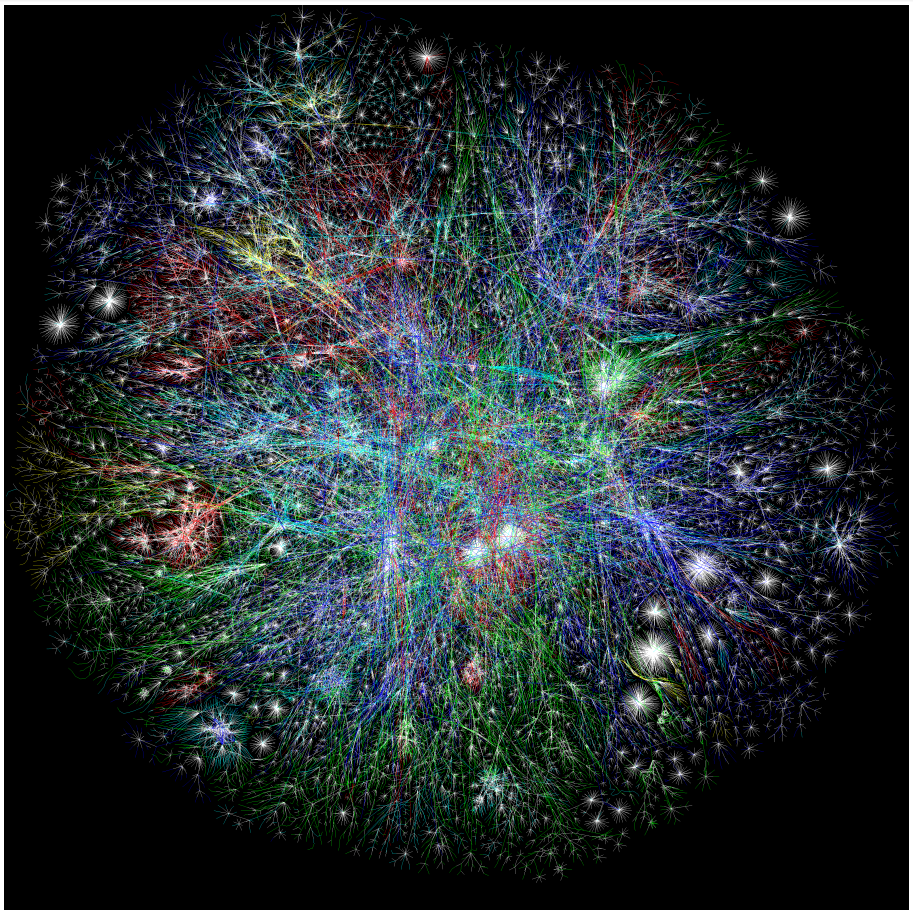
RES3
Introduction aux réseaux



UNIVERSITÉ DE LORRAINE | IUT Saint-Dié-des-Vosges
Génie Electrique et Informatique Industrielle

Eric TERNISIEN
IUT de Saint Dié des Vosges
Département Génie Electrique et informatique Industrielle

I - Introduction

1 - Définitions d'un réseau
2 - Quelles informations ?
3 - Performances d'un réseau
4 - Internet : origine et évolution
5 - Services disponibles sur Internet

Plan

I - Introduction

1 - Définitions d'un réseau
2 - Quelles informations ?
3 - Performances d'un réseau
4 - Internet : origine et évolution
5 - Services disponibles sur Internet

II - Structure des réseaux

1 - Topologies des réseaux
2 - Découpage géographique des réseaux
3 - Equipements d'interconnexion
4 - Le modèle OSI

Plan

I - Introduction

1 - Définitions d'un réseau
2 - Quelles informations ?
3 - Performances d'un réseau
4 - Internet : origine et évolution
5 - Services disponibles sur Internet

II - Structure des réseaux

1 - Topologies des réseaux
2 - Découpage géographique des réseaux
3 - Equipements d'interconnexion
4 - Le modèle OSI

III - Communication réseau

1 - Types de connexion
2 - Types de communication

IV - Ethernet

1 - Généralités
2 - La communication

Plan

IV - Ethernet

1 - Généralités

2 - La communication

V - TCP/IP

1 - Généralités

2 - Le Protocole TCP

3 - Le Protocole UDP

4 - Le protocole IP

5 - Le routage

6 - Les sous réseaux

Plan

IV - Ethernet

1 - Généralités

2 - La communication

V - TCP/IP

1 - Généralités

2 - Le Protocole TCP

3 - Le Protocole UDP

4 - Le protocole IP

5 - Le routage

6 - Les sous réseaux

VI - Wi-Fi

1 - Généralités

2 - Les normes 802.11x

3 - Structure des réseaux Wi-Fi

4 - Transmission en Wi-Fi

5 - Sécurité et Wi-Fi

Plan

I - Introduction

1 - Définitions d'un réseau

2 - Quelles informations ?

3 - Performances d'un réseau

4 - Internet : origine et évolution

5 - Services disponibles sur Internet

Au sens général

Un réseau est un ensemble de nœuds (ou pôles) reliés entre eux par des liens (canaux).

Au sens général

Un réseau est un ensemble de nœuds (ou pôles) reliés entre eux par des liens (canaux).

Au sens informatique

Un réseau est un ensemble d'équipements reliés entre eux pour échanger des informations, des résultats de traitement ou des ressources. Les ressources peuvent être matérielles ou logicielles.

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

Le réseau le plus connu est **Internet**.

Plan

I - Introduction

1 - Définitions d'un réseau

2 - Quelles informations ?

3 - Performances d'un réseau

4 - Internet : origine et évolution

5 - Services disponibles sur Internet

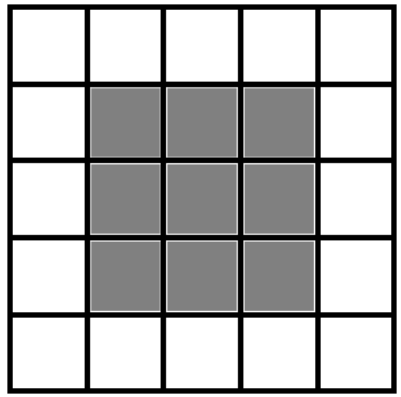
On veut envoyer l'image suivante d'une machine à une autre. On connaît la taille de l'image et l'ordre d'envoi des éléments (ex : carré par carré, ligne par ligne, en commençant en haut à gauche, pour finir en bas à droite).

Il est alors impossible d'envoyer l'image telle quelle sans la coder. La séquence de couleurs à envoyer est donc (en notant blanc B et noir N) :

BBBBB BNNNB BNNNB BNNNB BBBBB

Une manière de coder la couleur de chaque carré consiste à associer une valeur à chaque couleur possible, par exemple 1 à B (le pixel sur l'écran est allumé) et 0 à N (le pixel est éteint). La suite de chiffres codant l'image est alors :

11111 10001 10001 10001 11111



Représentation des données

Les données informatiques sont représentées par des nombres binaires (base 2).

L'utilisation de la base 2 garantit de pouvoir représenter un état stable d'un système physique, par exemple :

- circuit électrique ouvert/fermé.
- carte perforée avec un trou/sans trou.
- ...

Par conséquent, sur un système informatique, les données sont représentées par une suite de 0 et de 1 correspondant à des états différents sur le support physique. Ces états peuvent être des tensions différentes (en fonction du codage utilisé).

Plan

I - Introduction

1 - Définitions d'un réseau

2 - Quelles informations ?

3 - Performances d'un réseau

4 - Internet : origine et évolution

5 - Services disponibles sur Internet

Le débit

Définition

Le débit d'un réseau mesure la quantité d'informations que le réseau peut transmettre par unité de temps :

$$\text{débit} = \frac{\text{quantité d'information}}{\text{temps}}$$

L'unité est par conséquent le bit par seconde, noté b/s ou $b.s^{-1}$. Les réseaux actuels ayant un débit assez élevé, on utilise plus souvent des méga-bits par secondes, notés Mb/s ou $Mb.s^{-1}$.

Débit nominal

C'est la quantité théorique maximale d'informations pouvant être transmise par unité de temps.

Le débit

Débit utile

C'est la quantité d'informations effectivement transmise par unité de temps.

Taux d'utilisation

C'est le rapport du débit utile au débit nominal :

$$\text{taux d'utilisation} = \frac{\text{débit utile}}{\text{débit nominal}} \times 100$$

Le taux d'utilisation est inférieur à 100%. Ceci est dû entre autres aux pertes sur la voie de communication et à l'intervalle de temps laissé entre l'envoi de deux messages.

Les délais

Le délai total d'acheminement d'un message se compose de deux parties :

Le délai de transmission

C'est le temps mis pour transmettre la quantité d'informations du message, c'est-à-dire :

$$\text{délai}_{\text{transmission}} = \frac{\text{quantité information}}{\text{débit}}$$

Le délai de propagation

C'est le temps mis pour que le signal se propage sur le matériel. Les équipements traversés peuvent introduire des retards.

$$\text{délai}_{\text{propagation}} = \frac{\text{distance parcourue}}{\text{vitesse}} + \text{retards}$$

Les délais

Délai total

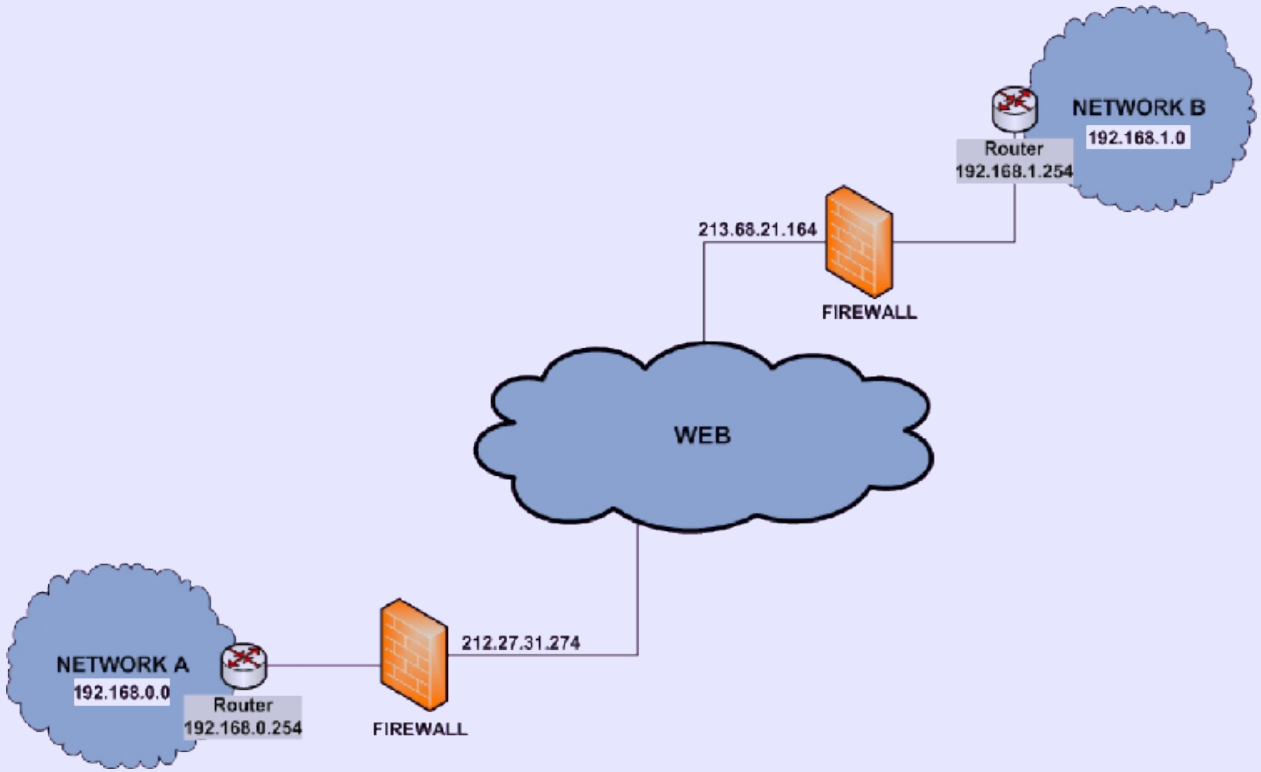
$$\text{délai}_{\text{total}} = \text{délai}_{\text{transmission}} + \text{délai}_{\text{propagation}}$$

Plan

I - Introduction

1 - Définitions d'un réseau
2 - Quelles informations ?
3 - Performances d'un réseau
4 - Internet : origine et évolution
5 - Services disponibles sur Internet

Internet : **Inter**connected **Net**works. C'est un réseau virtuel construit en interconnectant des réseaux physiques par des passerelles (les routeurs).



1962 :

- La DARPA (Defense Advanced Research Project Agency) lance un projet de réseau capable de supporter les conséquences d'un conflit nucléaire.
- Projet basé sur une transmission par paquet et sur un réseau non centralisé.

1962 :

- La DARPA (Defense Advanced Research Project Agency) lance un projet de réseau capable de supporter les conséquences d'un conflit nucléaire.
- Projet basé sur une transmission par paquet et sur un réseau non centralisé.

1968 :

Naissance d'ARPANET qui relie la DARPA avec 4 universités (nœuds) :

- Université de Californie (UCLA) ;
- Stanford Research Institute ;
- Université de Santa Barbara ;
- Université de l'Utah.

1962 :

- La DARPA (Defense Advanced Research Project Agency) lance un projet de réseau capable de supporter les conséquences d'un conflit nucléaire.
- Projet basé sur une transmission par paquet et sur un réseau non centralisé.

1968 :

Naissance d'ARPANET qui relie la DARPA avec 4 universités (nœuds) :

- Université de Californie (UCLA) ;
- Stanford Research Institute ;
- Université de Santa Barbara ;
- Université de l'Utah.

1972 :

Première application de courrier électronique.

1980 :

Séparation d'ARPANET en deux réseaux : un militaire (MILNet) et un universitaire (NFSNet : Network Science Foundation Network).

1980 :

Séparation d'ARPANET en deux réseaux : un militaire (MILNet) et un universitaire (NFSNet : Network Science Foundation Network).

1983 :

ARPANET adopte le protocole TCP/IP, c'est la naissance d'Internet.

1980 :

Séparation d'ARPANET en deux réseaux : un militaire (MILNet) et un universitaire (NFSNet : Network Science Foundation Network).

1983 :

ARPANET adopte le protocole TCP/IP, c'est la naissance d'Internet.

de 1986 à 1990 : période universitaire

La NSF décide de déployer des super-calculateurs pour augmenter les débits (débits x 1000, nombres de réseaux connectés x 100).

1980 :

Séparation d'ARPANET en deux réseaux : un militaire (MILNet) et un universitaire (NFSNet : Network Science Foundation Network).

1983 :

ARPANET adopte le protocole TCP/IP, c'est la naissance d'Internet.

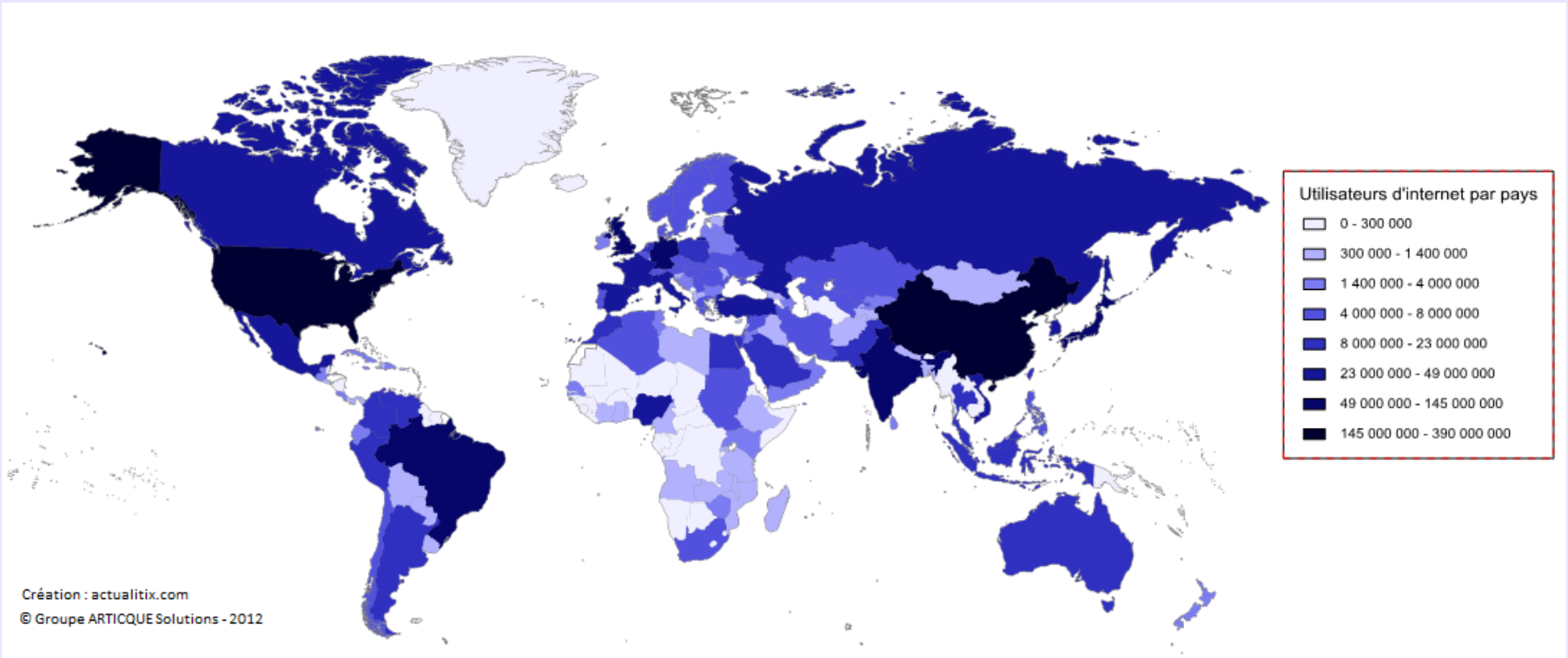
de 1986 à 1990 : période universitaire

La NSF décide de déployer des super-calculateurs pour augmenter les débits (débits x 1000, nombres de réseaux connectés x 100).

à partir de 1990 : période commerciale

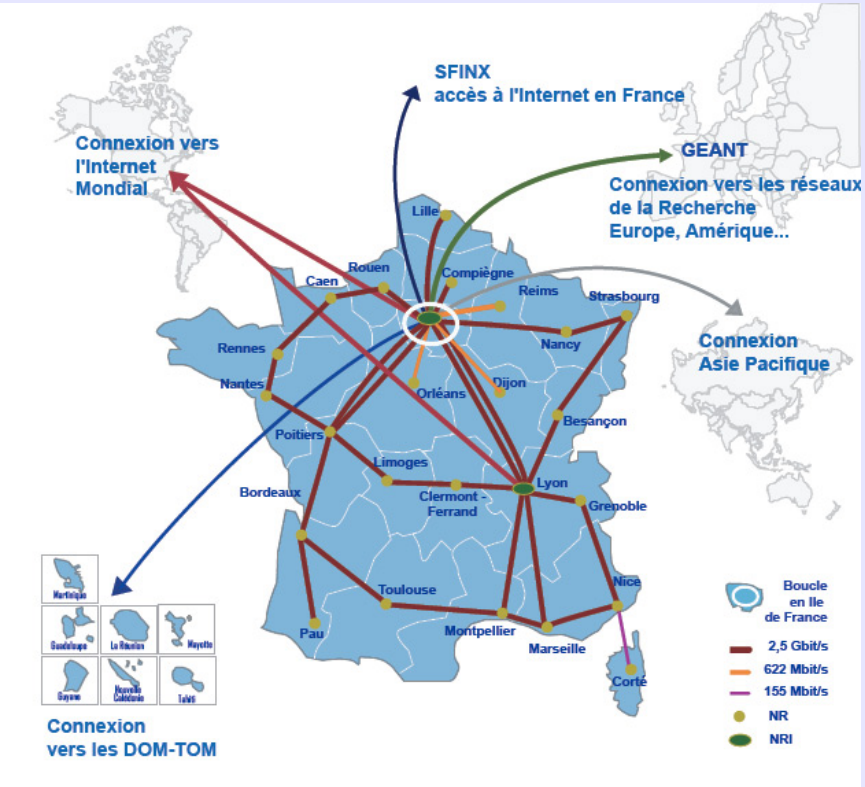
- 1993 : première interface conviviale de navigation : Mosaïc.
- 1995 : explosion du réseau : augmentation exponentielle des connexions et apparition du contenu multimédia.

2012 :


Utilisateurs d'internet par pays
0 - 300 000
300 000 - 1 400 000
1 400 000 - 4 000 000
4 000 000 - 8 000 000
8 000 000 - 23 000 000
23 000 000 - 49 000 000
49 000 000 - 145 000 000
145 000 000 - 390 000 000
Création : actualitix.com
© Groupe ARTICQUE Solutions - 2012

Et en France ?

- 1982 : naissance de EUNet.
- 1988 : connexion de la France à Internet.
- 1992 : naissance du réseau RENATER (**RE**seau **NA**tional pour la **T**echnologie, l'**E**nseignement et la **R**echerche).



Instances régissant Internet

Question : Internet n'est géré par personne ?

Instances régissant Internet

Question : Internet n'est géré par personne ?

