.TXT) et lorsqu'un administrateur changeait un nom de machine ou ajoute une machine, il informait le NIC et télécharge périodiquement le fichier HOSTS.TXT. Mais en raison de la croissance explosive du nombre d'hôtes, ce mécanisme est devenu trop lourd et a été remplacé par un nouveau concept: Système de noms de domaine ou DNS. En 1985, l'IETF standardise le DNS au travers les RFC1034 et RFC1035.

Considérons la structure interne typique d'une grande organisation organisée en divisions, chacune d'entre elles ayant une autonomie dans certaines limites. Les noms de domaine sont donc formés de la même manière et reflètent souvent la hiérarchie de l'organisation.

Exemple : myHost.myDept.myDiv.myCorp.com

Dans cet exemple, nous savons qu'il existe un nom d'hôte unique myHost qui existe dans le sous-domaine myDept.myDiv.myCorp. Le sous-domaine MyDept.myDiv.myCorp est l'un des sous-domaines du sous-domaine myDiv.myCorp.com qui est à son tour l'un des sous-domaines de myCorp.com. Enfin, myCorp.com est un sous-domaine de com.

Comment un système de noms peut-il prendre en compte un large ensemble de noms sans avoir recours à un site central de gestion?

- **Solution** : décentraliser le mécanisme de nommage
  - Partition de l'espace des noms au niveau le plus haut
  - Délégation de la responsabilité des choix des noms de sous-division.

DNS est le mécanisme qui implémente le nommage hiérarchique des machines pour l'Internet.

Nom de domaine = suite de labels séparés par un point

- Un nom de host peut désigner plusieurs adresses IP pour des interfaces différentes
- Une adresse IP peut être associée à plusieurs noms alias par exemple : ftp.domaine.xxx ; www.domaine.xxx ; mail.domaine.xxx

Partitionnement Internet

Fully qualified domain names (FQDNs) :

Lors de l'utilisation du système de noms de domaine, il est commun de travailler avec une seule partie de la hiérarchie de domaine, comme le domaine myDivision.myCorp.com.

Le système de nom de domaine fournit une méthode simple pour minimiser les saisies nécessaires dans cette circonstance. Si un nom de domaine se termine par un point (par exemple, MyDept.myDiv.myCorp.com.), il est supposé être complet. C'est ce qu'on appelle un nom de domaine entièrement qualifié (FQDN).

L'adresse FQDN permet de repérer de façon unique une machine sur le réseau des réseaux. Ainsi MyHost.MyDept.myDiv.myCorp.com. représente une adresse FQDN. FQDN est un nom de domaine qui révèle la position absolue d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine. On parle également de domaine absolu, par opposition aux domaines relatifs.

Si le nom de domaine ne se termine pas par un point (par exemple, myDept.myDiv), il est incomplet et le résolveur DNS peut compléter ceci en ajoutant un suffixe tel que .myCorp.com au nom de domaine. Les règles pour ce faire cette opération dépendent de l'implémentation et localement configurables.

Domaines génériques :

Les domaines se trouvant immédiatement sous la racine sont appelés domaine de premier niveau (TLD : Top Level Domain). Les noms de domaines ne correspondant pas à une extension de pays sont appelés des domaines génériques (gTLD), par exemple .org ou .com. Les noms correspondant à des codes de pays (fr, be, ch...) sont appelés ccTLD (country code TLD).

Com	entreprises commerciales
Edu	établissement d'enseignement
Gov	établissement gouvernementaux
....	
Code pays	Pays (Configuration géographique)

Image 27 Domaines

2. Résolution des noms et adresses

Le DNS peut être vu comme un espace de noms hiérarchique permettant de garantir l'unicité d'un nom dans une structure arborescente ainsi qu'un ensemble de serveurs de noms distribués qui coopèrent pour la résolution des correspondances nom-adresse.

- Les domaines se trouvant immédiatement sous la racine, représentée par un point, sont appelés domaine de premier niveau (TLD : Top Level Domain).
- Le serveur racine de l'arborescence connaît les domaines racine et les serveurs qui en sont responsables
- Un serveur de noms connaît les serveurs qui fournissent les réponses pour chacun des sous-domaines dont il est responsable .
- Les administrateurs peuvent créer des sous-domaines pour des groupes d'hôtes selon des critères de localisation géographique ou organisationnels, etc.
- L'administrateur d'un domaine peut déléguer la responsabilité de gestion du sous-domaine à quelqu'un d'autre et domaine parent maintient un lien vers

les sous-domaines délégués à d'autres.

- Dans le domaine racine de niveau supérieur, il existe une exception à cela. Il n'y a pas de système supérieur auquel l'autorité peut être déléguée, mais il n'est pas souhaitable que toutes les requêtes pour les noms de domaine entièrement qualifiés soient dirigées vers un seul système. Par conséquent, l'autorité pour les zones de niveau supérieur est partagée entre un ensemble de serveurs de noms racine1 coordonné par l'ICANN.
- A chaque fois qu'un administrateur délègue un sous-domaine, une nouvelle unité d'administration est créée, cette unité est appelée zone.

  - Le sous-domaine est son domaine parent sont maintenant administrés de manière indépendante

  - La frontière entre les zones est un point de délégation dans l'espace des noms

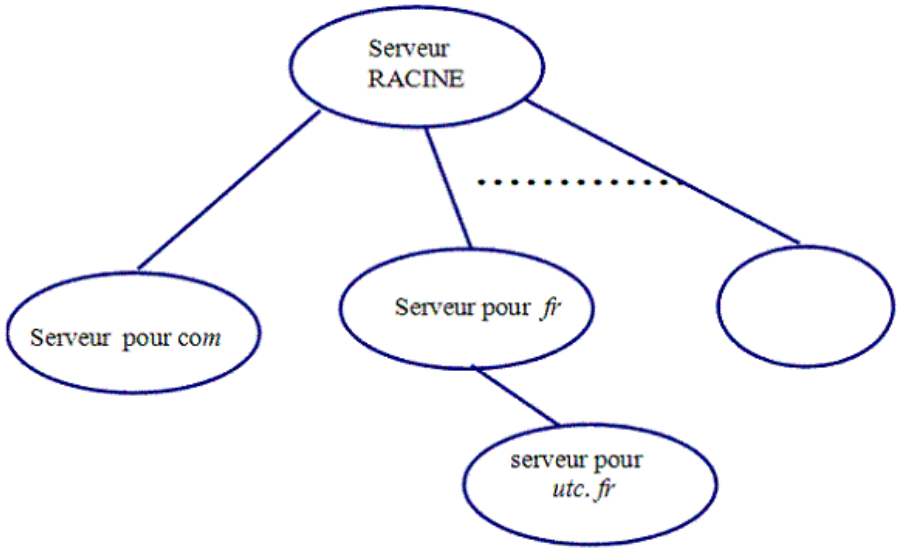


Image 28 Resolution DNS

- Chaque nœud définit un domaine (suite de noms séparés par des points) et certains nœuds définissent une zone sous l'autorité d'un serveur de noms SOA : start of a zone of authority (sphere of authority).
- Une zone est un sous arbre de l'arbre des noms de domaines sur lesquels un serveur d noms possède une information complète.
- Une zone est géré par une entité administrative particulière. L'autorité sur ce sous-arbre est déléguée et la délégation est totale (libre organisation, changements sans préavis et délégation de sous-zones)

vLe système de noms de domaine est transparent pour l'utilisateur. Cependant, il est nécessaire de configurer chaque ordinateur avec l'adresse d'une machine capable de faire la résolution de nom, appelée Serveur de noms (Domain Name Server). Cette information est fournie par l'administrateur du réseau. De plus, il est nécessaire de définir L'adresse IP d'un second serveur de noms (secondary Domain Name Server) pour faire face à des situations où le serveur primaire est défaillant.

On peut voir un serveur de noms comme :

- un serveur de base de données, répondant à des questions sur les parties de l'espace de nom dont il connaît (c'est-à-dire il a autorité) et

- un cache, stockant temporairement des données qu'il découvre à partir d'autres serveurs de noms, et

- un agent, aidant les résolveurs et autres serveurs de noms à trouver des données

Le processus de résolution des noms de domaine, c'est à dire le mécanisme consistant à trouver l'adresse IP correspondant au nom d'un hôte, peut être résumé

dans les étapes suivantes. Il fonctionne en mode Client-Serveur.

- **Coté CLIENT** : le résolveur élabore une demande de traduction au serveur de nom en lui envoyant une requête qui permet de demander l'adresse IP d'un hôte en fournissant son nom ou demander un nom d'hôte en fournissant son adresse IP. Cette requête est envoyée au serveur de nom primaire.
- **Coté SERVEUR** : à la réception d'une demande de traduction par le serveur de noms, celui-ci vérifie si la réponse est disponible dans sa base de données locale ou dans son cache:
  - Si la réponse est affirmative, alors il traduit le nom en une adresse et renvoie la réponse au client.
  - S'il ne peut résoudre l'intégralité de la traduction, alors :
    i. si le client a demandé une traduction complète de nom (récursive) :le serveur de noms interroge les autres serveurs de noms disponibles, en commençant par la racine de l'arbre DNS et les réponses obtenues alimente le cache local
    ii. le client a demandé une traduction complète non récursive (itérative): le serveur de noms ne peut fournir de réponse, il indique le nom du serveur à contacter.

Le résolveur : les fonctions permettant de réaliser respectivement la résolution et la résolution inverse de nom sont : gethostbyname() et gethostbyaddr()

Protocole DNS : ressources

- Les nœuds de l'espace sont décrits par des enregistrements appelés RR (Record Ressource) maintenus à jour sur des serveurs autorisés (opération manuelle) dont le rôle est de propager ces informations en répondant aux questions posées par des résolveurs.

L. Les applications

1. Telnet : Connexion à distance

Permet à un utilisateur d'établir, depuis son ordinateur, une connexion TCP avec le serveur d'un ordinateur distant.

Exemple

% telnet Asterix.utc.fr ou % telnet 192.114.28.1

2. FTP

FTP offre de nombreuses options qui dépassent le cadre du simple transfert de fichiers.

- **Accès interactif** : utilisation d'une interface interactive permettant à un utilisateur d'interagir avec le serveur distant.

Exemple :

Demande de la liste de tous les fichiers d'un répertoire situé sur un ordinateur distant.

- **Spécification du format** : un client peut préciser le type et le format des données stockées.

- **Authentification** : FTP exige d'un client un nom d'utilisateur et un mot de passe.

3. Protocole SMTP

- Emission/réception du courrier
- Indépendant de l'interface utilisateur
- Les messages sont envoyés en caractères ASCII
- Communication Client/Serveur
  - Etablissement de connexion client/serveur SMTP
  - Envoie du message en indiquant le récepteur
  - Le serveur répond par OK si le récepteur existe sinon il fait suivre à un serveur spécialisé.

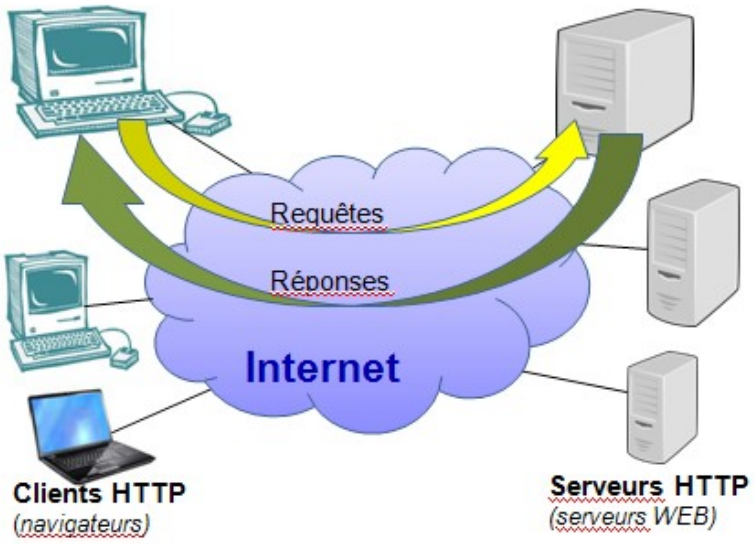
POP-3 : Post Office Protocol v3

- Lecture /écriture de mail hors connexion
- Le serveur répartit tous les courrier en provenance de l'Internet dans le dossier de chaque utilisateur
- L'accès à ces dossiers nécessite une autorisation
- Adapté à des liaisons PPP pour des connexions temporaires (réduction des coûts)

M. Intranet

1. Hypertext, World Wide Web, Navigateurs

- Le protocole de transfert hypertexte (HTTP : HyperText Transfer Protocol) est un protocole de niveau applicatif pour les systèmes d'information distribués, collaboratifs et hypermédia.
- Le protocole HTTP constitue la base de la communication de données pour le World Wide Web depuis 1990. C'est un protocole générique qui peut être utilisé à d'autres fins comme les serveurs de noms et les systèmes de gestion d'objets distribués, grace aux extensions de ses méthodes de demande, codes d'erreur et en-têtes .
- Fondamentalement, HTTP est un protocole de communication basé sur TCP/IP qui permet de fournir des données (fichiers HTML, fichiers image, résultats de requêtes, etc.) sur le World Wide Web. Le port par défaut est TCP 80, mais d'autres ports peuvent également être utilisés. Il fournit une manière standardisée pour que les ordinateurs communiquent entre eux.
- HTTP fonctionne en mode client/serveur et spécifie comment les requêtes des clients seront construites et envoyées au serveur et comment les serveurs répondent à ces requêtes.

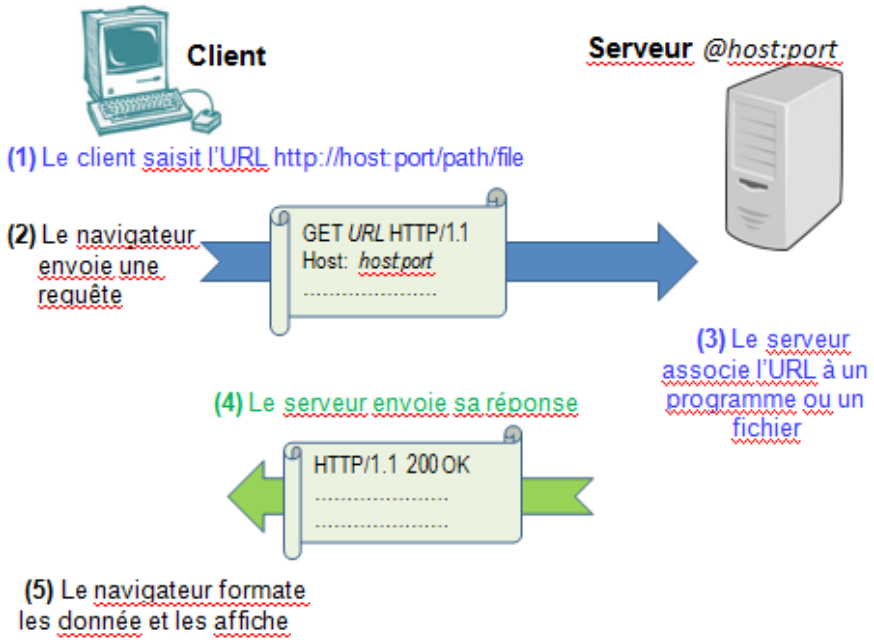


Il existe trois caractéristiques de base qui font de HTTP un protocole simple mais puissant:

- HTTP est sans connexion : le client HTTP envoie une requête HTTP et après il se déconnecte du serveur et attend une réponse. Le serveur traite la demande et rétablit la connexion avec le client pour lui envoyer une réponse.
- HTTP est indépendant des médias : cela signifie que tout type de données peut être envoyé par HTTP tant que le client et le serveur savent comment gérer le contenu des données. Il est nécessaire pour le client ainsi que pour le serveur de spécifier le type de contenu en utilisant le type MIME approprié.
- HTTP est sans état : la requête actuelle ignore complètement ce qui été fait avant. En raison de cette nature du protocole, ni le client ou le navigateur peuvent retenir des informations entre différents des demandes sur les pages Web.

HTTP / 1.0 utilise une nouvelle connexion pour chaque échange de requête/réponse, alors que la connexion HTTP / 1.1 peut être utilisée pour un ou plusieurs échanges de demande / réponse.

Navigateur : lorsqu'un utilisateur fournit une URL dans le navigateur pour obtenir une ressource Web à l'aide de HTTP, par ex. http://www.baali.com/index.html, le navigateur transforme l'URL en une requête et l'envoie au serveur HTTP. Le serveur HTTP interprète la requête et vous renvoie un message de réponse approprié, soit la ressource demandée, soit un message d'erreur comme illustré dans la figure ci-dessous.



Uniform Resource Locator (URL) : une URL (Uniform Resource Locator) est utilisée pour identifier de manière unique une ressource sur le Web. L'URL a la syntaxe suivante : protocol://hostname:port/path-and-file-name.

Une URL est composée de quatre parties :

- Protocole (protocol): protocole de niveau d'application utilisé par le client et le serveur, par exemple HTTP, FTP et telnet.

- Nom d'hôte (hostname) : le nom de domaine DNS (par exemple, www.baali.com) ou l'adresse IP (par exemple, 192.128.1.2) du serveur.

- Port: le numéro de port TCP sur lequel le serveur écoute les demandes reçues des clients.

- Path-and-file-name : nom et emplacement de la ressource demandée, sous le répertoire de base du serveur.

Exemples :

dans l'URL **http://www.baali.com/docs/index.html**, le protocole de communication est HTTP,

- Le nom d'hôte est www.baali.com.

- Le numéro de port n'a pas été spécifié dans l'URL et prend donc le numéro par défaut qui est le port TCP 80 pour HTTP.

- Le chemin d'accès et le nom de fichier de la ressource à localiser est "/docs/index.html".

Autres exemples d'URL :

- ftp://www.ftp.org/docs/test.txt
- mailto:user@essai.com
- news:soc.culture.france
- telnet://www.baali.com/

Le protocole HTTP

Comme mentionné ci-dessus, lorsqu'un un utilisateur saisit une URL dans la zone d'adresse du navigateur, celui-ci traduit l'URL dans une requête selon le protocole spécifié et l'envoie au serveur.

Une requête est un message structurés et composé de :

- une ligne initiale
- zéro ou plusieurs lignes d'en-tête (format :
  - Header1 : valeur1
  - Header2 : valeur2
- Une ligne vide (CRLF)
- Le corps (optionnel) du message

Les lignes doivent se terminer par CRLF.

Exemple :

Le navigateur associe à l'URL http://www.baali.com/doc/index.html la requête suivante:

GET /docs/index.html HTTP/1.1

Host: www.nowhere123.com

Accept: image/gif, image/jpeg, */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

(blank line)

Lorsque cette requête arrive au serveur, il exécute une des actions suivantes :

- Le serveur interprète la requête reçue, associe le fichier sous le répertoire du document du serveur, et renvoie le fichier demandé au client.

- Le serveur interprète la requête reçue, mappe la requête dans un programme conservé dans le serveur, exécute le programme et renvoie la sortie du programme au client.

- La demande ne peut pas être satisfaite, le serveur renvoie un message d'erreur.

Ligne initiale pour les messages de réponse :

comprend trois parties séparées par des espaces : version de HTTP, code de statut, description du code de statut.

- HTTP/1.0 200 OK

- HTTP/1.0 404 Not Found

Le code est un entier sur trois chiffre dont le premier chiffre identifie la catégorie :

- 1xx : message d'information
- 2xx : succès (plusieurs variantes)
- 3xx : redirection
- 4xx : erreur du côté du client
- 5xx : erreur du côté du serveur

Par exemple : 301 Moved Permanently, 302 Moved Temporarily, 500 Server Error, ...

Lorsque le navigateur reçoit le message de réponse, il l'interprète et affiche son dans la fenêtre du navigateur selon le type de média de la réponse (comme dans l'en-tête de réponse Content-Type). Le type de média peut être :"text / plain", "text / html", "image / gif", "image / jpeg", "audio / mpeg", "video / mpeg", "application / msword" Pdf ".

Le reste du temps, un serveur HTTP ne fait qu'écouter les adresses IP et les ports spécifiés dans les requêtes entrante. Lorsqu'une demande arrive, le serveur analyse l'en-tête du message, applique les règles spécifiées dans la configuration et prend les mesures appropriées.

2. Intranet (Intranet = Internet + LAN)

L'informatique a évolué selon plusieurs phase :

1. Mainframes : sauvegardes, administration, accès (mail propriétaire) (70)
2. LAN (années 80-90) : échange de données au sein de l'entreprise (localement)
3. LAN/WAN : système d'information englobant l'ensemble de l'entreprise : E-mail, accès distant, etc. (dimension géographique plus importante) mais ça reste une infrastructure pour le transport de l'information.
4. **Intranet** : est construit à partir des infrastructures réseaux locaux (LAN) et éventuellement réseaux longue distance (WAN) avec :
   - l'ajout de TCP-IP
   - l'intégration de services WEB
   - la possibilité de mettre en place des réseaux virtuels
   - la possibilité d'intégration des fournisseurs, partenaires, et clients par un accès distant via l'internet

3. Intranet et le monde exterieur

Intranet Stand-Alone

- LAN d'entreprise utilisant la technologie Internet
- Pas de connexion directe avec l'internet
- Raisons : connexion internet risquée, coût des protections adaptés chers

Intranet avec Internet

- Utilisation d'internet pour construire un réseau privé virtuel
- Les données sont partagées
- Solution "sûre" si l'intranet est protégé par un firewall

N. IP sur liaison série

1. PPP - protocole Point à Point

- Le protocole PPP a été développé par Internet Internet Engineering Task Force (IETF) comme moyen de transmission, sur une liaison point-à-point, de données issues de différents protocoles de la couche réseau (IPv4, IPv6, etc), et cela de manière standard et indépendante du fournisseur.
- PPP fournit des connexions directes sur des circuits synchrones et asynchrones.
- PPP dispose également d'une sécurité intégrée en s'appuyant sur les protocoles PAP (Password Authentication Protocol), CHAP (Challenge Authentification Handshake Protocol) et EAP (Extensible Authentication Protocol)
- Le protocole PPP se compose des composants principaux suivants:
  - Une méthode pour encapsuler des datagrammes sur une liaison série ou liaisons point à point comme HDLC (High Level Data Link Control), L2TP (Layer 2 Tunneling Protocol) et PPPoE (Point-à-Point Protocole sur Ethernet).
  - Un protocole de contrôle de liaison (LCP) pour établir, configurer et tester la liaison de données série.
  - Une famille de protocoles de contrôle réseau (NCP) pour établir et

configurer différents protocoles de la couche réseau. PPP permet l'utilisation simultanée d'une couche de réseau multiple Protocoles. Le protocole IPCP (Internet Protocol Control Protocol) est un NCP.

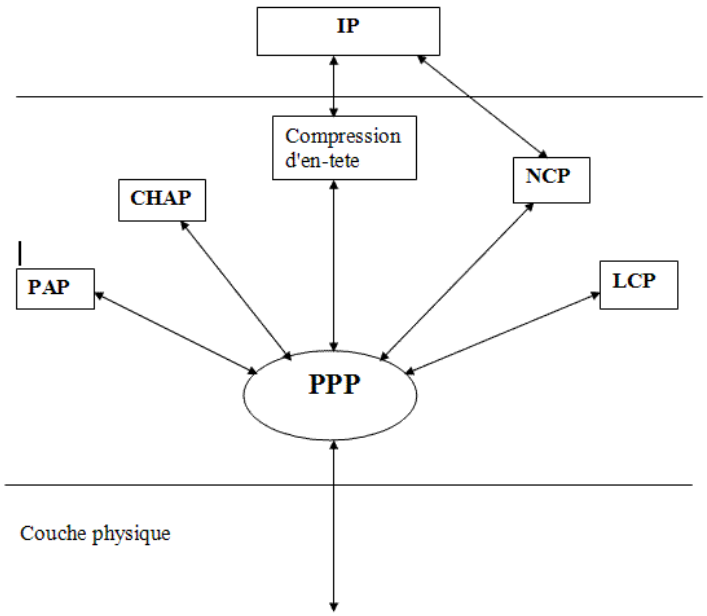


Image 29 PPP

La méthode utilisée par PPP pour transporter le trafic réseau consiste à ouvrir un lien avec un bref échange de trames. Une fois que le lien est ouvert, le trafic réseau est transporté avec un faible overhead : le trafic est transmis sous la forme d'une série de trames d'information non numérotées, ce qui signifie qu'aucune trame d'accusé de réception n'est exigée et aucune retransmission ne se produit. Une fois le lien établi, PPP agit comme un canal de données direct pour les protocoles de couche supérieure qu'il encapsule.

O. IP nouvelle generation : IPV6

1. Introduction

IP version 6 (IPv6) est une nouvelle version du Protocole Internet. Les changements entre IPv4 et IPv6 se répartissent en première approche dans les catégories suivantes :

Augmentation des possibilités d'adressage

IPv6 augmente la taille des adresses IP de 32 bits à 128 bits, pour supporter un plus grand nombre de nœuds adressables et une auto-configuration plus simple des adresses. Une plus grande souplesse de configuration du multicasting. Ensuite, un nouveau type d'adresse, l'adresse Anycast. IPv6 définit également une architecture de routage hiérarchique et flexible à plusieurs niveaux.

Simplification du format de l'en-tête

Certains champs de l'en-tête IPv4 ont été enlevés ou rendus optionnels, pour réduire dans les situations classiques le coût (en ressources de traitement) de la gestion des paquets et pour limiter le surcoût en bande passante de l'en-tête IPv6.

Support amélioré des options et des extensions futures

Des changements dans la façon dont les options de l'en-tête IP sont encodés permettent une transmission (forwarding) plus efficace, des limites moins strictes sur la longueur des options et une plus grande flexibilité dans l'introduction par la suite de nouvelles options. La plupart des en-têtes d'extension ne sont pas traitées par les nœuds intermédiaires, ce qui n'était pas le cas avec IPv4.

Fonctionnalité d'étiquetage de flux d'informations

Une nouvelle fonctionnalité est ajoutée pour étiqueter des paquets appartenant à des "flux" d'informations particuliers pour lesquels l'émetteur demande une gestion spéciale, comme un service " sans perte d'information " ou un service " temps réel ".

Fonctionnalité d'authentification et de confidentialité

Des extensions pour gérer l'authentification, l'intégrité des données ou une (optionnelle) confidentialité des données sont spécifiées par IPv6.

L'Anycast

Deux ou plusieurs interfaces sur un nombre arbitraire de nœuds sont désignées comme un groupe Anycast (ces nœuds sont configurés pour reconnaître les adresses Anycast). Un paquet envoyé à une adresse Anycast est délivré seulement à une interface dans le groupe. Typiquement, le plus proche.

2. Format de l'entete IPV6

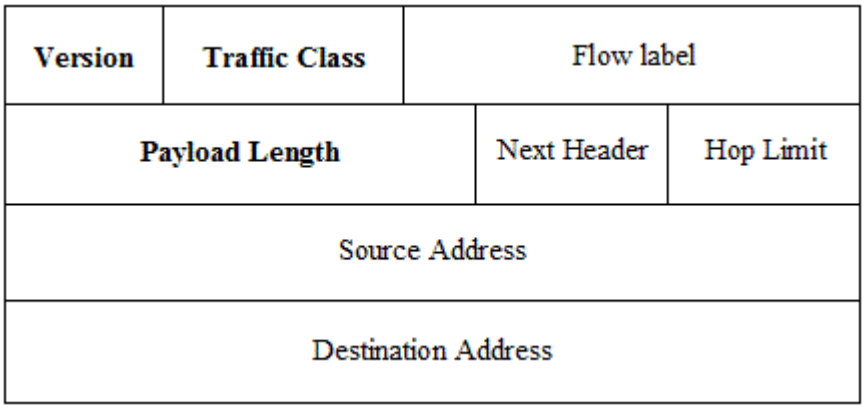


Image 30 Entete IPv6

- **Version (4 bits)** : numéro de version du Protocole Internet (= 6).
- **Traffic Class (8 bits)** : indique la classe de trafic.
- **Flow Label (20 bits)** : Label du flux d'information.
- **Payload Length** ou Longueur de la "Charge Utile" **(16 bits)** : indique la longueur en octets de la charge utile, i.e., le reste du paquet qui suit cet en-tête IPv6.

  Il faut noter que tous les en-têtes d'extension présents sont considérés comme faisant partie de la charge utile, i.e., inclus dans le décompte de la longueur.
- **Next Header** : Sélecteur sur 8 bits. Identifie le type de l'en-tête suivant immédiatement l'en-tête IPv6. Utilise les mêmes valeurs que le champ " protocole " d'IPv4
- **Hop Limit** ou Nombre de Sauts Maximum (8 bits) : il est décrémenté de 1

par chaque nœud que le paquet traverse. Le paquet est éliminé si le Nombre de Sauts Maximum arrive à zéro.

- **Adresse Source** (Source Address) : adresse sur 128 bits de l'expéditeur initial du paquet.
- **Adresse Destination** (Destination Address) : adresse sur 128 bits du destinataire projeté du paquet (qui peut ne pas être le destinataire ultime, si un en-tête de routage est présent).

3. Les en-têtes IPv6 d'extension

Avec IPv6, les informations optionnelles de la couche inter-réseaux sont encodées dans des en-têtes séparés qui peuvent être placés entre l'en-tête IPv6 et l'en-tête de couche supérieure d'un paquet.

Les en-têtes d'extension sont identifiés par une valeur distincte d' "Entete Suivant".