⇒ VRAI et FAUX

Instances régissant Internet

Question : Internet n'est géré par personne ?

⇒ VRAI et FAUX

- Pas de responsable du réseau Internet.

Instances régissant Internet

Question : Internet n'est géré par personne ?
⇒ VRAI et FAUX

- Pas de responsable du réseau Internet.
- Internet n'existe pas en tant que tel. Il n'existe que des réseaux publics ou privés reliés entre eux :
  - ✓ Réseau local (LAN).
  - ✓ Réseau d'un campus universitaire.
  - ✓ Réseau régional.
  - ✓ Réseau national des opérateurs (ex : France Telecom).
  - ✓ Réseau national d'opérateurs particuliers (ex : RENATER).
  - ✓ Réseau international (ex : liaison transatlantique).

Internet n'appartient à personne

$\Rightarrow$ Organismes de régulation/normalisation.

Internet n'appartient à personne

⇒ Organismes de régulation/normalisation.

- IAB : **I**nternet **A**ctivities **B**oard :
  - ✓ Responsable par rapport à l'architecture TCP/IP.
  - ✓ Responsable "Request for Comments" (RFC).
  - ✓ Tests et validations des propositions de nouveaux protocoles.
- ICANN : **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers :
  - ✓ Gestion des noms de domaines : DNSO (**D**omain **N**ame **S**upporting **O**rganisation).
  - ✓ Gestion des adresses IP : ASO (**A**ddress **S**upporting **O**rganization).
  - ✓ Gestion des protocoles : PSO (**P**rotocol **S**upporting **O**rganization).

Internet n'appartient à personne

⇒ Organismes de régulation/normalisation.

- IAB : **I**nternet **A**ctivities **B**oard :
  - ✓ Responsable par rapport à l'architecture TCP/IP.
  - ✓ Responsable "Request for Comments" (RFC).
  - ✓ Tests et validations des propositions de nouveaux protocoles.
- ICANN : **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers :
  - ✓ Gestion des noms de domaines : DNSO (**D**omain **N**ame **S**upporting **O**rganisation).
  - ✓ Gestion des adresses IP : ASO (**A**ddress **S**upporting **O**rganization).
  - ✓ Gestion des protocoles : PSO (**P**rotocol **S**upporting **O**rganization).
- W3C : **W**orld **W**ide **W**eb **C**onsortium :
  - ✓ Ne concerne pas le réseau Internet mais le service Web uniquement.
  - ✓ Protocoles gérant l'échange de fichiers :
    - Couche Application.
    - Gestion des langages standardisés : langage HTML, XHTML, XML ...

Plan

I - Introduction

1 - Définitions d'un réseau
2 - Quelles informations ?
3 - Performances d'un réseau
4 - Internet : origine et évolution
5 - Services disponibles sur Internet

Services spécifiques

- Web :
  $\Rightarrow$ Publication de documents hypertextes au format HTML.

Services spécifiques

- Web.
- Transfert de fichiers :
  $\Rightarrow$ Connexion temporaire entre deux machines.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique :
  $\Rightarrow$ Échange asynchrone de messages entre deux ou plusieurs utilisateurs d'Internet.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News :
  $\Rightarrow$ Forums de discussions organisés en thématiques.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante :
  $\Rightarrow$ Prise de contrôle à distance d'une station de travail à condition d'avoir un compte.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante.
- Streaming :
  $\Rightarrow$ Radio sur internet, visioconférence.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante.
- Streaming.

Protocoles spécifiques

- HTTP : **H**yper **T**ex**T** **P**rotocol.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante.
- Streaming.

Protocoles spécifiques

- HTTP : **H**yper **T**ex**T** **P**rotocol.
- FTP : **F**ile **T**ransfert **P**rotocol.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante.
- Streaming.

Protocoles spécifiques

- HTTP : **H**yper **T**ex**T** **P**rotocol.
- FTP : **F**ile **T**ransfert **P**rotocol.
- SMTP : **S**imple **M**ail **T**ransfert **P**rotocol (POP, IMAP).

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante.
- Streaming.

Protocoles spécifiques

- HTTP : **H**yper **T**ex**T** **P**rotocol.
- FTP : **F**ile **T**ransfert **P**rotocol.
- SMTP : **S**imple **M**ail **T**ransfert **P**rotocol (POP, IMAP).
- NNTP : **N**etwork **N**ews **T**ransfert **P**rotocol.

Services spécifiques

- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante.
- Streaming.

Protocoles spécifiques

- HTTP : **H**yper **T**ex**T** **P**rotocol.
- FTP : **F**ile **T**ransfert **P**rotocol.
- SMTP : **S**imple **M**ail **T**ransfert **P**rotocol (POP, IMAP).
- NNTP : **N**etwork **N**ews **T**ransfert **P**rotocol.
- Telnet, SSH.

Services spécifiques

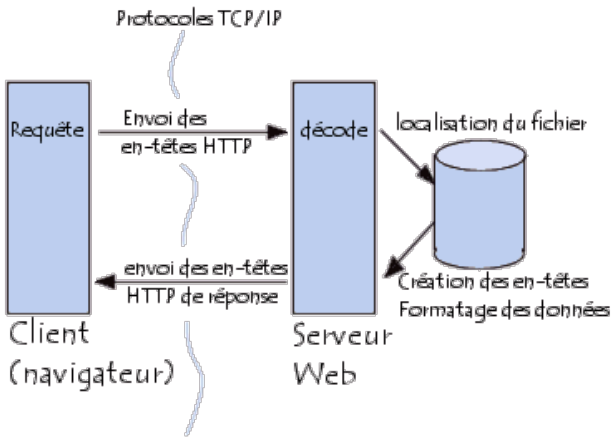
- Web.
- Transfert de fichiers.
- Courrier électronique.
- Usenet News.
- Session distante.
- Streaming.

Protocoles spécifiques

- HTTP : **H**yper **T**ex**T** **P**rotocol.
- FTP : **F**ile **T**ransfert **P**rotocol.
- SMTP : **S**imple **M**ail **T**ransfert **P**rotocol (POP, IMAP).
- NNTP : **N**etwork **N**ews **T**ransfert **P**rotocol.
- Telnet, SSH.
- RTP : **R**eal **T**ime **P**rotocol.

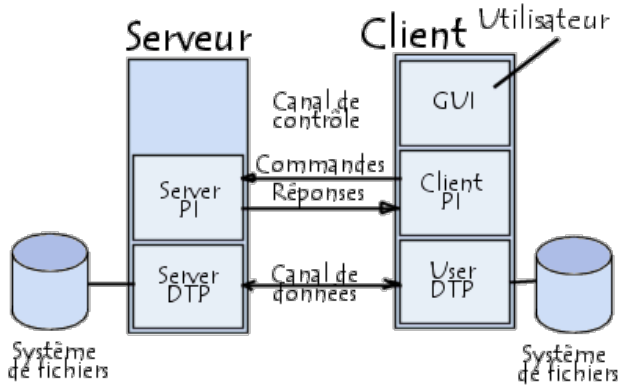
HTTP : le protocole du web

- Web : architecture client / serveur
  - ✓ clients = navigateurs (browsers) : Mozilla (Firefox), Microsoft IE, Google Chrome, Opera, Lynx, ...
- Fonctions principales d'un navigateur
  - ✓ communication via le protocole HTTP (port TCP 80).
  - ✓ mise en forme (affichage) des documents HTML.
  - ✓ interprétation code JavaScript
  - ✓ extensions (« plugins ») : Flash, ...
- Normalisation : `http://www.w3.org`.



FTP : le protocole pour transférer des fichiers

- Le protocole FTP a pour objectifs de :
  - ✓ permettre un partage de fichiers entre machines distantes.
  - ✓ permettre une indépendance aux systèmes de fichiers des machines clientes et serveur.
  - ✓ permettre de transférer des données de manière efficace.
- FTP s'inscrit dans un modèle client-serveur, c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur).
- Lors d'une connexion FTP, deux canaux de transmission sont ouverts :
  - ✓ Un canal pour les commandes (canal de contrôle).
  - ✓ Un canal pour les données.



- De nombreux logiciels permettent de gérer le protocole FTP (Ex : Filezilla).

URL : Uniform Ressource Locator

- Moyen universel de pointer un document où qu'il soit.

URL : Uniform Ressource Locator

- Moyen universel de pointer un document où qu'il soit.
- Formes :
  - ✓ La plus courante : `protocole://serveur/chemin/document`
  - ✓ Complète : `protocole://login:motdepasse@serveur:port/document`

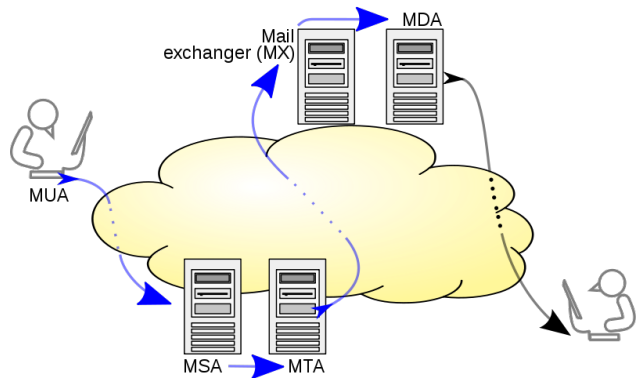
URL : Uniform Ressource Locator

- Moyen universel de pointer un document où qu'il soit.
- Formes :
  - ✓ La plus courante : `protocole://serveur/chemin/document`
  - ✓ Complète : `protocole://login:motdepasse@serveur:port/document`
- l'URL spécifie :
  - ✓ Le protocole lié au service (http, ftp, https...).
  - ✓ Le serveur utilisé (nom ou adresse IP).
  - ✓ Le port utilisé.
  - ✓ Le chemin d'accès au document.

SMTP : le protocole pour le courrier électronique

- SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique ⇒ courrier sortant.
- SMTP ne permet pas de récupérer des mails arrivés dans une boîte aux lettres sur un serveur. Les standards POP et IMAP ont été créés dans ce but.

- POP permet de récupérer les mails sur les serveurs de messagerie en les transférant sur le poste client.
- IMAP permet de récupérer les mails sur les serveurs de messagerie mais en les laissant sur le serveur.

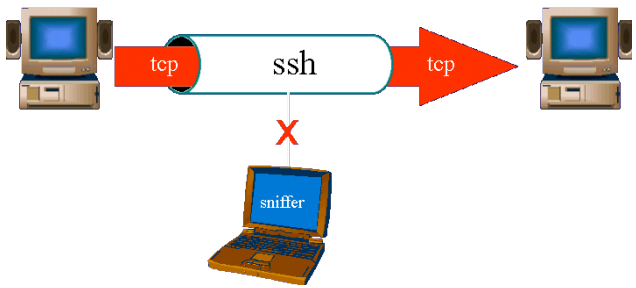


SSH : protocole sécurisé

- Protocole pour établir un canal de communication sûr entre deux machines distantes.
- Authentification, cryptage, intégrité des données

Le SSH offre les fonctionnalités suivantes :

- Connexion sécurisée à distance (client ssh).
- Exécution de commandes à distance.
- Tranfert de fichiers sécurisés.
- Gestion de clés cryptographiques.



Plan

II - Structure des réseaux

1 - Topologies des réseaux

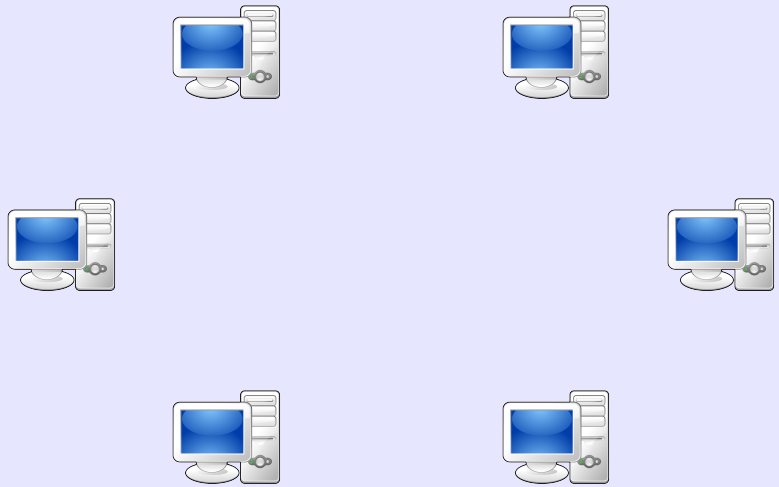
2 - Découpage géographique des réseaux

3 - Equipements d'interconnexion

4 - Le modèle OSI

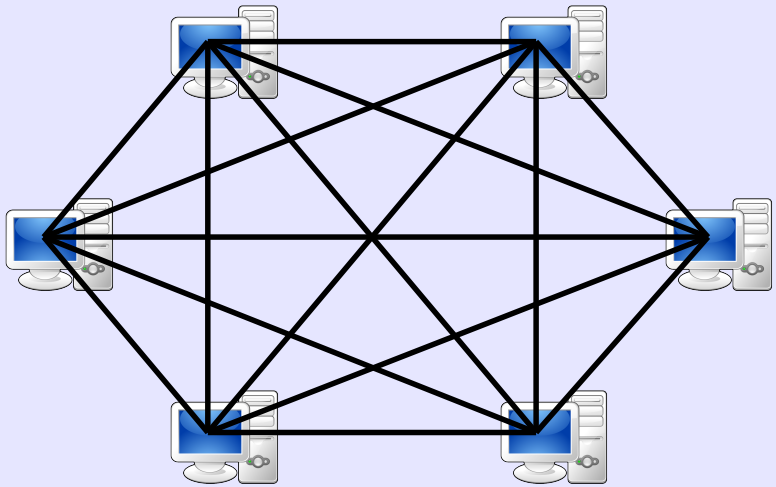
Topologie en maille

- Chaque machine est reliée à toutes les autres.
- Interconnexion totale.
- Pratiquement jamais mis en œuvre.



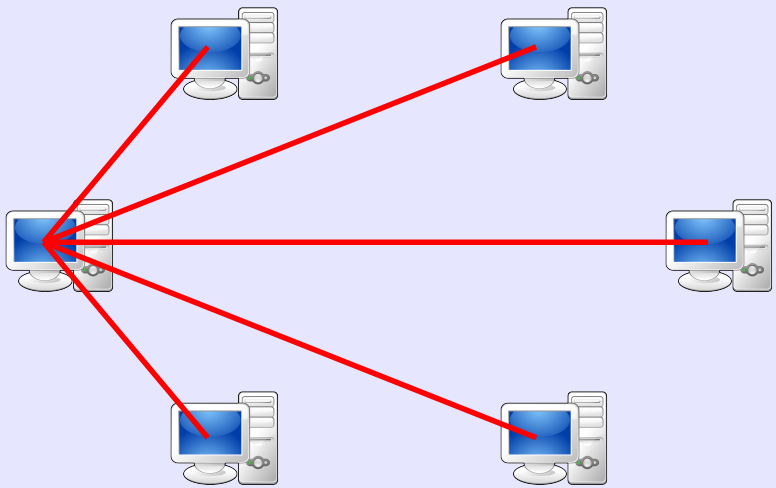
Topologie en maille

- Chaque machine est reliée à toutes les autres.
- Interconnexion totale.
- Pratiquement jamais mis en œuvre.



Topologie en maille

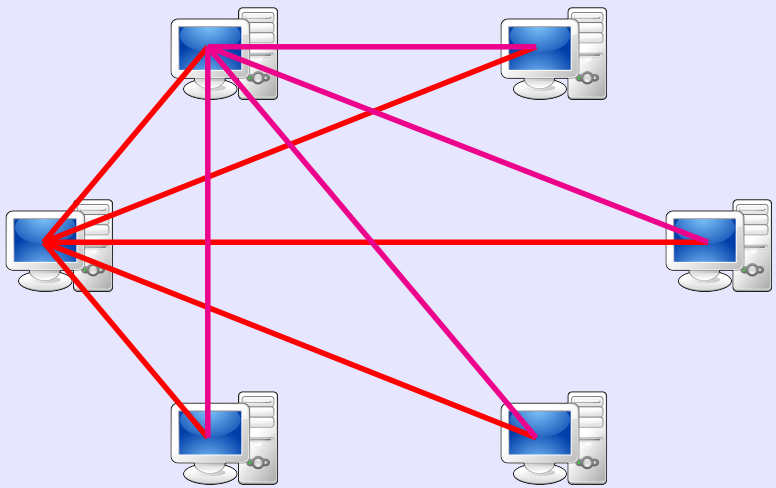
- Chaque machine est reliée à toutes les autres.
- Interconnexion totale.
- Pratiquement jamais mis en œuvre.



Inconvénient majeure :
Nombre de câbles : $\frac{n(n-1)}{2} = (n-1)$.

Topologie en maille

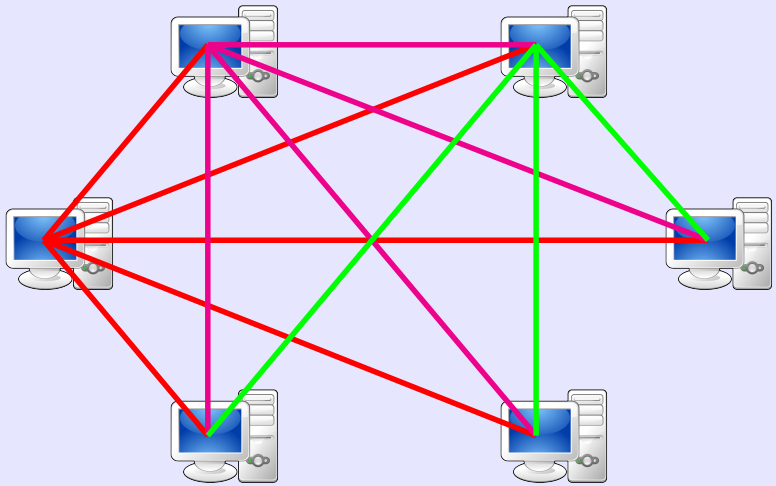
- Chaque machine est reliée à toutes les autres.
- Interconnexion totale.
- Pratiquement jamais mis en œuvre.



Inconvénient majeure :
Nombre de câbles : $\frac{n(n-1)}{2} = (n-1) + (n-2)$.

Topologie en maille

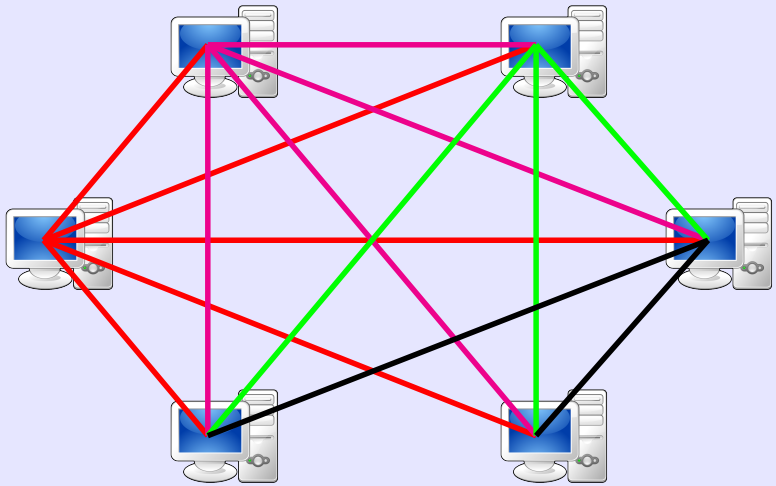
- Chaque machine est reliée à toutes les autres.
- Interconnexion totale.
- Pratiquement jamais mis en œuvre.



Inconvénient majeure :
Nombre de câbles : $\frac{n(n-1)}{2} = (n-1) + (n-2) + (n-3)$.

Topologie en maille

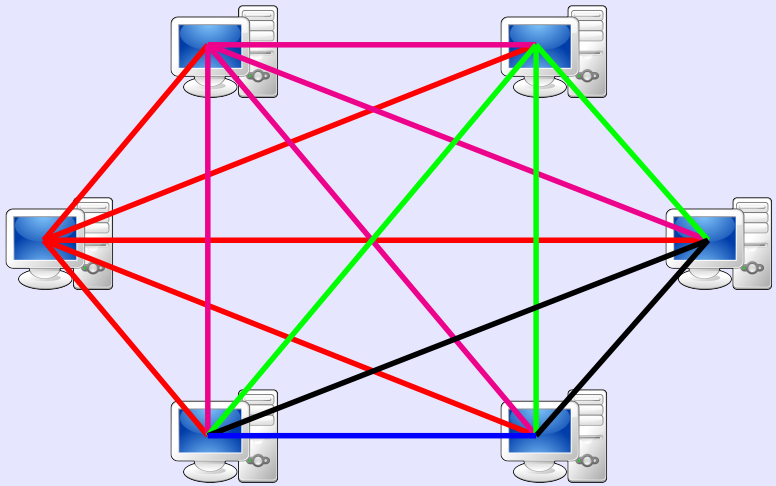
- Chaque machine est reliée à toutes les autres.
- Interconnexion totale.
- Pratiquement jamais mis en œuvre.



Inconvénient majeure :
Nombre de câbles : $\frac{n(n-1)}{2} = (n-1) + (n-2) + (n-3) + (n-4)$.

Topologie en maille

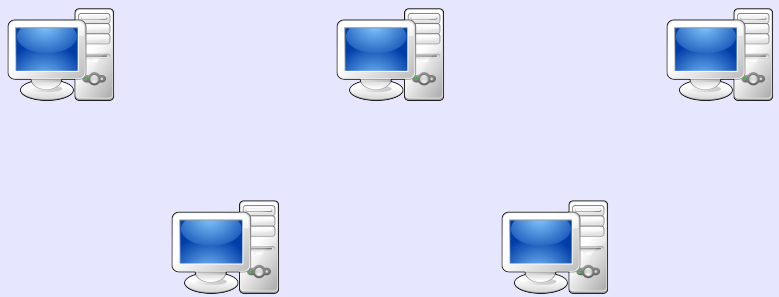
- Chaque machine est reliée à toutes les autres.
- Interconnexion totale.
- Pratiquement jamais mis en œuvre.



Inconvénient majeure :
Nombre de câbles : $\frac{n(n-1)}{2} = (n-1)+(n-2)+(n-3)+(n-4)+(n-5)$.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

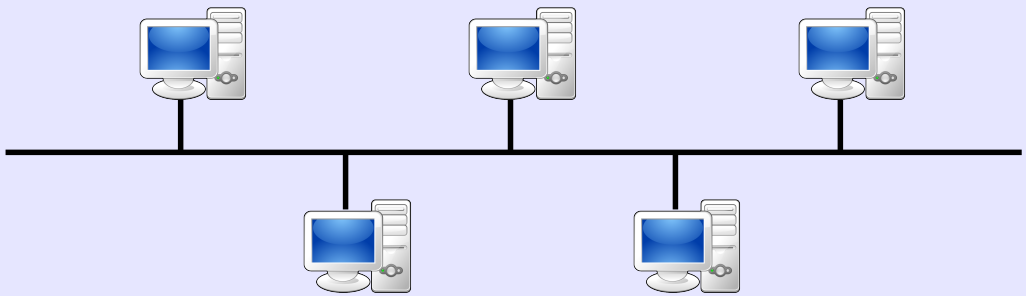
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

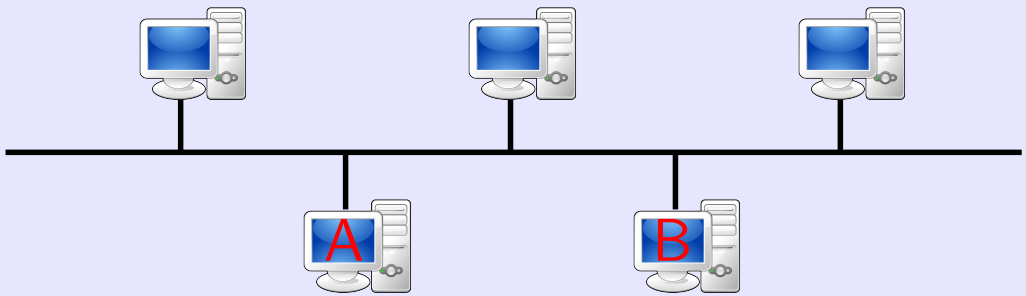
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

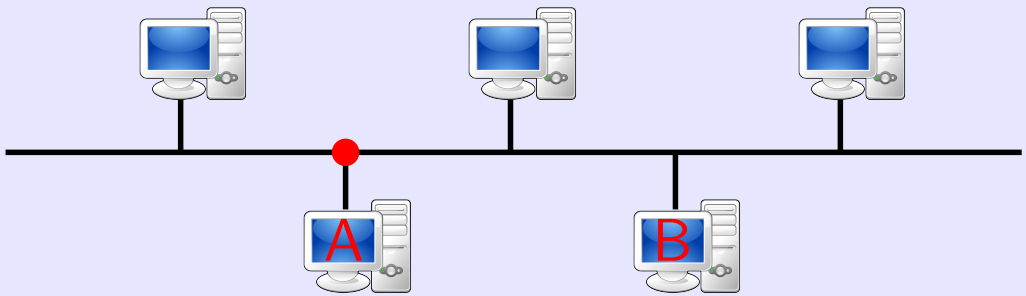
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

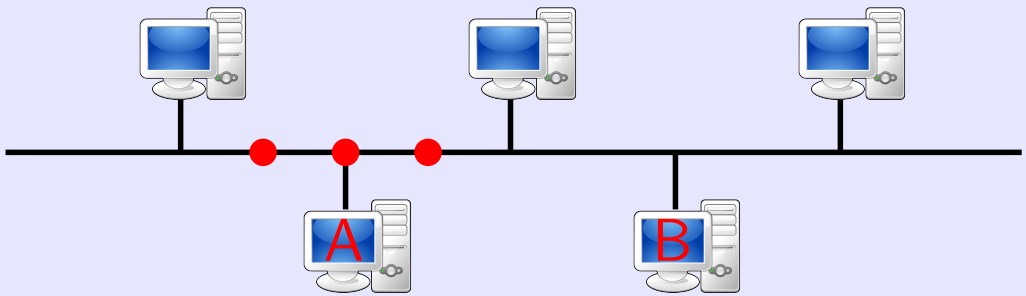
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

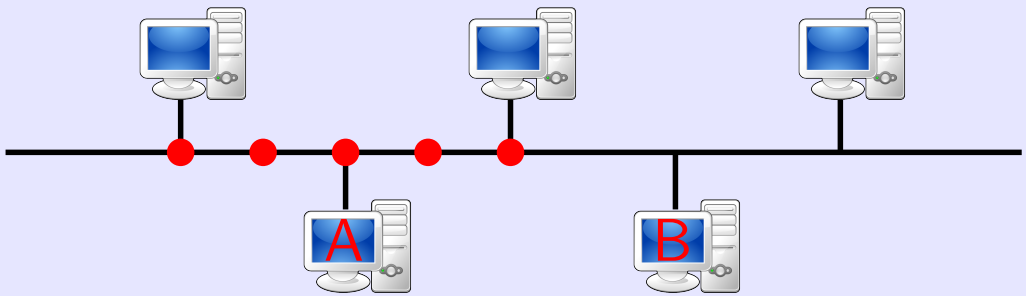
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

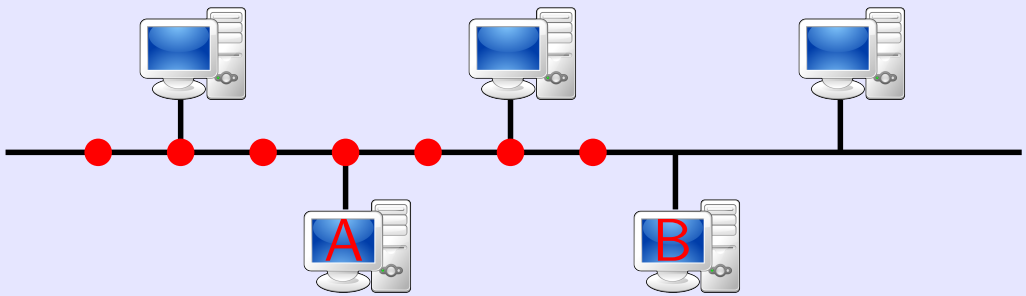
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

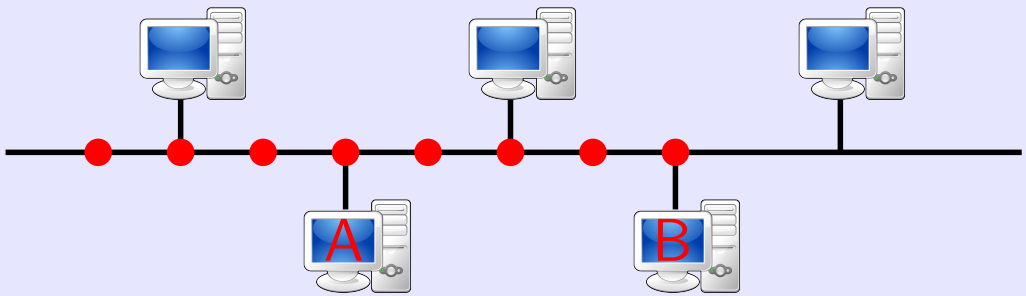
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

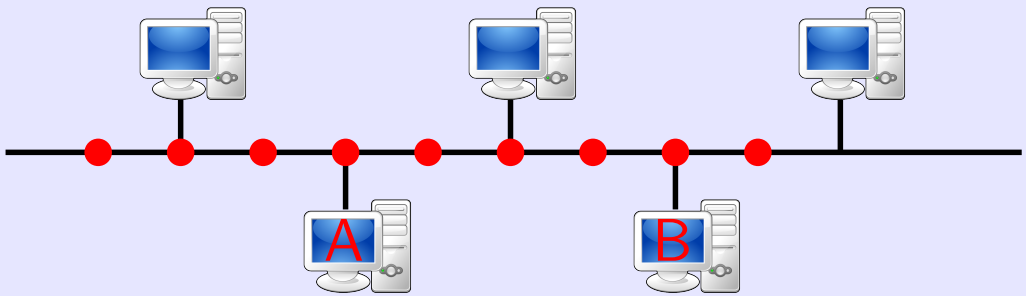
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

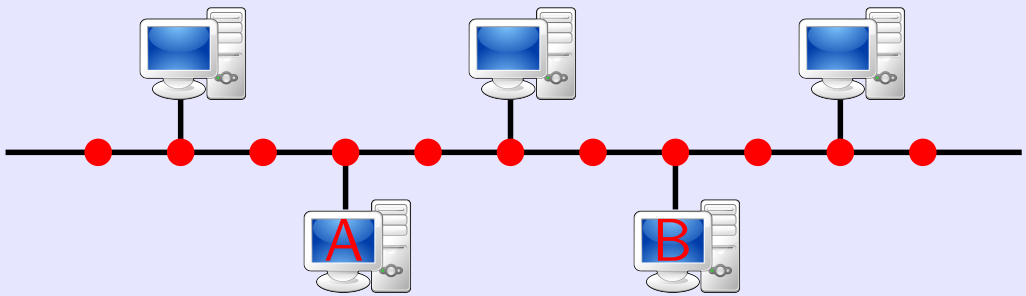
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en bus

- Historiquement la plus ancienne.
- Tous les ordinateurs sont reliés à un même support (câble coaxial).
- Tout le monde reçoit l'information.



Avantages

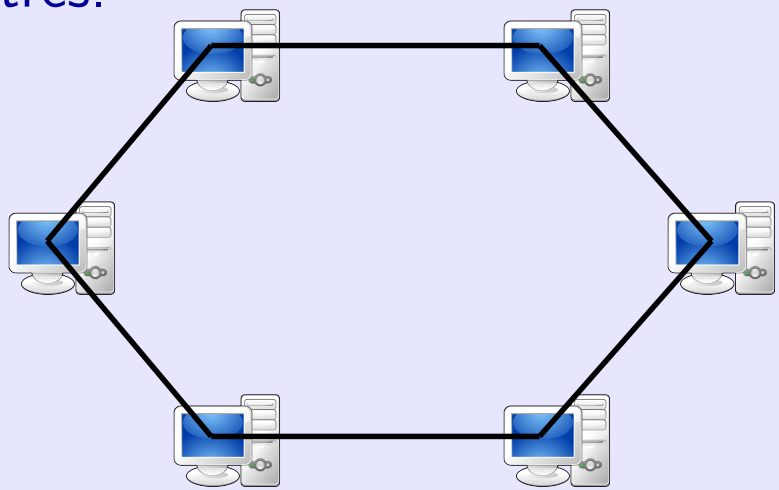
- Simplicité.
- Peu de câble : 1 câble coaxial.
- Qualité du support.

Inconvénients

- Panne sur la câble.
- Collisions.
- Signal jamais régénéré.

Topologie en anneau

- Chaque ordinateur relié à deux autres.
- Connexion *point à point*.
- Unidirectionnel.



Avantages

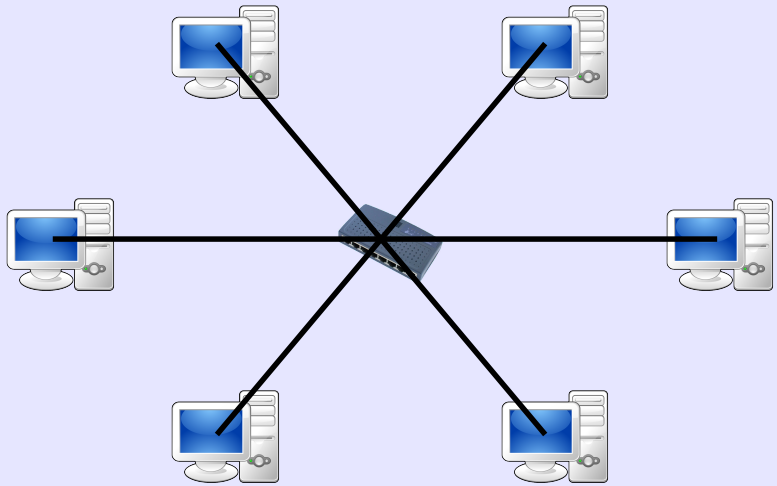
- Performances régulières.
- Signal régénéré par chaque machine.
- Utilisé sur les longues distances.

Inconvénients

- Contraintes pour le rajout de machines.
- Interruption du réseau si une seule machine est en panne.
- Une station maître doit gérer le réseau.

Topologie en étoile

Tous les ordinateurs sont reliés à un élément central.



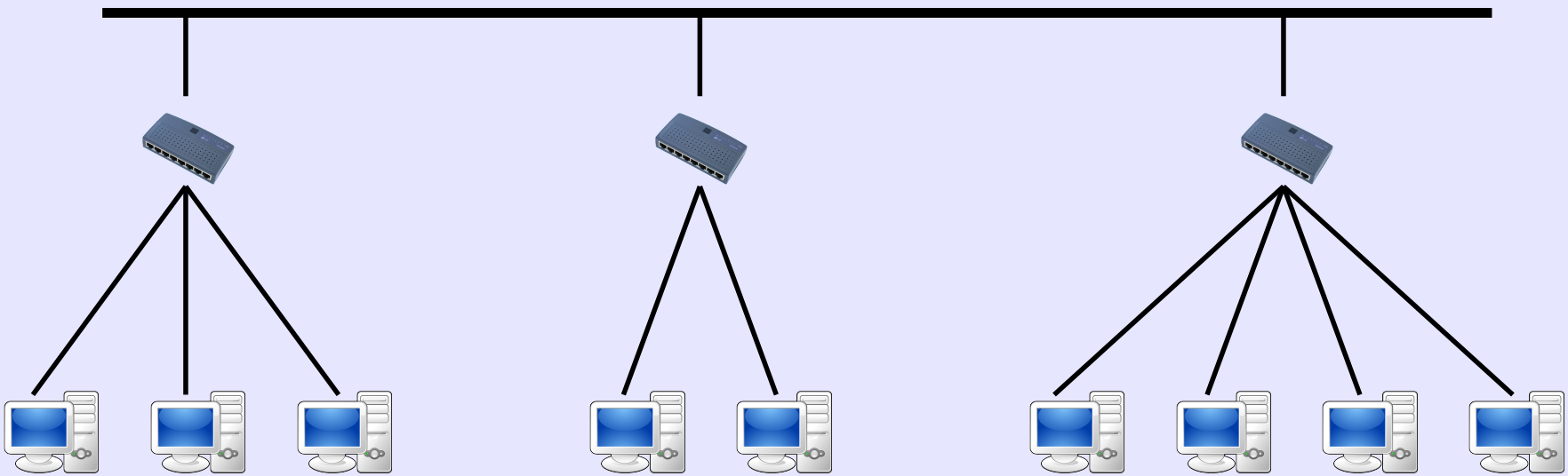
Avantages

- Performances régulières.
- Signal régénéré par chaque machine.
- Topologie la plus rencontrée aujourd'hui en entreprise.

Inconvénients

- Interruption du réseau si l'élément central est en panne (rare).
- (Rajout de machines pas illimité).

Topologie mixte



Plan

II - Structure des réseaux

1 - Topologies des réseaux
2 - Découpage géographique des réseaux
3 - Equipements d'interconnexion
4 - Le modèle OSI

PAN : Personnal Area Network

- La distance qui sépare les éléments est de quelques mètres.
- La vitesse atteint quelques dizaines de Mbit/s.

PAN : Personnal Area Network

- La distance qui sépare les éléments est de quelques mètres.
- La vitesse atteint quelques dizaines de Mbit/s.

LAN : Local Area Network

- Relie les ordinateurs ou postes téléphoniques situés dans la même pièce ou dans le même bâtiment.
- Vitesse entre 10 Mbit/s et 10 Gbit/s.
- La distance entre les équipements peut atteindre 2Km.

MAN : Metropolitan Area Network

- Réseau à l'échelle d'une ville.
- Permet à 2 équipements de communiquer comme s'ils appartenaient au même LAN
- Interconnection de plusieurs LAN géographiquement proche ($\leqslant$ 100Km).
- Vitesse entre 100 Mbit/s et 10 Gbit/s.

MAN : Metropolitan Area Network

- Réseau à l'échelle d'une ville.
- Permet à 2 équipements de communiquer comme s'ils appartenaient au même LAN
- Interconnection de plusieurs LAN géographiquement proche ($\leqslant$ 100Km).
- Vitesse entre 100 Mbit/s et 10 Gbit/s.

WAN : Wide Area Network

- Relie plusieurs sites ou des ordinateurs du monde entier.
- La distance varie de quelques centaines de Km au monde entier.
- Vitesse :

MAN : Metropolitan Area Network

- Réseau à l'échelle d'une ville.
- Permet à 2 équipements de communiquer comme s'ils appartenaient au même LAN
- Interconnection de plusieurs LAN géographiquement proche ($\leqslant$ 100Km).
- Vitesse entre 100 Mbit/s et 10 Gbit/s.

WAN : Wide Area Network

- Relie plusieurs sites ou des ordinateurs du monde entier.
- La distance varie de quelques centaines de Km au monde entier.
- Vitesse : **quelques Mbit/s**.

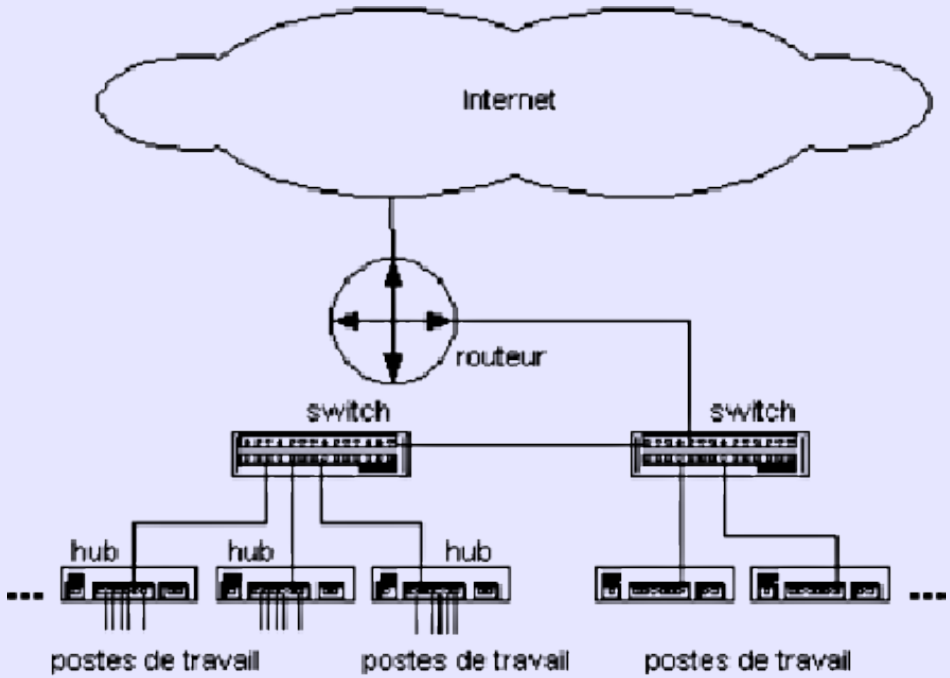
Plan

II - Structure des réseaux

1 - Topologies des réseaux
2 - Découpage géographique des réseaux
3 - Equipements d'interconnexion
4 - Le modèle OSI

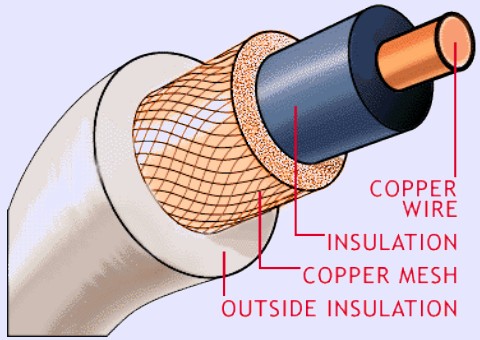
Les systèmes d'interconnexions physiques

Un réseau ouvert comporte des éléments physiques indispensables à la bonne livraison des données dans le temps : ce sont les hubs, switchs, routeurs, répéteurs, passerelles et autres communicateurs.