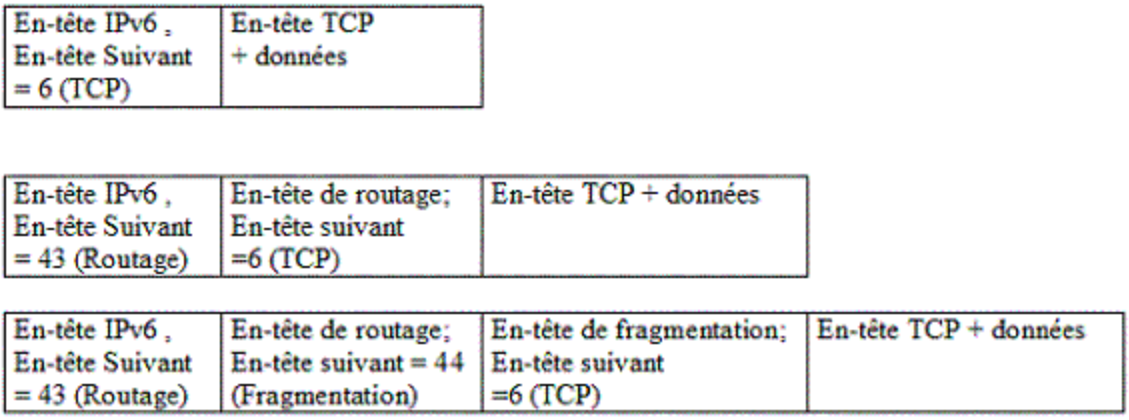


Image 31 entetes d'extension IPv6

Contrairement à IPv4 où toutes les options sont examinées par les routeurs intermédiaires, les routeurs IPv6 examinent uniquement l'en-tête Hop-by-Hop.

Le démultiplexage normal à partir du champ " En-tête Suivant " de l'en-tête IPv6 appelle le module pour gérer le premier en-tête d'extension ou l'en-tête de plus haut niveau s'il n'y a pas d'en-tête d'extension.

Les en-têtes d'extension doivent être analysés dans l'ordre exact où ils apparaissent dans le paquet.

Si, lors du traitement des en-têtes, un nœud atteint une valeur d'" En-tête Suivant " non reconnue à l'intérieur de l'en-tête qu'il traite, il devrait éliminer le paquet et envoyer à la source un message ICMP "Parameter Problem message".

Tout en-tête d'extension a une longueur multiple de 8 octets, dans le but de maintenir un alignement sur 8 octets des en-têtes suivants.

Une implémentation complète d'IPv6 inclut l'implémentation des en-têtes d'extension suivants

- en-tête des options sauts après sauts
- en-tête de routage
- en-tête de fragmentation
- en-tête des options de destination
- en-tête d'authentification [RFC-2402]
- en-tête d'encapsulation de charge utile sécurisée [RFC-2406]

Value (in decimal)	Header
0	Hop-by-Hop Options Header
6	TCP
17	UDP
41	Encapsulated IPv6 Header
43	Routing Header
44	Fragment Header
46	Resource ReSerVation Protocol
50	Encapsulating Security Payload
51	Authentication Header
58	ICMPv6
59	No next header
60	Destination Options Header

Image 32 Valeurs du champs en-tête

4. Ordre des en-têtes d'extension

Quand il y a plus d'un en-tête d'extension dans un même paquet, il est recommandé que ces en-têtes apparaissent dans l'ordre suivant :

- en-tête IPv6
- en-tête des options Hop-By-Hop
- en-tête des options de destination
- en-tête de routage (source routing)
- en-tête de fragmentation
- en-tête d'authentification
- en-tête d'encapsulation de charge utile sécurisée
- en-tête des options de destination
- en-tête de couche supérieure

5. Options

Deux des en-têtes d'extension actuellement définis (l'en-tête des options Hop-by-Hop et l'en-tête des options de destination) transportent un nombre variable d'options encodées (Type, Longueur, Valeur (TLV)), comme suit :

Type d'Option (8bits)	L Données Opt (8bits)	Données de l'Option (lg. Variable)

Image 33 Options

- Type d'Option (Option Type) : Identificateur du type d'option.
- L Données Opt (Opt Data Len) : longueur en octets du champ Données de l'Option de cette option.
- Données de l'Option (Option Data) : Champ de longueur variable, données spécifiques au Type d'Option.

La séquence d'options à l'intérieur d'un en-tête doit être traitée strictement dans

l'ordre où apparaissent ces options dans l'en-tête.

Les RFCs 2460,2675, et 2711 définissent les options suivantes :

- Pad1 (type =0) : utilisée pour insérer un seul octet d'alignement
- Pad2 (Type=1) : utilisée pour insérer deux ou plusieurs octets d'alignement
- Jumbo payload (Type=194) : est utilisé pour indiquer que la taille des données utiles est supérieur à 65535
- Router Alert option (Type=5) : est utilisé pour indiquer au routeur que le contenu de ce paquet nécessite un traitement supplémentaire (Ex : RSVP)

6. En-tête des options hop by hop

L'en-tête des options Hop-by-Hop est utilisé pour transporter des informations optionnelles qui doivent être examinées par chaque nœud le long du chemin emprunté par le paquet.

L'en-tête des options Hop-by-Hop est identifié par une valeur d'En-tête Suivant à 0 dans l'en-tête IPv6 et a le format suivant :

En-tête Suivant (8 bits)	**L En-tête Ext** (8 bits)	.
.	**Options** (lg variable)	

Image 34 En-tête des options Hop-by-hop

- **En-tête suivant (Next Header)** : Identifie le type de l'en-tête suivant immédiatement l'en-tête des options Hop-by-Hop.

  Utilise les mêmes valeurs que le champ " protocole " d'IPv4.
- **L En-tête Ext (Hdr Ext Len)** : Entier 8 bits non signé.

  Longueur de l'en-tête des options sauts après sauts en mots de 8 octets, sans compter les 8 premiers octets.
- **Options** : Champ de longueur variable, telle que l'en-tête des options Hop-by-Hop complet soit un entier multiple de 8 octets.

  Contient au moins une option encodée TLV.

7. En-tête de routage

L'en-tête de routage est utilisé par une source IPv6 pour lister au moins un nœud intermédiaire à " aller voir " sur le chemin emprunté par le paquet vers la destination.

Cette fonction est très similaire aux options " Loose Source " ou " Record Route " d'IPv4.

L'en-tête de routage est identifié par une valeur d'entete Suivant à 43 dans l'en-tête le précédent immédiatement et a le format suivant :

En-tête Suivant (8 bits)	**L En-tête Ext** (8 bits)	. **Type de routage** (8 bits)	**NbSeg Restant** (8 bits)
.	**Données Spécifiques**	(lg variable)	

Image 35 7

- **En-tête Suivant (Next Header)** : Identifie le type de l'en-tête suivant immédiatement l'en-tête de routage.

Utilise les mêmes valeurs que le champ " protocole " d'IPv4.

- **L En-tête Ext (Hdr Ext Len)** : Longueur de l'en-tête de routage en mots de 8 octets, sans compter les 8 premiers octets.
- **Type de Routage (Routing Type)** : Identificateur de la variante particulière de l'en-tête de routage.
- **NbSeg Restant (Segments Left)** : indique le nombre de segments de chemin restant, i.e., nombre de nœuds intermédiaires listés explicitement qu'il reste à traverser avant d'atteindre la destination finale.
- **Données Spécifiques (type-specific data)** : Champ de format déterminé par le Type de Routage, et de longueur telle que l'en-tête de routage complet soit un multiple entier de 8 octets.
- **Si**, au cours du traitement d'un paquet reçu, un nœud rencontre un en-tête de routage avec une valeur de Type de Routage inconnue, alors :
  - Si le NbSeg Restant est zéro, le nœud doit ignorer l'en-tête de routage et procéder au traitement de l'en-tête suivant dans le paquet.
  - Si le NbSeg Restant est différent de zéro, le nœud doit éliminer le paquet et envoyer un message ICMP Problème de Paramètre, Code 0, pointant sur le Type de Routage inconnu, à l'adresse source du paquet.

Entete de routage de type 0

En-tête Suivant (8 bits)	L En-tête Ext (8 bits)	Type de routage (8 bits)	NbSeg Restant (8 bits)
	Réservé		
	Adresse1		
	Adresse2		
	. . .		
	Adresse(n)		

Image 36 Format de l'entete de routage de Type 0

- **Next Header** : Identifie le type de l'en-tête suivant immédiatement l'en-tête de routage. Utilise les mêmes valeurs que le champ " protocole " d'IPv4.
- **L En-tête Ext (Hdr Ext Len)** : Longueur de l'en-tête de routage en mots de 8 octets, sans compter les 8 premiers octets.
- **Routing Type** : 0.
- **NbSeg Restant (Segments Left)** : Nombre de segments de chemin restant
- **Réservé** : Initialisé à zéro pour la transmission ; ignoré en réception.
- **Adresse[1..n]** : Vecteur d'adresses de 128 bits, numérotées de 1 à n.

Pour le routage de type 0, le champ données spécifiques contient une liste d'adresses. Lorsqu'un nœud reçoit un paquet, il le traite et met l'adresse destination IPv6 la prochaine dans la liste.

Les adresses multicast ne doivent pas apparaître dans un en-tête de routage de type 0 ou dans le champ Adresse Destination IPv6 d'un paquet transportant un en-

tête de routage de type 0.

8. En-tête de fragmentation

L'en-tête de fragmentation est utilisé par une source IPv6 pour envoyer un paquet plus large que celui qui tiendrait dans le MTU de chemin vers la destination. Contrairement à IPv4, la fragmentation dans IPv6 n'est réalisée que par les nœuds sources. L'en-tête de fragmentation est identifié par une valeur d'En-tête Suivant de 44 dans l'en-tête le précédent immédiatement.

Il a le format suivant :

En-tête Suivant (8 bits)	Réservé (8 bits)	Offset Fragment (13 bits)	Res (2bits)	P (1)
	identification			

Image 37 Entete de fragmentation

- **En-tête Suivant** : Identifie le type d'en-tête initial de la Partie Fragmentable du paquet original (définie ci-après). Utilise les mêmes valeurs que le champ Protocole d'IPv4
- **Réservé (Reserved)** : Initialisé à zéro pour la transmission ; ignoré en réception.
- **Offset de fragmentation** : donné en nombre de mots de 8 octets, par rapport au début de la Partie Fragmentable (Fragmentable Part) du paquet original.
- **Rés (Res)** : Champ réservé de 2 bits. Initialisé à zéro pour la transmission ; ignoré en réception.
- **Drapeau P (M flag)** : 1 = plus de fragments ; 0 = dernier fragment
- **Identification** : pour chaque paquet devant être fragmenté, le nœud source génère une valeur d'Identification. L'Identification doit être différente de tout autre identification de paquet fragmenté envoyé récemment (à l'intérieur du temps de vie maximum vraisemblable incluant le temps de transit de la source à la destination et le temps passé à attendre l'assemblage des autres fragments du même paquet.) avec les mêmes Adresse Source et Adresse Destination. Si un en-tête de routage est présent, l'Adresse Destination concernée est celle de la destination finale.

Paquet original

Le paquet initial, long et non fragmenté est dénommé le " paquet original " et est considéré comme constitué de deux parties, comme illustré ci-après :

Partie non fragmentable	Partie fragmentable

Image 38 Paquet original

- **La partie non fragmentable** est constituée de l'en-tête IPv6 et de tous les en-têtes d'extension qui doivent être traités par des nœuds en cours de route vers la destination.
- **La partie fragmentable** est constituée du reste du paquet, il s'agit de tout en-tête d'extension qui ne nécessite que le traitement du (des) nœud(s) destination finale ainsi que l'en-tête et les données de couche supérieure. La partie fragmentable du paquet original est divisée en fragments, chacun, excepté peut-être le dernier (" le plus à droite "), étant un multiple entier de mots de 8 octets.
- Les fragments sont transmis dans des " paquets fragmentés " (" fragment

packets ") comme illustré ci-après.

Partie non fragmentable	premier fragment	Deuxième fragment	....	dernier fragment

Paquets fragmentés :

Partie non fragmentable	En-tête de fragmentation	premier fragment

Partie non fragmentable	En-tête de fragmentation	Deuxième fragment

Image 39 Paquets fragmentés

Composition d'un paquet fragmenté

Chaque paquet fragmenté est composé de :

1. **La partie non fragmentable** du paquet original, avec la Longueur de la Charge Utile de l'en-tête IPv6 original changé en la longueur de ce fragment uniquement (en excluant la longueur de l'en-tête IPv6 lui-même), et le champ d'En-tête Suivant du dernier en-tête de la partie non fragmentable changé en 44.
2. **Un en-tête de fragmentation** contenant :
   - la valeur d'En-tête Suivant qui identifie le premier en-tête de la partie fragmentable du paquet original.
   - Un offset de fragmentation contenant l'offset du fragment, en nombre de mots de 8 octets, par rapport au début de la partie fragmentable du paquet original. L'offset de fragmentation du premier fragment (" le plus à gauche ") est 0.
   - Une valeur du drapeau P à 0 si le fragment est le dernier (" le plus à droite "), sinon une valeur du drapeau P à 1.
   - La valeur d'identification générée pour le paquet original.
3. **Le fragment lui-même** : Les longueurs des fragments doivent être choisies telles que les paquets fragmentés résultants tiennent dans le MTU de chemin vers la (les) destination(s) du paquet. Arrivés à destination, les paquets fragmentés sont rassemblés pour obtenir leur forme originale, non fragmentée.

9. En-tête des options de destination

L'en-tête des options de destination est utilisé pour transporter des informations optionnelles qui ont besoin d'être examinées par les nœuds intermédiaires ou par le(s) nœud(s) destination du paquet. L'en-tête des options de destination est identifié par une valeur d'En-tête Suivant à 60 dans l'en-tête le précédent immédiatement.

Il a le format suivant :

En-tête Suivant (8 bits)	**L En-tête Ext** (8 bits)	
	Options (lg variable)	

Image 40 Entete des options de destination

- **En-tête Suivant** : Identifie le type de l'en-tête suivant immédiatement l'en-tête des options de destination. Utilise les mêmes valeurs que le champ " protocole " d'IPv4
- **L En-tête Ext** : non signé. Longueur de l'en-tête des options de destination en mots de 8 octets, sans compter les 8 premiers octets.
- **Options** : Champ de longueur variable, telle que l'en-tête des options de destination complet soit un entier multiple de 8 octets. Contient au moins une option.

Les options sont les mêmes que celles définies dans l'option Hop-by-Hop.

L'en-tête des options de destination est utilisé de deux manières :

1. Si un en-tête de routage est présent, cette option spécifie les options de traitement ou de livraison des paquets en chaque nœud intermédiaire
2. Il spécifie les options de traitement et de livraison au destinataire final

10. Pas d'entete suivant

La valeur 59 dans le champ En-tête Suivant d'un en-tête IPv6 ou tout autre en-tête d'extension indique que rien ne suit cet en-tête. Si le champ Longueur de la Charge Utile de l'en-tête IPv6 indique la présence d'octets après la fin de l'en-tête dont le champ En-tête Suivant contient 59, ces octets doivent être ignorés et envoyés tels quels si le paquet doit être transmis.

11. Adressage IPv6 (RFC 3513)

Présentation

L'adressage IPv6 permet d'augmenter l'espace d'adressage en comparaison avec IPv4 et ainsi apporter une solution au problème de pénurie d'adresses.

Une adresse IPv6 tient sur 128 bits (IPv4 sur 32 bits). Cet adressage permet de définir 6.6*1023 adresses/m2 (dans la planète) et a été conçu pour être organisé en domaines de routage hiérarchiques (souplesse,...), ce qui n'était pas le cas en IPv4.

Syntaxe de l'adresse IPv6

Une adresse IPv6 tient sur 128 bits.

L'adresse suivante est une forme binaire d'une adresse IPv6.

- 00100001110110100000000011010011000000000000000000010111100111011
- 00000010101010100000000011111111111111110001010001001110001011010

Les 128 bits sont divisés en blocs de 16 bits, chaque bloc est représenté en quatre chiffres hexadécimaux.

La représentation hexa de l'adresse ci-dessus serait :

- 0010000111011010 0000000011010011 0000000000000000 0010111100111011
- 0000001010101010 0000000011111111 1111111000101000 1001110001011010

Chaque bloc de 16 bits est convertit en hexa et on obtient : 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

La représentation IPv6 peut également être simplifiée en supprimant des zéros de chaque bloc de bits contigus.

L'adresse ci-dessus devient : 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Compression des zéros

Certaines adresses contiennent plusieurs séquences de zéros.

Pour simplifier la représentation de l'adresse, une suite de blocs de 16 bits à "0" contigües peut être compressée en "::"

Exemple 1 :

- L'adresse FE80:0:0:0:2AA:FF:FE9A:4CA2 peut être compressée en FE80::2AA:FF:FE9A:4CA2 et l'adresse FF02:0:0:0:0:0:0:2 peut être compressée en FF02::2
- Cette compression ne peut etre utilisée qu'une seule fois.

Exemple 2 :

- Il n'est pas autorisé de compresser FF02:30:0:0:0:0:0:5 en FF02:3::5
- La compression correcte serait : FF02:30::5.

12. Les préfixes IPv6

Le préfixe indique la partie de l'adresse traitée comme adresse réseau.

Cette notation est similaire à celle utilisée dans CIDR.

Un préfixe est noté par : **adresse/longueur-prefixe**

Exemple de Préfixe de routage : 21DA:D3::/48

Exemple de Préfixe de sous-réseau : 21DA:D3:0:2F3B::/64

La notion de masque réseau utilisé en IPv4 n'existe pas en IPv6

13. Types d'adresses IPv6

Il existe trois types d'adresses :

1. **Unicast** : identifie une seule interface dans le "scope" du type d'adresse. Les paquets sont délivrés à cette adresse
2. **Multicast** : identifie plusieurs interfaces. Les paquets envoyés à une adresse multicast sont livrés à toutes les interfaces identifiés par cette adresse
3. **Anycast** : identifie plusieurs interfaces. Les paquets envoyés à une adresse anycast sont livrés à une seule interface, c'est la plus proche interface identifiée par cette adresse

Il est à noter que :

- La RFC 3513 ne définit pas l'adresse broadcast.
- Le broadcast est réalisé par un multicast en IPv6.

Liens et sous-réseaux

Comme dans IPv4, un préfixe sous-réseau (ID de sous-réseaux) est affecté à un seul lien. Plusieurs ID de sous-réseau peuvent être affecté au même lien. Cette technique est appelée **Multinetting**

14. Adresses Unicast

Adresse Unicast Globale

Est équivalente à une adresse IPv4 publique.

Elle est routable et accessible sur le réseau IPv6.

La figure suivante donne la structure de l'adresse unicast globale actuellement allouée par l'IANA et telle que définie dans la RFC3587.

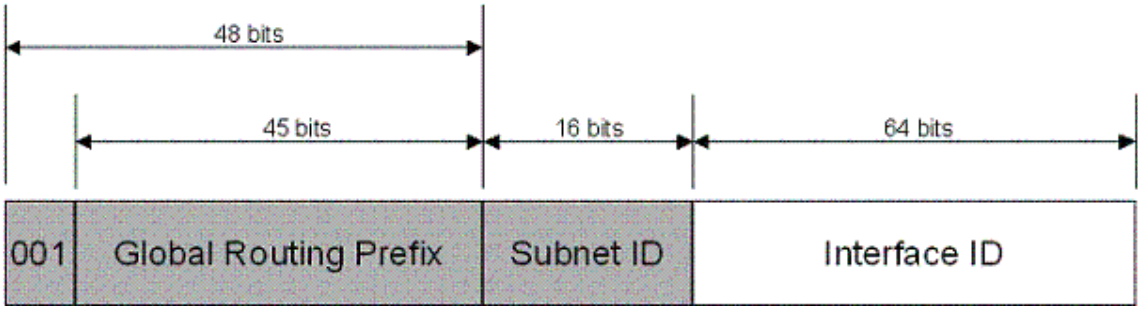


Image 41 Adresse Unicast globale

- **Bits 001** : les trois bits de poids fort sont à 001. Le préfixe des addresses global est 2000::/3
- **Global Routing Prefix** : indique le préfixe d'un site d'une organisation. Les 3 bits fixe et les 45 bits de ce champ forment le préfixe d'un site d'une organisation. Une fois affecté, les routeurs du réseau IPV6 routent les paquets destinés à cette adresse aux routeurs du site de cette organisation.
- **Subnet ID** : est utilisé à l'intérieur du site d'une organisation pour identifier des sous-réseaux. Les sites peuvent créer 65536 sous-réseaux ou plusieurs niveaux hiérarchiques ainsi qu'une infrastructure de routage.
- **Interface ID** : Identifie une interface d'un sous-réseau d'un site spécifique.

Utilisation locale des adresses Unicast

Il existe deux types d'utilisation locale des adresses Unicast :

- **Adresses de lien local** : sont utilisées par les nœuds lorsqu'ils souhaitent communiquer avec des nœuds voisins sur le même lien. Une adresse link local est exigée pour le processus de découverte de voisins et elle est toujours configurée automatiquement même en absence des autres adresses unicast.

  La structure d'une adresse link local est la suivante :

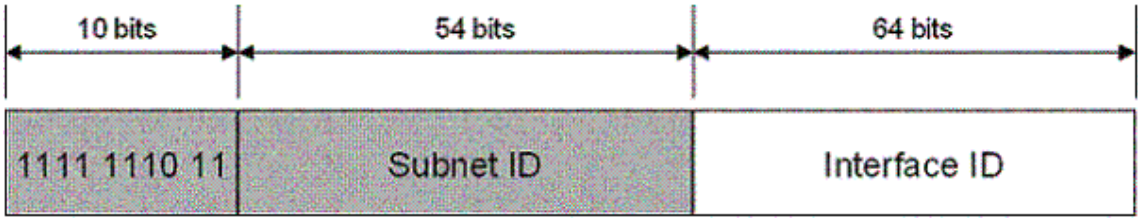


Image 42 Adresse de lien local

- Une adresse lien local commence toujours par FE80. Avec l'identificateur d'interface 64 bits, le préfixe d'une adresse lien local est FE80::/64.

  Un routeur IPv6 ne forwarde jamais le trafic link local au-delà du lien.

- **Adresses de Site local** : Les adresses site local sont équivalentes aux adresses privées dans IPv4. Contrairement aux adresses lien local, les adresses site local ne sont pas configurées automatiquement et doivent être affectées via un processus de configuration d'adresses.

  La structure d'une adresse site local est la suivante :

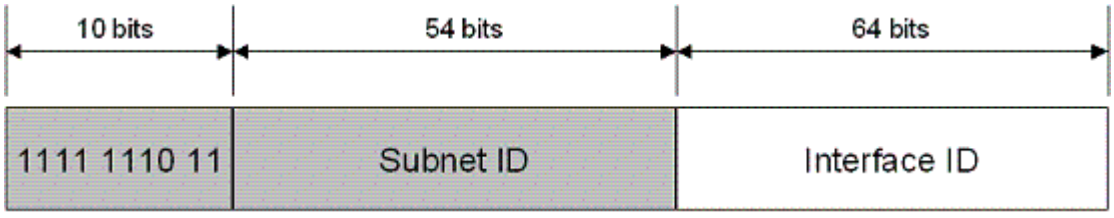


Image 43 Adresse de site local

15. Adresses IPv6 particulieres

Adresse indéterminée

- 0:0:0:0:0:0:0:0 ou ::
  - est utilisée uniquement pour indiquer l'absence d'une adresse.
  - Elle est équivalente à l'adresse IPv4 0.0.0.0.

Adresse de bouclage

- 0:0:0:0:0:0:0:1 ou ::1
  - Elle est équivalente à l'adresse 127.0.0.1.

Compatibilité d'adresses

- Pour faciliter la migration de IPv4 à IPv6 et la co-existence des deux types d'adresses, les adresses suivantes ont été définies :
  - **Adresses compatibles IPv4** : ont le format 0:0:0:0:0:0:w.x.y.z ou ::w.x.y.z (où w.x.y.z est une adresse IPv4). Ces adresses sont utilisées par les nœuds qui supportent IPv4 et IPv6 et communiquant en IPv6. Quand une adresse compatible IPv4 est utilisée comme adresse destination IPv6, le trafic IPv6 est automatiquement encapsulé dans un en-tête IPv4 et envoyé à une destination sur une infrastructure IP4.
  - **Adresses IPv4 mappées** : sont utilisées pour représenter un nœud IPv4 à un nœud IPv6. C'est uniquement une représentation interne. Cette adresse n'est jamais utilisée comme adresse source ou adresse destination d'un paquet IPv6.
  - **Adresses 6to4 (RFC 3056)** : sont utilisées pour la communication entre nœuds supportant IPv4 et IPv6 (tunneling), et communiquant via une infrastructure de routage IPv4. Elle est formée en combinant le préfixe 2002::/16 avec l'adresse IPv4 publique du nœud pour former le préfixe 48 bits.

16. Adresses multicast

Les adresses IPv6 Multicast ont le format suivant :

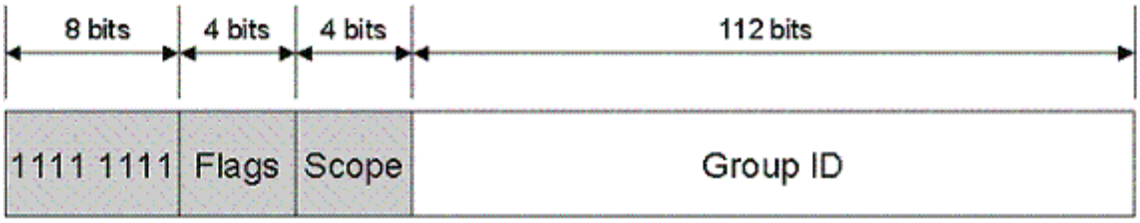


Image 44 Adresse IPv6 multicast

- **Flags** : d'après la RFC 3513, le seul flag définit est le bit T (Transient) qui est le bit de poids faible du champs flag.
  - T=0 signifie que l'adresse multicast est permanente (Well known) affectée par l'IANA
  - T=1 signifie que l'adresse est transitoire (non permanente)
- **Scope** : Indique la portée du trafic multicast. En plus des informations fournies par le routage multicast, les routeurs utilisent ce champs pour décider de l'acheminement du trafic multicast.
  - Scope = 1 : la portée est l'interface-local
  - Scope = 2 : la portée est le lien local
  - Scope = 5 : la portée est le site local

- **Group ID** : Identifie le groupe multicast et il est unique dans le scope.

Notons également qu'une interface sur un lien donné doit automatiquement s'abonner aux groupes multicast particuliers suivants :

- le groupe dont l'adresse est FF02::1 et qui comporte tous les équipements IPv6 (« All-Nodes Group») qui se trouvent sur le même lien
- Le groupe dont l'adresse est l'adresse multicast sollicité («solicited node address») de l'interface en question. Cette adresse est construite en concaténant le préfixe FF02::1:FF00:0/104 aux 24 derniers bits extraits de l'identificateur d'interface. Ainsi l'équipement IPv6 écoute les paquets émis vers cette adresse. Les autres stations sur le lien connaissent l'adresse IPv6 d'un équipement, mais ignorent son adresse liaison. Elles peuvent alors utiliser l'adresse de multicast sollicité pour le joindre. Les adresses de multicast sollicité sont entre autres utilisées par le protocole de découverte des voisins.

17. Adresses de nœuds sollicités

IPv6 utilise le message **Neighbor Solicitation** pour faire la résolution d'adresses (pb. ARP en IPv4) en évitant d'envoyer le message Neighnor Solicitation à l'adresse multicast comprenant tous les nœuds lien local, ainsi réduit la charge réseau, et cela en s'adressant uniquement à l'adresse multicast contenant cette adresse à résoudre.

L'adresse multicast nœud sollicité est composée du préfix FF02::1:FF00:0/104 et les 24 derniers bits de l'adresse IPv6 à résoudre comme le montre la figure suivante :

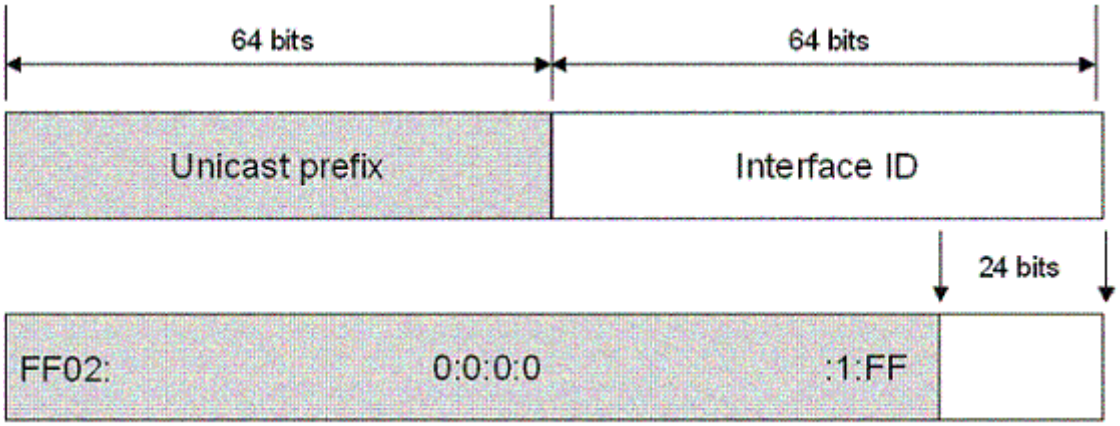


Image 45 Adresses de noeuds sollicités

18. Adresses Anycast

Une adresse anycast est affectée à plusieurs interfaces. Les paquets envoyés à cette adresse sont relayés par les routeurs jusqu'à ce qu'ils atteignent l'interface la plus proche à laquelle l'adresse anycast est affectée.