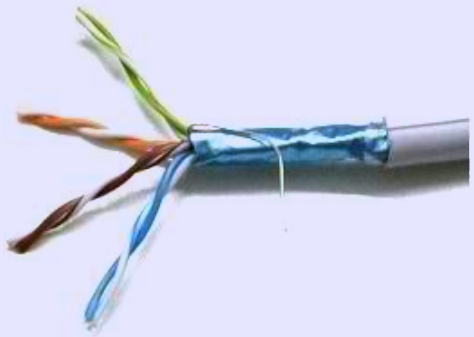


Les câbles

- Câbles coaxiaux : presque plus utilisés, sauf lorsque des contraintes particulières (interférences électromagnétiques, contraintes mécaniques...) interdisent d'autres solutions.

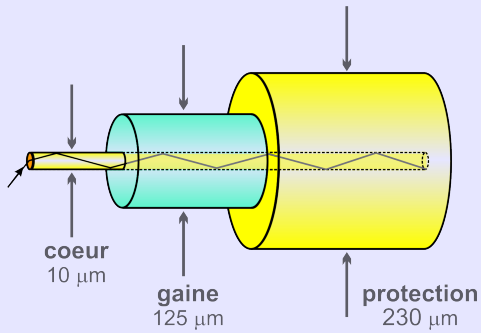


- Paires torsadées :
  - ✓ Utilisées pour 10BaseT, 100BaseT, 1000BaseT et récemment par 10GBASE-CX4 (10Gb/s) ;
  - ✓ Connecteurs de type RJ45 (8 broches) ;
  - ✓ 4 paires : 2 pour la réception et deux pour l'emission ;
  - ✓ Câbles blindés ou non blindés ;
  - ✓ Coût peu élevé (moins de 1€ le mètre - catégorie 5 à 4 paires) ;
  - ✓ Faible risque d'interférences électriques ;
  - ✓ Atténuation faible ;
  - ✓ Robustesse physique.

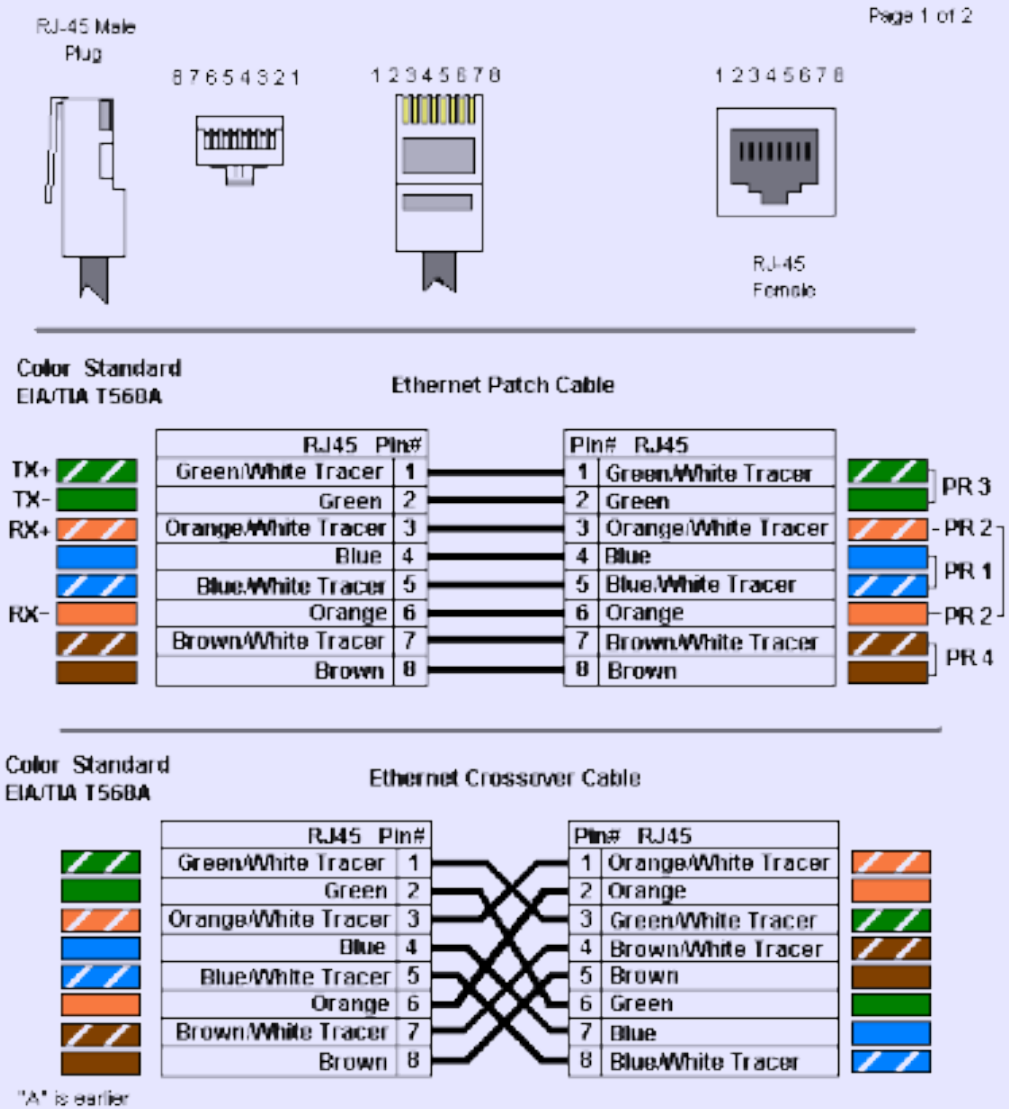


Les câbles

- Fibres optiques :
  - ✓ Utilisées pour 10BaseF, 100BaseFX, 1000BaseSX ;
  - ✓ Très haut débit ;
  - ✓ Légères, solides ;
  - ✓ Insensibles aux parasites ;
  - ✓ Coût élevé.



Câblage câble RJ45



Le répéteur

- Équipement qui permet de pallier la longueur maximale imposée par la norme d'un réseau (exemple : 100m pour Ethernet).
- Le répéteur est en lien avec la couche 1 du modèle OSI.

Le concentrateur (hub)

- Equipement le plus simple.
- Amplifie le signal réseau.
- Toutes les informations arrivant sur l'appareil sont renvoyées sur toutes les lignes.
- Le hub est en lien avec la couche 1 du modèle OSI

Le commutateur (switch)

- À la différence du hub, lorsque le commutateur reçoit une information, il décode l'entête pour connaître le destinataire.
- Nécessite une table de correspondance entre adresse MAC et numéro de port de connexion.
- Envoie les données uniquement vers le port Ethernet associé. Ceci réduit le trafic sur le câblage réseau par rapport à un hub.
- Le switch est en lien avec les couches 1, 2 et 3.

Le routeur

- À la différence d'un hub ou d'un switch qui permettent de connecter des appareils faisant partie d'un même réseau, un routeur est nécessaire pour faire transiter des données entre des machines qui ne sont pas dans le même réseau
- Il décode les trames, reconnaît certaines données des entêtes et peut ainsi transmettre les informations sur d'autres routeurs qui reconduisent les informations vers le destinataire final.
- Le routeur intervient au niveau de la couche 3.

La passerelle (Gateway)

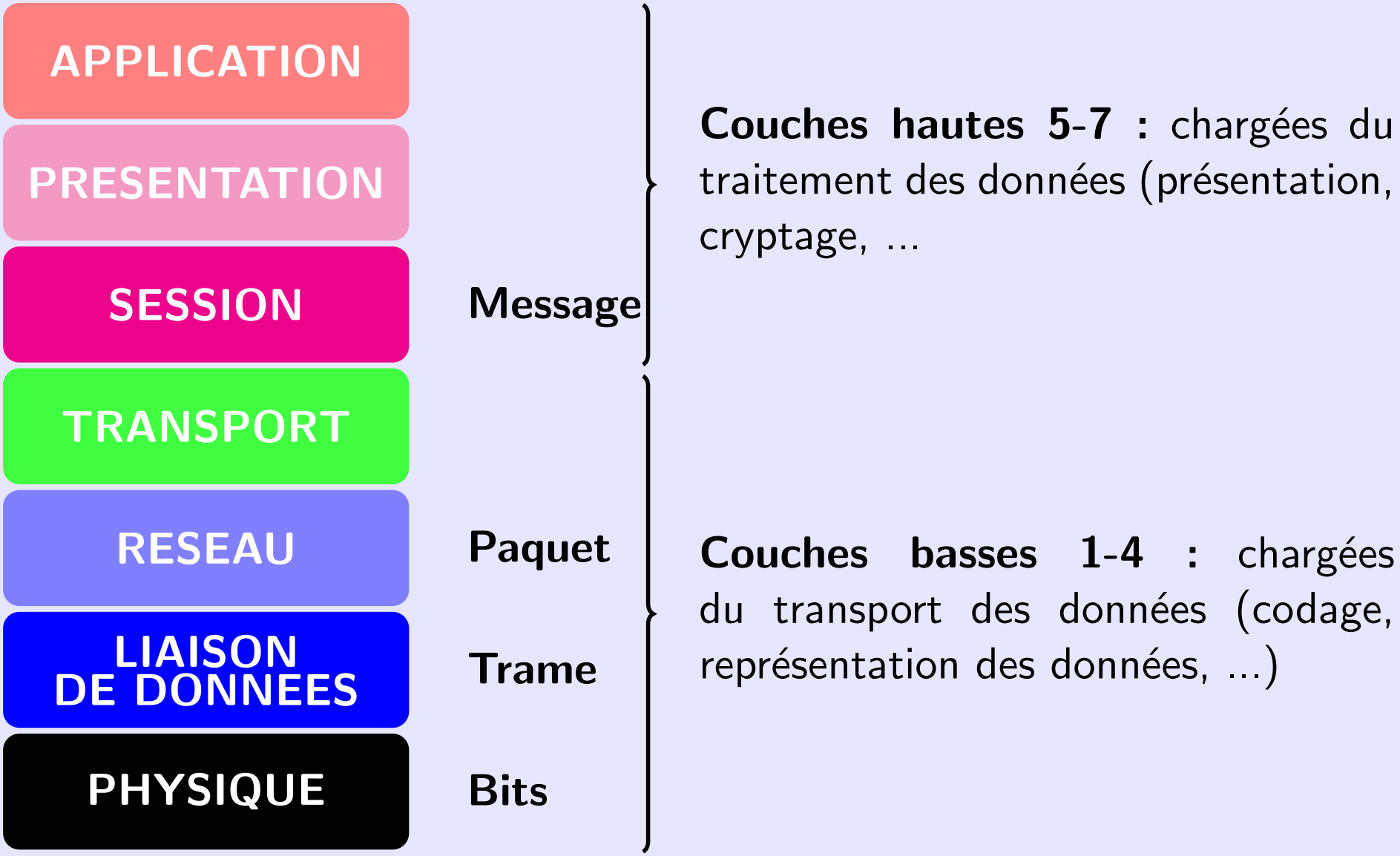
- Système d'interconnexion le plus complexe car il permet de relier des réseaux entièrement hétérogènes. Par contre, ce gros travail d'adaptation à faire ralentit la vitesse de transmission. Ex : passerelle entre un réseau local et internet.
- Physiquement, la passerelle est souvent un PC.
- Fonctionne sur les couches 3 à 7 du modèle OSI.

Plan

II - Structure des réseaux

1 - Topologies des réseaux
2 - Découpage géographique des réseaux
3 - Equipements d'interconnexion
4 - Le modèle OSI

Modèle théorique (Open System Interconnection)



Modèle théorique (Open System Interconnection)

APPLICATION

PRESENTATION

SESSION

TRANSPORT

RESEAU

LIAISON DE DONNEES

PHYSIQUE

Couche 1 :

S'occupe de la transmission "physique" des bits.

Elle définit :

- Le mode de codage des bits.
- Le mode de transmission.
- Le support utilisé (type de câble, fibre optique, ...).

Modèle théorique (Open System Interconnection)

APPLICATION

PRESENTATION

SESSION

TRANSPORT

RESEAU

LIAISON DE DONNEES

PHYSIQUE

Couche 2 :

- Structure les bits en trames.
- S'occupe de la retransmission des trames perdues.
- Gère les adresses MAC (insertion et suppression).

Modèle théorique (Open System Interconnection)

APPLICATION

PRESENTATION

SESSION

TRANSPORT

RESEAU

LIAISON DE DONNEES

PHYSIQUE

Couche 3 :

- Regroupe les données en paquets.
- Détermine le chemin que vont suivre les paquets (adressage et routage).

Modèle théorique (Open System Interconnection)

APPLICATION

PRESENTATION

SESSION

TRANSPORT

RESEAU

LIAISON DE DONNEES

PHYSIQUE

Couche 4 :

- Couche uniquement logicielle.
- Permet de créer plusieurs connections simultanées (multiplexage).
- Gère les connexions de bout en bout entre processus.

Modèle théorique (Open System Interconnection)

APPLICATION

PRESENTATION

SESSION

TRANSPORT

RESEAU

LIAISON DE DONNEES

PHYSIQUE

Couche 5 :

- Gère la synchronisation des échanges.
- Permet l'ouverture et la fermeture d'une connexion (session) entre 2 applications sur 2 ordinateurs différents.

Modèle théorique (Open System Interconnection)

APPLICATION

PRESENTATION

SESSION

TRANSPORT

RESEAU

LIAISON DE DONNEES

PHYSIQUE

Couche 6 :

- Se charge du codage des données pour l'application.
- Fait communiquer les applications indépendamment du système d'exploitation.

Modèle théorique (Open System Interconnection)

APPLICATION

PRESENTATION

SESSION

TRANSPORT

RESEAU

LIAISON DE DONNEES

PHYSIQUE

Couche 7 :
point d'accès au services réseau (FTP, mail, ...).

Plan

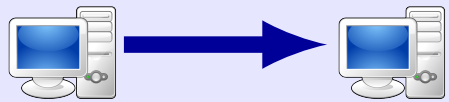
III - Communication réseau

1 - Types de connexion

2 - Types de communication

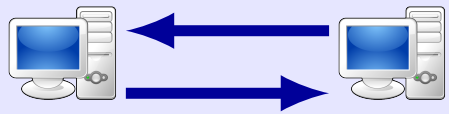
Connexion Simplex

Les données circulent dans un seul sens.



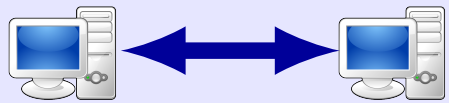
Connexion Half Duplex

Les données circulent dans un sens ou l'autre, mais pas les deux simultanément. Liaison bidirectionnelle utilisant la capacité totale de la ligne



Connexion Full Duplex

Les données circulent de façon bidirectionnelle et simultanément. La bande passante est divisée par deux.

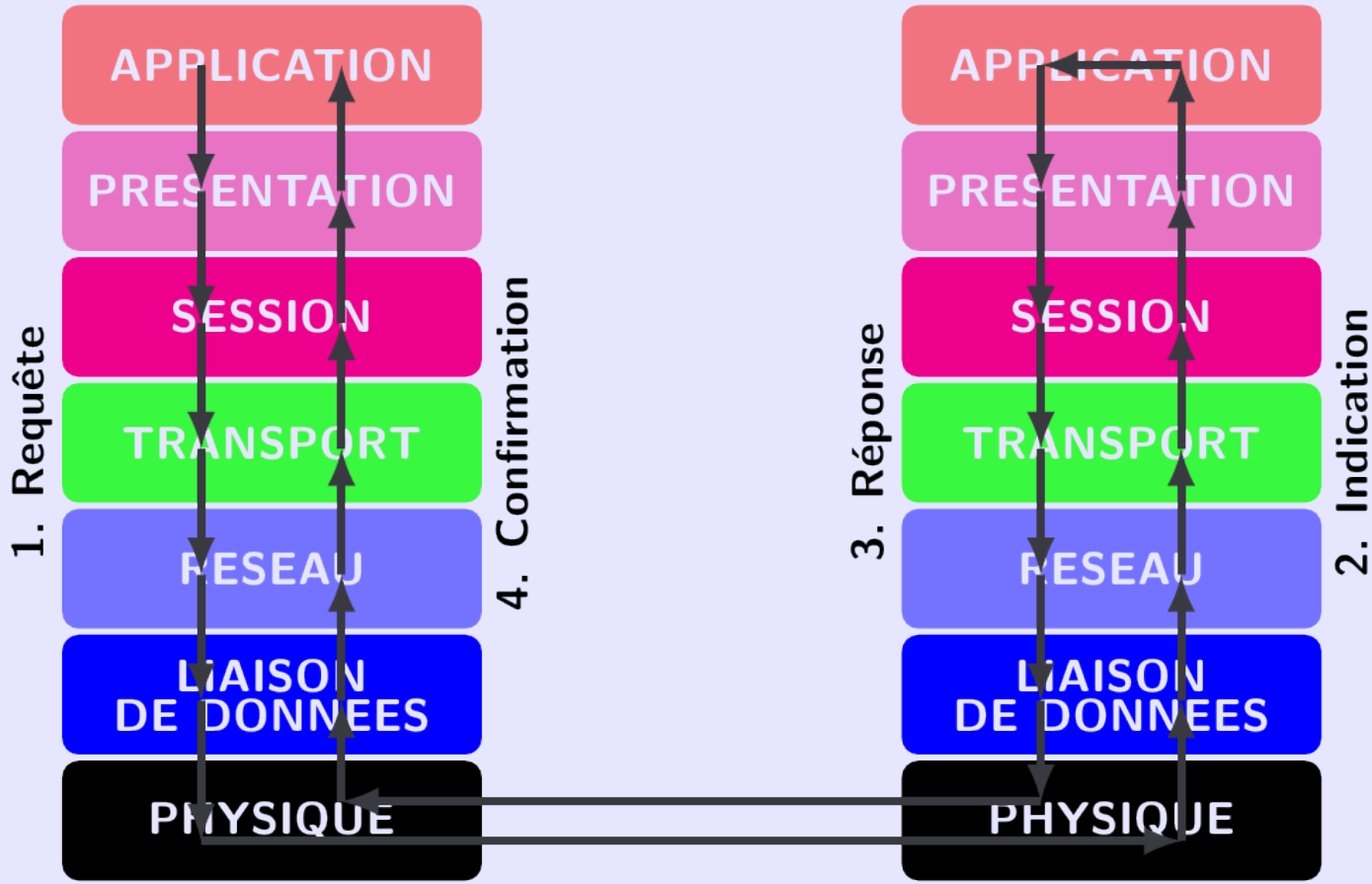


Plan

III - Communication réseau

1 - Types de connexion
2 - Types de communication

Communication entre 2 machines

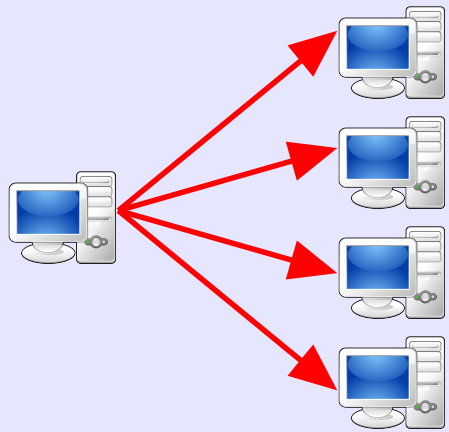


Communication point à point : Unicasting

- Seulement 2 correspondants pendant la communication.
- Communication adressée à un seul destinataire.
- Ex : liaison série, câble RJ45 croisé, ...

Communication multi-point : Broadcasting

- Communication de 1 $\longrightarrow$ n.
- Communication adressée à un ou plusieurs destinataires.
- C'est l'adresse ou le contenu de message qui permettra à chaque nœud de déterminer si le message lui est adressé ou non.



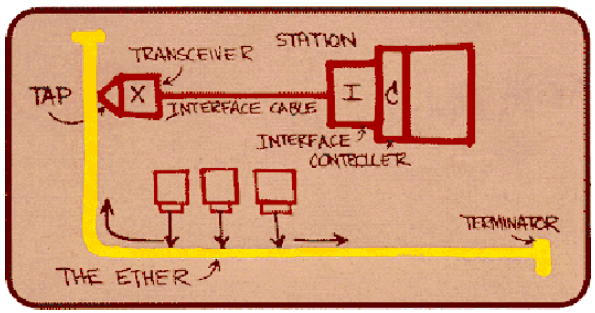
Plan

IV - Ethernet

1 - Généralités
2 - La communication

Caractéristiques

- Créé par Robert Metcalfe et David Boggs en 1973 (2,94 Mbps).
- Les sociétés Xerox, DEC, Intel en font un standard : **norme IEEE 802.3**.
- Débits : 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps.
- Topologie en bus ou en étoile.
- Multi-support : coaxial, paires torsadées, fibre optique, ondes radio.
- Usage d'un protocole entièrement décentralisé (CSMA/CD) synonyme de simplicité. Toutes les stations sont égales vis-à-vis du réseau, il n'y a pas d'équipement maître de contrôle du réseau.
- Il est possible de connecter ou retirer une machine du réseau sans perturber le fonctionnement de l'ensemble.
- Coût de l'équipement faible.



Principe

- L'Ethernet est basé sur un principe de dialogue sans connexion et donc sans fiabilité (pas de procédure type *handshake* avec le destinataire).
- Le service sans connexion d'Ethernet est non-fiable, car pas d'information sur la bonne réception de la trame par le destinataire (pas de retour sur le CRC).
- Cette absence de fiabilité est la clé de la simplicité et des coûts modérés des systèmes Ethernet.
- Ethernet se situe sur la couche 2 du modèle OSI.