Afin de faciliter la livraison des paquets, l'infrastructure de routage doit connaître les interfaces auxquelles une adresse anycast est affectée et elles sont à quelle distance (selon la métrique). Les adresses anycast sont utilisées uniquement comme adresses destination et sont affectées uniquement aux routeurs. Elles sont prises dans l'espace d'adressage unicast et leur portée (scope) est celle du type d'adresse auquel appartient cette adresse.

Une adresse anycast dans le sous-réseau du routeur doit être définie. Elle est créée

à partir du préfixe sous-réseau de l'interface : le préfixe sous-réseau est gardé et les bits restants sont mis à 0. Toutes les interfaces d'un routeur connectées à un sous-réseau se verront affecté l'adresse anycast du routeur pour ce sous-réseau.

19. Les adresses IPv6 d'un hote

Contrairement à IPv4, un hôte ayant une seule interface peut avoir plusieurs adresses IPv6.

Les adresses unicast suivantes sont affectées à un hôte IPv6 :

- Une adresse link local pour chaque interface
- Des adresses unicast à chaque interface (qui peuvent être une adresse site local et une ou plusieurs adresses unicast globales)
- L'adresse de bouclage (::1)

Typiquement, les hôtes IPv6 sont multihomes car ils ont au moins deux adresses sur lesquelles ils peuvent recevoir les paquets : une adresse lien local pour le trafic lien local et une adresse routable (adresse site local ou adresse globale)

De plus, chaque hôte écoute le trafic multicast sur les adresses suivantes :

- all-nodes multicast address (FF01::1) de portée interface locale
- all-nodes multicast address (FF02::1) de portée lien local
- adresse du nœud sollicité pour chaque adresse unicast sur chaque interface
- les adresses multicast des groupes connectés sur chaque interface

20. Les adresses IPv6 d'un routeur

Les adresses unicast suivantes sont affectées à un routeur :

- Une adresse lien local pour chaque interface
- Des adresses unicast à chaque interface (qui peuvent être une adresse site local et une ou plusieurs adresses unicast globales)
- Une adresse anycast du sous réseaux du routeur
- Des adresses anycast supplémentaires (optionnelles)
- L'adresse de bouclage (::1)

De plus, chaque routeur écoute le trafic multicast sur les adresses suivantes :

- all-nodes multicast address (FF01::1) de portée interface locale
- all-routers multicast address (FF01::2) de portée interface locale
- all-nodes multicast address (FF02::1) de portée lien local
- all-routers multicast address (FF05::2) de portée site local
- adresse du nœud sollicité pour chaque adresse unicast sur chaque interface
- les adresses multicast des groupes connectés sur chaque interface
- les adresses multicast des groupes connectés sur chaque interface

21. Les identificateurs d'interfaces IPv6.

Les 64 derniers bits d'une adresse IPv6 forment l'identificateur de l'interface IPv6.

Il est déterminé de la manière suivante :

- Dériver les 64 bit de l'adresse "Extended Unique Identifier (EUI)"
- Un identificateur généré aléatoirement et qui change de temps en temps pour offrir un anonymat
- Un identificateur affecté par autoconfiguration (DHCPv6 par exemple).

Les identificateurs d'interfaces basés sur l'adresse EUI-64

L'adresse EUI-64 est un nouveau standard d'adressage défini par l'IEEE. Cette adresse est affectée à une carte réseau ou construite à partir d'une adresse MAC (IEEE 802).

Les 24 bits identifiant le constructeur de la carte restent les mêmes, les 40 bits restants permettent de créer un espace d'adressage plus important. Cet adressage utilise les bits U/L et I/G comme dans l'adressage IEEE.

Le format de l'adresse EUI-64 est le suivant :

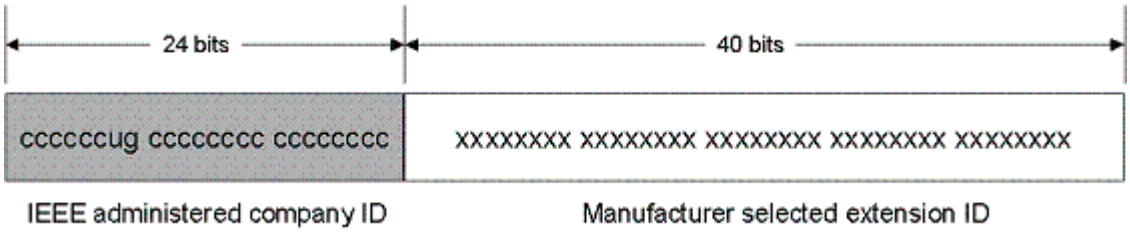


Image 46 Adresse EUI-64

Mapping des adresses IEEE 802 en EIU-64

L'adresse EIU est construite en insérant 11111111 11111110 (0xFFFE) entre la partie adresse constructeur et l'identifiant de la carte.

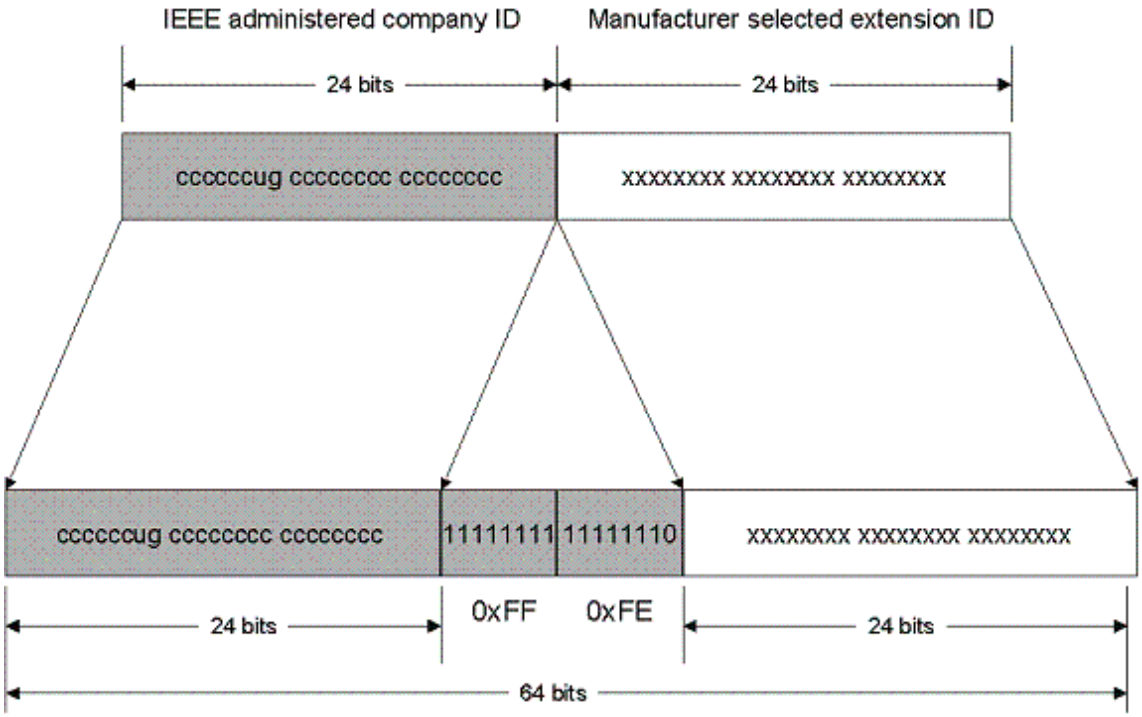


Image 47 Mapping en EIU-64

Mapping des adresses EUI-64 en identificateurs d'interface IPv6

Pour obtenir l'identificateur d'interface 64 bits de l'adresse unicast IPv6, le bit U/L de l'adresse EIU est complémenté à 2 (s'il est à 1, il est remis à 0; et s'il est à 0, il est remis à 1).

La figure suivante montre le processus.

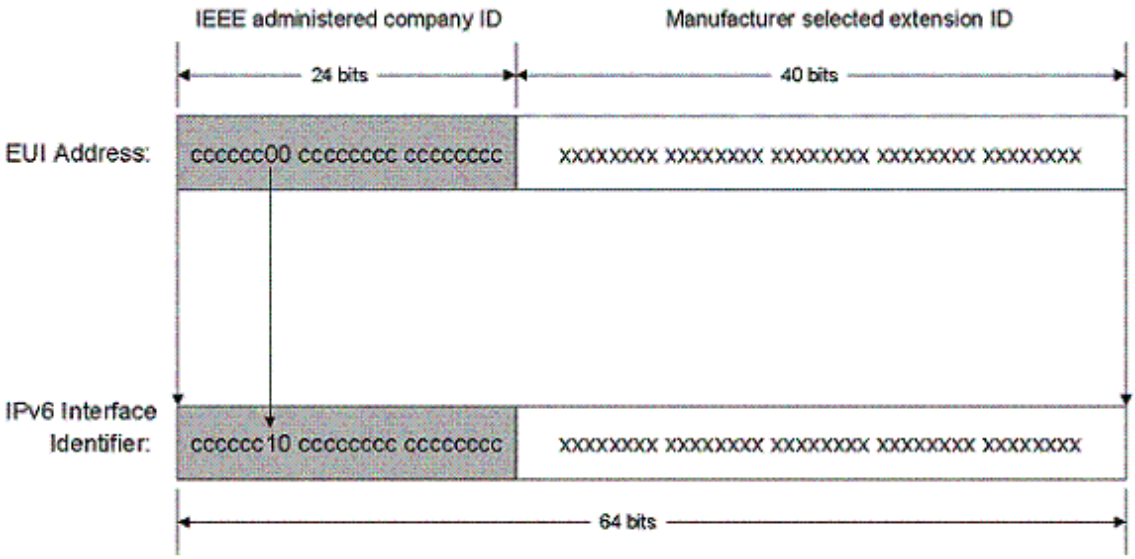


Image 48 Mapping en identificateurs d'interface IPv6

Pour obtenir l'identificateur d'interface à partir d'une adresse IEEE 802, il faudra effectuer les deux opérations décrites ci-dessus et présentées dans la figure ci-dessous :

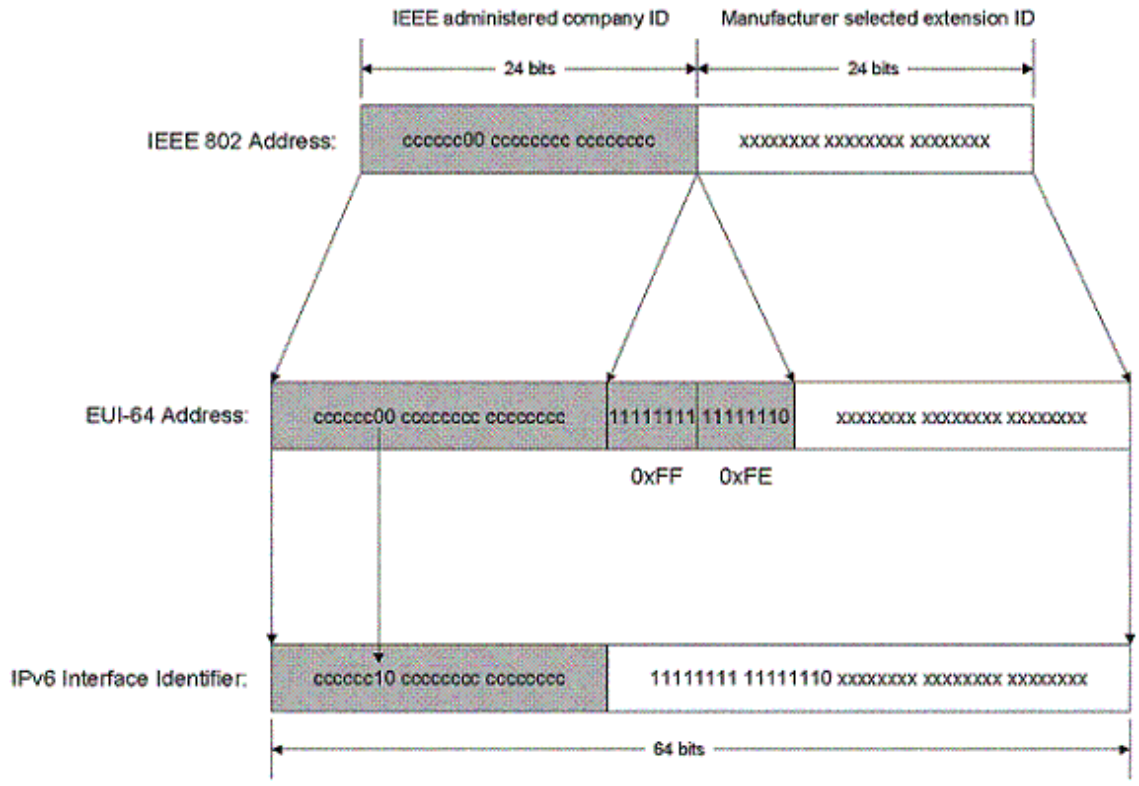


Image 49 Combinaison des 2 operations

Les réseaux locaux

III

A. Topologies LAN

1. Introduction

Caractéristiques

Les réseaux locaux (LAN) ont les caractéristiques suivantes :

- **ils sont géographiquement limités** comme un campus universitaire, une entreprise, un centre hospitalier,etc.

- ils offrent un **haut débit de transmission** contrairement aux réseaux existants avant la naissance des LANs qui offrait des débits faible.

- ils permettent la **communication de groupes** qui consiste à envoyer des trames d'une machine à un ensemble de machines simultanément, ce qui n'était pas le cas aussi dans les réseaux existants avant les LANs qui eux nécessitaient l'émission de plusieurs exemplaire du message (un par membre du groupe) vu que les topologies réseau étaient point-à-point. Pour atteindre cet objectif, il est nécessaire d'utiliser des topologies multipoint qui permettent d'envoyer une seule copie d'un message à un ensemble de récepteurs, voir à tous.

C'est quoi une topologie réseau?

Avant de répondre à cette question, , il faut savoir qu'il existe deux types de topologies : la topologie physique et logique.

Topologie physique : une topologie physique est en fait la structure physique de votre réseau. C'est donc la forme, l'apparence du réseau. Il existe plusieurs topologies physiques : le bus, l'étoile (la plus utilisée), l'anneau, hybride, etc.

Topologie logique : Une topologie logique est la structure logique d'une topologie physique, c'est à dire que la topologie logique définit comment se passe la communication dans la topologie physique.

Types de réseaux

- WAN (Wide Area Networks) ou réseaux longue distance:
  - Faible débit (10Kbits/s - 2Mbits/s)
  - Longue distance
  - Exemple : réseau couvrant une dimension géographique d'un pays, continent
- LAN (Local Area Networks) ou réseaux locaux :
  - Débits assez élevé (5-50 Mbits/s)
  - Courte distance (1-10km classiquement)
  - Exemple : réseau couvrant une dimension d'une entreprise, campus universitaire, etc.
- MAN (Metropolitan area Networks) ou réseaux metropolitains :
  - Débits élevé (100-200 Mbits/s)
  - Longue distance (100-200km classiquement)
  - Exemple : réseau couvrant une dimension géographique d'une ville

2. Topologie Bus

Dans la topologie BUS, tous les ordinateurs sont connectés entre eux par le biais d'un seul câble réseau débuté et terminé par des terminateurs. Les terminateurs ont pour but d'empêcher le retour du signal quand celui-ci a atteint l'extrémité du câble (BUS).

Dans la topologie BUS, quand une trame est émise par une station, celle-ci est reçue par toutes les autres stations (broadcast)

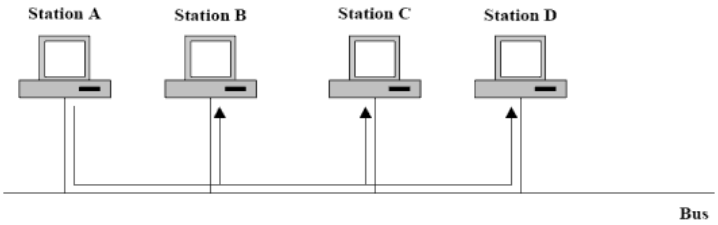


Image 50 topologie en bus

3. Topologie en anneau

Les stations sont rattachées au moyen d'interfaces selon une topologie en boucle.

▮ Une interface de boucle retarde la trame dans un registre et régénère le signal.

▮ Une trame envoyée par une station fait un tour complet et est retirée par la carte réseau de la station émettrice.

▮ L'adresse destinataire permet de déterminer si une interface donnée doit prélever le message ou non.

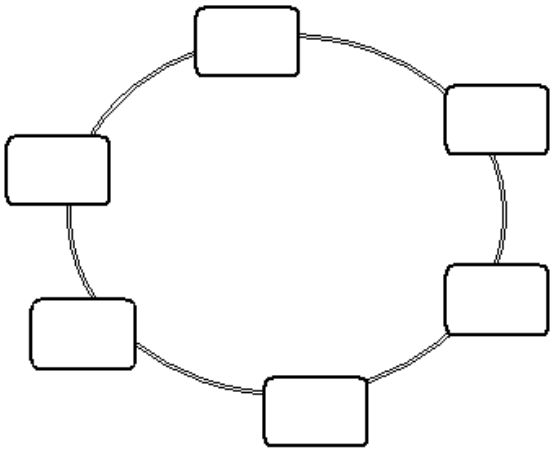


Image 51 Topologie en anneau

4. Topologie en étoile

- Chaque station est reliée au concentrateur
- Une trame envoyée par une station est reçue par toutes les autres stations

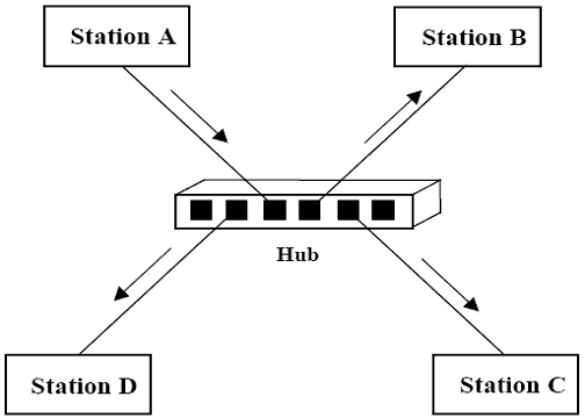


Image 52 Topologie en étoile

5. Topologies logiques (cas 1)

Etoile ou anneau ?

- Une topologie physique en étoile peut être une topologie en anneau

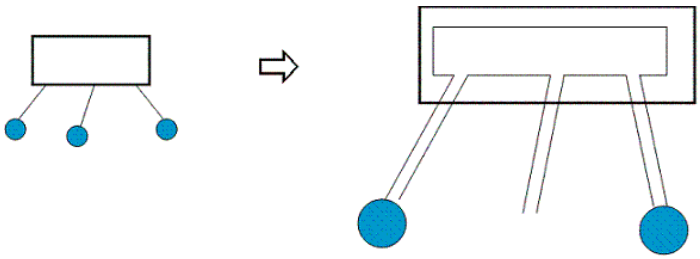


Image 53 Topologie en anneau

Exemple : Token-ring

6. Topologies logiques (cas 2)

Etoile ou anneau ?

Une topologie physique en étoile peut être une topologie en bus

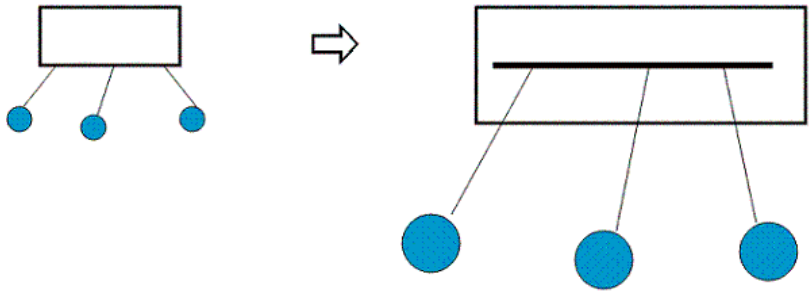


Image 54 Topologie en bus

Exemple : Ethernet

B. Achitecture LAN : Couches 1 et 2

Le LAN ne concerne que les couche 1 et 2 du modèle OSI.

Couche 1

- **But** : rendre la plus petite possible la partie purement dépendante du support physique
- **Types de supports** : paires torsadée, câble coaxial, fibre optique, infrarouge, laser,

Couche 2

But : la transmission correcte de l'information sur le support.

- Nécessité de partager un support commun
  -------> **Sous-couche MAC**
- Nécessité de détecter les erreurs et éventuellement de les corriger
  ------> **Sous-couche LLC**

1. Couche 1 : Supports de transmission

- Trois principaux supports utilisés :
  - La paire torsadée
  - Le câble coaxial
  - La fibre optique
- Autres supports :
  - Faisceaux hertziens
  - Laser
  - Infrarouge

2. Couche 1 : Paire torsadée

- Peu coûteux, flexible, facile à installer
- Très utilisées dans les LAN et la téléphonie
- Longueur limitée à 100 m car relativement sensible aux perturbations

électromagnétique

- Bande passante 10 Mbps -> 1Gbit/s
- Probleme : Diaphonie (passage du signal d'un fil à l'autre)
- Solution : Blindage (3 types suivant le niveau de blindage)
  - paires torsadées non blindées (UTP) : les fils sont regroupés deux à deux et torsadés -> réduit la diaphonie
  - paires torsadées écrantées (FTP) : idem mais écran aluminium entre les fils et la gaine
  - paires torsadées blindées (STP) : chaque paire possède son propre écran

Catégorie	Débit max	Utilisation
1 & 2	1 Mb/s	Voix (Téléphonie)
3	16 Mb/s	Voix, Ethernet(10Mb/s), Token Ring 4Mbps,...
4	2O Mb/s	Voix, Ethernet(10Mb/s), Token Ring 4/16Mb/s,...
5	100 Mb/s 155 Mb/s	Voix, Ethernet(10/100Mb/s), Token Ring 4/16Mb/s, ATM 155Mb/s
6/7	1 Gb/s	Voix, Fast/Gigabit Ethernet, ATM 155/622 Mb/s

Image 55 Catégories de paires torsadées

3. Couche 1 : Câble coaxial

- Plus coûteux, moins Flexible, plus difficile à installer
- Distances plus importantes (200m-500m) car plus résistant aux perturbations
- Bande passante 10Mbit/s

4. Couche 1 : Fibre optique

Fibre Optique

- Support très coûteux (surtout les équipement : convertisseurs)
- Faible atténuation
- Offre une très grande BP sur longue distances
- Utilisée principalement dans le cœur des réseaux

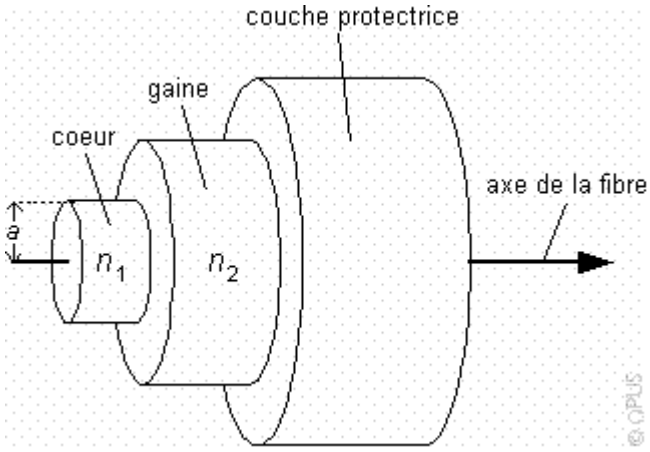


Image 56 Structure d'une fibre optique

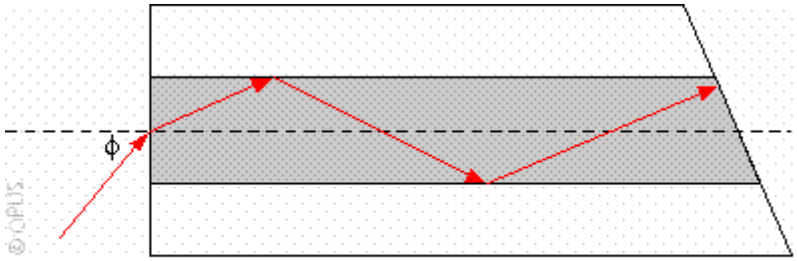


Image 57 Propagation

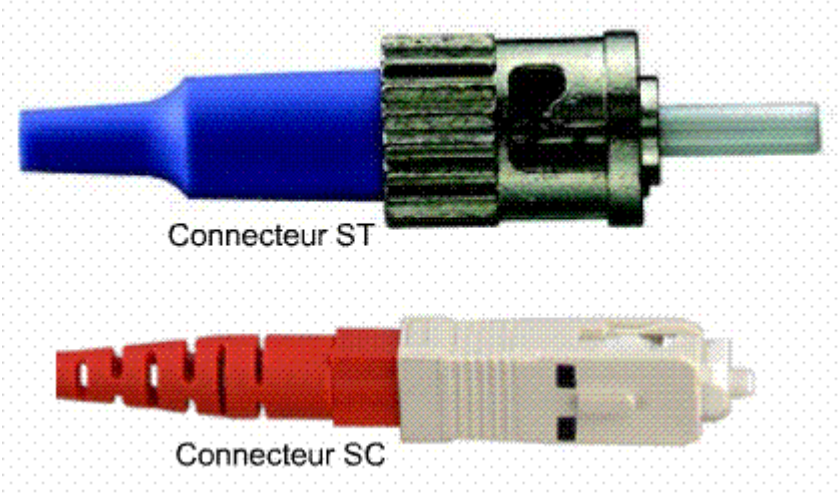


Image 58 Connecteurs

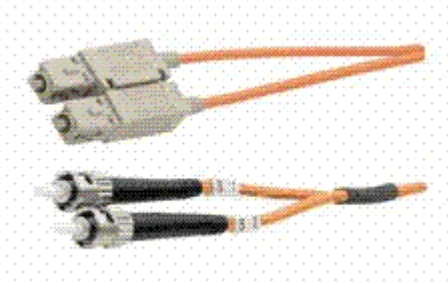


Image 59 Connecteurs

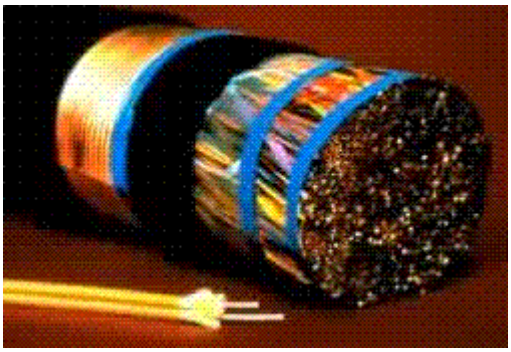


Image 60 Vue interne

5. Couche 1 : Fibre optique (suite)

- Fibre Multimodes
  - 50MHz-500Mhz sur 1Km
  - Utilisée pour les LAN haut débit
- Fibre Monomodes
  - 100 GHhz sur 1km ;

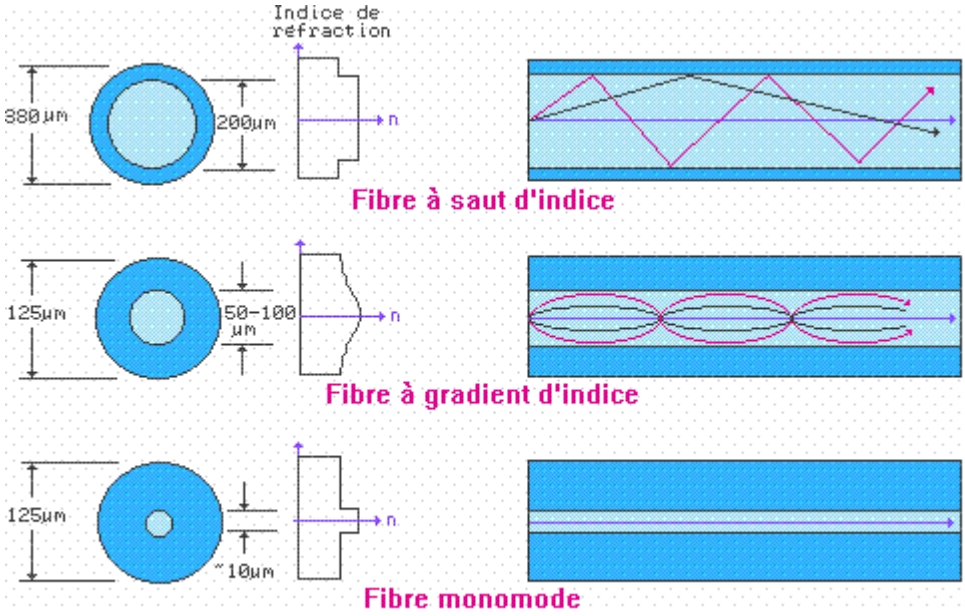


Image 61 Structure

La communication dans les réseaux sans fil sera présentée par la suite.

6. Couche 2 : sous-couche MAC

Cette sous-couche assure les fonctionnalités suivantes :

1. Structuration des trains de bits en trames
2. Adressage MAC : L'adresse MAC permet l'identification des utilisateurs connectés au même support physique
3. Méthode d'accès : permet de régler les conflits d'accès au support multipoints
   - Méthodes d'accès déterministes (bus à jeton, anneau à jeton ou Token-Ring) : avec l'approche déterministe (Token-Ring par exemple), un jeton circule en permanence dans le réseau et seul le nœud possédant le jeton

a le droit de transmettre une trame pendant une durée maximale déterminée. En conséquence,le temps d'attente pour accéder au canal est borné.

- Méthodes d'accès aléatoires (CSMA/CD, CSMA/CA) : avec la méthode d'accès aléatoire, un nœud n'a pas la garantie d'accéder au canal au bout d'un temps fini.

Le protocole CSMA/CD

Le principe de fonctionnement du protocole CSMA/CD (Carrier Sens Multiple Access with Collision Detection) est le suivant :

- Un coupleur écoute constamment les trames qui circulent sur le support (écoute la porteuse) : si la trame lui est destinée alors il la traite et la délivre à la couche supérieure sinon il n'en fait rien.
- Lorsqu'une station veut émettre une trame, elle se met à l'écoute du canal. Si elle détecte que le support est occupé, elle se met en attente que celui-ci devient libre. Si elle détecte que le canal est libre, elle envoie les bits composant la trame et écoute le canal (pour détecter d'éventuel collision).
- Si deux ou plusieurs trames entrent en collision sur le support physique (trames envoyées par deux ou plusieurs machines ayant trouvé le canal libre à un instant donné), elles deviennent inexploitables. Lorsqu'une station (émettrice) détecte la collision de sa trame avec une autre, elle interrompt dès que possible sa transmission et envoie des signaux spéciaux, appelés « jam sequence » de telle sorte que tous les coupleurs des autres machines soient prévenus de la collision. Elle tente de nouveau son émission ultérieurement suivant un algorithme de redémarrage, appelé algorithme de back-off, qui lui permettra de calculer le temps d'attente avant la prochaine tentative de réémission de la même trame.

La méthode de détection des collisions nécessite des techniques de codage suffisamment performantes pour permettre de reconnaître facilement une interférence de signaux.

- Pour expliquer la procédure de reprise sur une collision, il est nécessaire de définir des paramètres permettant de fixer le temps aller-retour maximal qui s'écoule entre les deux points les plus éloignés du réseau local. Ce temps maximal est celui qui s'écoule à partir du début de l'émission d'une trame jusqu'au retour d'un signal de collision. Ethernet définit cette durée, de 51,2 µs, comme « une tranche de temps » ou "Slot-time", qui est le temps minimal avant retransmission.

  Le temps d'attente avant retransmission de la trame dépend du nombre k de collisions qui se sont produite sur la même trame : à la tentative k, l'algorithme fait un tirage aléatoire d'un nombre r ($0 \leq r < 2k$), et la station reviendra pour écouter si le canal est libre après un temps égal à $r \times 51{,}2$ µs si k<=10.

  Si, au bout de seize tentatives, la trame est encore en collision, l'émetteur abandonne sa transmission. Une reprise s'effectue alors à partir des protocoles de niveaux supérieurs.

  Cet algorithme sera étudié plus en détail lors des travaux dirigés.

7. Couche 2 : Adressage MAC

Une adresse MAC (Media Access Control), parfois nommée adresse physique, est un identifiant physique stocké dans une carte réseau.

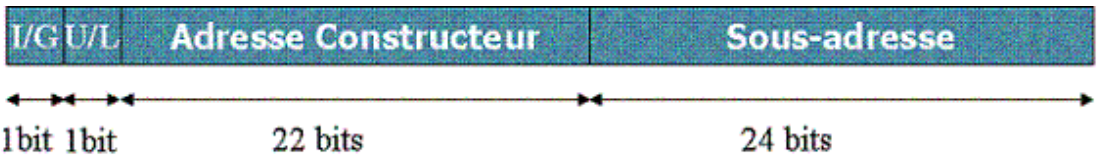
L'adresse MAC est définie sur 48 bits. Les adresses suivantes sont des exemples d'adresses MAC :

- 08:00:20:09:E3:D8 ou

- 8:0:20:9:E3:D8 ou
- 08-00-20-09-E3-D8 ou
- 08002009E3D8

Format d'adresse MAC

Le format d'une adresse MAC est le suivant :



Structure d'une adresse MAC

- I/G (Individual/Group)
  - Si le bit est à 0 alors l'adresse spécifie une machine unique
  - Si le bit est à 1 alors c'est une adresse de groupe (multicast)
- U/L (Universal/Local)
  - Si le bit est à 0 alors l'adresse est universelle
  - Si le bit est à 1 alors l'adresse n'est signifiante que localement

Types d'adresses :

- Adresse de diffusion (Broadcast) : tous les bits à 1 (FF:FF:FF:FF:FF:FF)
- Adresse individuelle pour une machine : Bit I/G à 0
- Adresse pour la diffusion restreinte (de groupe multicast) :Bit I/G à 1

Une adresse universelle est attribuée par l'IEEE à chaque constructeur sur 3 octets (24 bits). Par exemples les adresses suivantes ont été attribuées aux constructeurs suivants :

- CISCO : 00000C

- 3COM : 00008D, 0020AF, 02608C,080002

8. Couche 2 : Sous-couche LLC

- La sous-couche LLC fournit un service standard de liaison de donnée et permet d'offrir une indépendance de la couche MAC utilisée
- Le protocole LLC est basé sur le protocole de liaison HDLC (décrit dans le chapitre architecture réseau- couche liaison) et utilise une adresse étendue de 2 octets. Le premier octet d'adresse indique un point d'accès au service de destination (DSAP) et la deuxième adresse un point d'accès au service source (SSAP). Ils identifient les entités de protocole réseau qui utilisent le service couche de liaison.
- 3 types de sous-couche LLC :
  - LLC vide (Ethernet)
  - LLC en mode non connecté (pile ISO 8473)
    - Pas de garantie de remise
    - Pas de garantie de séquencement
  - LLC mode connecté (pile SNA)
    - Garantie de remise
    - Garantie de séquencement

Adressage LLC

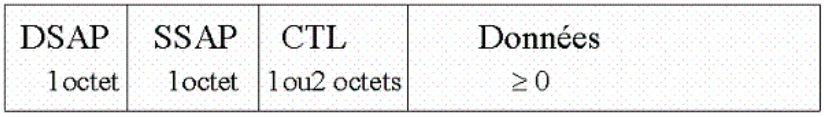
Objectif : l'adressage LLC permet d'identifier les utilisateurs de la couche 2.

L 'adressage LLC (SAP) :

- Est réalisé sur un octet
- Définit le concept unicast/multicast (par le 1er bit)
- Définit le concept LAA/GAA (par le 1eme bit)
- La représentation conventionnelle est en hexadécimale

Exemple : IP :06 ; couche 3 OSI : FE

Trame LLC (PDU LLC)



Trame LLC

Structure du SAP

9. Couche 2 : LLC - Protocole SNAP

Dans le modèle IEEE 802, la fonction d'aiguillage vers le niveau supérieur est assurée par le protocole LLC à l'aide de No appelés N-SAP (Network Service Access Point).

Bien que le numéro de N-SAP 6 ait été attribué au protocole IP, son emploi est interdit par l'organisme qui standardise IP. En effet, l'en-tête LLC fait 3 octets de long, ce qui casse l'alignement des en-têtes IP sur des mots de 32 bit. Pour permettre quand même l'utilisation d'IP sur des réseaux ne proposant qu'une encapsulation LLC (par exemple l'anneau à jeton), le protocole SNAP (SubNetwork Access Protocol) a été défini. Avec une taille d'en-tête de cinq octets, il réaligne les données sur des mots de 32 bit. De plus, la désignation des protocoles de niveau 3 se fait comme sous Ethernet, ce qui assure une plus grande compatibilité avec les pilotes de périphériques existants.

- La taille du champs SAP limite le nombre de protocoles réseau qui peuvent utiliser LLC
- La sous-couche SNAP a été développée pour supporter un plus grand nombre de protocoles
- SNAP est souvent utilisé par IP

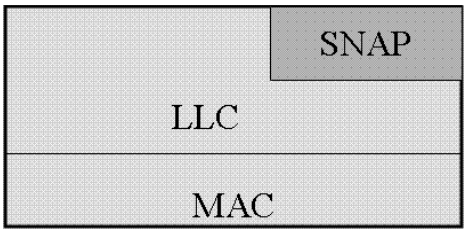


Image 62 Positionnement du protocole SNAP

Le protocole 802.2 LLC peut également être utilisé pour transporter un champs "type" identifiants de protocoles de niveau supérieur. En effet, lorsqu'une machine envoie une trame sur une technologie LAN non Ethernet qui ne donne pas la possibilité d'insérer un champ "type" dans sa trame, il existe un moyen d'utiliser des champs dans l'en-tête de la trame LLC pour fournir un identifiant de type. La raison d'être de cette approche vient du fait que les champs de l'en-tête de la LLC ne sont pas importants/suffisants.

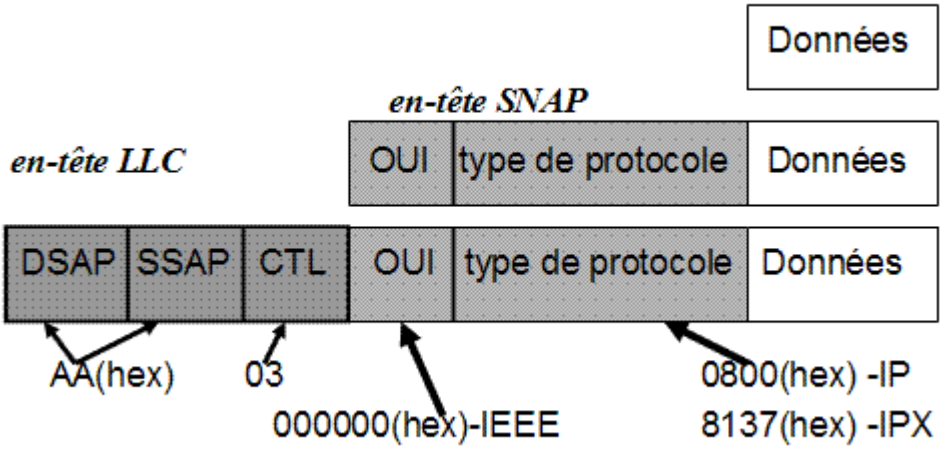
Étant donné cette limitation, l'IEEE n'a pas voulu utiliser le nombre limité de bits

dans les champs LLC pour fournir des identifiants pour tous les anciens types de protocoles de haut niveau. Pour cela, une méthode a été créée pour préserver l'ensemble des identifiants de type de protocole de haut niveau existants et les réutiliser dans le système IEEE LLC.

Cette approche fournit un autre ensemble d'octets dans le champ de données de la trame LLC, connu sous le nom LLC Encapsulation du protocole d'accès au sous-réseau (SNAP).

Dans SNAP, le contenu des champs LLC de la trame est utilisé pour identifier un autre ensemble de bits dans le champ de données qui sont organisés en fonction de la spécification SNAP. Les champs SNAP sont utilisés pour transporter les anciens identificateurs de type de protocole.

Le Standard pour l'utilisation de l'encapsulation SNAP via IP est documenté dans RFC 1042.



LLC et SNAP

C. Le réseau Ethernet

1. Introduction

- Technologie très répandue
- Infrastructure locale de transfert de données à haut débit
- Conçue par trois constructeurs : DEC, INTEL, XEROX
  - DIX Ethernet
  - Normalisée IEEE 802.3
- Plusieurs variantes : 10 BASE 5 , 10 Base 2 , 10 Base T

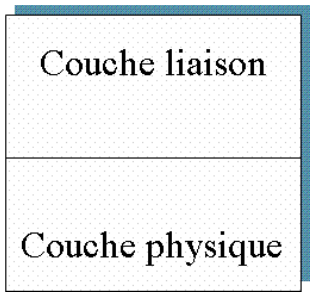


Image 63 20

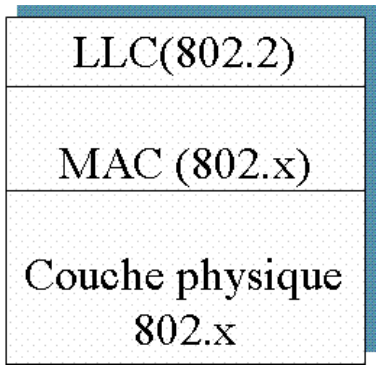


Image 64 21

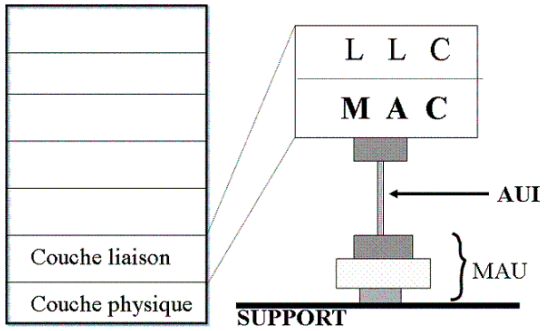


Image 65 21

2. Ethernet 10 Mbits/s : 10 base 5

- 10Mbit/s en bande de base sur câble coaxial d'une longueur maximale par segment de 500m.
- Distance entre stations : multiple de 2,5 mètre (marques sur le câble)

Matériel

- Codage Manchester
- Topologie physique = bus
- Câble coaxial épais (10mm), câble de liaison, bouchons de terminaison (limite échos), connecteur DB15, répéteurs entre deux segments
- Transceiver (ou MAU) : conversion des signaux, détection collisions
- Carte Ethernet : gère l'algorithme CSMA/CD, ...

3. Ethernet 10 Mbit/s : 10 Base 2

- Moins coûteux et plus facile d'installation

- Architecture la plus économique pour des petits réseaux (dizaines de stations)
- Matériel :
  - Codage Manchester
  - Topologie physique = bus
  - Câble coaxial fin (5mm), bouchons de terminaison (limite échos), connecteur BNC en T, répéteurs entre deux segments (30 stations max par segment)
  - Longueur maximale d'un segment : 185m
  - Distance entre 2 noeuds : 0,5m
  - Transceiver intégré à la carte Ethernet

4. Ethernet 10 Mbit/s : 10 Base T

- Réutilisation du câblage téléphonique (paire torsadée)
- Topologie physique en étoile Connecteurs RJ45
- Un Hub émule un bus (émulation logique)
  - Concentrateur / répéteur (hub)
  - Diffusion des messages sur tous les ports
  - Détection des collisions (le signal de collision est retransmis à l'ensemble des stations)
  - Liaison Hub/Station ou Hub/Hub en paires torsadées (1 pour l'émission, 1 pour la réception)
  - Nombre de niveaux limités par la fenêtre de collision

Exemple :

- 2 paires torsadées UTP catégorie 5
- Longueur d'un maximale d'un brin (liaison hub/station ou hub/hub) : 100m ou 150m
- 3 niveaux de Hub au maximum

5. Ethernet : couche 1

Répéteurs

- Relient deux segments
- Retransmission du signal après régénération
- 5 segments max dans une connexion
- 4 répéteurs max
- Au maximum 3 segments actifs (+ 2 IRL)

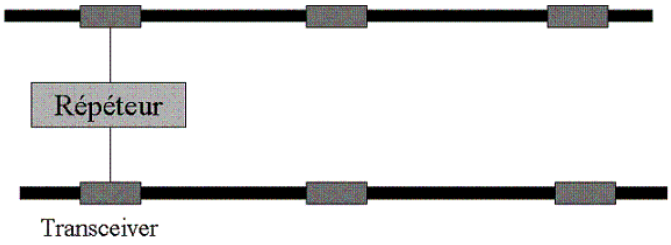


Image 66 Répéteur

6. Ethernet : Couche 2

Format des trames

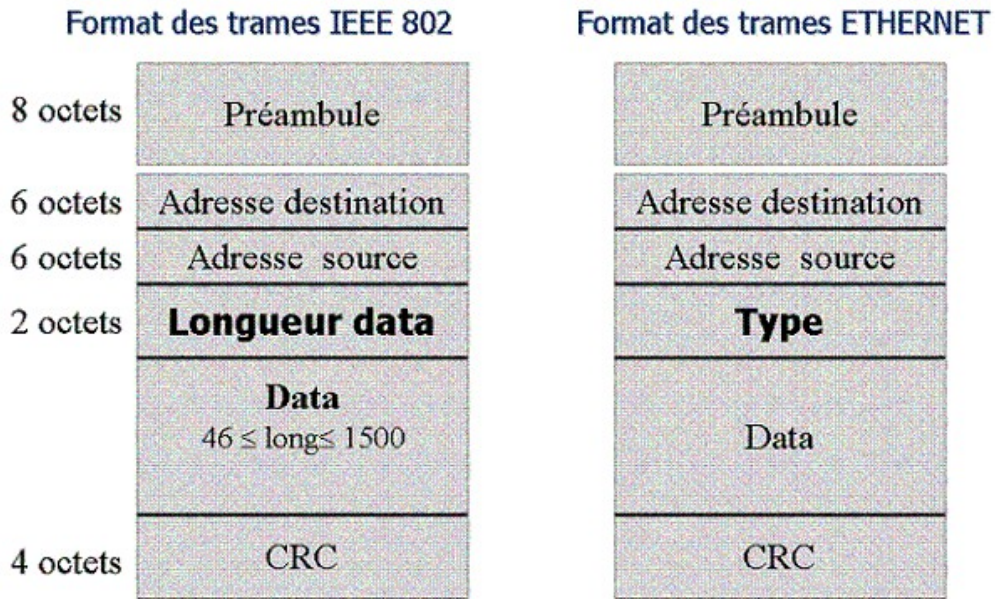


Image 67 Format des trames

7. Ethernet haut débit

Avec le développement des applications Client/Serveur, Multimédia, etc, les besoins en bande passante n'ont cessé d'augmenter. Malgré la segmentation des réseaux afin d'optimiser l'utilisation de la bande passante, les performances restaient faibles!! Cela est du au développement de l'Internet (accès vers l'extérieure) qui induit que le trafic va de partout à partout.

----> Il y a donc nécessité d'une bande passante plus importante.

L' offre Ethernet à débit plus élevée s'est développée selon trois technologies :

- 100 Base T
- Switchs
- 100 VG AnyLan

Les 3 technologies

1. **Les concentrateurs commutés (Switched Hub)**
   - Débit d'accès pour les stations = 10Mbits
   - Support physique à 10 Mbits/s est utilisé par chaque station
   - Rôle du commutateur : Mise en relation de la station émettrice avec la station réceptrice pendant la durée de la trame (sauf cas de diffusion). D'ou la réduction des collision.
2. **Ethernet 100Mbits/s :100 BASE T (IEEE 802.14)**
   - Conserve les propriétés d'Ethernet, (câblage aussi)
   - Augmente le débit du support
   - Coupleurs différents
3. **La norme 100BASE VG -Any- LAN (HP)**
   - Débit égale à 100 Mbits/s
   - N'utilise pas le principe d'Ethernet (utilise Polling)
   - Coupleur différents
   - Conservation des principaux systèmes de câblage

Les trois technologies :

- Utilisent une architecture en étoile (autour d'un HUB)
- Conservent le format des trames Ethernet, compatibles avec les réseaux existants
- Réutilisent l'infrastructure du câblage existant

Architecture

- L'architecture de ces trois technologies est une architecture en étoile basée sur des HUB
- Chaque HUB permet de connecter plusieurs stations ou HUB
- Sur chaque points d'accès du HUB on peut raccorder une seule station ou un seul HUB

8. Ethernet 100 Base T (Fast Ethernet)

- Proposition soutenue initialement par 3COM
- Groupe de travail IEEE 802.14
- Utilise le protocole CSMA/CD
- La taille minimale d'une trame est de 64 octets
- Tranche du canal 5.12 ?s
- Silence (Interframe Gap) est de 0.96 ?s
- Chaque station peut être raccordée au réseau par un câble appelé Média Indépendant Interface (MII) de longueur maximale égale à 0.5 m.

La topologie du cablage

Le standard définit une interface HUB universelle. Ces HUB sont classés en deux catégories : HUB classe I et HUB classe II.

HUB classe I :

- ne supporte qu'un seul répéteur entre deux équipements terminaux (stations)
- utilise un pont ou un routeur pour accroître la taille du réseau
- Câble UTP
- Distance entre station et HUB <= 100 m
- Supportent les 2 interfaces physiques 10 BASE TX et 100 BASE T4

HUB classe II :

- accepte que deux HUB (au maximum) puissent être raccordés ensemble. Au delà, utiliser un pont ou un routeur.
- Acceptent des distances max de 205 m (entre deux stations).
- Un protocole d'auto-négociation(sur le HUB) permet l'adaptation automatique du port du HUB au débit du coupleur (10 ou 100 Mbits/s). Cette auto-négociation peut être invalidée par les fonctions d'administration.

Ethernet 100 BASE TX

Utilise la paire torsadée catégorie 5, soit non blindée (UTP catégorie 5) soit STP mais sur une longueur réduite (100 m au maximum) pour autoriser des débits de 100 Mbits/s. Les interfaces physiques sont conformes aux spécification RJ 45.

Ethernet 100 BASE FX

- Fibre optique multimode
- Distances <= 400m

- Fibre optique à gradient d'indice de diamètre 152 micron

Ethernet 100 BASE T4

- Utilise des câbles comprenant 4 paires torsadées catégorie 3,4, ou 5
  - 3 paires servent à la transmission de données
  - Une paire est utilisée pour la détection des collisions
- Longueur du câble ne doit pas dépasser 100 m.

9. Ethernet commuté (Switch)

- L'Ethernet commuté conserve une compatibilité totale des équipements avec le câblage Ethernet 100 Mbits/s
- Amélioration de la bande passante par rapport à Ethernet 10Mb.
- Lorsqu'un message est émis vers une adresse individuelle, le concentrateur le dirige exclusivement vers le destinataire.
  - Pendant la durée d'émission d'un message, l'émetteur est en liaison exclusive avec son correspondant.
- La bande passante du HUB est de (N / 2) * 10 Mbits/s
- Cette technologie permet donc de limiter les collisions au seul cas où deux stations, veulent envoyer un message correspondant simultanément.

  Dans ce cas, pendant l'émission d'une trame, la paire de réception n'est plus monopolisée par la détection de collision et on peut recevoir en même temps, c'est à dire travailler en mode bidirectionnel (full duplex).

  Il faut souligner aussi que l'absence de collision supprime les limitations de distance que leur détection impliquait.

Fonctionnement d'un switch

Le switch a besoin de connaître les adresses individuelles (adresses MAC) des stations connectées à ses port,

Le switch fonctionne par auto-apprentissage : le switch maintient une table de correspondance n° de port / adr.MAC, qui est vide au démarrage (il ne sait pas quelle station est connectée à chaque port)

- quand il reçoit une trame, il inscrit dans sa table l'adr.MAC source et le n° de port
- ensuite, à chaque trame reçue,
  1. il cherche le n° de port destinataire dans la table. S'il le trouve, il n'envoie la trame que sur ce port, sinon il l'envoie sur tous les ports
  2. il vérifie la correspondance adr.MAC source et n° de port, au cas où une station aurait été déplacée ou une carte réseau remplacée

Avantage : conserve les coupleurs Ethernet existant mais la seule modification à faire consiste à remplacer le HUB 10 BASE T par un switch.

Techniques de commutation

Commutation à la volée (on the fly) : dès que le commutateur a lu l'adresse destinataire (les 6 premiers octets de la trames), il sait vers quel port il doit la ré-émettre.

- avantage : temps de latence très court, de l'ordre de 40µs
- inconvénient : toutes les trames sont ré-émises même celles qui sont erronées

Commutation bufferisée (store and forward) : le commutateur lit toute la trame, la stocke dans un buffer et la ré-émet sur le port destinataire.

- avantage : la trame est vérifiée avant aiguillage et celles qui sont erronées ne sont pas transmises

- inconvénient : un temps de latence supérieur au précédent

10. 100 BASE VG Any LAN

- Proposée par Hewlett-Packard
- Norme IEEE 802.12
- 10 Mbits/s sur câbles téléphoniques 4 paires :
  - Catégorie 3 : 100 m (max) entre station et le HUB.
  - Catégorie 4 : longueur maximum 100 m
  - Catégorie 5 : UTP, longueur maximum 150 m
- Des extensions pour supporter des câbles de catégorie 2 (UTP ou STP) ainsi que la fibre optique sont possible.
- Avec la fibre optique, la longueur maximal du câble est 2000 m
  - N'utilise pas le protocole CSMA/CD
  - Utilise un contrôle d'accès centralisé appelé "**DEMANDE DE PRIORITE"**
- Basé sur le principe de scrutation périodique (Polling)
- Le contrôle d'accès permet de garantir un délai d'accès déterministe
- Deux niveaux de priorités sont utilisés pour faciliter la mise en œuvre d'application sensibles aux contraintes de temps
- 100 BASE VG permet la compatibilité avec Ethernet et Token-ring : un réseau supportera l'un ou l'autre de ces formats.

Le HUB 100 VG Any LAN

HUB 100 VG Any LAN est un contrôleur qui gère continuellement le réseau.

Il écoute à tour de rôle sur chacun de ses ports les demandes de service.

- Le HUB reçoit les paquets et les dirige vers le port destinataire.
- Le hub est individuellement configuré pour traiter les trames ETHERNET ou TOKEN-RING.
- Tous les HUB d'un même segment doivent être configurés avec le même format.
- Le passage d'un segment (utilisant trame Ethernet) à un autre segment (utilisant Token-Ring) doit se faire par la technique de pontage (ou Routeur).
- Chaque HUB dispose d'un lieu vers la racine (up link) et de n ports (down link) vers l'arborescence.

  Le port vers la racine sert à remonter les messages dont l'adresse destination n'est pas connue localement.

11. Ethernet 1000 Mbits/s : Gigabit Ethernet

Avec un commutateur Gigabit Ethernet, la mise en relation entre équipement est de type point-à-point :

- Pas de diffusion, pas de détection de collision (pas CSMA/CD)
- La taille de trame minimale reste de 64 octets

Avec un répéteur (hub) Gigabit Ethernet, pour garder un diamètre du réseau suffisant (200m), la trame minimale peut être augmentée à 512 octets pour ne pas gaspiller la bande passante par le bourrage, un mécanisme de groupage de trames (burst) est mis en place

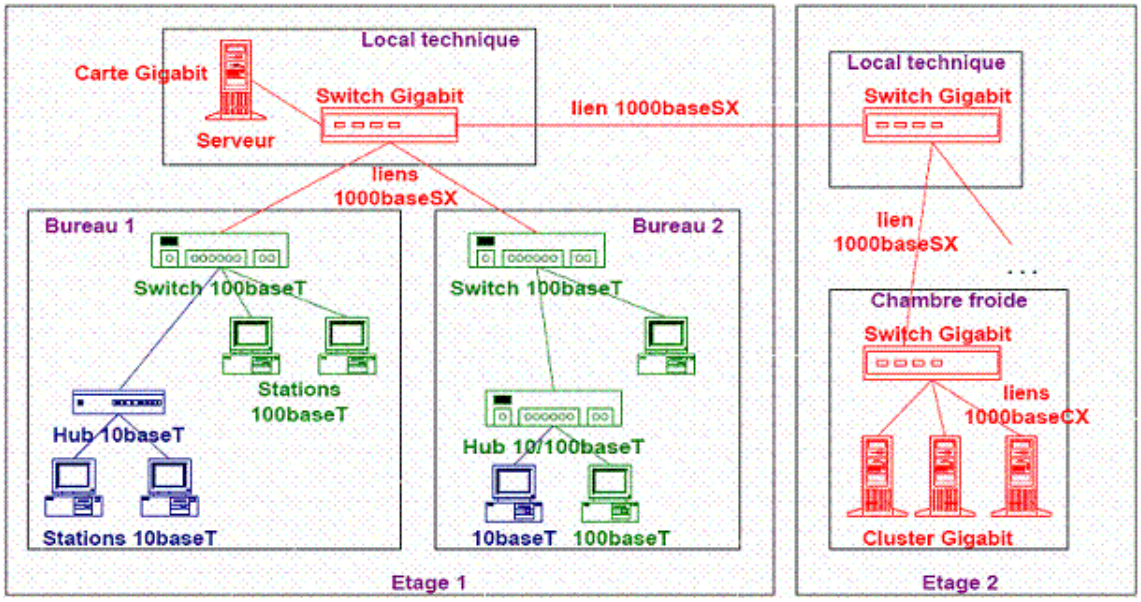
Il est généralement utilisé pour l'interconnexion de réseaux à 10 ou 100 Mbit/s. Le support de prédilection est la fibre optique.

Un équipement Gigabit Ethernet contient généralement des ports 10, 100 et 1000 avec des ports pour la fibre optique.

Les différents types :

- 1000 Base CX : 2 paires blindées (STP) sur 25m -> limité à l'interconnexion de hub ou clusters
- 1000 Base SX : fibre optique courte longueur d'onde sur 260/550m -> interconnexion à l'intérieur d'un bâtiment
- 1000 Base LX : fibre optique grande longueur d'onde sur 3km (monomode) -> interconnexion sur un campus
- 1000 base T : 4 paires cat. 5/6 UTP sur 100m, coûteux car traitement du signal complexe

Sur la figure suivante, nous donnons un exemple de déploiement d'un réseau Giga Ethernet.



Gigabit Ethernet

D. Les réseaux locaux sans fils

- Développement très rapide des réseaux sans fils :
  - Représentent un marché énorme
  - Les prix deviennent de plus en plus abordables
  - Les performances et les débits augmentent
  - Les réseaux domestiques et la population de travailleurs mobiles augmentent
- 1990 : travaux du groupe IEEE 802.11
- 1997 : standard IEEE 802.11
- Norme d'interopérabilité
  - WIFI (WIreless FIdelity) du WECA, Wireless Ethernet Compatibility Alliance pour IEEE 802.11b
- WIFI : un réseau local radio
  - Définition sur les deux niveaux physique et liaison
- WIFI : **deux protocoles différents** d'accès au médium
  - **PCF** 'Point Coordination Function' (en coopération)
  - **DCF** 'Distributed Coordination Function' (en compétition).

- Peuvent être utilisés simultanément par une station.