Plan

IV - Ethernet

1 - Généralités
2 - La communication

- Lorsqu'une machine émet, toutes les machines reçoivent l'information.
- Comment une machine peut savoir si le message lui est destiné ?

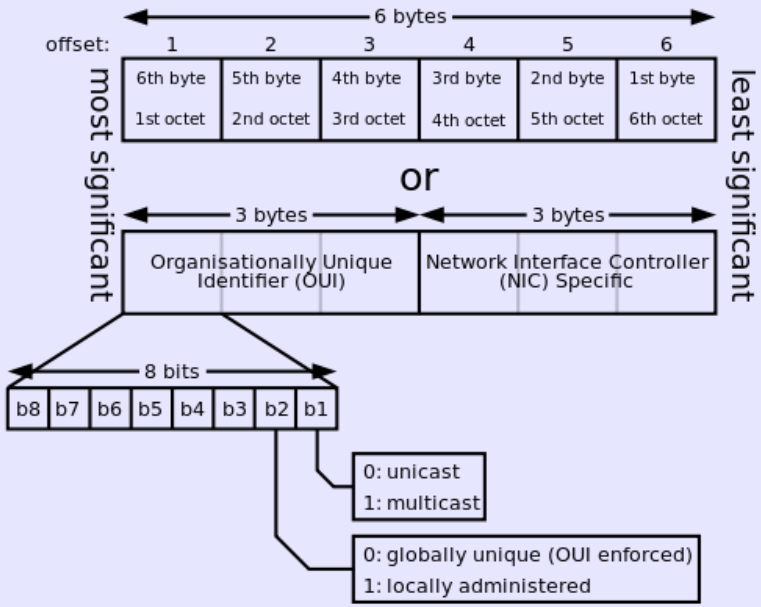
- Lorsqu'une machine émet, toutes les machines reçoivent l'information.
- Comment une machine peut savoir si le message lui est destiné ?
  $\Rightarrow$ par l'adresse MAC (**M**edia **A**ccess **C**ontrol).

- Lorsqu'une machine émet, toutes les machines reçoivent l'information.
- Comment une machine peut savoir si le message lui est destiné ?

M'sieur, c'est quoi une adresse MAC ?

- Adresse physique unique gravée en dur à la fabrication et associée à chaque composant réseau.
- L'adresse est composée de deux couples de 3 octets. Ex : `88:51:fb:5e:fd:80`.
- Les trois premiers octets désignent le constructeur. C'est le l'organisation OUI (**O**rganizationally **U**nique **I**dentifier) gérée par l'IEEE, qui référence ces correspondances. Ex : `00:00:0C` → Cisco, `08:00:20` → Sun, ...
- Les trois derniers octets désignent le numéro d'identifiant de la carte, dont la valeur est laissée à l'initiative du constructeur qui possède le préfixe.

M'sieur, c'est quoi une adresse MAC ?



Problème de la transmission

- Le principe de la transmission Ethernet consiste à envoyer la trame, détecter si une collision a eu lieu, et si c'est le cas, appliquer une méthode de résolution de conflits.
- Cette méthode met en œuvre un accès au support par compétition.
- Il est impossible de prédire l'arrivée d'une trame : **l'accès est dit non déterministe ou aléatoire**.

Résolution du problème de transmission

Ethernet repose sur un algorithme d'accès multiple CSMA/CD, signifiant **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection. Ce protocole permet la discussion et la gestion des erreurs sur le réseau Ethernet.

Les règles du protocole CSMA/CD sont :

- Les composants peuvent commencer à transmettre à n'importe quel moment.
- Les composants ne transmettent jamais lorsqu'ils détectent une activité sur le canal de transmission.
- Les composants interrompent leur transmission dès qu'ils détectent l'activité d'un autre composant au sein du canal (détection de collisions).
- Avant de procéder à la retransmission d'une trame, les adaptateurs patientent pendant une durée aléatoire relativement courte.

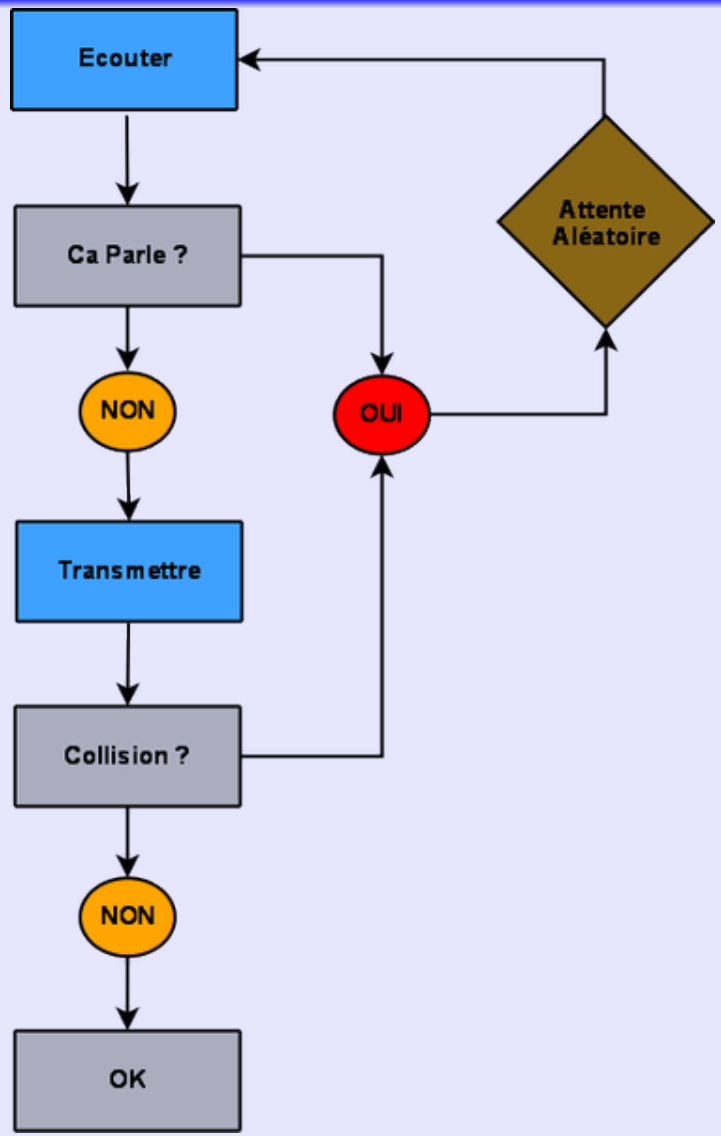
Résolution du problème de transmission

Afin que la détection de collisions soit possible, il faut que le temps de transmission d'une trame soit 2 fois supérieur à son temps de propagation.

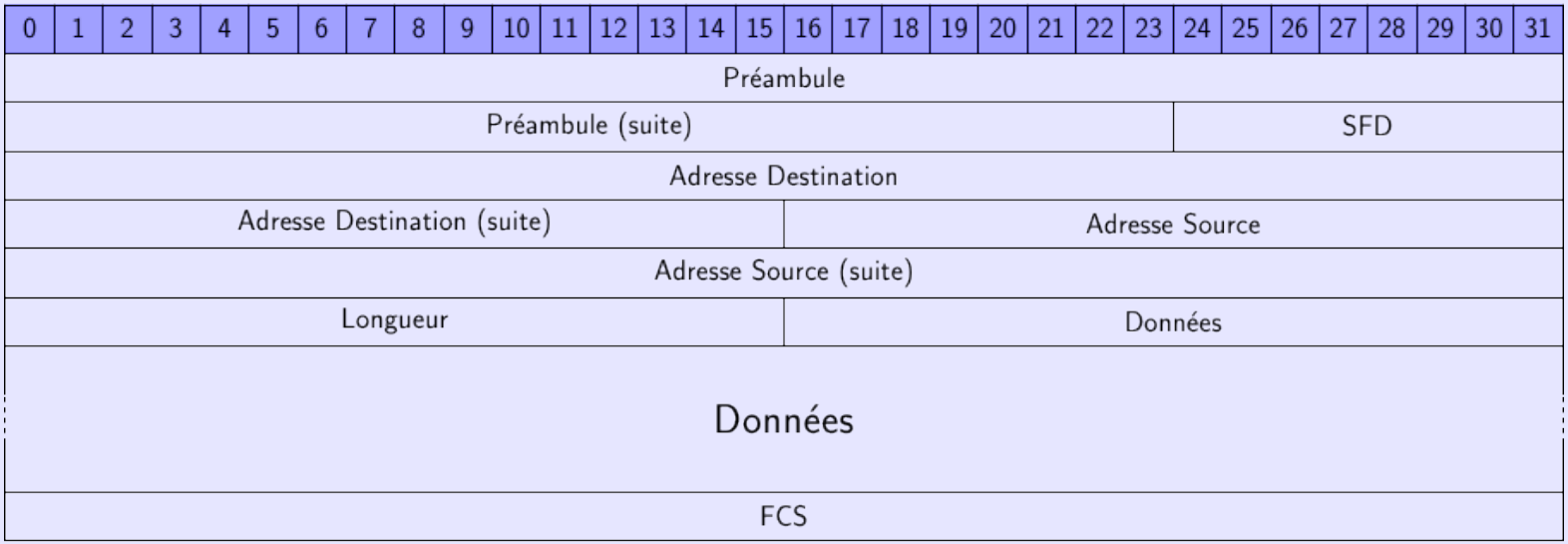
Ainsi, la station qui veut émettre doit envoyer un signal suffisamment long pour parcourir tout le réseau. La trame doit avoir une taille minimale qui dépend de la topologie. Si une trame n'atteint pas cette taille minimale, on fait un bourrage avec des bits neutres (padding).

Par conséquent plus une trame est grande plus elle est efficace et moins de collisions se produiront sur le réseau.

Algorithme du CSMA/CD



La trame Ethernet



Préambule	Permet de synchroniser l'envoi. Chacun des octets vaut 10101010. Cela permet à la carte réceptrice de synchroniser son horloge.
SFD	Indique à la carte réceptrice que le début de la trame va commencer. La valeur de SFD (Starting Frame Delimiter) est 10101011.
Adresse de destination	Adresse MAC de la machine destinataire.
Adresse de la source	Adresse MAC de la machine source.
Longueur	Longueur du champ de données.
Données	Contient les données de la couche 3 (entre 46 et 1500 octets). Si la taille des données est inférieure à 46 octets, alors elle devra être complétée avec des octets de bourrage (padding) et c'est la couche réseau qui sera chargée de les éliminer.
FCS	Représente la séquence de contrôle de trame. Il permet à la machine qui réceptionnera cette trame de détecter toute erreur pouvant s'être glissée au sein de la trame.

Plan

V - TCP/IP

1 - Généralités
2 - Le Protocole TCP
3 - Le Protocole UDP
4 - Le protocole IP
5 - Le routage
6 - Les sous réseaux

Introduction

TCP/IP désigne une architecture réseau, mais aussi 2 protocoles étroitement liés :

- Un protocole de transport TCP (**T**ransmission **C**ontrol **P**rotocol).
- Un protocole réseau IP (**I**nternet **P**rotocol).

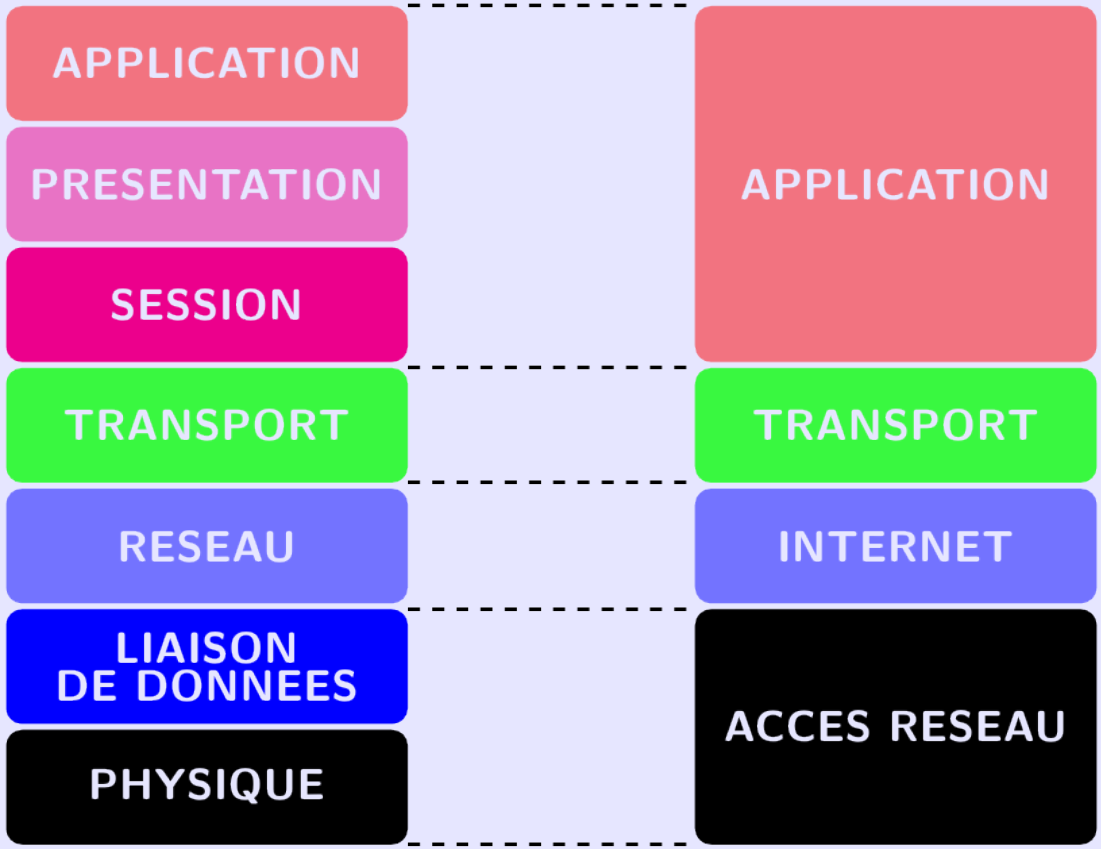
Le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite.

L'origine de TCP/IP remonte au réseau ARPANET (1974).

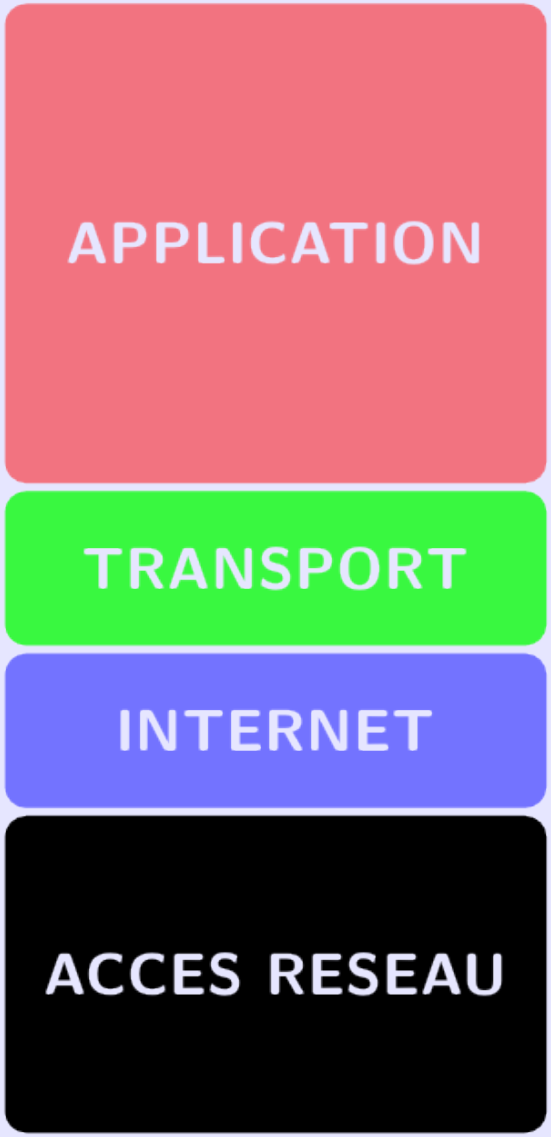
Il est basé sur la technologie de commutation par paquet (mode datagramme).

TCP/IP vs OSI

- Modèle en 4 couches, plus souple que le modèle OSI.
- Créé pour des applications pratiques.



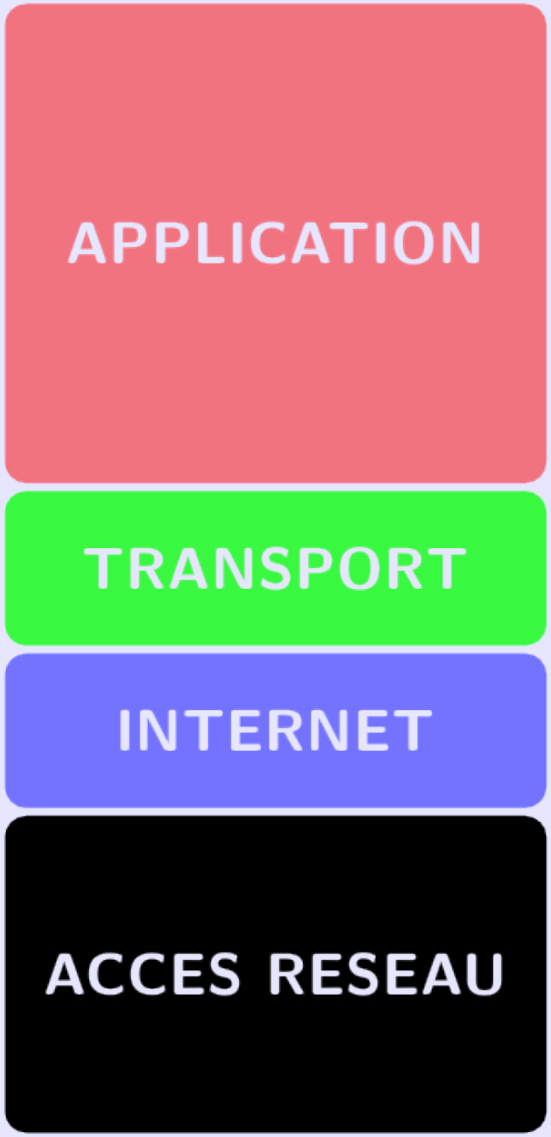
Modèle TCP/IP



Couche 1 :

- Regroupe les couches physique et liaison de données du modèle OSI.
- Permet à un hôte d'envoyer des paquets IP sur le réseau.
- Ethernet est une implémentation de cette couche.

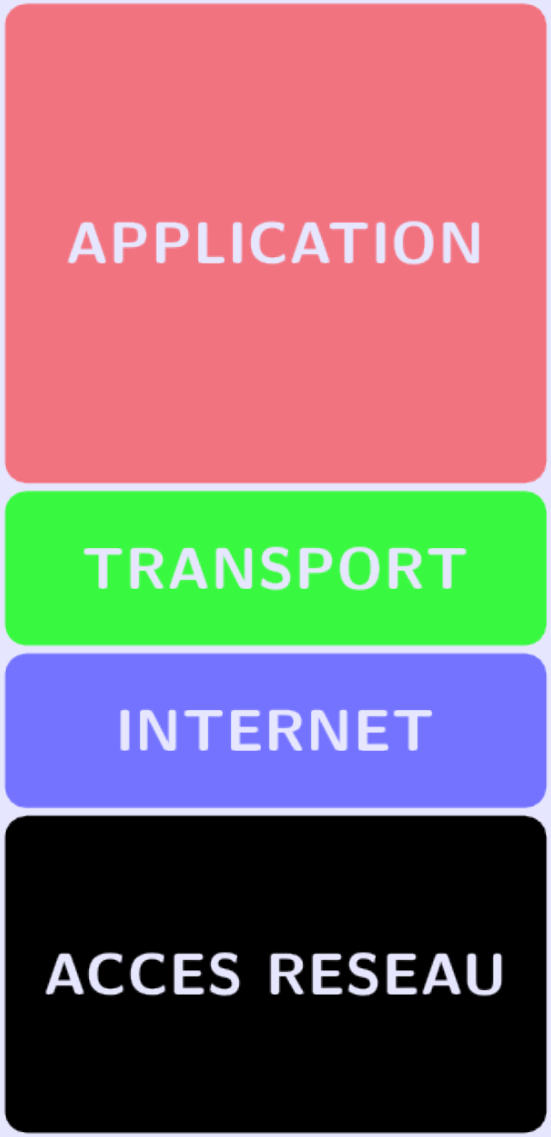
Modèle TCP/IP



Couche 2 :

- Cette couche est la clé de voûte de l'architecture.
- L'implémentation officielle de cette couche est le protocole IP (Internet Protocol).
- Permet l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination (y compris dans le désordre).