- WIFI : **différents niveaux physiques** selon le débit, le codage, la bande de fréquences utilisée
  - 802.11, 802.11a, 802.11b, 802.11g, en cours 802.11n.
- Consortium de développement : **WIFI Alliance**

1. Le modèle de référence Wifi

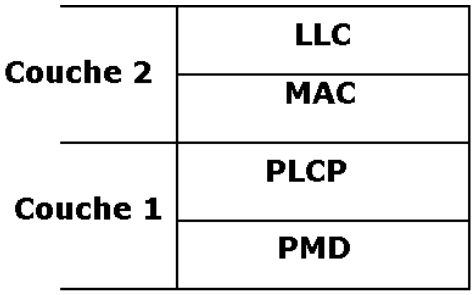


Image 68 Modèle de reference

PLCP (Physical Layer Convergence Protocol)

- Gère l'écoute du support et informe la couche MAC que le support est libre par un CCA (Clear Channel Assesment).

PMD (Physical Medium Dependent)

- Gère le codage des donnée et la modulation

2. Wireless : technologies et normes

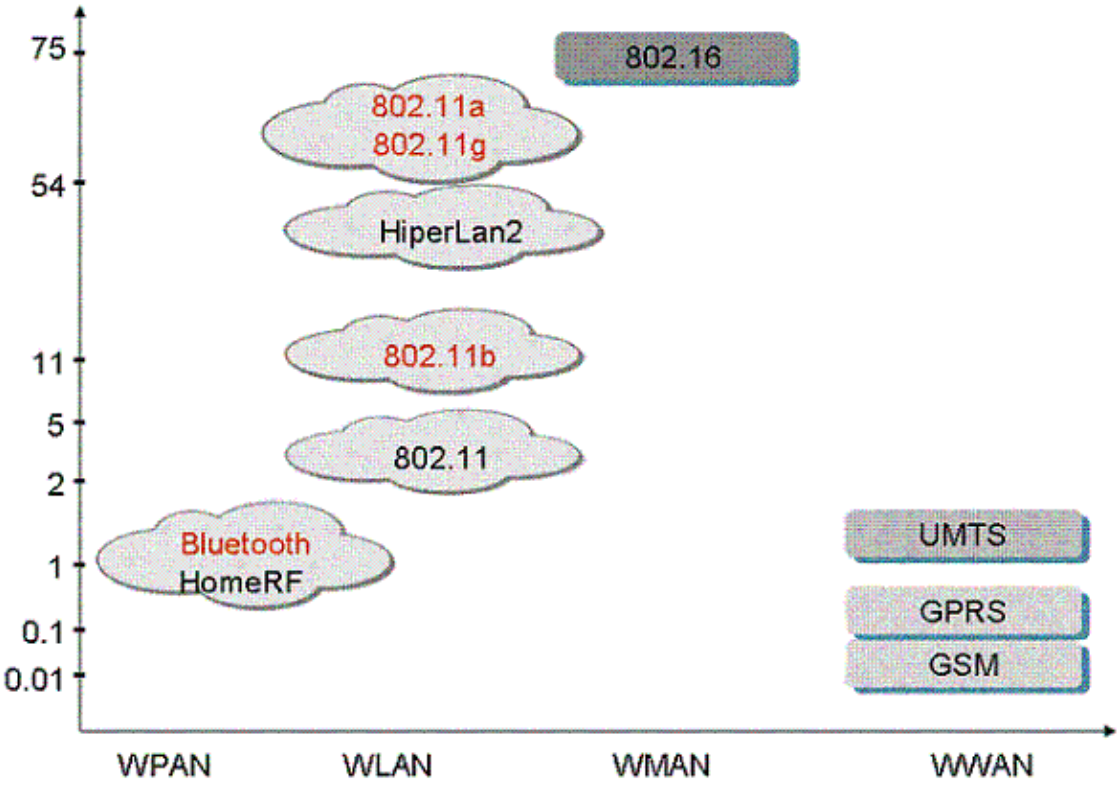


Image 69 Normes et applications

3. Avantages et inconvenients des WLAN's

Avantages

- Mobilité
- Topologie dynamique
- Facilité d'installation
- Coût de plus en plus faible

Inconvénients

- Problèmes liés aux ondes radios
  - Taux d'erreur plus important
  - Interférences (provenant d'autres réseaux)
    Exemple entre un Bluetooth et un 802.11
- La sécurité
- La réglementation : le choix des fréquences diffère de pays en pays

4. La couche MAC

Il existe 2 types de topologies :

Mode infrastructure

Désigne un réseau composé d'une infrastructure permettant l'échange d'information entre stations.

L'infrastructure est le point d'accès.

Une cellule = 1BSS = 1 point d'accès

- **AP** (**Access Point**) : commutateur
- **Station de travail** avec un coupleur WIFI
- **BSS** (Basic Service Set): un seul AP
- **ESS** (**Extended Service Set**) :
  - plusieurs AP connectés par un autre réseau
  - Cellules recouvrantes (service mobilité, IEEE 802.11F) ou non
- **handover / roaming** (**itinérance**) : changement de point d'accès

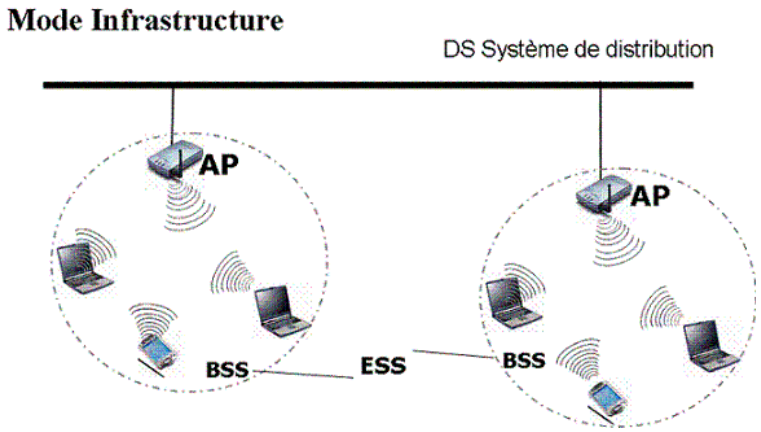


Image 70 Le mode infrastructure

Mode Ad-hoc

- **IBSS** (**Independent Basic Service Set**) : ensemble de stations avec coupleurs sans fils, communicantes dans la même bande (mode point à point)

- Permet l'échange d'informations lorsque aucun point d'accès n'est disponible.
- **Protocole DCF** : Distributed Coordination Function.

5. Architecture des réseaux 802.11x

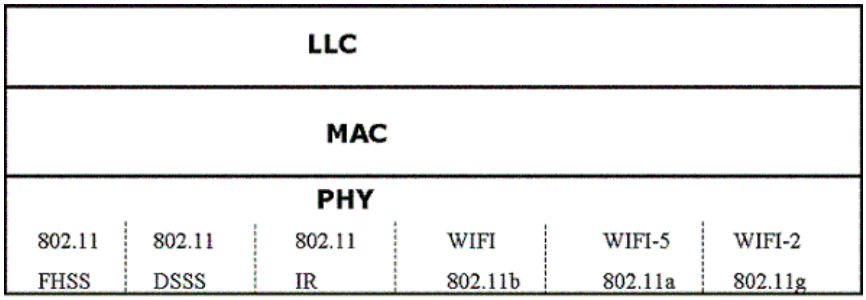


Image 71 Trame 802.11x

- FHSS : Frequency Hoping Spread Spectrum
- DSSS : Direct Sequence Spread Spectrum
- IR : InfraRed
- OFDM : Orthogonal Frequency Division Multiplexing (802.11g)

6. Couche physique

- **FHSS : Frequency Hoping Spread Spectrum**
  - 79 canaux de 1Mhz de largeur de bande
- **DSSS : Direct Sequence Spread Spectrum**
  - Technique la plus répandu : 802.11b
  - 14 canaux de 20 MHz
  - Bande : 2,4 GHz – 2,4835 GHz (largeur = 83,5 MHz)
  - Fréquences crête espacées de 5 MHz
    - Canal 1 = 2,412 GHz
    - Canal 14 = 2,477 GHz
  - Un seul canal utilisé par transmission : sensible aux interférences
- **OFDM : Orthogonal Frequency Division Multiplexing**
  - Bande de 5 GHz
  - Division des deux premières sous-bandes en 8 canaux de 20 MHz
  - Chaque canal contient 52 sous canaux de 300 KHz
  - Utilisation de tous les sous canaux en parallèle pour la transmission

7. Couche liaison

Couche MAC

- Elle est similaire à la couche MAC d'Ethernet
- Fonctionalités :
  - Adressage, formatage des trames
  - Contrôle d'erreurs
  - Fragmentation et réassemblage
  - Qualité de service
  - Gestion de la mobilité
  - Gestion de l'energie
- Deux méthodes d'accès :
  - DCF (Distributed Coordination Function) : avec contention

- PCF (Point Coordination Function) : sans contention

8. Couche Liaison WIFI : le mode Distributed Coordination Function (DCF)

- Protocole CSMA/CA.
- **Détection** de collisions par accusé de réception.
- **Retransmission** sur collision (binary backoff).
- Gestion de **la fragmentation**.
- Pas de **gestion de connexion**.
- Pas de **contrôle de flux**.
- Pas de garantie de **livraison sans erreurs**.
- Pas de **qualité de service** (en version de base)
- **Reserve le support** via la couche physique
- Deux types de mécanismes :
  - Réservation par RTS/CTS
  - Utilisation d'un timer NAV (Network Allocation Vector) calculé par toutes les stations à l'écoute.

4 types d'espacements inter-trames IFS (Inter Frame Spacing)

- **SIFS** (**Short IFS**) : sépare les différentes trames d'un même dialogue (données et ACK ; RTS et CTS ; fragments d'une trame segmentée ; trame de polling dans PCF)
- **PIFS** (**PCF IFS**) = SIFS + 1 timeslot
- **DIFS** (**DCF IFS**) = SIFS + 2 timeslots
- **EIFS** (**Extended IFS**) :
  - Uniquement en mode DCF
  - Le plus long
  - Utilisé lorsqu'une trame de données est erronée attente de l'acquittement.

Emission

- Écouter avant d'émettre
- Si le réseau est encombré, la transmission est différée
- Si le media est libre pendant un temps donné (DIFS), alors la station peut émettre.
  - La station envoie un RTS contenant des infos sur le volume de données à envoyer et la vitesse de transmission
  - Le récepteur (un Point d'accès) répond avec CTS
  - Ensuite, la station envoie les données
  - A la réception de toutes les données, le récepteur envoie un ACK, et toutes les stations avoisinantes patientent alors pendant le temps nécessaire à la transmission du volume de données annoncé auparavant

Accès au canal avec 802.11

- Écoute du canal
- Quand il devient libre tirage au sort d'un certain nombre de ”slots” de temps d'attente aléatoire (”backoff”)
- Le temps d'attente ne s'écoule que lorsque le canal est libre (et sa décrémentation est mise en pause quand il est occupé)
- Une fois le temps complètement écoulé, si le canal est libre, on peut émettre.

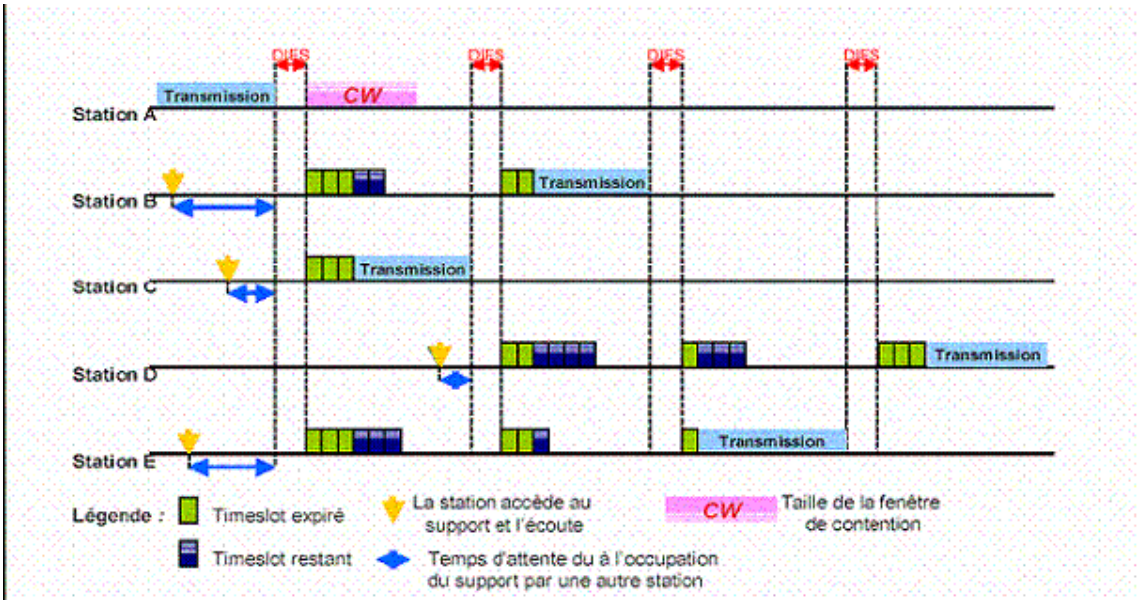


Image 72 Transmission

9. Probleme de la station cachée

Exposé du probleme

- Deux stations situées chacune à l'opposé de l'AP ou d'une autre station
- Ne peuvent pas s'entendre mutuellement pour cause de distance ou de présence d'obstacles
- Effectuent des transmissions : Bande passante perdue

Solution

- Réservation du support trames : RTS/CTS
- Etat du support : NAV (network allocation vector)

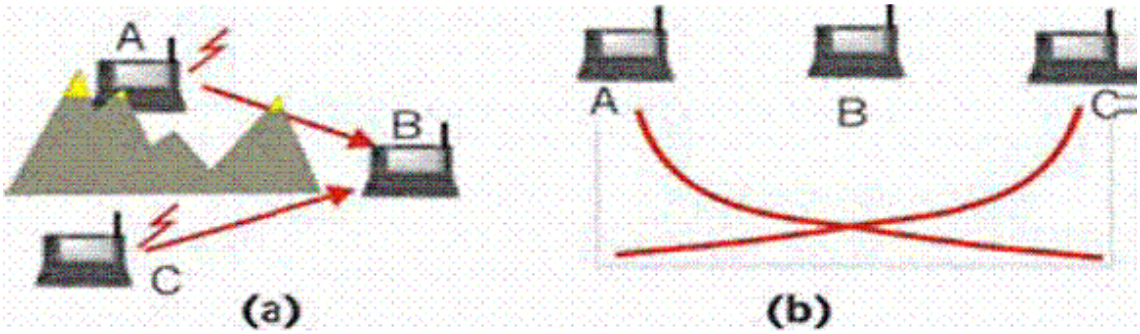


Image 73 Probleme de la station cachée

10. RTS-CTS

Principe

- Emetteur transmet un paquet RTS (request to send) : indiquant l'émetteur le récepteur et la durée de la transmission
- Récepteur répond avec un paquet CTS (clear to send) avec les mêmes infos.
- Autres stations :
  - Mettent à jour leur NAV avec les informations du RTS-CTS

- Ne transmettent pas pendant la durée spécifiée par le NAV

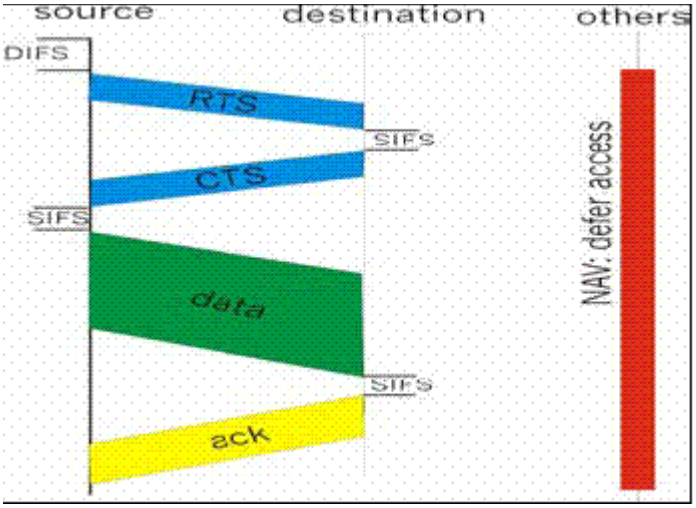


Image 74 NAV

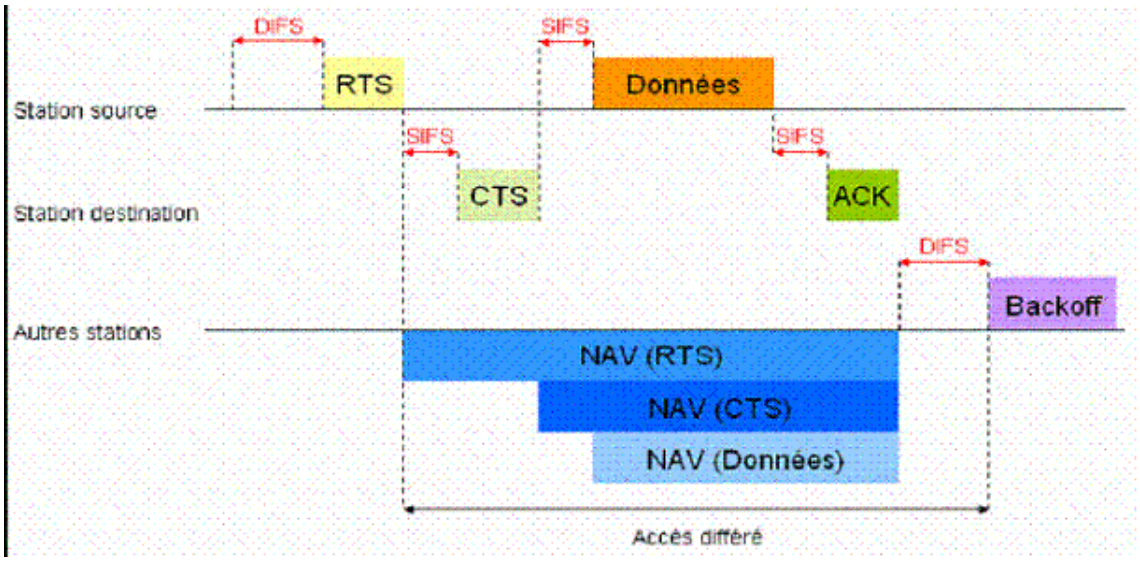


Image 75 NAV et DIFS

- Mécanisme habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante
- Les stations peuvent choisir :
  - D'utiliser le mécanisme RTS / CTS
  - De ne l'utiliser que lorsque la trame à envoyer excède une variable RTS_Threshold
  - De ne jamais l'utiliser

11. PCF : Point Coordination Function

- Fonctionnement en scrutation (polling) par le PC (Point Coordinator).
- Une station émet si elle est autorisée par le PC.
- Le PC sélectionne une station en plaçant son adresse dans la trame.
- Les trames sont acquittées. Si l'acquittement ne revient pas le PC ou la station effectuent la retransmission.
- PCF a plutôt été destiné à des échanges à qualité de service.

12. Fragmentation et reassemblage

Fragmentation

- Vu que le taux d'erreurs des liaisons sans fil est plus important que celui des liaisons filaires, il est donc nécessaire de transmettre de petites trames.
- Les trames de données (MSDU) et celles de gestion (MMPDU) sont fragmentées en plusieurs trames MPDU (MAC PDU)
- La fragmentation est réalisée si la taille est supérieure à un seuil
- Les fragments sont envoyés de manière séquentielle
- Le destinataire acquitte chaque fragment
- Le support n'est libéré qu'une fois tous les fragments transmis avec succès
- Si les stations utilisent le mécanisme RTS / CTS, seul le premier fragment envoyé utilise les trames RTS / CTS

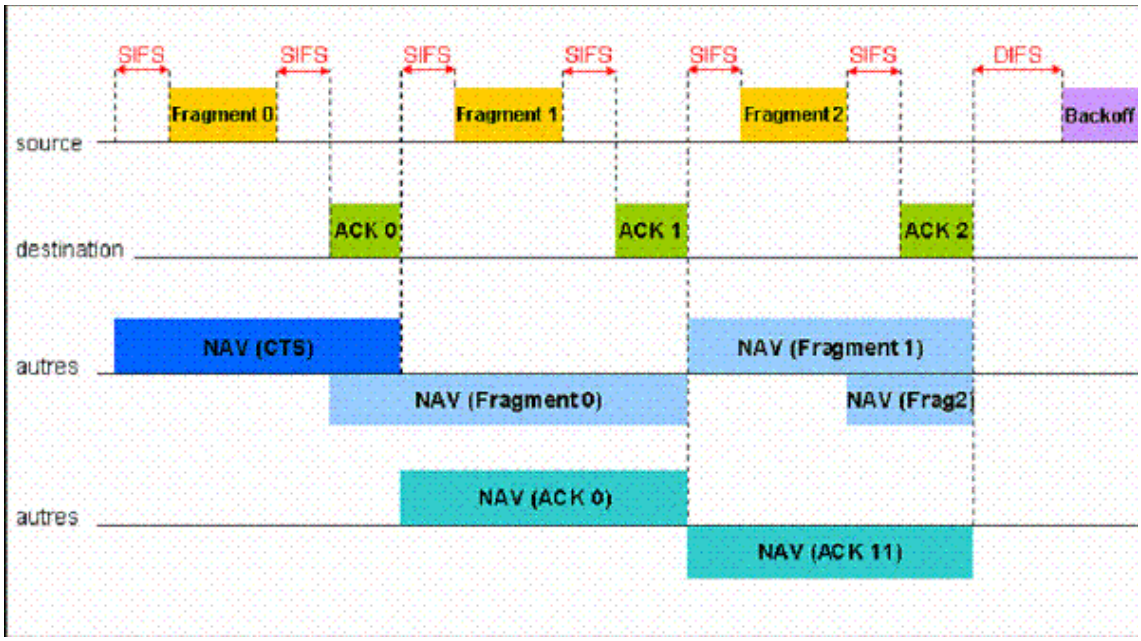


Image 76 Fragmentation

Réassemblage

- Deux champs permettent le réassemblage des fragment :
  - **Sequence Control** : permet le réassemblage de la trame grace à un
    - Sequence number : les fragments d'une même trame ont le même No. De séquence
    - Fragment Number : indique le No. De fragment dans la trame
  - **More Fragment** : indique si d'autres fragments suivent. Egal à 0 si c'est le dernier fragment

13. Gestion de la mobilité

- Des trames balises permettent aux stations mobiles de rester synchronisées
- Association-réassociation :
  - Choix du point d'accès : puissance du signal, taux d'erreur, charge
  - Ecoute du support :
    - Passive : attente d'une trame balise
    - Active : envoie d'une requête (Probe Request Frame) et attente de la réponse contenant les caractéristiques du point d'accès
  - Authentification : deux mécanismes

- Open System Authentication : mode par défaut
  - Requête d'authentification / Confirmation
- Shared key authentication : véritable mécanisme d'authentification (clé secrète)
  - Requête authentification (station -> AP)
  - Challenge Text - (station <- AP)
  - Challenge response - (station -> AP)
  - Confirmation (station <- AP)

- Protocole IAPP, Inter Access Point Protocol (IEEE 802.11f)
  - Protocole au dessus d'UDP
  - Utilise RADIUS pour permettre des handovers sécurisés
  - S'appuie sur un serveur centralisé ayant une vue globale du réseau (connaît correspondance entre adresse IP/@MAC)

14. Format de trame (MAC)

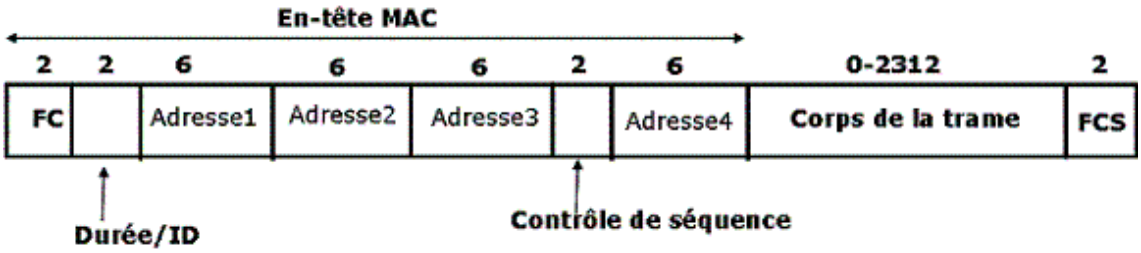


Image 77 Trame MAC

1. **FC** (Frame Control): version de protocole, type de trame ...etc.
2. **Durée / ID** : Durée d'utilisation du canal de transmission.
3. **Champs adresses** : Une trame peut contenir jusqu'à 4 adresses (mode ad hoc adresse 1 destination et adresse 2 source).
4. **Contrôle de séquence** : pour la fragmentation
   - Numéro de séquence de la trame (12 bits)
   - Numéro de fragment (4 bits).
5. **Corps de la trame** : charge utile d'au maximum 2312 octets.
6. **FCS** (Field Check Sequence): somme de contrôle de niveau MAC

Champs "Controle de trame"

Version (2bits)		Type (2bits)		Sous type (4 bits)			
To DS	From DS	More Frag.	Retry	Power Mngt	More Data	WEP	Order

Image 78 contrôle de trame

- **Version du protocole** : Actuellement 0 en première version.
- **Type et sous type** : Définition du type de la trame (2 bits + 4 bits).
- **To et From DS (Distribution System)** : Trame vers ou en provenance du système de distribution (AP point d'accès).
  Les 2 bits à 0 mode Ad hoc.
- **More** : Il reste des fragments à émettre (bit more de la fragmentation).
- **Retry** : La trame est une retransmission d'une trame précédente erronée.
- **Power management** : A 1 la station entre en mode économie.
- **More data** : A 1 des données sont à émettre vers une station en économie.

- **WEP** : A 1 la trame est chiffrée en WEP (Wireless Equivalent Privacy).
- **Order** : Trame de la classe de service strictement ordonné.

E. Les réseaux locaux virtuels (VLANs)

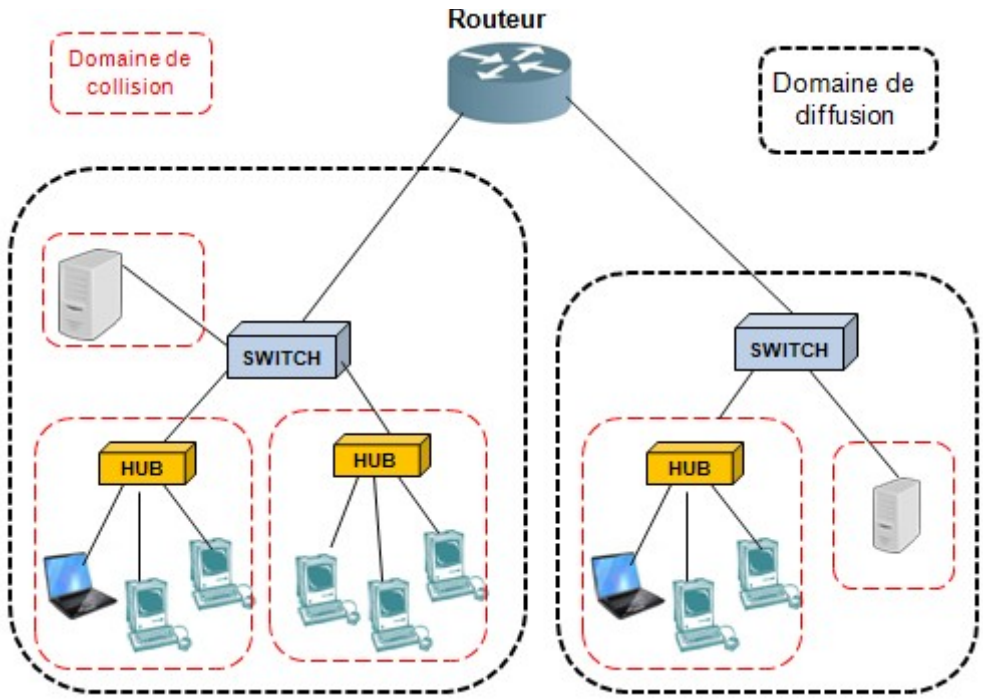
1. Ponts et switchs

Les apports de la commutation

- Sécurité :
  - Il n'y a plus de possibilité (en mode promiscuous) de voir un trafic qui ne nous concerne pas
  - La baisse d'administrabilité qui en résulte a été compensée par l'insertion de sondes logicielles RMON par port dans la plupart des switches
- Performance : chacun a une bande apparente de 10 Mb/s (ou 16)
- Avec les commutateurs de première génération, la séparation des flux gérés par la couche 2 ne peut se faire qu'en regroupant géographiquement les groupes de travail. En effet, si le commutateur segmente les domaines de collision, il maintient cependant un seul domaine de diffusion.

Rappel : domaine de collision

- Un domaine de collision désigne une partie du réseau dans laquelle toutes les trames sont vues par tous les équipements. Il concerne les support multipoints comme les bus et les « hubs » ou concentrateurs.
- Un domaine de collision est limité par les « switchs » ou commutateurs et les routeurs.



2. Les concepts des VLANs

Objectifs

- Avec les commutateurs de première génération, la séparation des flux gérés par la couche 2 ne peut se faire qu'en regroupant géographiquement les groupes de travail. En effet, si le commutateur segmente les domaines de collision, il maintient cependant un seul domaine de diffusion.
- La séparation et la sécurité des domaines de diffusion exigeaient une séparation géographique des domaines de diffusion et une interconnexion par routeur
- Si l'interconnexion du réseau repose sur les commutateurs et non sur les routeurs (ce qui est de plus en plus le cas) cela pose deux problèmes

  - les trames de diffusion sont propagées sur tout le réseau, or ces trames sont nombreuses (ARP, DHCP, Netbios, etc.).

  - en mettant une carte réseau en mode 'promiscuous', il est possible de capturer ces trames ou encore en utilisant un « sniffer » tel que

  « WireShark » par exemple. Des problèmes de confidentialités peuvent donc se poser.
  - **Le concept VLAN permet de limiter la portée des broadcasts.**

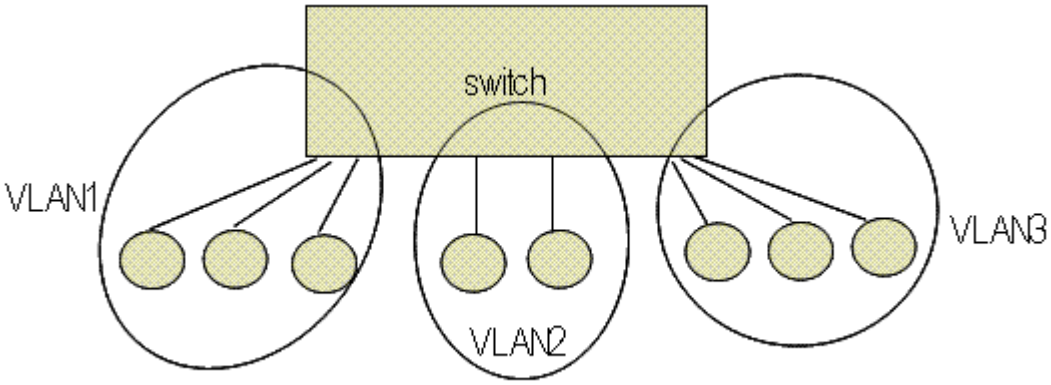


Image 79 Séparation en 3 VLANs

Avantages des VLANs :

- réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN.
- création de groupes de travail indépendants de l'infrastructure physique ; possibilité de déplacer les utilisateurs (+mobilité) sans changer de réseau virtuel.
- augmentation de la sécurité par filtrage (en définissant des politiques de sécurité) et le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).
- Il est également possible
  - de construire des VLANs avec des ports multi-stations
  - de mêler plusieurs VLAN sur le même segment, le bénéfice de la réduction des broadcasts s'amoindrit.

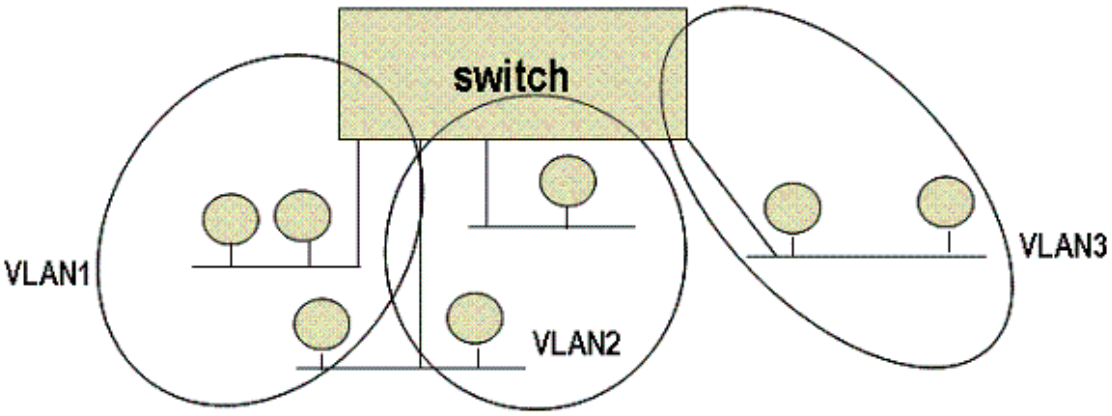


Image 80 Plusieurs VLANs sur le même segment

- La même approche est envisageable à plusieurs switches

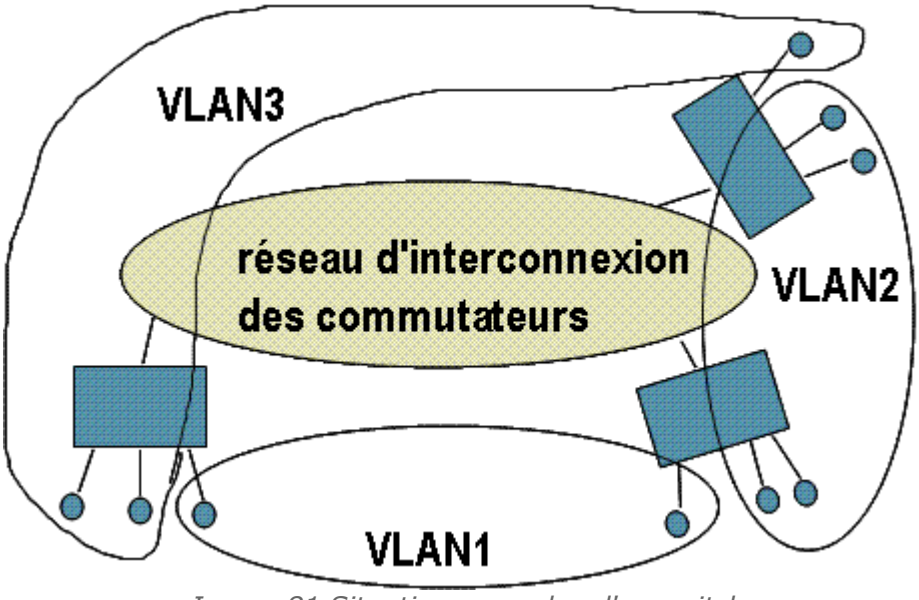


Image 81 Situation avec plus d'un switch

- Avec de très nombreuses questions :
  - Nature du "core network" : débit, protocoles de communication entre switches (IEEE 802.1Q par exemple)
  - Maillage et sécurité des switches entre eux ?

Objectifs de construction des VLANs

- Pousser plus loin la performance en réduisant les broadcasts inutiles
- Pousser plus loin la sécurité en réduisant les trafics inutiles et les communications "agressives" interdites
- Mais aussi se donner une approche "logique" de la construction de ses réseaux locaux
  - Constitution des réseaux via un outil d'administration et non plus via un branchement physique
  - Mobilité / souplesse des changements (en fonction des règles d'affectation au VLAN)

Pour atteindre ces objectifs, il est nécessaire de répondre aux questions suivantes :

1. Quelles sont les règles de constitution des VLAN ?
   réponse : VLAN de niveau 1, VLAN de niveau 2, VLAN de niveau 3
2. Quelles sont les architectures et protocoles permettant de propager

l'appartenance à un VLAN et donc de constituer des VLAN étendus ?
réponse : privé, 802.10, 802.1q, LANE, ...

3. Comment gérer la communication entre VLANs ?
   - pas de communication
   - routage interne
   - routage externe

3. VLANs de niveau 1

Les VLANs de niveau 1 sont des VLANs par ports où chaque port du commutateur est affecté à un VLAN.

L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur.

- Les ports sont donc affectés de manière **statique** à un VLAN.

En cas de besoin de déplacer physiquement une machine, il est nécessaire de désaffecter son port du Vlan puis affecter le nouveau port sur lequel la station vient d'être connectée au bon Vlan.

En cas de besoin de déplacer logiquement une station (on veut la changer de Vlan) il est nécessaire de modifier l'affectation du port au Vlan.

- **Dans les VLAN de niveau 1 on dit : "tel port appartient à tel VLAN"**

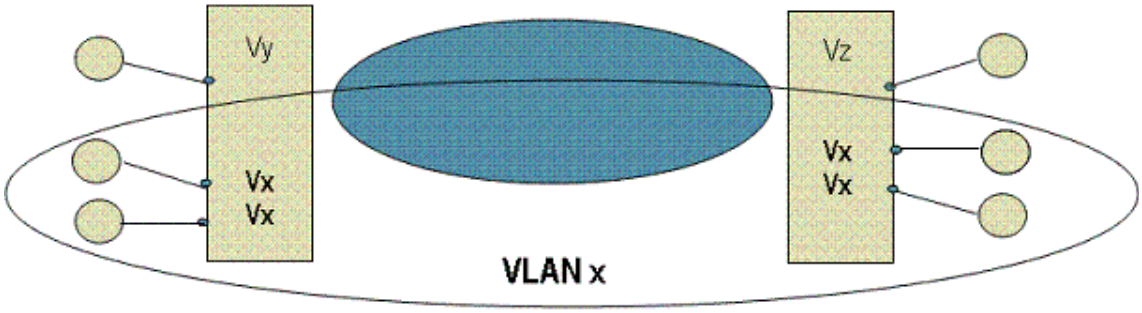


Image 82 Vlan de niveau 1

- **Possibilité** : on peut avoir plusieurs VLANs sur un port
- **Avantages** : simple, performant, aisé à concevoir, mais moins aisé à faire vivre
- **Inconvénients** :
  - La mobilité physique des stations est ingérable sauf au travers de l'administration des switches et donc jamais automatique)
  - Pas de gestion simple des liens multi-stations
- **Contexte** :
  - Faible mobilité des stations
  - Séparation fonctionnelle entre (par exemple) un réseau de développement et un réseau bureautique

Le cas des liens multi_stations

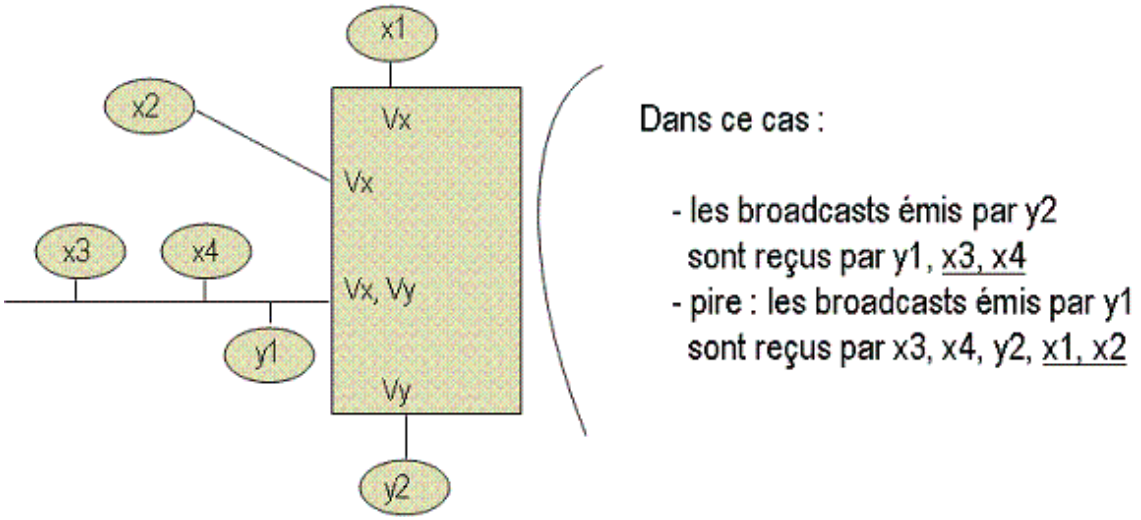


Image 83 Liens multi-stations

4. VLANs de niveau 2

Les VLANs de niveau 2 sont des VLANs par adresses MAC. Chaque adresse MAC est affectée à un VLAN

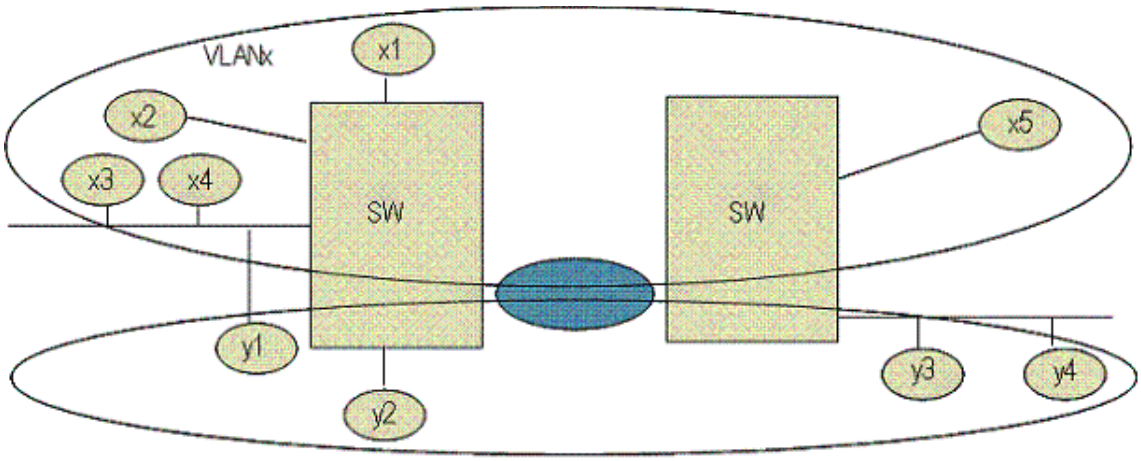


Image 84 VLAN de niveau 2

- **Possibilités** :
  - Plusieurs VLAN pour une adresse MAC
  - Plusieurs adresses sur un port, bien sûr
- **Avantages** :
  - Simple et performant
  - Broadcast plus sélectifs (x3 reçoit les broadcast de y2, mais y2 ne reçoit pas les broadcast x3)

5. VLANs de niveau 3

- Dans ces VLANs, une adresse de niveau 3 est affectée à un VLAN et l'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de niveau 3 ou supérieur qu'elle contient (le commutateur doit donc accéder à ces informations). En fait, il s'agit à partir de l'association adresse niveau

3/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

- Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3 par analyse protocolaire. Ceci est un fonctionnement moins rapide que le Vlan de niveau 2.
- Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.
- Dans certaines situations, on associe une trame à un Vlan en fonction du protocole qu'elle transporte. Ce protocole peut être un protocole de niveau 3 pour isoler les flux IP, IPX, Appletalk, etc. Mais on peut trouver aussi des Vlan construits à partir de protocole supérieur (notamment H320). On parle quelquefois de Vlan par règles ou par types de service.
- Dans les réseaux Wi-fi, on peut construire des Vlan par SSID. Cela permet d'apporter une solution au problème de sécurité.
- Idée : le VLAN est choisi en examinant le niveau 3
  - Soit simplement le protocole transporté
  - Soit l'adresse de niveau 3 origine
- Les usages possibles
  - Construire un VLAN à partir de l'adresse IP
  - Définir des VLANs différents en fonction des protocoles : un VLAN pour des stations IP et un pour les équipements IPX
- Naturellement, les VLANs de niveau 3 exigent qu'une station puisse appartenir à plusieurs VLAN

6. Extension des VLANs à Plusieurs switches

Extension de VLANs à plusieurs switchs : la norme IEEE 802.1q

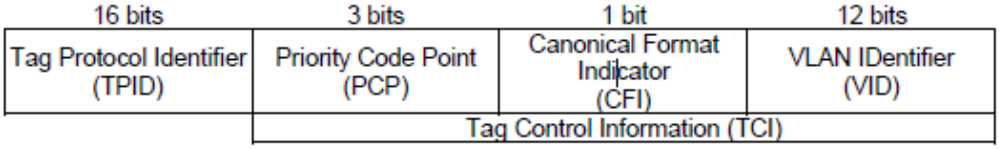
- La norme IEEE 802.1q a été développée pour permettre l'extension de VLANs sur plusieurs switchs. Elle utilise un étiquetage des trames en ajoutant une information dans l'en-tête de la trame.
- L'étiquette ajoutée, appelée « tag », permet d'identifier le VLAN auquel la trame est destinée, on parle alors de VLANs « taggés ». Le format de la trame est donc modifiée, ce qui peut entraîner des problèmes de compatibilité avec les switchs ne supportant pas les VLANs.
- L'étiquetage des trames n'est réalisé que par les switchs qui ajoutent et enlèvent les « tags » dans les trames. Les machines ne gèrent donc pas l'étiquetage qui leur est inconnu.
- Trois types de trames sont définis :

  - les trames non étiquetées (untagged frame) : elles ne contiennent aucune information sur leur appartenance à un VLAN ;

  - les trames étiquetées (tagged frame) : elles possèdent une étiquette qui indique à quel VLAN elles appartiennent ;

  - les trames étiquetées avec priorité (priority-tagged frame) : sont des trames qui possèdent en plus un niveau de priorité défini selon la norme IEEE 802.1P.

Format de la trame IEEE802.1q



- le champ TPID a une valeur fixe, 0x8100 qui identifie une trame de type 802.1q ;
- le champ TCI est constitué de trois champs :
  - le champ Priority indique le niveau de priorité de la trame et est utilisé lorsque que le champ VID est nul ;
  - le champ CFI indique que le format est standard (Ethernet) ou non ;
  - le champ VID contient l'identifiant du VLAN auquel appartient la trame.

Enregistrement dynamique des VLANs : Mutiple VLAN Registration Protocol (MVRP)

Les VLANs peuvent être déclarés manuellement ou dynamiquement. Dans la déclaration dynamique, l'administrateur définit les VLANs sur un switch et un seul et !e protocole MVRP (Mutiple VLAN Registration Protocol) permet la diffusion de ces informations aux autres switchs du réseau.

F. Interconnexions de LANs

- Les différentes raisons pour lesquelles une entreprise aurait intérêt à étendre et à regrouper ses moyens de communication sont :
  - Le besoin croissant des échanges dont le volume est en perpétuelle augmentation.
  - Le besoin de segmenter un réseau local pour en améliorer, soit les performances, soit la sécurité ou encore l'organisation, en filtrant le trafic.
  - Le besoin de partager certaines ressources difficiles à gérer et coûteuses pour l'entreprise.
- Le problème de base est le choix du niveau d'interconnexion en fonction des besoins et des solutions disponibles en termes de techniques et d'équipements d'interconnexion. Nous allons :
  - Tracer les étapes de l'approche méthodologique
  - Analyser les différences entre les protocoles de communication
  - Recenser les techniques d'interconnexion

1. Analyse architecturale des composants

Le but de cette étape est d'avoir une représentation unique des différents éléments du réseau.

Cette étape comprend :

- La prise en compte de la topologie.
- L'étude des configurations.
- La modélisation des architectures de chaque composant réseau suivant le

modèle en couches.

2. Définition des unités d'interconnexion

Dans cette étape, on pourra ressortir les niveaux architecturaux incompatibles.

Ainsi, on pourra définir les frontières d'hétérogénéité.

Suivant les objectifs à atteindre pour l'interconnexion étudiée, on définit les spécifications fonctionnelles des unités d'interconnexion (UI) entre chaque sous-réseau.

Les différents relais sont alors choisis.

3. Eléments d'hétérogénéité

L'analyse des architectures de chaque composant du réseau global permet de classer les éléments homogènes et hétérogènes de la nouvelle configuration.

Différences protocolaires

1. Les protocoles se différencient essentiellement par leur mode de connexion (mode connecté et non connecté), et la structure des unités de données du protocole (par exemple les trames 802.3 sont au maximum de 1518 octets, celles de 802.4 de 8191 octets et pour le 802.5 elles sont de 5000 octets.)
2. Les mécanismes mis en œuvre :chaque fonction assurée par un protocole se traduit par un algorithme qui, pour la réalisation, pour le traitement, met en oeuvre des mécanismes. Cependant, il existe plusieurs mécanismes permettant d'obtenir la même fonctionnalité. Parfois les mécanismes sont les mêmes mais les paramètres diffèrent. Voilà une autre source de différence entre deux protocoles (Exemple : les "timers" qui auront rarement les mêmes valeurs dans les différents sous-réseaux.
3. La structure d'adressage choisie : dans l'interconnexion de réseaux l'adressage est un point crucial car on doit garantir l'unicité des adresses où s'effectue l'interconnexion.

La frontière d'hétérogénéité

Elle s'étudie à travers les services rendus par la pile de protocoles des architectures que l'on veut interconnecter.

L'analyse des architectures repère deux ensembles :

- L'un regroupant les éléments homogènes, se trouvant en général dans la partie haute de l'architecture
- L'autre, les éléments hétérogènes, regroupant les couches constituées de services et de protocoles présentant des différences.

La frontière entre ces deux ensembles définit le niveau de l'interconnexion.

4. Equipements d'interconnexion

Nous allons analyser, suivant le niveau d'interconnexion, les techniques et les mécanismes à mettre en œuvre dans les passerelles à savoir :

- **Répéteurs** (passerelle de niveau 1)
- **Ponts** (passerelle de niveau 2)
- **Routeurs** (passerelle niveau 3)

Il est à noter aussi qu'il est parfois nécessaire de faire appel à des passerelle de plus haut niveau appelées : **Passerelles applicatives**

Passerelle

Une passerelle est un équipement intermédiaire assurant le relais entre deux réseaux et permettant ainsi la mise en relation de deux entités.

Une passerelle sera modélisée par le **niveau auquel elle opère** et par **son mode de fonctionnement**.

- Le niveau d'une passerelle est la plus haute couche concernée par la passerelle
- La passerelle est en conséquence invisible des couches au dessus de ce niveau

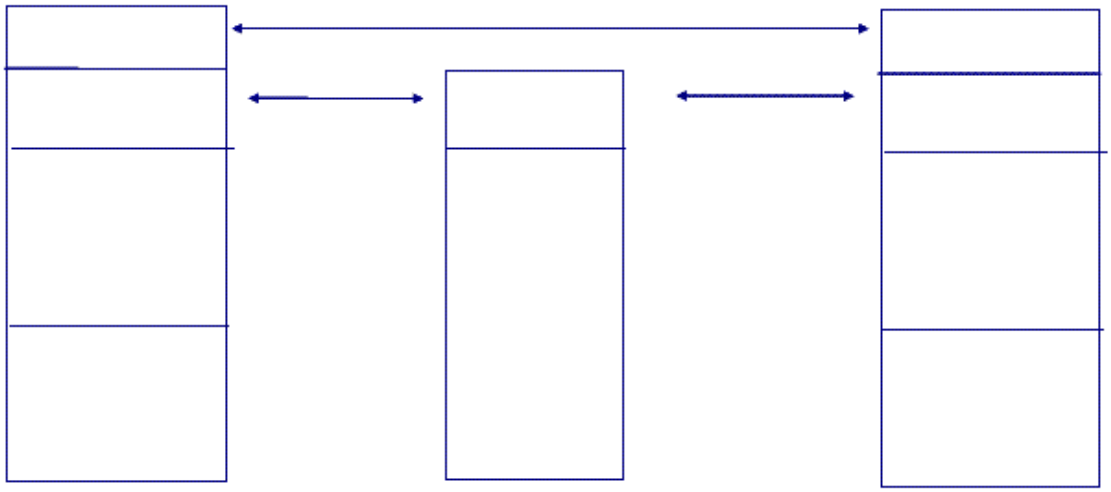


Image 85 Niveau d'une passerelle

- Plus le niveau de la passerelle est plus haut plus elle est évoluée et moins elle est performante, plus elle est chère.
- Une architecture réseau cherche à utiliser des passerelles basses
- Une passerelle de niveau N dépasse les limites de la passerelle de niveau N-1

Remarque :

Les protocoles de niveau 1 ont des limites de fonctionnement en distance conduisant à utiliser des passerelles de niveau 2.

5. Modes de fonctionnement d'une passerelle

Commutation

Mise en correspondance de protocole de même nature au niveau N

Image 86 Commutation

Conversion

Mise en correspondance de protocoles de natures différentes

Image 87 Conversion

Exemple : Pont Ethernet/Toking Ring

Encapsulation

Une passerelle coopère avec une autre passerelle afin de restituer le même protocole de la part et d'autre des 2 passerelles.

Exemple : interconnexion de réseaux IPv6 via un réseau intermédiaire IPv4

Résumé

On peut résumer les différents cas possibles à travers les questions suivantes :

- Comment relier deux réseaux locaux identiques dépassant la longueur autorisée, (répéteurs impossible), bien que l'on soit à courte distance ?
- Que fait-on à grande distance ?
- Peut-on isoler le trafic de chacun des réseaux ?
- Comment relier deux réseaux locaux différents?

6. Interconnexion de niveau physique : Les répéteurs

Les Répéteurs permettent l'extension géographique d'un réseau local en interconnectant plusieurs segments sans dégradation de la qualité de service.

Ils ont pour rôle la régénération du signal d'un segment à un autre.

Leur fonction se situe donc au niveau physique du modèle OSI.

Une interconnexion de niveau 1 signifie que les architectures sont identiques à partir du niveau MAC.

C'est le cas de l'interconnexion de deux réseaux locaux identiques sur courte distance.

Exemple : Dans la norme IEEE 802.3, un segment de câble coaxial est de longueur maximum de 500m. En utilisant des répéteurs le réseau peut couvrir une distance de 2500m.

Les répéteurs peuvent être utilisés pour interconnecter des segments dont les supports physiques de transmission sont différents.

Le réseau construit à partir de plusieurs segments reliés par des Répéteurs constitue un **RESEAU PHYSIQUE**.

7. Interconnexion de niveau 2 : Le pont

Les ponts permettent l'interconnexion de réseaux locaux au niveau de la sous-couche MAC (Medium Access Control).

Un pont ne s'occupe pas des protocoles de haut niveau, il s'occupe de l'isolation du trafic.

C'est à dire qu'un pont reliant deux segments ne laisse pas passer sur l'autre segment une trame destinée à une station de ce segment.

======> Les différents segments reliés par un pont forment un même **RESEAU LOGIQUE**.

- L'interconnexion des réseaux locaux a été abordée par le comité IEEE 802.
- Le standard IEEE 802.1d définit l'interconnexion par "Pont locaux" au niveau MAC et repris par l'ISO (norme ISO 100038), et le projet de standard IEEE 802.1g celle par "Pont distant".
- On aura recours à la conversion de service ou la conversion de protocole quand les couches MAC sont hétérogènes et à l'encapsulation quand les couches MAC sont les mêmes aux extrémités, mais on traverse un troisième réseau intermédiaire ayant des protocoles différents.

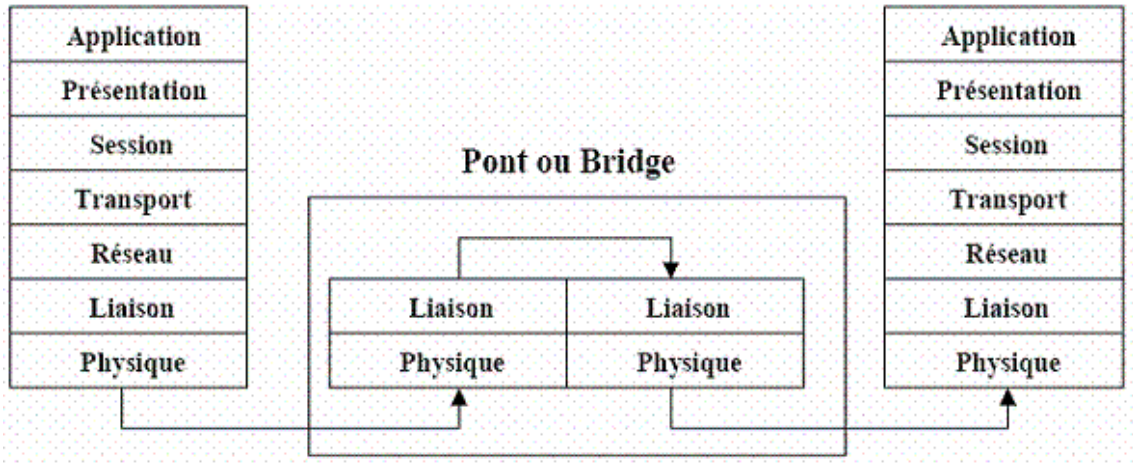


Image 88 Interconnexion de niveau 2

- Le critère distance permet de diviser les ponts en deux catégories :
  - **Les ponts locaux** : les pont locaux (Local Bridges) sont utilisés pour relier des réseaux locaux géographiquement voisins.
  - **Les ponts distants** : les ponts distants (remote Bridges) ou demi-ponts sont utilisés pour relier des LANs géographiquement éloignés. Ils sont composé de demi-ponts reliés par une liaison moyen ou haut débit.
- **Pont simple** : sans filtrage, fonctionne en "passthrough" et ne sert qu'à couvrir la distance.
- **Pont intelligent** : (Mode Transparent MT) avec table d'adressage à configuration dynamique (auto apprentissage) et filtrage de trames. Il permet d'isoler les trafics et de maintenir les performances de chaque sous-réseau.
- Avec ces ponts l'algorithme utilisé est l'algorithme "Spanning Tree" préconisé par la norme IEEE 802.1d.
- Un pont filtrant possède la fonction de filtrage d'adresses : les trames ne sont pas toutes propagées à travers tout le réseau.
- Le pont prélève la trame et l'envoie sur le deuxième réseau auquel il est relié sans lui apporter de modifications (cas où les deux réseaux sont identiques).
- Le pont voit passer tous les messages, il lit l'adresse source et il vérifie si elle est présente dans la table des stations actives du réseau d'origine, sinon il l'ajoute. Quant à l'adresse destination, elle lui permet de ne laisser passer que les adresses n'appartenant pas à cette table.
- Cette fonction de filtrage n'a qu'une visibilité MAC. Le pont est bien transparent pour les utilisateurs (LLC) de la sous-couche MAC.
- Les ponts filtrant disposent d'une table dynamique en mémoire volatile (RAM).

- En mode auto-apprentissage le pont, constamment à l'écoute du réseau, enregistre dans sa table les adresses source des stations qui émettent sur les tronçons auxquels il est relié ainsi que les directions (les ports de données) correspondants à ces stations :
  - Si la destination est sur le même tronçon que la source, la trame n'est pas transmise vers les autres tronçons
  - Si la destination est dans la table du pont avec une direction différente de celle de la source, la trame est transmise dans la direction adéquate c'est à dire sur le port correspondant
  - Si la destination n'est pas connue du pont, il transmet la trame sur tous ses ports sauf sur celui par lequel il a reçu celle-ci. On évite donc de surcharger

Pont Source Routing

Il utilise un protocole de recherche de chemin par la station émettrice

Pont Spanning Tree

- Afin de structurer les chemins entre les différents ponts sans boucles, un échange d'informations entre les ponts permet de définir l'état de leurs ports comme actif ou bloqué.
- L'algorithme élit un pont particulier appelé **pont racine** et à choisir un chemin unique entre les ponts et la racine.
- En plus de l'adresse MAC, chaque pont possède un identificateur.