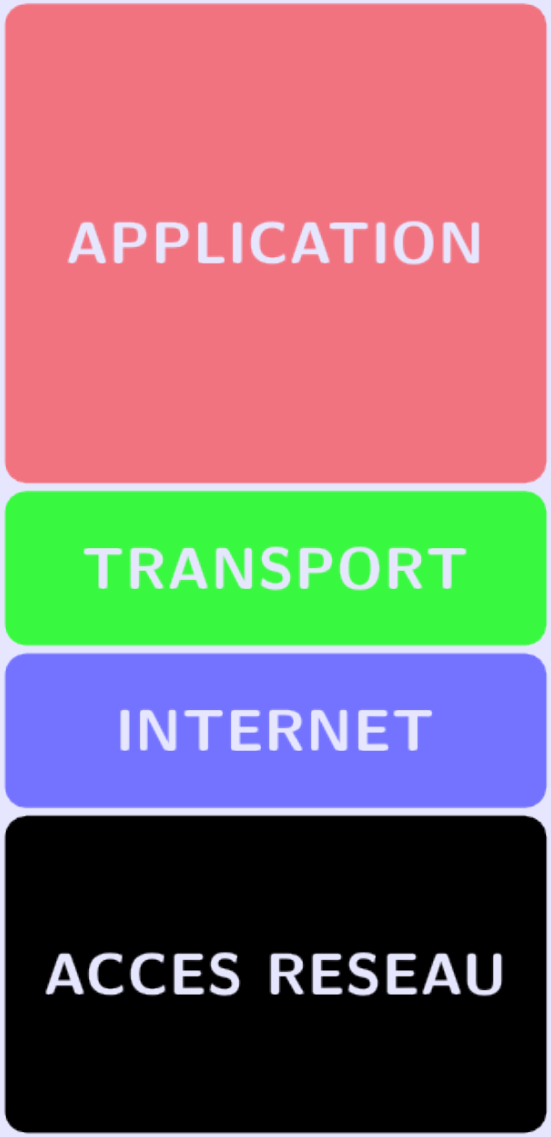
Modèle TCP/IP



Couche 3 :

- Même rôle que celle du modèle OSI : permettre à des entités de soutenir une conversation.
- Implémentation du protocole TCP.
- Implémentation du protocole UDP (**U**ser **D**atagram **P**rotocol), plus simple que TCP mais non fiable et sans connexion.

Modèle TCP/IP



Couche 4 :

- Cette couche contient tous les protocoles de haut niveau (Telnet, FTP, SMTP, HTTP).

Plan

V - TCP/IP

1 - Généralités
2 - Le Protocole TCP
3 - Le Protocole UDP
4 - Le protocole IP
5 - Le routage
6 - Les sous réseaux

Principe

TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine à une autre machine.

Sur la machine émetteur, TCP s'occupe de découper les données en paquet et s'assure de leur bonne livraison. La transmission (routage) est ensuite assurée par le protocole IP.

A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche IP pour reconstruire le message initial.

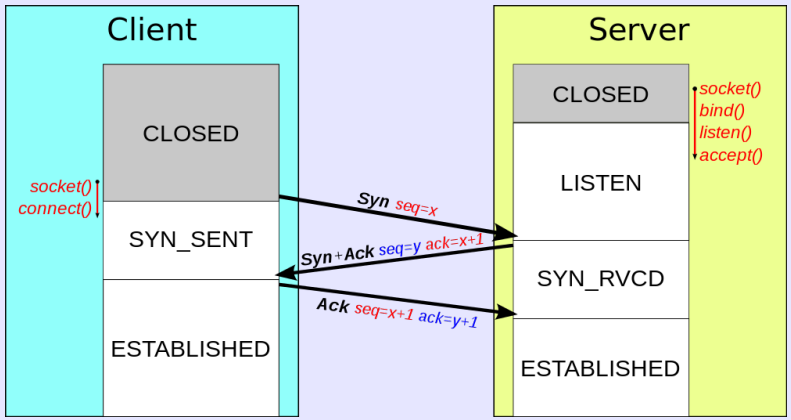
TCP s'occupe également du contrôle de flux de la connexion afin d'éviter les saturations.

La communication en TCP

La connexion

Dans le protocole TCP, une connexion entre deux machines s'établit en trois étapes : le *three way handshake*

- SYN : Le client qui désire établir une connexion avec un serveur va envoyer un premier paquet SYN (synchronized) au serveur. Le numéro de séquence de ce paquet est un nombre aléatoire A.
- SYN-ACK : Le serveur va répondre au client à l'aide d'un paquet SYN-ACK (synchronize, acknowledge). Le numéro du ACK est égal au numéro de séquence du paquet précédent (SYN) incrémenté de un (A + 1) tandis que le numéro de séquence du paquet SYN-ACK est un nombre aléatoire B.
- ACK : Pour terminer, le client va envoyer un paquet ACK au serveur qui va servir d'accusé de réception. Le numéro de séquence de ce paquet est défini selon la valeur de l'acquittement reçu précédemment p.e. A + 1 et le numéro du ACK est égal au numéro de séquence du paquet précédent (SYN-ACK) incrémenté de un (B + 1).



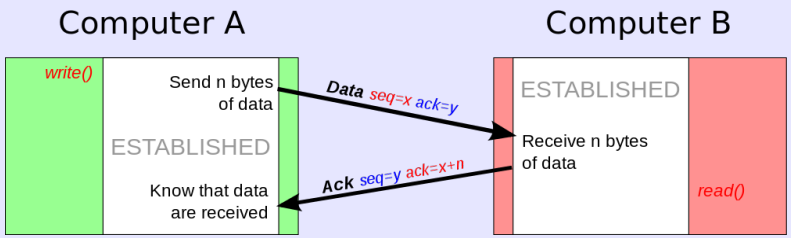
Une fois le handshake effectué, une communication full-duplex est maintenant établie entre le client et le serveur.

La communication en TCP

Le transfert de données

Pendant la phase de transferts de données, certains mécanismes permettent d'assurer la robustesse et la fiabilité de TCP :

- Les numéros de séquence permettent d'ordonner les segments TCP reçus et de détecter les données perdues.
- Les sommes de contrôle permettent la détection d'erreurs.
- Les acquittements ainsi que les temporisations permettent la détection des segments perdus ou retardés.



La communication en TCP

Exemple de Communication en TCP

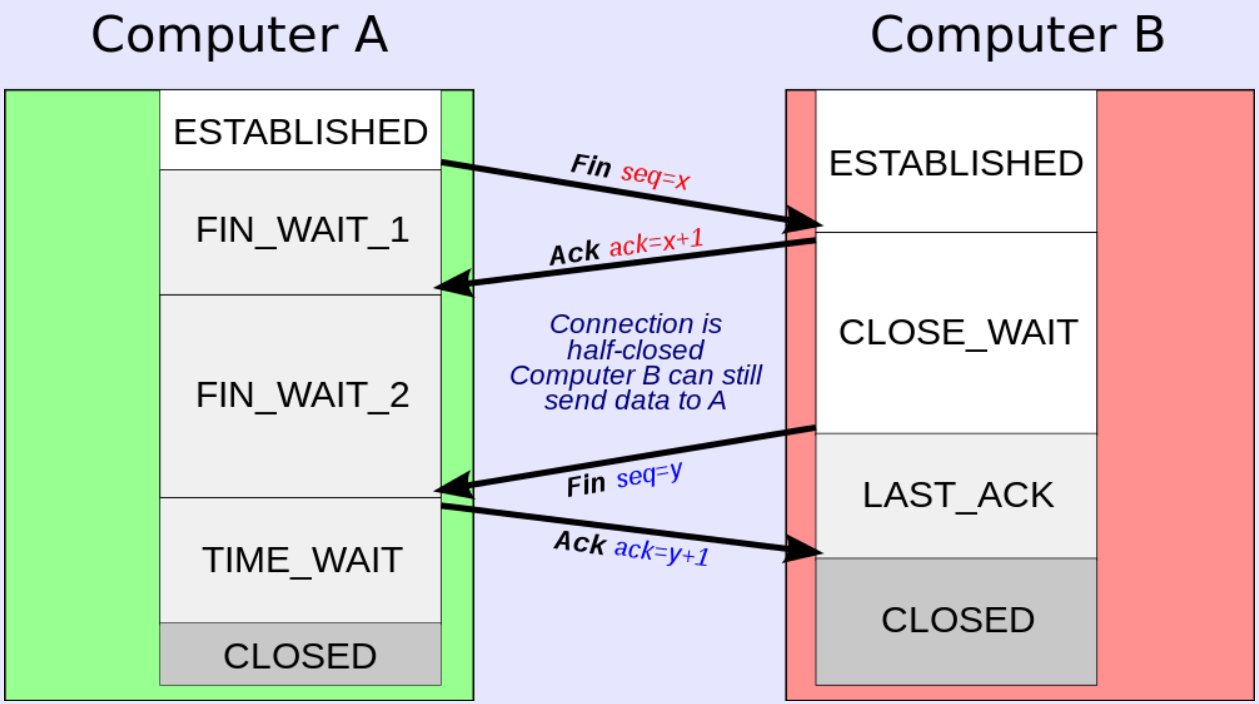
Dans le cas d'un échange de segments par Telnet :

1. A envoie un segment à B contenant deux octets de données, un numéro de séquence égal à 42 (Seq = 42) et un numéro d'acquittement égal à 79 (Ack = 79).
2. B envoie un segment ACK à A. Le numéro de séquence de ce segment correspond au numéro d'acquittement de A (Seq = 79) et le numéro d'acquittement au numéro de séquence de A tel que reçu par B, augmenté de la quantité de données en octets reçue (Ack = 42 + 2 = 44).
3. A confirme la réception du segment en envoyant un ACK à B, avec comme numéro de séquence son nouveau numéro de séquence, à savoir 44 (Seq = 44) et comme numéro d'acquittement le numéro de séquence du segment précédemment reçu, augmenté de la quantité de données reçue (Ack = 79 + 2 = 81).

La communication en TCP

La fin de connexion

La phase de terminaison d'une connexion utilise un handshaking en quatre temps, chaque extrémité de la connexion effectuant sa terminaison de manière indépendante. Ainsi, la fin d'une connexion nécessite une paire de segments FIN et ACK pour chaque extrémité.

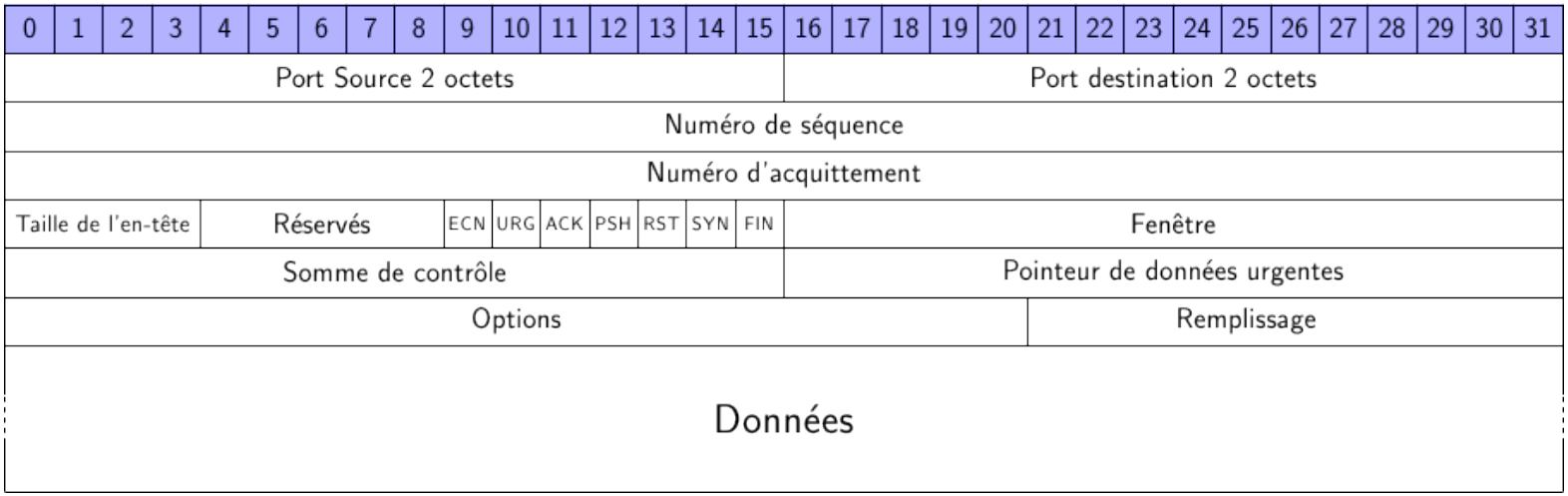


Les ports de communication en TCP

Les ports de communication sont associés au différents services proposés par la couche application

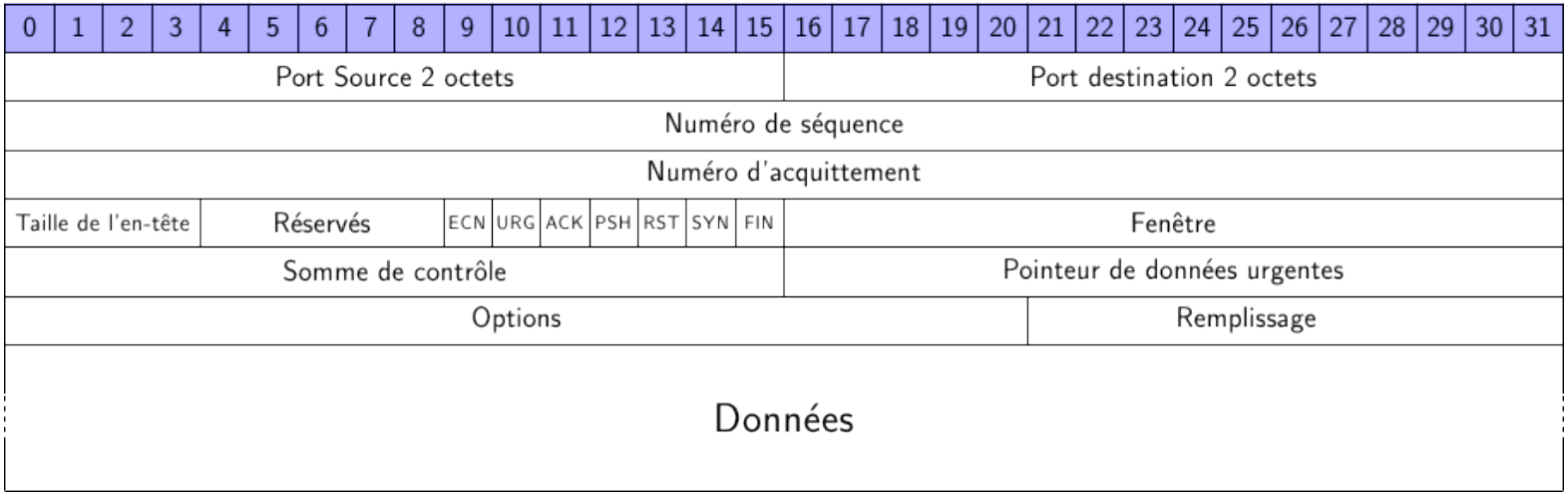
Services	Port TCP
FTP (File Transfer Protocol)	21
SSH (Secure SHell)	22
Telnet	23
SMTP (Single Mail Transfer Protocol)	25
HTTP (Hyper Text Transfer Protocol)	80
POP (Post Office Protocole)	110
IMAP (Internet Message Access Protocol)	143
VNC (Virtual Network Computing)	5900

La trame TCP



- Port source : Numéro du port source.
- Port destination : Numéro du port destination.
- Numéro de séquence : Numéro de séquence du premier octet de ce segment.
- Numéro d'acquittement : Numéro de séquence du prochain octet attendu.
- Taille de l'en-tête : Longueur de l'en-tête en mots de 32 bits (les options font partie de l'en-tête).
- Drapeaux :
  - ✓ Réservé : Réservés pour un usage futur.
  - ✓ ECN : signale la présence de congestion.
  - ✓ URG : Signale la présence de données urgentes.
  - ✓ ACK : Signale que le paquet est un accusé de réception .
  - ✓ PSH : Données à envoyer tout de suite (PuSH).
  - ✓ RST : Rupture anormale de la connexion (ReSeT).
  - ✓ SYN : Demande de synchronisation ou établissement de connexion.
  - ✓ FIN : Demande la fin de la connexion.

La trame TCP



- Fenêtre : Taille de fenêtre demandée, c'est-à-dire le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception.
- Checksum : Somme de contrôle calculée sur l'ensemble de l'en-tête TCP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP).
- Pointeur de données urgentes : Position relative des dernières données urgentes.
- Options : Facultatif.
- Remplissage : Zéros ajoutés pour aligner les champs suivants du paquet sur 32 bits, si nécessaire.
- Données : Séquences d'octets transmis par l'application.

Plan

V - TCP/IP

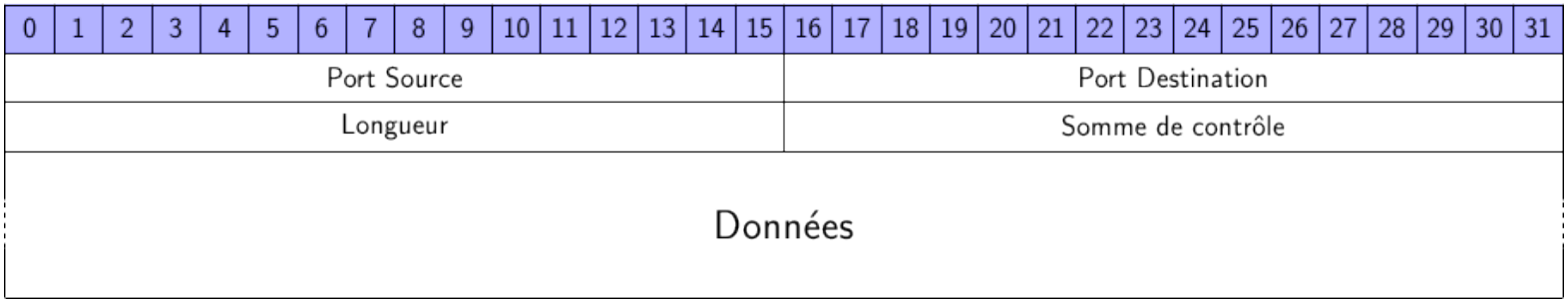
1 - Généralités
2 - Le Protocole TCP
3 - Le Protocole UDP
4 - Le protocole IP
5 - Le routage
6 - Les sous réseaux

Principe

UDP signifie **U**ser **D**ata **P**rotocol. C'est un protocole de transport non orienté connexion donc moins robuste et moins fiable que TCP. Il est sur la même couche que TCP.

- Simple à mettre en œuvre et plus rapide que TCP car il n'y a pas de connexion à gérer (*handshaking*) $\Rightarrow$ pas de garantie de bonne livraison des paquets.
- Pas de séquencement des données $\Rightarrow$ les datagrammes peuvent arriver dans le désordre et UDP ne gère pas leur ordre ni leur ré-assemblage.
- Contrôle d'erreur rudimentaire.
- Convient bien à un environnement de réseau local où la probabilité de dispersion des données est faible.
- Utilisé pour des applications de commande/réponse tenant dans un seul datagramme.
- UDP est utilisé par les applications DNS, Voie sur IP, jeux en ligne.

La trame UDP



- Port Source : indique depuis quel port le paquet a été envoyé.
- Port de Destination : indique à quel port le paquet doit être envoyé.
- Longueur : indique la longueur totale (exprimée en octets) du segment UDP (en-tête et données). La longueur minimale est donc de 8 octets (taille de l'en-tête).
- Somme de contrôle : permet de s'assurer de l'intégrité du paquet reçu quand elle est différente de zéro.

Plan

V - TCP/IP

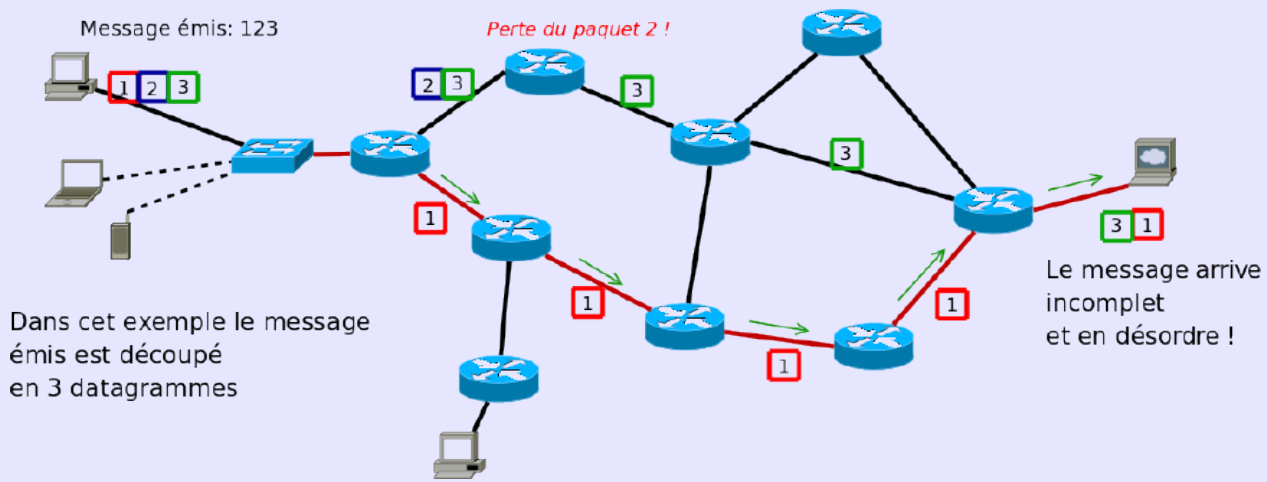
1 - Généralités
2 - Le Protocole TCP
3 - Le Protocole UDP
4 - Le protocole IP
5 - Le routage
6 - Les sous réseaux

Caractéristiques

- Protocole conçu pour s'adapter à des types de réseaux différents (en fonction de la taille maximale des paquets ⇒ fragmentation).
- IP achemine les paquets (datagrammes) :
  - ✓ indépendamment les uns des autres (pas de notion de connexion, c'est TCP qui s'en charge) ;
  - ✓ sans garantie de remise ;
  - ✓ sans qualité de service (délais de transmission).
- Les routeurs IP font "au mieux" : politique dite *Best Effort*.