8. Interconnexion de niveau 3 : Les routeurs

Un routeur est un équipement permettant l'interconnexion de plusieurs réseaux quand certaines différences protocolaire ne peuvent se résoudre au niveau 2 ou lorsque le niveau d'hétérogénéité est au niveau 3.

Il est aussi utilisé pour définir des sous-réseaux afin de faciliter l'administration et d'améliorer les performances.

Un routeur :

- est référencé comme un système intermédiaire ou comme relais.
- prend des décisions d'acheminement d'informations, il n'examine que les paquets qui lui sont destinés.
- permet la séparation logique des différents sous-réseau : chaque sous-réseau a une adresse.
- ne s'occupe ni de la topologie du réseau ni du protocole d'accès des segments

Les routeur sont souvent utilisés entre des segments réseau ayant les mêmes protocoles de haut niveau.

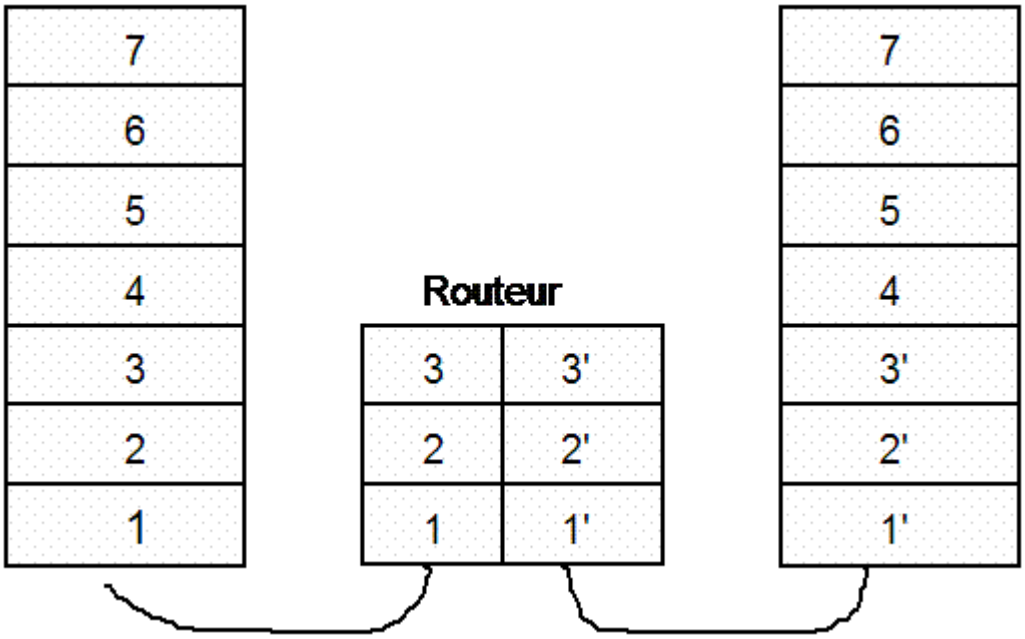


Image 89 Interconnexion de niveau 3

9. Passerelles applicatives

Elles permettent l'interconnexion de réseaux dont les architectures sont hétérogènes jusqu'au niveau applicatif.

Transmission de données

IV

A. Composition d'une liaison de transmission de données

1. Présentation

Les besoin de connecter des terminaux passifs à un ordinateur central sont apparus vers les années 60 et a donné naissance au développement des modems qui permettent de réaliser ces connexions. La vitesse des premiers modem était de 300 bits par seconde (bits/s) s. Une liaison de transmission de données peut être vue comme est composée de deux types d'équipements l'ETTD (Equipement Terminal de Traitement de Données) et l'ETCD (Equipement Terminal de Circuit de Données) reliés par une ligne de communication.

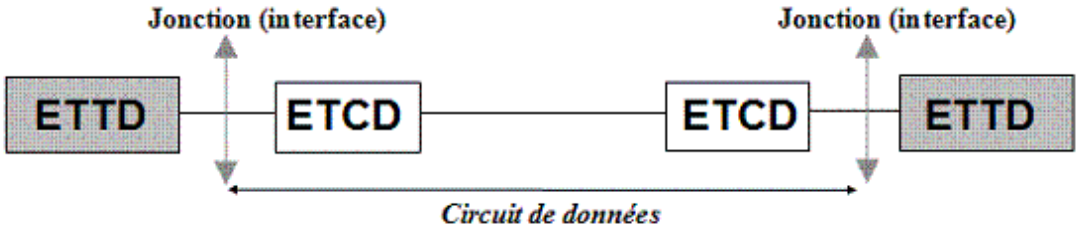


Image 90 Liaison de transmission de données

B. Modes d'exploitation d'une liaison

1. Présentation

L'échange d'information entre deux systèmes informatiques peut s'effectuer selon trois modes : unidirectionnel, bidirectionnel à l'alternat, et bidirectionnel simultané.

1. **Liaison unidirectionnelle (simplex)**
   - Dans ce mode d'exploitation de la liaison, les données transitent dans un seul sens.
2. **Liaison bidirectionnelle a l'alternat (half-duplex)**
   - Dans ce mode d'exploitation de la liaison, les données transitent dans les deux sens mais pas simultanément .
3. **Liaison bidirectionnelle simultanée (full-duplex)**
   - Dans ce mode d'exploitation de la liaison, les données transitent dans les deux sens.

C. Caractéristiques d'une voie de transmission

Les voies de transmission acheminent des ondes électromagnétiques, la plus élémentaire des ondes est l'onde sinusoïdale.

X(t)=Asin(Bt+C)

- A : amplitude maximale
- B : la pulsation
  B =2 * PI * F
- F : la frequence
- t : le temps
- C : la phase
- X(t) : l'amplitude a l'instant t.

X(t) : l'amplitude a l'instant t.

Image 91 Voie de transmission

- Le bruit est un signal parasite provenant de différentes sources câbles proches acheminant des signaux de données, interférences radioélectriques provenant de signaux tiers proches, interférences électromagnétiques, etc.) qui peuvent être naturelles ou technologiques qui s'ajoute au signal de données.
- les signaux de données correspondent à des niveaux de tension, représentés par des 1 et des 0, qui sont mesurés à partir d'un niveau de référence de 0 volt appelé la terre de signalisation. Il est fondamental pour les équipements d'émission et de réception de données d'avoir le même point de référence de

0 volt.

1. Affaiblissement

L'affaiblissement se traduit par la perte de puissance d'un signal sur une voie de transmission. Des câbles longs et des fréquences de signaux élevées contribuent à augmenter l'atténuation. Pour cette raison, l'affaiblissement se mesure à l'aide d'un testeur de câble réglé sur les fréquences les plus élevées que les câbles peuvent supporter.

L'affaiblissement se mesure en décibels

$A=10\log_{10}(S/N)$

S étant la puissance du signal émis et N la puissance du bruit.

Les signaux sont transmis avec des affaiblissements d'amplitude négligeables jusqu'à une certaine fréquence fc dite **fréquence de coupure.**

2. Bande passante

On appelle **bande passante** d'une voie de transmission pour un affaiblissement donné a, l'intervalle de fréquences soumises à un affaiblissement inférieur ou égal à a.

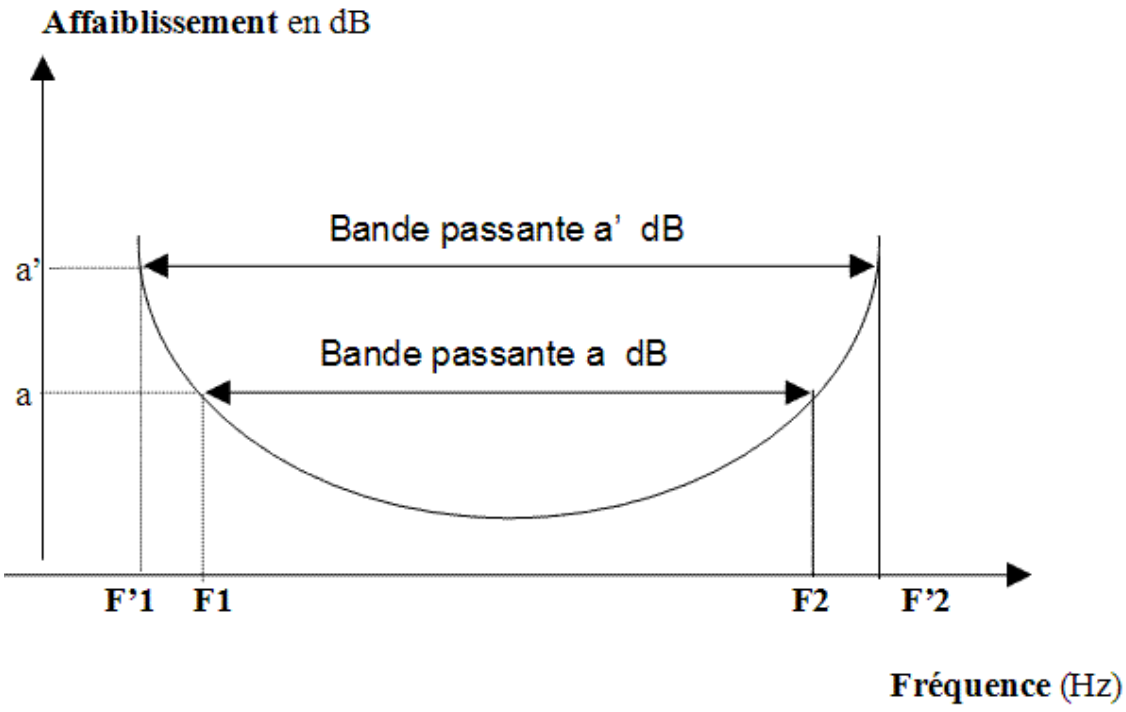


Image 92 La bande passante

Exemple

Une ligne téléphonique ordinaire ne laisse passer que des signaux de fréquence comprise entre 300Hz et 3400Hz.

En dehors de cette bande, les signaux sont très affaiblis et ne sont plus compréhensibles.

On dit alors que la bande passante d'une telle ligne est 300-3400Hz. L'affaiblissement est alors d'environ 6dB.

La largeur de bande est de 3100Hz.

3. Rapidité de modulation et capacité

Les travaux de Shannon montrent qu'une voie de transmission ayant une largeur de bande de B (Hz) permet une cadence de 2B signaux ou échantillons par unité de temps.

Cette cadence porte le nom de **rapidité de modulation** ou **vitesse de signalisation** et s'exprime en **Bauds**.

La **capacité** d'un canal ou le **débit binaire maximum (D)** est la quantité maximale qu'il peut transporter par unité de temps. Elle s'exprime en **bits/sec**.

Valence (n) : est le nombre d'états significatifs distincts employés dans une modulation pour caractériser les éléments de signal à transmettre.

Les deux grandeurs précédentes (rapidité de modulation et débit binaire) ont des valeurs identiques lorsque l'on transmet des signaux à deux états (valence du signal égale a 2).

La relation qui lie les deux grandeurs est : $\mathbf{D = Rm\log_2 n}$

- D : débit binaire (en bits/sec.)
- Rm : rapidité de modulation (en Bauds)
- n : valence du signal

Théorème de Shannon

La capacité de transmission d'une ligne soumise a du bruit est donnée par la relation suivante :

D = B log2(1+S/N)

- S/N étant le rapport signal sur bruit
- B étant la largeur de bande

Exemple : dans le réseau téléphonique, pour un rapport signal/bruit de 100 (20dB), le débit maximum est de l'ordre de 20000 bits/sec.

D. Modes de transmission

1. Transmission synchrone

Dans une transmission synchrone l'émetteur et le récepteur utilisent le même intervalle de temps

- le signal d'horloge de l'émetteur est transmis sur la ligne au récepteur.

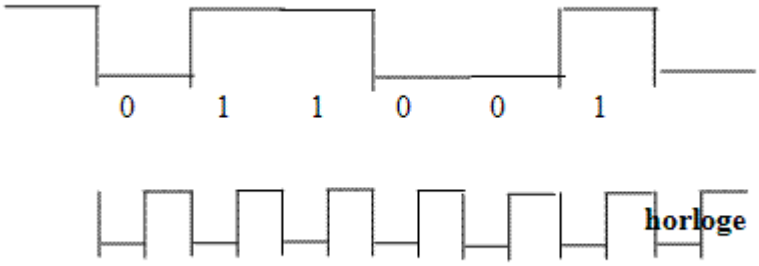


Image 93 Transmission synchrone

2. Transmission asynchrone

- Dans une transmission asynchrone, l'émetteur envoie des caractères à des instants qui ne sont pas prédéterminés.
- Un bit appelé **BIT START** est envoyé au début et sert à déclencher l'horloge locale du récepteur pour qu'il échantillonne les bits du caractère.
- Un ou deux bits appelés **BITS STOP** sont envoyés pour marquer la fin du caractère.

E. Interfaces de communications

La connexion d'un ETTD à un ETCD (ou de deux ETTD en cas d'absence d'ETCD) est réalisée par l'intermédiaire d'une **jonction** ou **interface**.

L'interface a trois principales caractéristiques :

- Mécaniques
- Electriques
- Fonctionnelles.

Les principales normes rencontrées dans les liaisons séries sont définies par les différents avis et recommandation du CCITT, de l'ISO, de l'EIA (Electrical Industry Association).

Image 94 Une interface

1. Les interfaces de communication

La liaison de communication série de type RS232 (normalisé par V24/V28) est encore très utilisée dans l'industrie ainsi que dans les équipements informatiques

comme les routeurs par exemple. En effet, la plupart des composantes (commutateur administrable, routeur...) d'un système de gestion de réseau informatique contiennent une liaison série de type RS232. Ceci permet, en cas de problèmes, d'intervenir en utilisant de simples commandes en lignes à partir d'un PC connecté sur ces équipements. C'est la raison pour laquelle, se trouve encore la traditionnelle prise DB9 mâle à 9 broches en façade des matériels réseaux professionnels.

La recommandation V24

- Spécifications mécaniques : connecteur 25 broches
- Caractéristiques fonctionnelles de la jonction
- Indépendance du mode de transmission, du support utilise, du type de connexion,

Les spécifications électriques sont décrites dans les recommandation V28, V11, et V35.

La recommandation V28

- Définit les caractéristiques électriques des signaux
- Une masse commune
- A un niveau logique 1 correspond une tension T, -25V <= T <= -3V
- A un niveau logique 0 correspond une tension T, +3V <= T <= +25V,

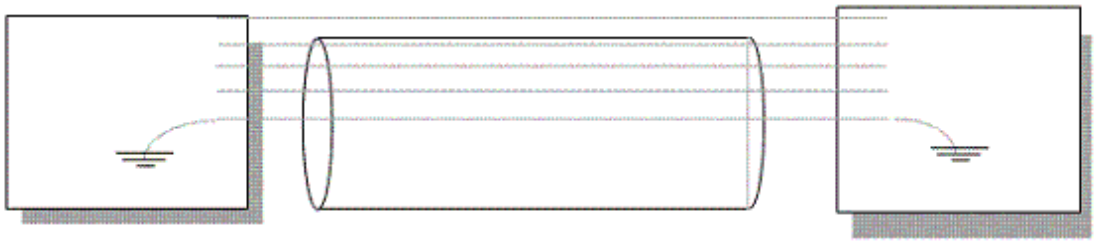


Image 95 V28

Le tableau suivant donne les circuits de jonction RS232 ainsi que les signaux correspondant en V24.

V24	Appellation CCITT V24	Abr.	RS232	Abr.	25 br.	9 br.	Sens
101	Terre de Protection	TP	Protective ground	PG	1		
102	Terre du Signal (0V)	TS	Signal Ground	SG	7	5	
103	Emission de Données	ED	Send Data	SD	2	3	S
104	Réception de Données	RD	Receive Data	RD	3	2	E
105	Demande Pour Emettre	DPE	Request To Send	RTS	4	7	S
106	Prêt A Emettre	PAE	Clear To Send	CTS	5	8	E
107	Poste de Données Prêt	PDP	Data Set Ready	DSR	6	6	E
108.2	Terminal Données Prêt	TDP	Data Terminal Ready	DTR	20	4	S
109	Détecteur de Porteuse	DP	Data Carrier Detect	DCD	8	1	E
111	Sélecteur de Débit Binaire	SDB	Data Signal Rate Selector	DSRS	23		S
113	Base de Temps Emission	BTE	Transmit Clock (DTE)	TC	24		S
114	Base de Temps Emission	BTE	Transmit Clock (DCE)	TC	15		E
115	Base de Temps Réception	BTR	Receive Clock (DCE)	RC	17		E
118	ED sur voie secondaire	SED	Secondary TD	STD	14		S
119	RD sur voie secondaire	SRD	Secondary RD	SRD	16		E
120	DPE sur voie secondaire	SDPE	Secondary RTS	SRST	19		S
121	PAE sur voie secondaire	SPAE	Secondary CTS	SCTS	13		E
122	DP sur voie secondaire	SDP	SRLSD: Secondary RLDS	SDCD	12		E
125	Indicateur d'Appel	IA	Ring Indicator	RI	22	9	E
140	Bouclage/Essai de Maintenance	BEM	Remote Loopback	RL	21		S
141	Bouclage Local	BL	Local Loopback	LL	18		S
142	Indicateur d'Essai	IE	Test Indicator	TI	25		E

avec : S : Sortie de l'ETTD
E : Entrée de l'ETTD

Avec V24/V28, les débits binaires sont limités à 20 Kbits / s et la longueur du câble de jonction est limitée à 15m.

C'est la transmission en mode commun

La recommandation V11 : Deux conducteurs par signal

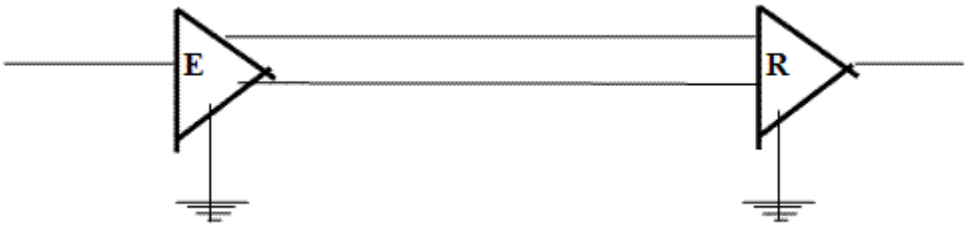


Image 96 V11

Ce mode de transmission est appelé **transmission en mode différentiel**

Débits binaires atteignant 2 Mbits / s sur des distances d'environ 60m

- Conducteur 37 broches (norme ISO 4902)
- Transmission sur des distances plus grandes et pour des débits élevés.

2. La liaison V24

La norme V24 décrit la fonction des signaux et la manière de les utiliser pour réaliser une transmission de données.

A chaque broche correspond :

- Un numéro d'identification ou numéro de circuit
- Sa fonction

Etablissement d'une liaison V24

Les principaux circuits participant à l'établissement d'une liaison V24 sont :

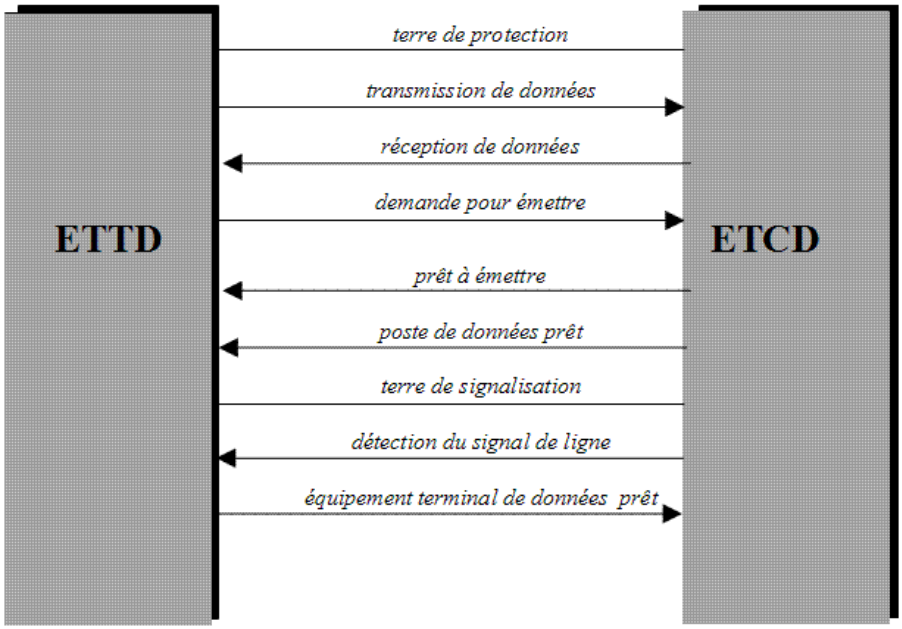


Image 97 V24

- Le seul câblage normalisé correspond à une liaison V24 entre ETTD et ETCD.

Liaison normalisée CCITT

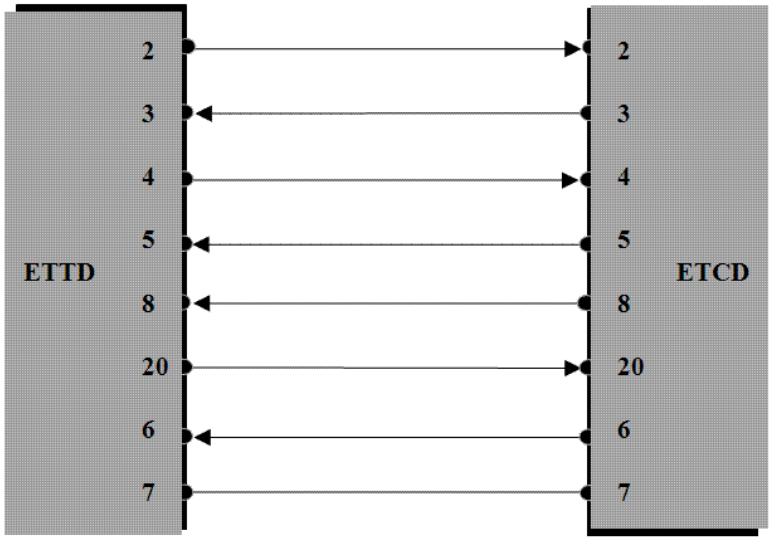


Image 98 Liaison normalisée CCITT

Liaisons hors norme CCITT

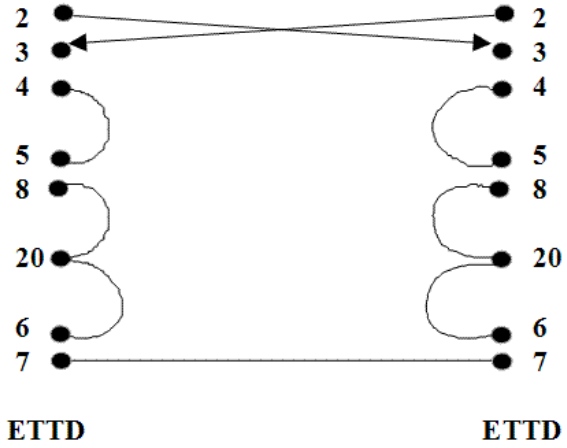


Image 99 Liaison hors norme CCITT

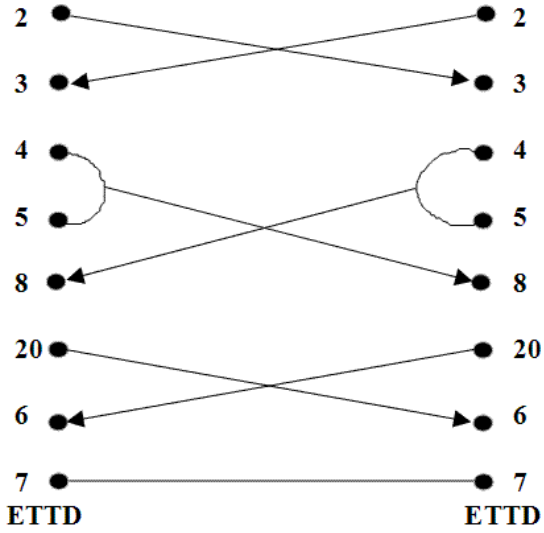


Image 100 Liaison hors norme CCITT

F. Transmission analogique et numérique

1. Les différents cas

Selon la nature des informations à transmettre et la nature de transmission on peut distinguer :

La transmission analogique d'informations analogiques

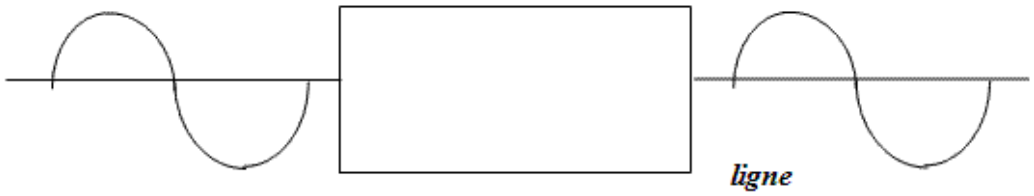


Image 101 transmission analogique d'informations analogiques

La transmission analogique d'informations numériques

Pour réaliser la transmission d'un signal numérique sur une voie analogique, on procède à une adaptation du signal numérique à la voie.

Cette opération est appelée **modulation**.

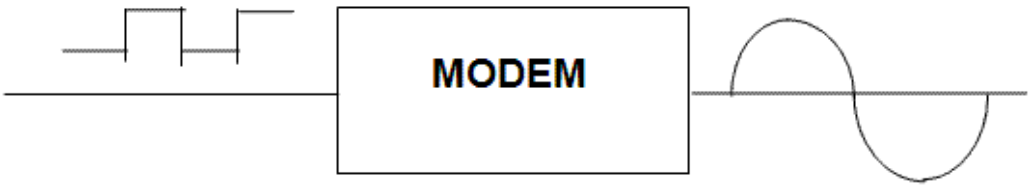


Image 102 transmission analogique d'informations numériques

La modulation consiste à modifier un ou plusieurs paramètres de la porteuse, tels que la phase, l'amplitude ou la fréquence.

Les opérations de modulation en émission et de démodulation en réception sont réalisées par l'ETCD couramment appelé **MODEM** (Modulateur DEModulateur).

La transmission numérique d'informations analogiques

La transmission numérique d'un signal analogique se fait selon la technique de Modulation par Impulsion Codée (MIC).

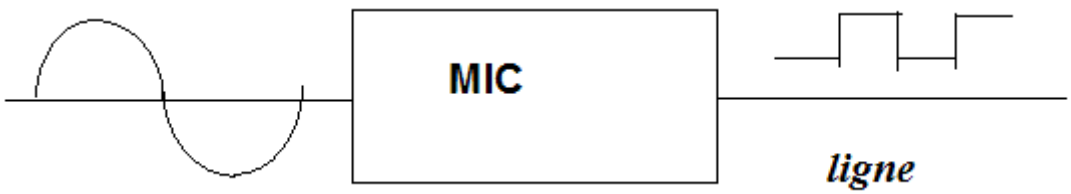


Image 103 Transmission numérique d'informations analogiques

La transmission numérique d'informations numériques

Les signaux sont transmis directement.

Cette transmission est dite **transmission en bande de base** et réalisée par un

codeur bande de base.

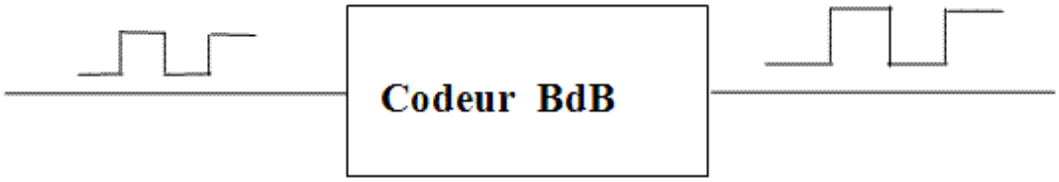


Image 104 transmission numérique d'informations numériques

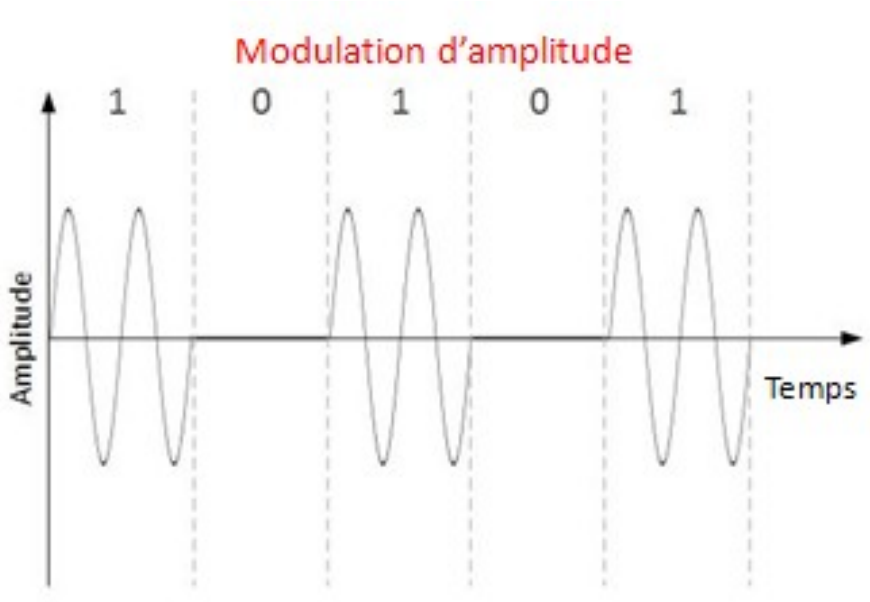
2. Techniques de modulation

Modulation d'amplitude

Consiste à modifier l'amplitude du signal porteur, en relation avec les informations numériques a transmettre, selon diverses techniques.