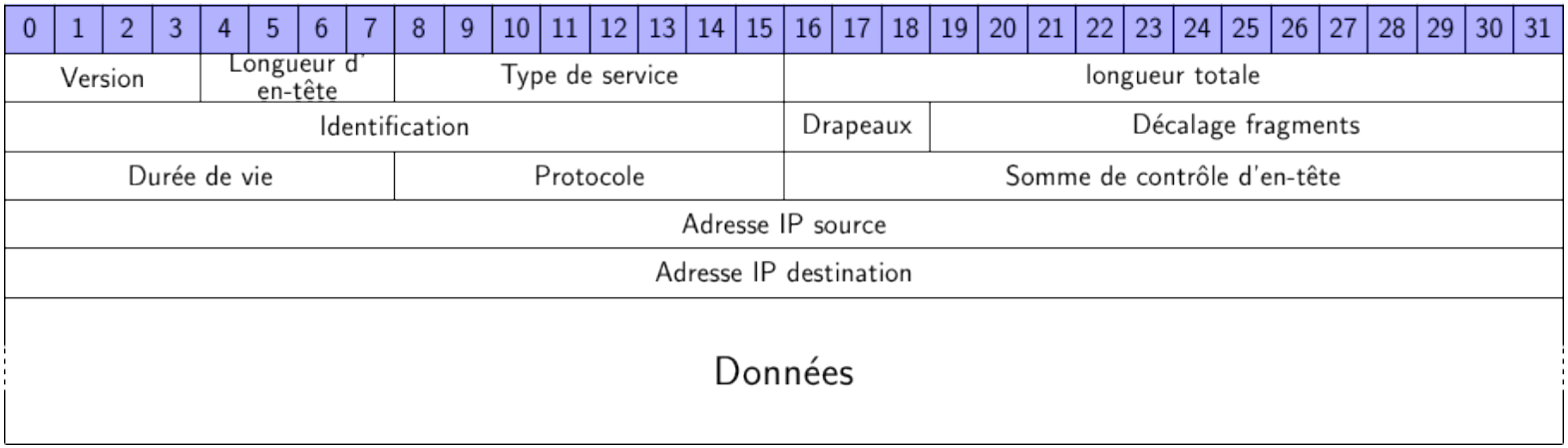
Rôle

1. assurer le routage : les équipements IP ne connaissent que le prochain élément sur le chemin et utilisent des tables de routages.
2. gérer la fragmentation : les réseaux empruntés imposent des restrictions à la taille maximum des paquets : MTU (**M**aximum **T**ransfer **U**nit). :
   - ✓ si le MTU est inférieur à la taille du paquet, il faut le fragmenter ;
   - ✓ la machine destination est responsable du ré-assemblage des fragments.



Le MTU d'Ethernet est de 1500 octets

La trame IP

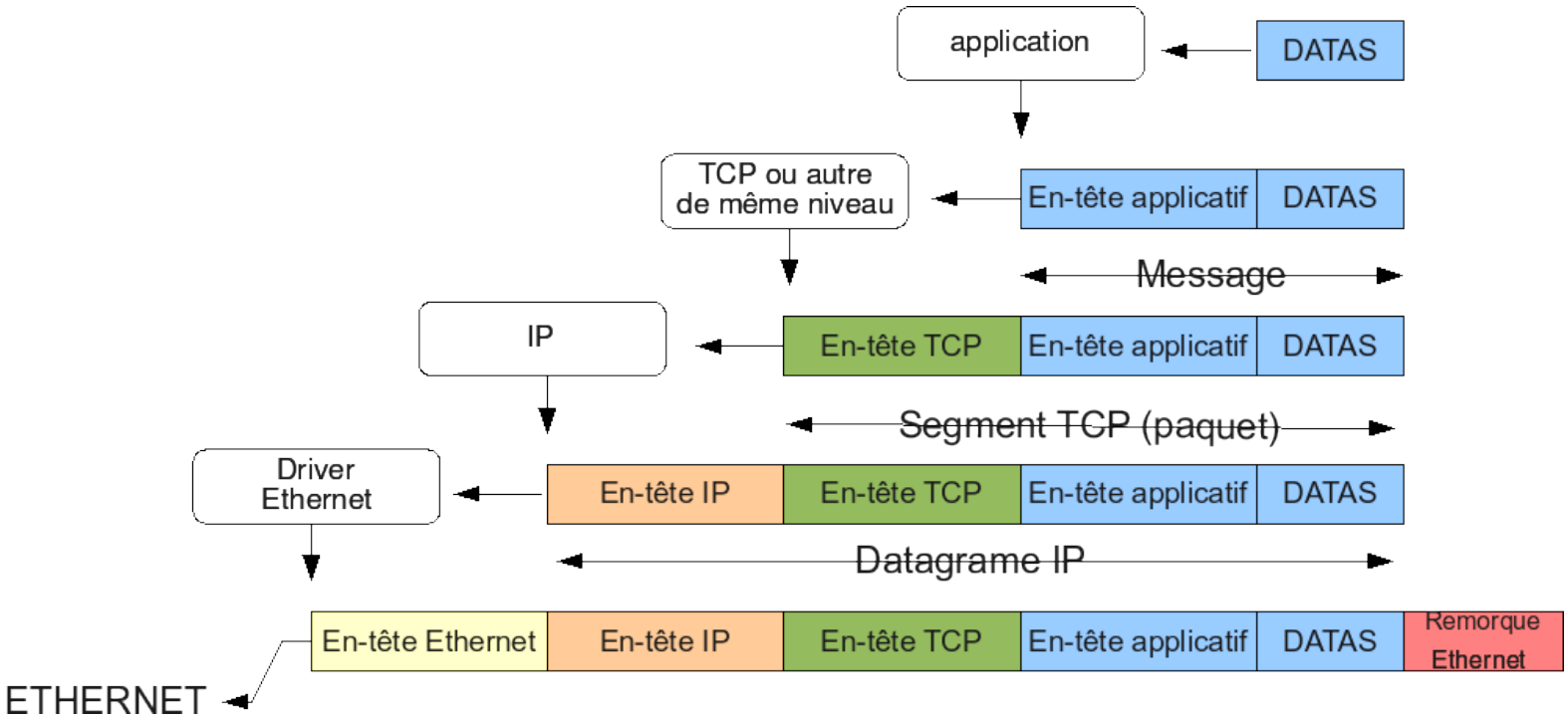


- Version : version du protocole IP que l'on utilise (actuellement on utilise la version 4 IPv4).
- Longueur d'en-tête (IHL) : nombre de mots de 32 bits constituant l'en-tête (la valeur minimale est 5).
- Type de service : indique la façon selon laquelle le datagramme doit être traité.
- Longueur totale : indique la taille totale du datagramme en octets. La taille maximale du datagramme est de 65536 octets.
- Identification, drapeaux et déplacement de fragment sont des champs qui permettent la fragmentation des datagrammes.
- Durée de vie : indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer.
- Protocole : permet de savoir de quel protocole est issu le datagramme (ICMP : 1, IGMP : 2, TCP : 6, UDP : 17).
- Somme de contrôle de l'en-tête : contient une valeur qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission.
- Adresse IP source : adresse IP de la machine émettrice, il permet au destinataire de répondre.
- Adresse IP destination : adresse IP du destinataire du message.

Encapsulation des données

L'encapsulation est un procédé consistant à inclure les données d'un protocole dans un autre protocole.

Internet est basé sur l'Internet Protocol version 4 (IPv4). Ainsi un fragment de données est encapsulé dans un datagramme TCP (ou UDP) qui lui même est encapsulé dans un paquet IP, ce dernier étant envoyé via un protocole de la couche de liaison : Ethernet.



L'adressage

Définition

- Une machine reliée sur Internet prend le nom d'hôte.
- Un hôte possède une adresse IP unique au monde pour chacun de ses accès au service. Cette adresse est indépendante de l'adresse MAC qui est elle aussi unique.
- Adresse IP : mot binaire sur 32 bits associé à un nom de machine.

ATTENTION ! ! !

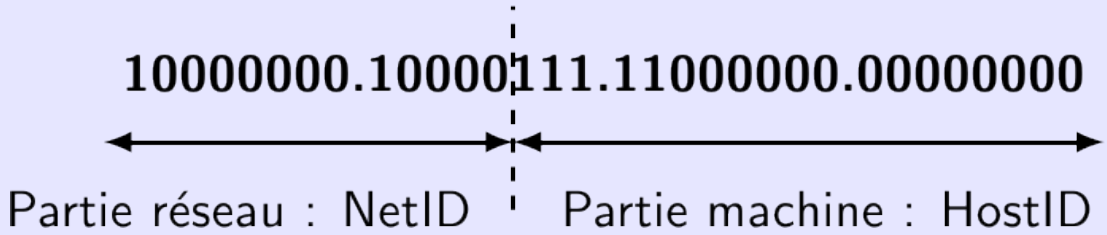
Si une machine possède deux cartes réseaux, chacune devra porter une adresse unique.

L'adressage

L'adresse IP

Une adresse IP se décompose en deux parties distinctes :

- Une partie réseau.
- Une partie machine.



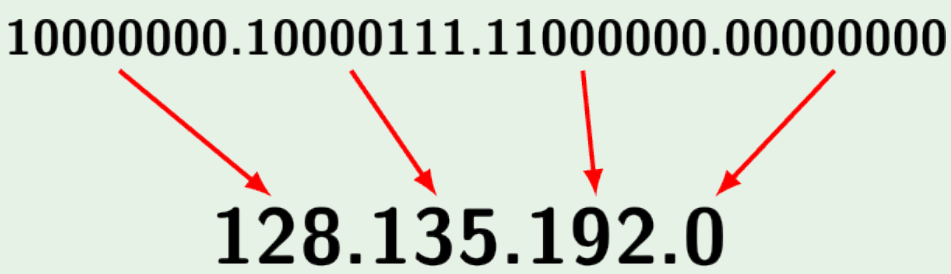
Le nombre de bits affectés à la partie machine dépend de la classe d'adresse IP.

L'adressage

L'adresse IP

Pour que l'adresse IP puisse être identifiée facilement et mémorisable, on découpe les 32 bits en 4 groupes de 8 bits :

⇒ Chaque groupe de 8 bits représentera un entier entre 0 et 255.



L'adressage

Adresses IP particulières

Il existe des adresses qui ne peuvent pas désigner une machine particulière.

- Partie machine entièrement à 0 : désigne l'adresse du réseau lui-même.

01111110.00000000.00000000.00000000 :

- ✓ Les 8 premiers bits désignent donc le numéro du réseau (126)
- ✓ Les 24 restants à 0 désignent le numéro du réseau.

$\Rightarrow$ Réseau : 126.0.0.0

L'adressage

Adresses IP particulières

- Partie machine entièrement à 1 : ⇒ Désigne l'intégralité du réseau. C'est l'adresse *broadcast* ou adresse de diffusion.

01111110.11111111.11111111.11111111 = 126.255.255.255

Il s'agit du réseau précédant (126.0.0.0). Un datagramme portant l'adresse ci-dessus sera diffusé à toutes les machines de ce réseau et non à une machine particulière.

Adresses IP particulières

- Adresse de rebouclage : 127.X.X.X
  - ✓ Les adresses 127.X.X.X ne circulent jamais sur les réseaux.
  - ✓ Ces adresses (127.0.0.1 (*localhost*) ou 127.0.0.0) servent à tester la configuration de TCP/IP sur une machine donnée.

L'adressage

On distingue 4 grandes classes d'adresses IP :

Classe A : (ou "/8" (slash 8))

Une adresse de classe A est définie par un 0 en tête du premier bit. Elle est de la forme :

Les adresses peuvent donc varier de 1.0.0.1 à 126.255.255.254

Ex : 01000000.00000000.00000000.00000001 = 64.0.0.1

$\Rightarrow$ 126 réseaux différents $(2^7 - 2)$ contenant chacun 16 777 214 machines $(2^{24} - 2)$.

L'adressage

Classe A : (ou "/8" (slash 8))

Les réseaux de classe A sont énormes et sont réservés pour les opérateurs ou les multinationales.

Exemples : (d'après IANA : `http://www.iana.org`)

003/8	General Electric Company
009/8	IBM
015/8	Hewlett-Packard Company
017/8	Apple Computer Inc.

L'adressage

Classe B : (ou "/16")

Une adresse de classe B est de la forme :

Les adresses peuvent varier de 128.0.0.1 à 191.255.255.254 $\Rightarrow$ 2^{14} réseaux possibles contenant chacun $2^{16} - 2$ machines.

Classe C : (ou "/24")

Une adresse de classe C est de la forme :

Les adresses peuvent varier de 192.0.0.1 à 223.255.255.254 $\Rightarrow$ Il ne peut y avoir que 254 ordinateurs dans un réseau de classe C.

L'adressage

Classe D : Multicast

Classe particulière :

- Il s'agit d'une classe d'adresse multi-destinataires.
- Réservées aux envois en multi-cast.
- Peuvent être seulement des adresses de destination.

Les adresses peuvent varier de 224.0.0.0 à 239.255.255.255

L'adressage

En résumé

Classe	Nombre de réseaux possibles	Nombre d'ordinateurs possibles sur chaque réseau
A	126	16 777 214
B	16384	65534
C	2 097 152	254

L'adressage

Adresses IP privées

Un certain nombre d'adresses privées ne circulent pas sur les réseaux :

- Adresses IP dans des réseaux locaux fermés.
- Les datagrammes de ces machines ne seront pas propagés à travers les routeurs de sortie sur internet.
- Adresses privées peuvent être utilisées sans rien demander à l'*IANA*.

Exemple d'adresse privées

- 10.0.0.0 à 10.255.255.255 (réseau de classe A ; 10.0.0.0)
- 172.16.0.0 à 172.31.255.255 (adresse de classe B) (IUT)
- 192.168.0.0 à 192.168.255.255. (adresse de classe C) (Réseau chez les particuliers : Freebox, Livebox, ...)

L'adressage

Qui attribue les adresses IP ?

Les adresse IP sont attribuées aux machines de 2 manières :

- Adresses IP fixes données par l'administrateur et rentrées "à la main" lors de la configuration de la machine.
- Adresses IP distribuées automatiquement par un serveur DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol).

le protocole DHCP

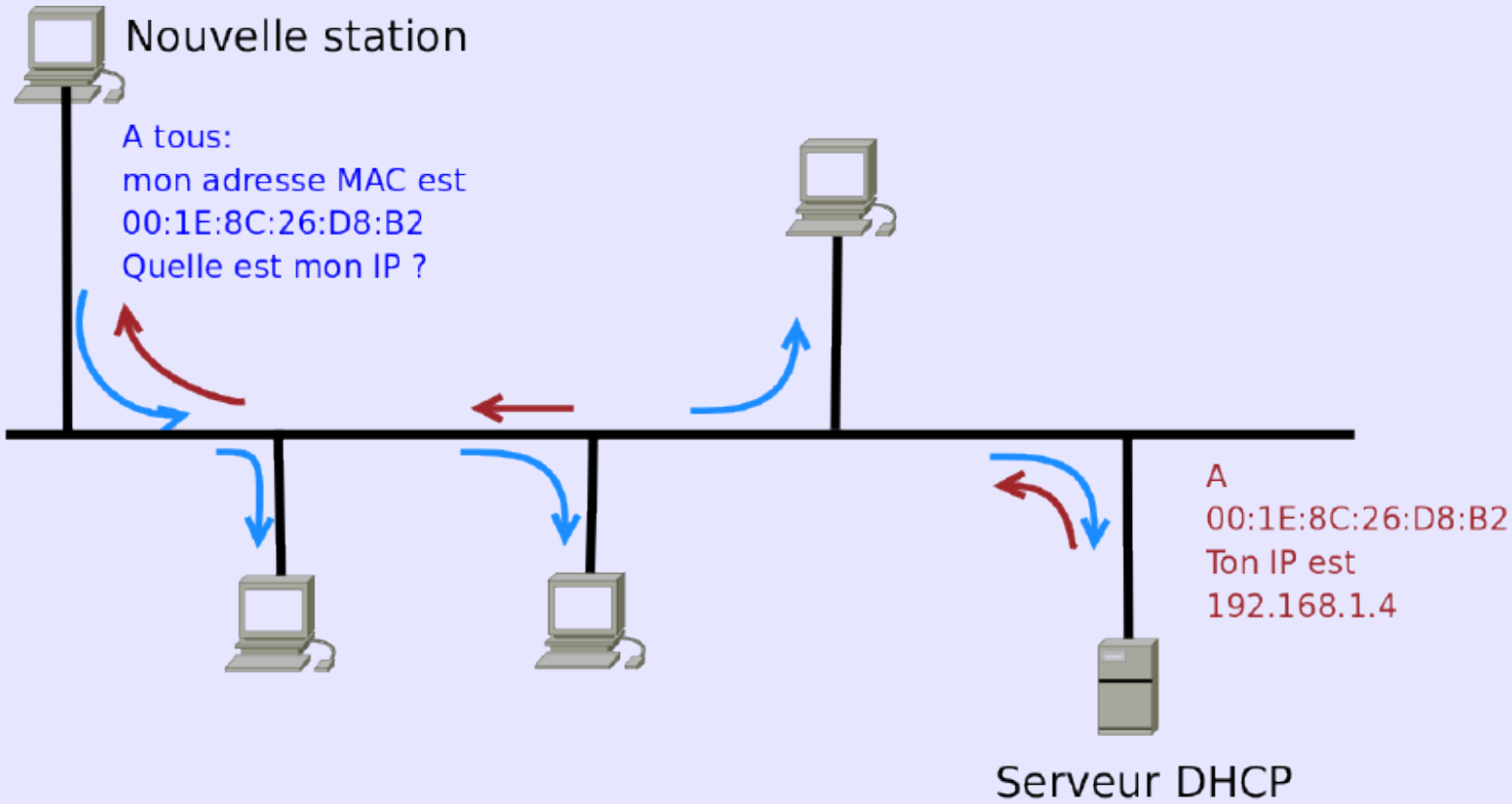
Pour se connecter à un réseau IP, il faut au moins :

- une adresse IP.
- un masque de réseau (netmask).
- l'adresse du routeur de sortie (passerelle ou gateway).

C'est le rôle du serveur DHCP de fournir dynamiquement ces informations.

L'adressage

Principe du DHCP



L'adressage

Comment fait on pour connaître toutes les adresses IP ?

Connaissez vous l'adresse IP de Google ? Sûrement pas.

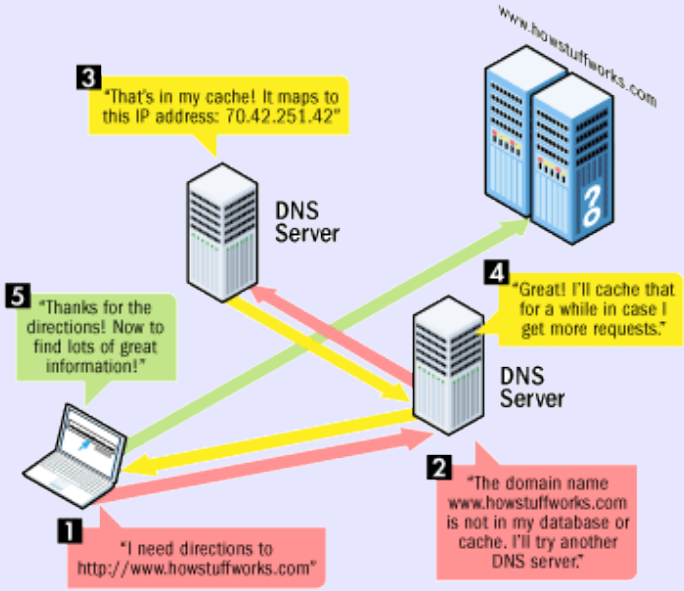
Il faut associé un nom à chaque adresse IP

- Localement, chaque machine peut connaître un nombre d'associations nom-IP.
- A l'échelle d'un réseau, il faut un serveur de nom de domaine.

L'adressage

Principe du DNS (Domain Name System)

- Permet pour un nom d'hôte internet de retrouver l'adresse IP. Ex : `www.iutsd.univ-lorraine.fr` ⇒ IP = `194.199.52.129`.
- Organisation hiérarchique : `sous-domaines.domaine.toplevel`. Ex : `admin.iutsd.u-nancy.fr` ⇒ IP = `194.199.52.119`.
- La résolution d'un nom de domaine se passe également de manière hiérarchique : un serveur DNS doit connaître toutes les adresses de son nom de domaine inférieur.



Le masque de sous réseau

Pour la configuration du protocole IP d'une machine, on doit toujours indiquer :

- L'adresse IP.
- Mais aussi le masque de sous-réseau.

Rôle

Aider le système à séparer dans l'adresse IP la partie réseau de la partie machine

Principe

Un masque de sous-réseau se présente sous la même forme qu'une adresse IP, à la seule différence que **tous les 1 et 0 sont groupés** :

- Les 1 occupent la partie de gauche et indiquent la partie réseau.
- Les 0 occupent la partie de droite et indiquent la partie machine.