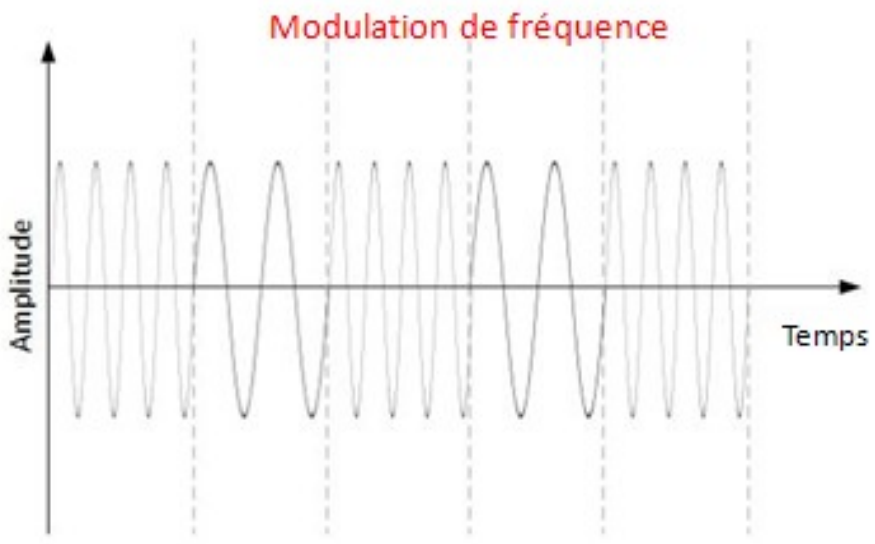
Par exemple :

- une amplitude de valeur a est attribuée à 0
- une amplitude de valeur A est attribuée à 1



Modulation de fréquence

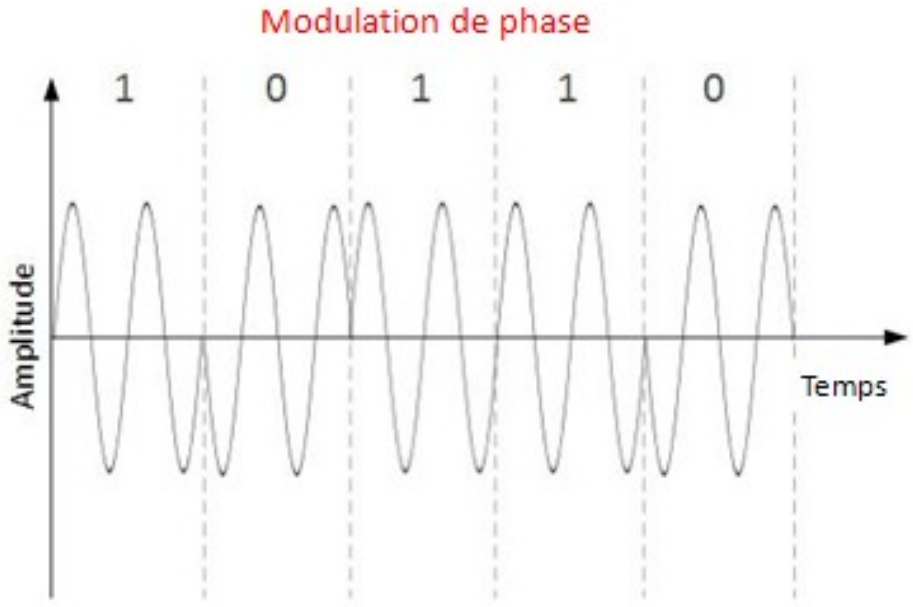
Elle utilise le même principe mais cette fois cela consiste à utiliser deux fréquences différentes : une pour transmettre 0 et une autre pour transmettre 1.



Modulation de phase

Elle consiste à faire varier la phase de la porteuse.

En utilisant des codes binaires de 2,3 bits ou plus, on peut augmenter la vitesse de transmission sans augmenter la fréquence de modulation.



Modulation de phase et d'amplitude

Pour obtenir des vitesses de transmission encore plus élevées, il est nécessaire d'augmenter le nombre d'états de phase.

Exemple

La modulation de phase mise en œuvre dans le modem V29 est une modulation de phase et d'amplitude

3. Transmission en bande de base

Permet la transmission directe des signaux numériques sur les supports.

Elle utilise un codeur **bande de base**.

La transmission en bande de base est utilisée sur des distances limitées (de l'ordre de 30km).

Le codeur bande de base transforme une suite de bits a_i en une suite de symbole en une suite de symboles d_k .

IL existe plusieurs techniques de codage en bande de base.

Codage NRZ (Non Retour a Zero)

- Si a_i=0 alors le signal vaut -a
- Si a_i=1 alors le signal vaut +a

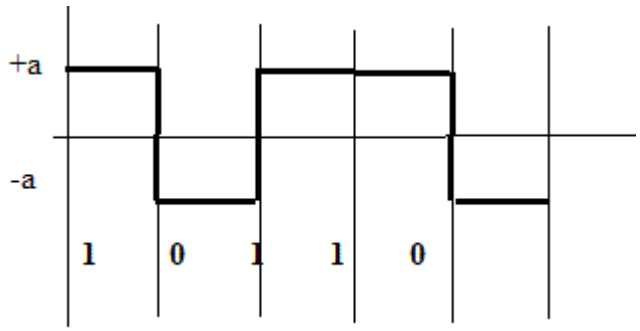


Image 105 Codage NRZ

Codage Manchester

- Si a_i=0 alors transition du signal au milieu de l'intervalle en front montant
- Si a_i=1 alors transition du signal au milieu de l'intervalle en front descendant

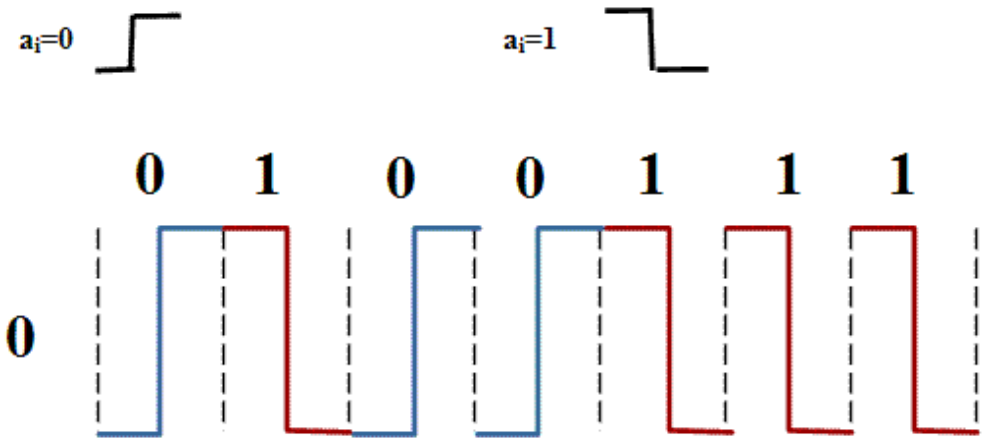


Image 106 Codage Manchester

4. Numérisation d'un signal

La numérisation d'un signal se fait en trois étapes :

1. Echantillonnage
2. Quantification
3. Codage.

La technique de base est le MIC : Modulation par Impulsion et Codage.

Echantillonnage

L'échantillonnage consiste a transformer une fonction x(t) continue en une fonction x'(t) discrète, constituée par la suite des valeurs x(t) aux instants d'échantillonnage.

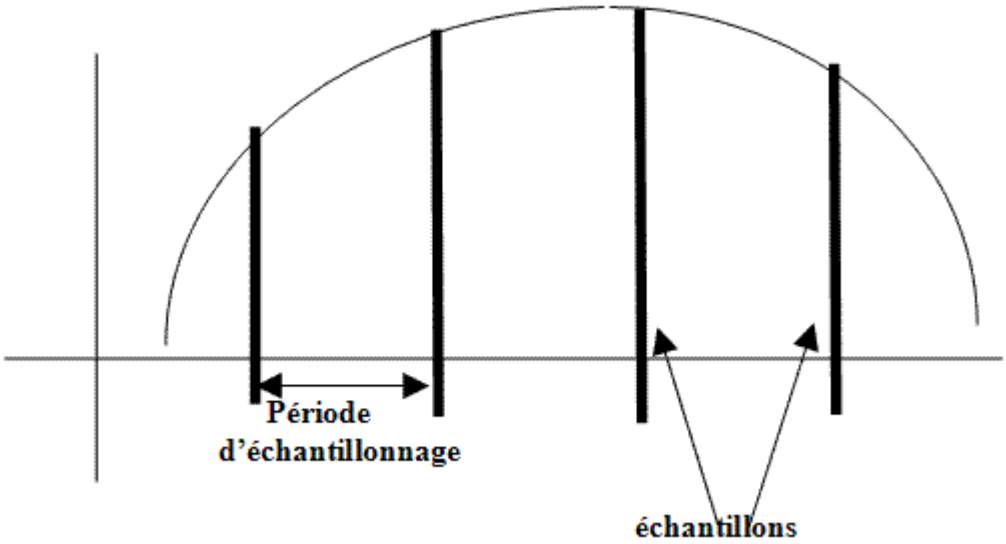


Image 107 Echantillonage

La période d'échantillonnage ne peut pas être quelconque.

Il faut prélever suffisamment d'échantillons pour ne pas perdre d'informations contenue dans le signal.

La fréquence d'échantillonnage est donnée par le théorème de Shanon suivant :

- Si fmax est la fréquence la plus élevée d'un signal, alors la fréquence d'échantillonnage fe doit être supérieure ou égale a 2fmax.

Le codec prélève 8000 échantillons par seconde de l'information analogique, soit 125 micro-sec.

Cette cadence est suffisante pour échantillonner un signal de fréquence comprise entre 0 et 4000 Hz.

L'IUT (ex-CCITT) propose une structure de trame pour un canal MIC a 2048 Kbits/s.

La durée de la trame est de 125 micro-sec.

Elle regroupe 32 voies téléphoniques (30 voies transportent l'information utile, 2 pour transporter la signalisation).

Les échantillons multiplexés dans le temps sont codés sur 8 bits.

Quantification

Consiste à reporter chaque échantillon à une échelle.

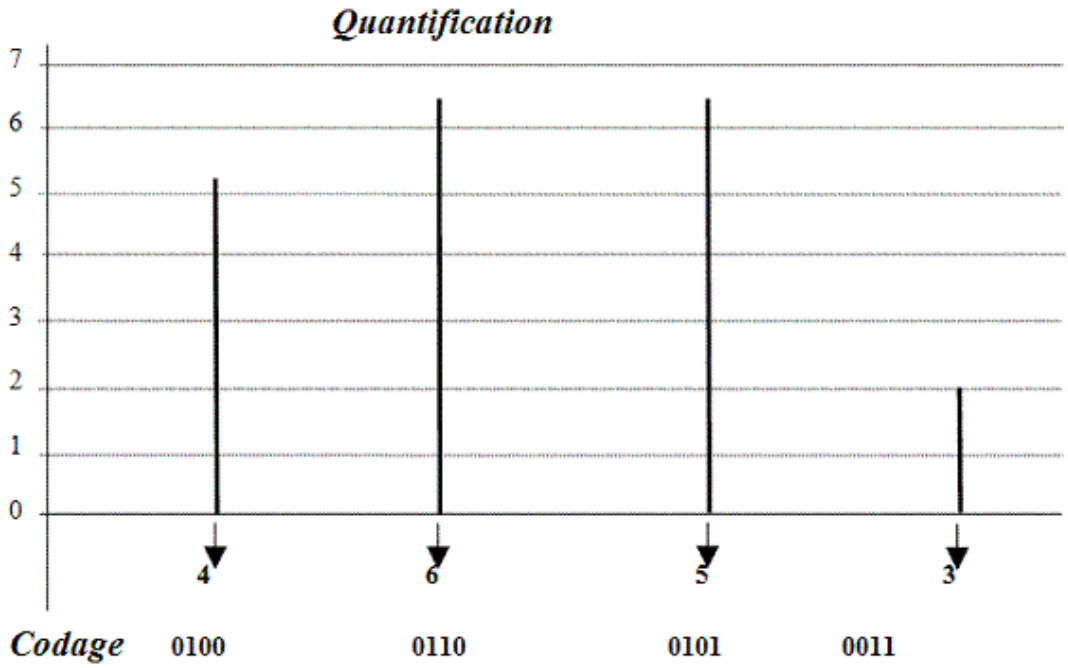


Image 108 Quantification

G. Multiplexage

1. Présentation

Lorsque plusieurs liaisons sont nécessaires entre deux sites, il est plus économique d'utiliser une seule ligne partagée sur laquelle seront transmis les messages des différents équipements plutôt que de réaliser autant de liaisons point à point.

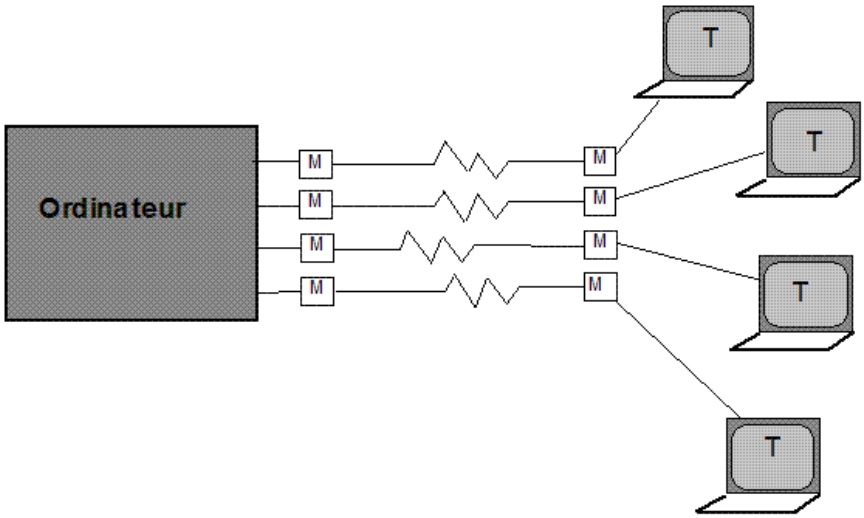


Image 109 Multiplexage

Le partage d'une seule ligne est mis en œuvre par un multiplexeur.

Les multiplexeurs ont pour rôle de regrouper sur un circuit de données unique appelé **circuit composite** (**voie haute vitesse**), les informations provenant de

plusieurs circuits de données (**voies basse vitesse**).

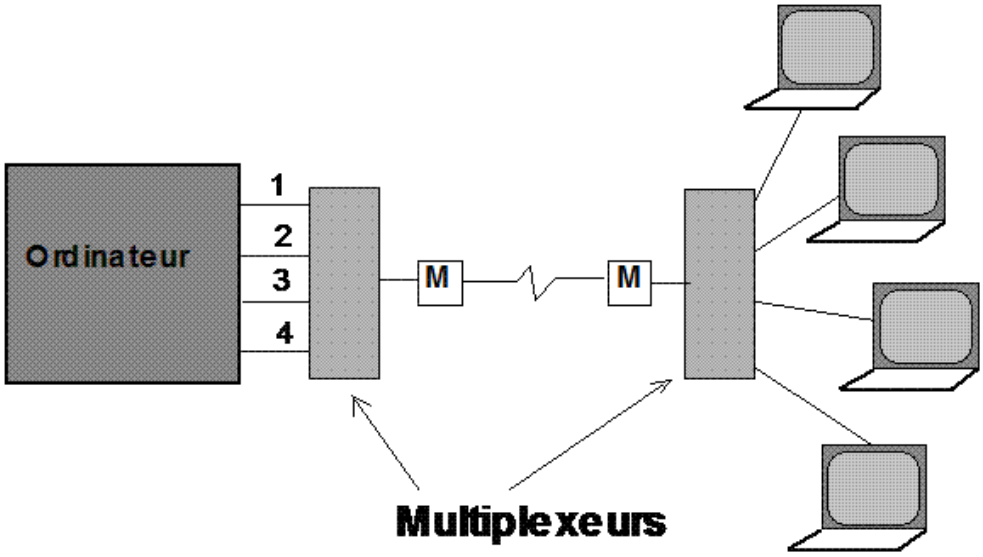


Image 110 Les multiplexeurs

2. Multiplexage fréquenciel

Le multiplexage de fréquences nommé AMRF (Accès Multiple à Répartition de Fréquence) consiste à diviser la bande passante de la voie composite en sous-bandes ou canaux.

Chaque voie basse vitesse correspond alors à un canal.

Ce type de multiplexage est généralement utilisé pour la transmission de signaux analogiques.

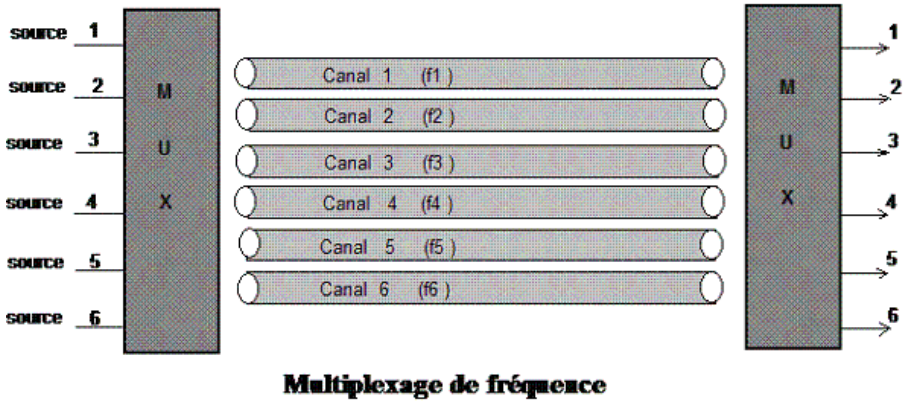
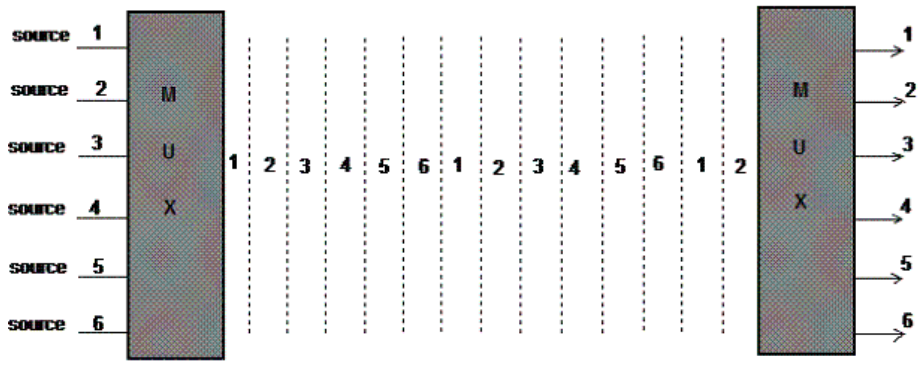


Image 111 Multiplexage de fréquence

3. Multiplexage temporel

Le multiplexage temporel (Time Division Multiple Access) consiste à associer des intervalles de temps d'utilisation de la voie composite à chacune des voies basses vitesse et à un rythme régulier.

L'affectation des intervalles de temps aux voies basse vitesse est fixe et le démultiplexage s'effectue selon le même rythme.



Multiplexage temporel

Image 112 Multiplexage temporel

4. Multiplexage statistique

Si chaque source a un taux d'activité très faible, le multiplexeur temporel utilise très mal la capacité de transmission sur la voie composite.

Les multiplexeurs statistiques allouent la voie composite à une source seulement lorsqu'elle a besoin de transmettre.

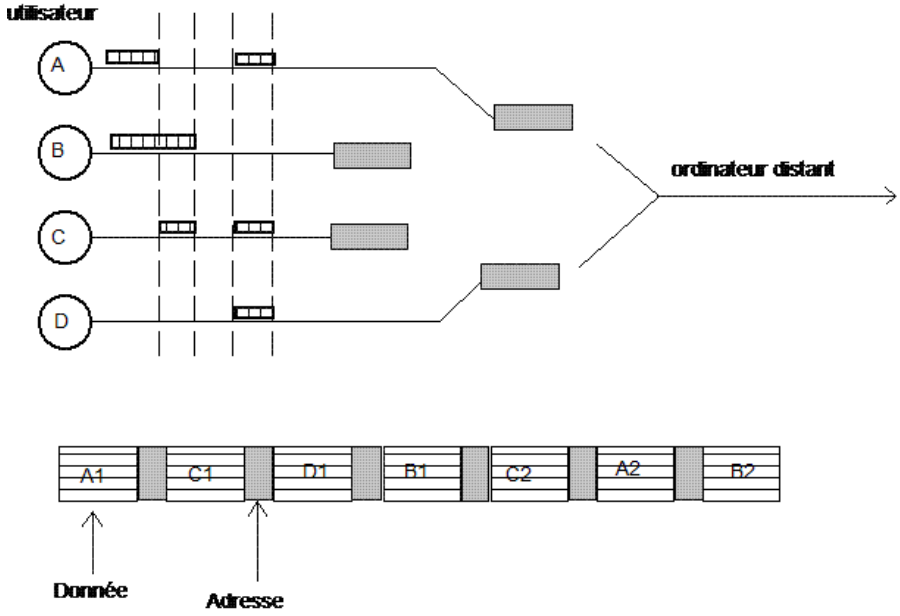


Image 113 Multiplexage statique

Technologies Backbone

V

A. Interconnexion de réseaux locaux d'entreprises

1. Présentation

Une chaîne d'interconnexion de réseaux locaux d'entreprises comprend tous les éléments réseaux locaux des deux sites d'extrémité, équipements d'interconnexion, et réseaux intermédiaires (réseaux WAN).

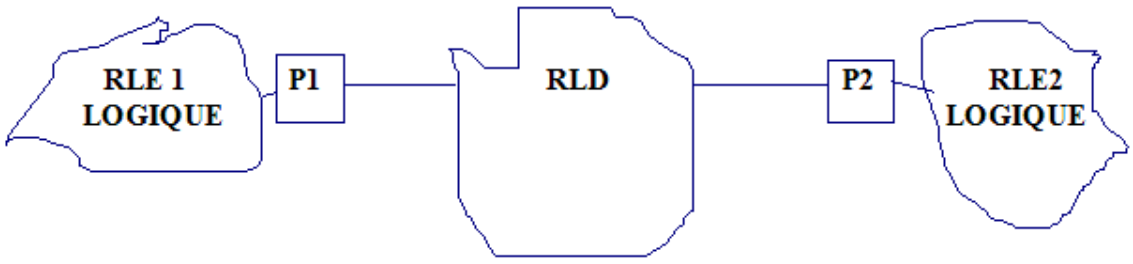


Image 114 Interconnexion

Niveaux des passerelles

Les passerelles P1 et P2 peuvent être de :

- Niveau 2 (Ponts) :
  - Création d'un véritable réseau local logique (RLE, RLD, RLE)
  - Supporter la diffusion comme dans un LAN pose problème :
    - Si les débits du RLD sont faibles
    - La possibilité offerte dans certaine passerelles de niveau 2 de supprimer le passage de trames en diffusion perturbe le fonctionnement d'un grand nombre de protocoles comme ARP, RIP,...
- Niveau 3 :
  - Le cas le plus fréquent

- Niveau 4 ou plus :
  - Performances réduites

B. Caracteristiques d'une chaine IRLE

1. Présentation

Les caractéristiques d'une chaine d'interconnexion sont :

1. Le temps de traversée (T)
2. Le débit de la chaîne
3. La transparence
4. La stabilité du temps de traversée
5. Les attributs sécurité / administrabilité

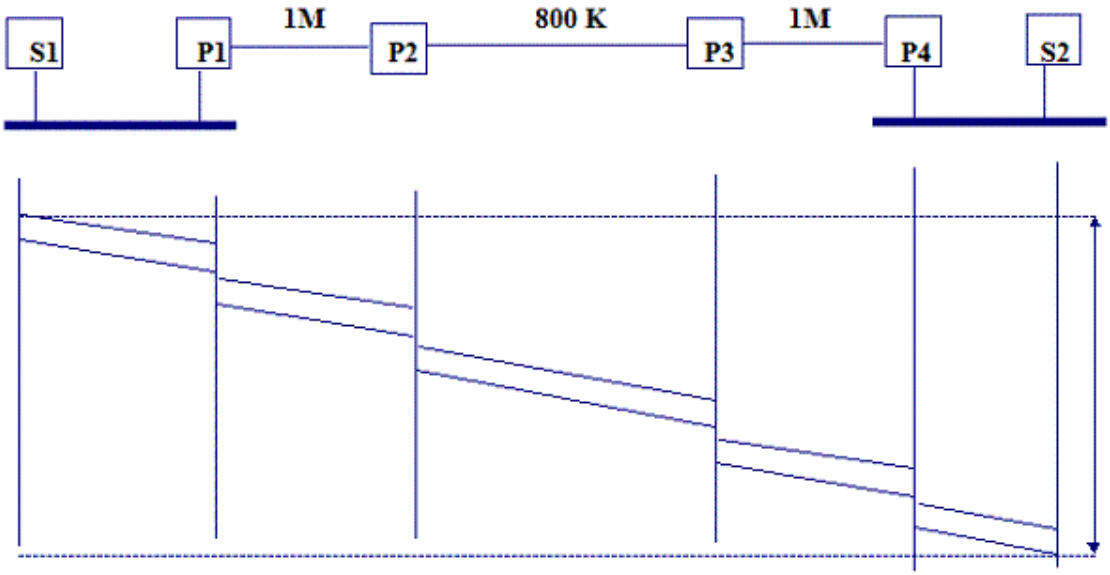


Image 115 chaine IRLE

C. Caractéristiques des flux

Un réseau intersites est généralement amené à véhiculer des données issues de différentes applications générant plusieurs types de flux.

Les échanges de données résultants qui transitent à travers un réseau d'interconnexion peuvent être caractérisé par plusieurs attributs.

1. Attributs des flux

- Granularité des flux : taille moyenne des unités de données échangées
  - Granularité faible : caractère
  - Granularité moyenne : flux SQL coopératifs
  - Granularité forte : transfert de fichiers
- Mode de dialogue : flux interactifs, monodirectionnel

- Fréquence d'émission de données :
  - Fréquence moyenne : quelques échanges/minute
  - Fréquence faible ou forte
  - Fréquence illimitée : à saturation (transfert de fichiers)

2. Modèle de flux

	granularité	dialogue	fréquence
Modèle sporadique	moyenne	monodirectionnel	faible
Modèle à saturation	forte ou très forte	monodirectionnel	illimitée
Client/serveur	moyenne ou forte	interactif	faible
distribution transparente	moyenne	interactif	assez élevée
Modèle interactif	faible ou moyenne	interactif	moyenne.

Image 116 Modèle de flux

- Modèle distribution transparente
  - Désigne l'ensemble des techniques de déport d'interface programmatiques au travers de mécanismes de type RPC

3. Adéquation des flux aux chaînes IRLE

besoins en / Flux	*temps de traversée*	*débit(Te)*
sporadique (mail)	*insensible*	insensible
mail + attachement	*insensible*	insensible
saturation (transfert de fichiers)	*insensible*	sensible
interactif (mode bloc) SNA, DSA,...	*très sensible*	19
interactif (caractère) (*telnet*) UNIX	*très sensible*	64 K
Client/serveur traitement	*sensible (100ms)*	≥64K
Client/serveur données (mode rafales)	*sensible (10ms)*	≥128K, 512K, 1M
Voix	*assez sensible*	64K (QS)
Télé	*Assez sensible*	155Mbits (QS)
Télé numérique	*Assez sensible*	1- 2Gigabits/s (QS)
distribution transparente	*sensible*	2M

Image 117 Relations entre type de flux et besoins

D. Empilements protocolaires sur RLE et IRLE

1. RLE et IRLE, mode connecté et non connecté

- Mode connecté : établissement et maintient d'un contexte de conversation
  - Protocoles assez lourds
  - Moins performants
  - Complexes à implémenter
  - Garantissent le séquencement des données
- Mode non connecté :
  - Protocoles légers
  - Performants
  - Aisés à implémenter
  - Incapables de garantir le séquencement des données

Dans les offres actuelles, il n'existe pas de protocole de niveau 3 en mode connecté qui gère lui même le reséquencement ou la récupération de perte.

Deux écoles

- A.1
  - Niveau 4 : mode connecté
  - Niveau 3 : mode non connecté
  - Niveau 2 : mode non connecté
- A.2
  - Niveau 4 : mode non connecté
  - Niveau 3 : mode connecté
  - Niveau 2 : mode connecté
- On ne verra pas la différence entre les architectures A1 et A2 lorsque ces deux architectures relient deux machines voisines.
- B.1
  - Reprendre A1 avec des routeurs intermédiaires : on commute 30000 à 100000 paquets/sec
- B.2
  - Reprendre A2 avec des nœuds intermédiaires : on commute 400 à 1000 paquets/sec
- Il y a différence entre B1 et B2
  - Passer de B1 à B2 permet de faire du client/serveur plus facilement
  - Avant de passer à tout IP,
  - Pour les station d'extrémité il n'y a pas de différence, par contre la différence de charge pour les passerelles de niveau 3 entre le mode connecté et le mode non connecté sont de l'ordre de 1 à 10.
- L'évolution est de réduire les charges des réseaux d'interconnexion.
  - Utilisation des IRLE de niveau 3 en mode non connecté