Il suffit ensuite de faire un ET logique (&) entre le l'adresse de la machine et le masque de sous réseau pour savoir sur quel réseau se trouve la machine.

Le masque de sous réseau

Exemple

Si l'on considère l'adresse suivante : 139.199.53.7 (adresse de classe B)

Adresse IP : 10001011.11000111.00110101.00000111

Masque : 11111111.11111111.00000000.00000000

La machine est donc disponible sur le réseau 139.199.0.0.

Masques par défaut

Pour chaque classe d'adresse IP, il est possible de déterminer son masque de sous-réseau par défaut de manière automatique :

- Classe A : masque par défaut : 255.0.0.0 (11111111.00000000.00000000.00000000)
- Classe B : masque par défaut : 255.255.0.0 (11111111.11111111.00000000.00000000)
- Classe C : masque par défaut : 255.255.255.0 (11111111.11111111.11111111.00000000)

Plan

V - TCP/IP

1 - Généralités
2 - Le Protocole TCP
3 - Le Protocole UDP
4 - Le protocole IP
5 - Le routage
6 - Les sous réseaux

- Le routage est le processus permettant à un datagramme d'être acheminé vers son destinataire quand celui-ci n'est pas sur le même réseau physique que l'émetteur.
- Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le datagramme.
- Les routeurs forment une structure coopérative afin qu'un datagramme transite de routeur en routeur jusqu'à ce que l'un d'entre eux le délivre à son destinataire.
- On distingue deux types de routages principaux :
  - ✓ routage statique : on entre manuellement une table de routage qui indique la manière d'atteindre les destinataires dans le routeur.
  - ✓ routage dynamique : le routeur gère dynamiquement et construit automatiquement sa table de routage selon des protocoles d'échanges entre routeurs dans le but de construire la meilleure route jusqu'au destinataire. Ex : RIP (Routing Informing Protocol) ou OSPF (Open Shortest Path First)

Principe et organisation

Internet est immense et de nouveaux réseaux apparaissent sans cesse.

$\Rightarrow$ Impossible pour un routeur de connaître le plan total d'internet.

Puissance du protocole IP :

- Une machine n'a pas besoin de connaître le plan exact du réseau mondial.
- Seule la connaissance des machines proches d'un routeur suffit.

Deux formes de remise des datagrammes :

- Remise directe : transfert du datagramme d'un ordinateur à un autre (ordinateurs faisant partie du même réseau ou sous-réseau).
- Remise indirecte : les datagrammes doivent passer par au moins un routeur.

Le routage statique

Définition

On parle de routage statique lorsque dans chaque routeur se trouvent des indications de routage fixes.

Problème

Si le réseau est modifié, le routage statique doit être mis à jour.

Table de routage

Le rôle de la table de routage est de déterminer le routeur suivant en fonction de la destination à atteindre.

$\Rightarrow$ Tables à deux colonnes : **Destination** et **Gateway** (passerelle).

Le routage statique

Table de routage

La table de routage répond à la question :

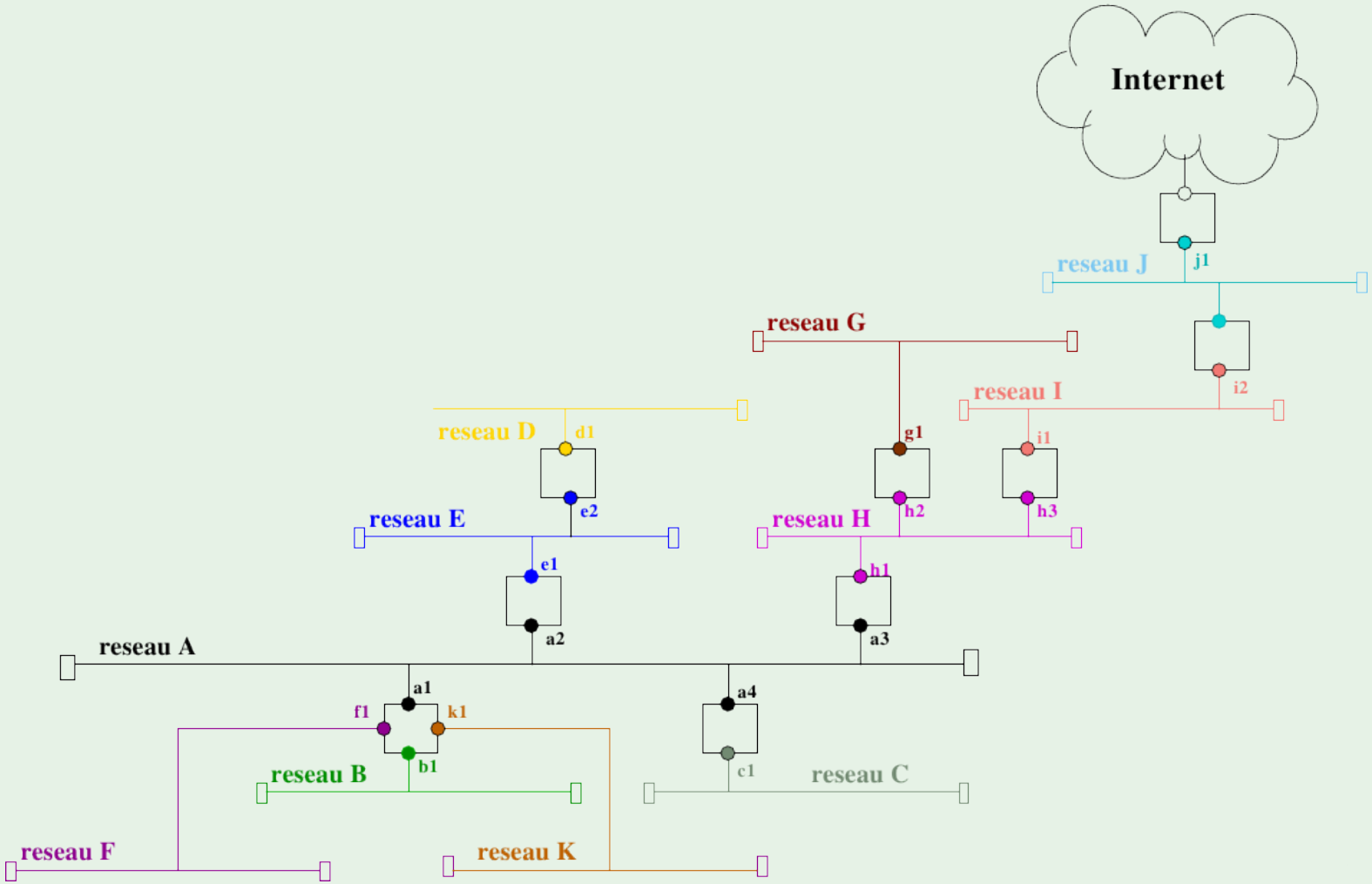
Pour atteindre la "destination" quel routeur dois-je emprunter ?

$\Rightarrow$ Ici, la destination ne correspond pas à une machine en particulier mais à un réseau. (la taille serait bien plus importante.)

La table de routage permet à une machine de savoir vers quelle adresse **locale** (c'est à dire sur un réseau sur lequel est reliée une de ses interfaces) diriger son paquet en fonction de son adresse de destination.

Le routage statique

Exemple de routage statique



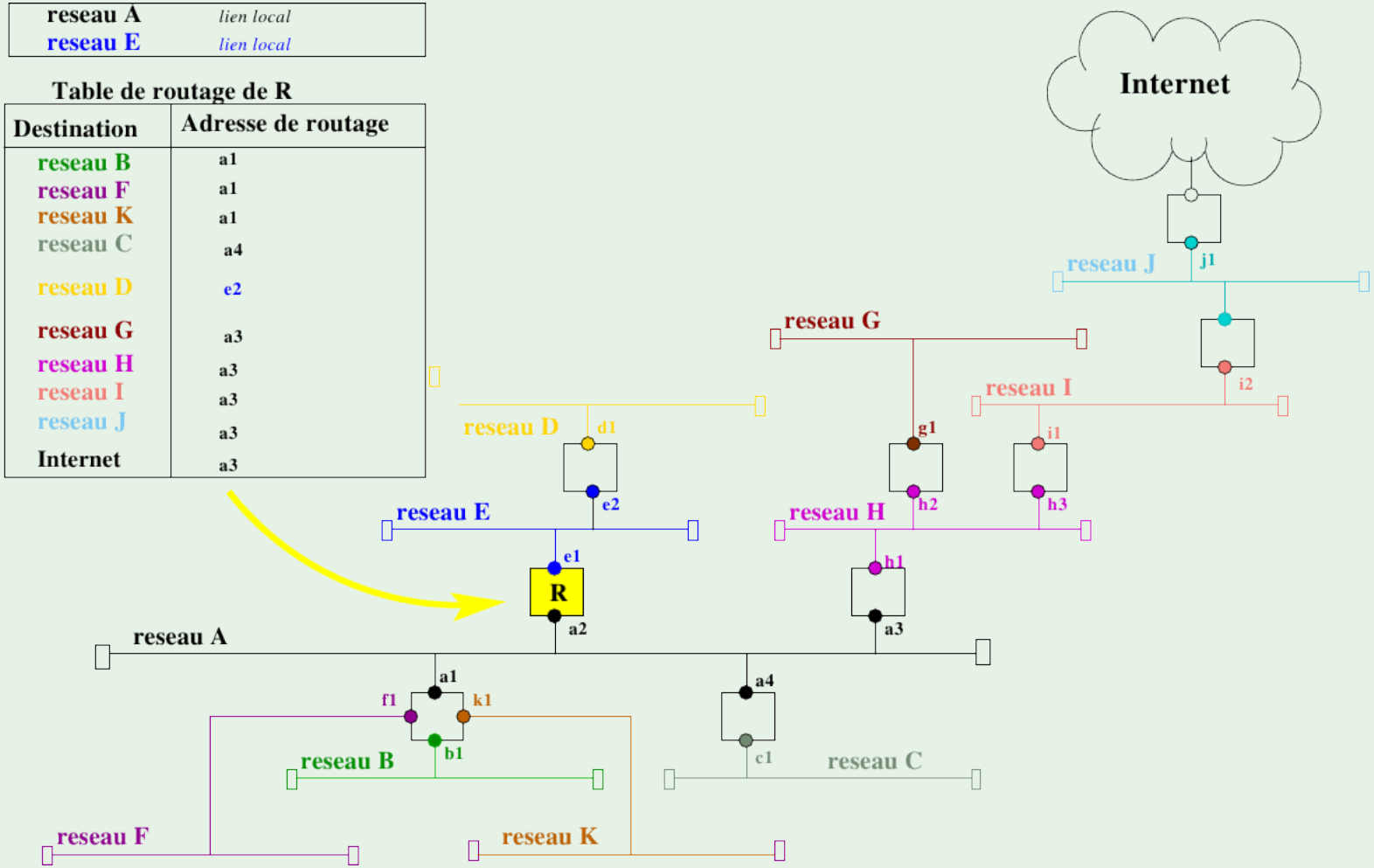
Le routage statique

Exemple de routage statique

reseau A	*lien local*
reseau E	*lien local*

Table de routage de R

Destination	Adresse de routage
reseau B	a1
reseau F	a1
reseau K	a1
reseau C	a4
reseau D	e2
reseau G	a3
reseau H	a3
reseau I	a3
reseau J	a3
Internet	a3



Le routage statique

L'entrée default

L'entrée par défaut **default** (parfois appelée 0.0.0.0 de masque 0.0.0.0) désigne le routeur vers lequel il faut aller dans le cas où le réseau destination n'est pas une des destination réseau listée explicitement, ni n'est sur le lien local.

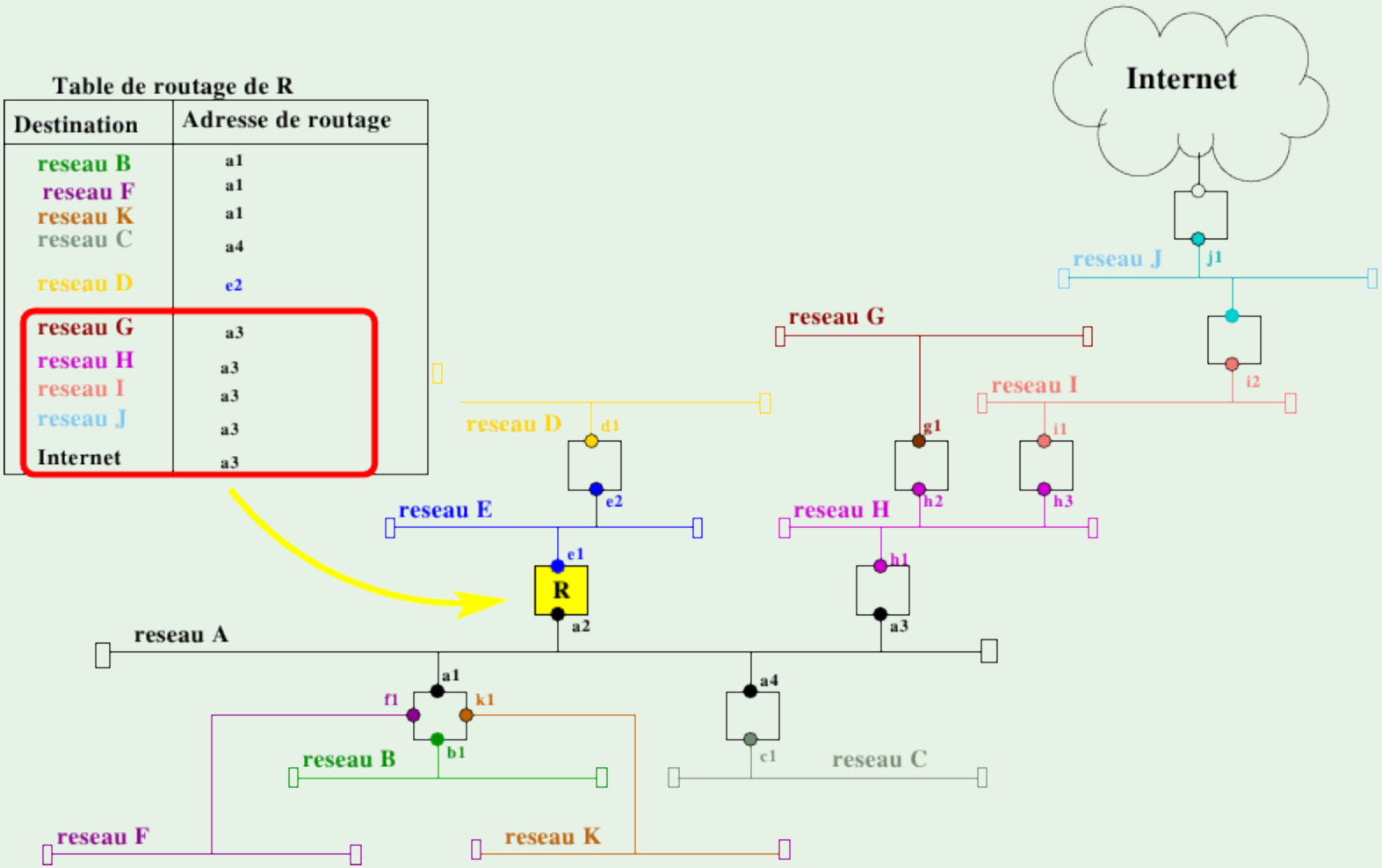
Il ne peut y avoir qu'une seule entrée par défaut.

Le routage statique

Exemple de routage statique

Table de routage de R

Destination	Adresse de routage
reseau B	a1
reseau F	a1
reseau K	a1
reseau C	a4
reseau D	e2
reseau G	a3
reseau H	a3
reseau I	a3
reseau J	a3
Internet	a3

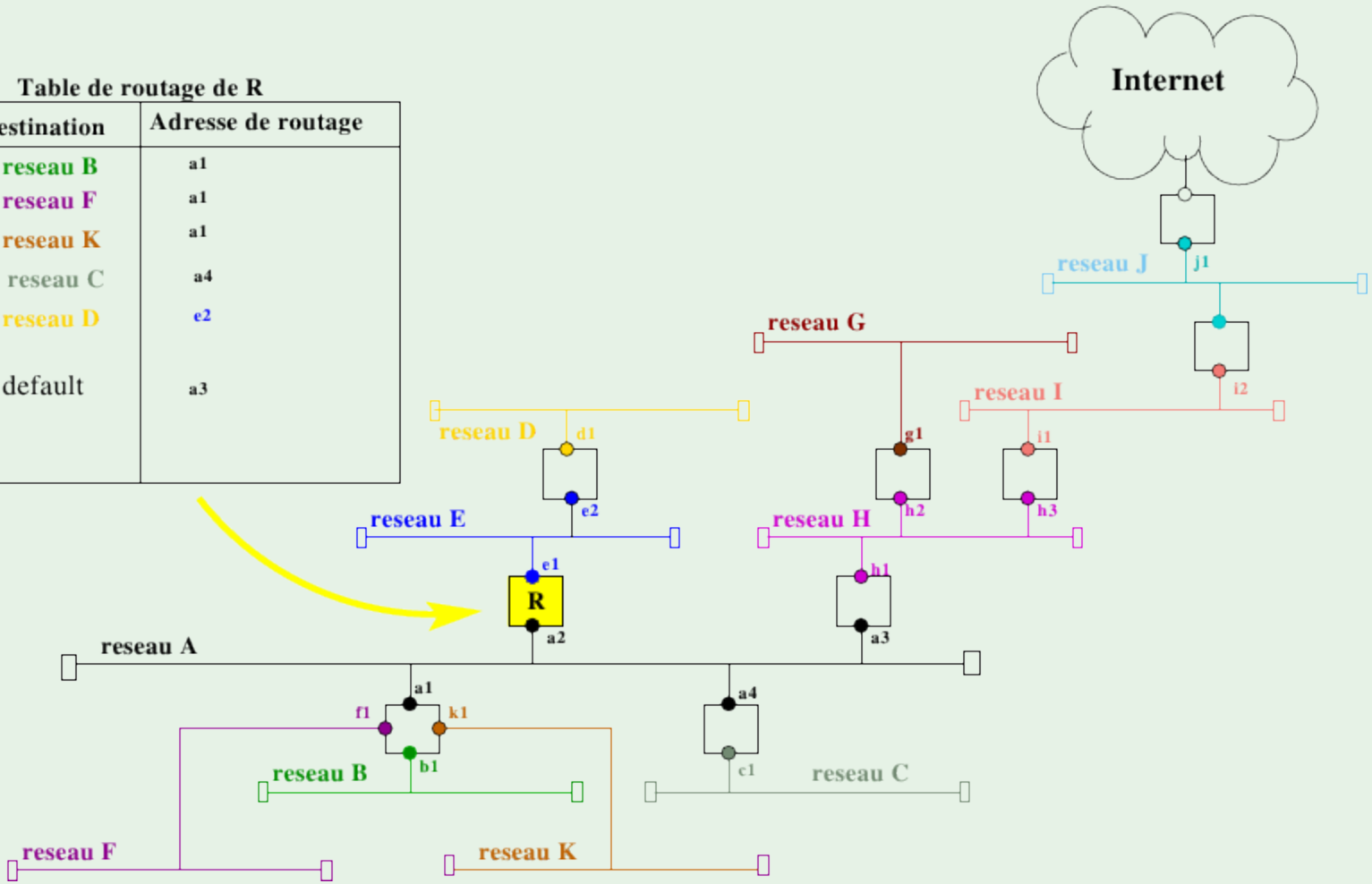


Le routage statique

Exemple de routage statique

Table de routage de R

Destination	Adresse de routage
reseau B	a1
reseau F	a1
reseau K	a1
reseau C	a4
reseau D	e2
default	a3



Le routage statique

Exemple de routage statique

Les 4 réseaux suivants sont séparés par 3 routeurs

Pour le routeur B :

Pour atteindre les ordinateurs sur le réseau :	Router vers cette adresse :
20.0.0.0	Remise directe
30.0.0.0	Remise directe
10.0.0.0	20.0.0.1 (Remise indirecte)
40.0.0.0	30.0.0.2 (Remise indirecte)

Le routage statique

Exemple de routage statique

Table de routage réelle :

Destination	Gateway	FLAG
127.0.0.1	127.0.0.1	UH
20.0.0.2	127.0.0.1	UH
30.0.0.1	127.0.0.1	UH
20.0.0.0	20.0.0.2	U
30.0.0.0	30.0.0.1	U
40.0.0.0	30.0.0.2	UG
DEFAULT	20.0.0.2	UG

Flag :

- U = la route est en service. (in Use)
- G = la route est indirecte et doit passer par un autre routeur. (Gateway)
- H = indique une remise directe (Host)

Le routage dynamique

Pourquoi du routage dynamique ?

- Dans un environnement complexe, la mise en œuvre du routage statique est souvent difficile à maintenir.
- La mise en place d'un mécanisme de routage dynamique permet de faciliter les mises à jour.

Principe de fonctionnement général

- Chaque routeur diffuse la liste des réseaux sur lesquels il est connecté.
- Chaque routeur met à jour sa table de routage à partir des informations reçues depuis les autres.

Mise en œuvre

- Démons de routage.
- Suite logicielle de routage
- Routeur matériel dédié

Le routage dynamique

Protocoles de routage

Le protocole de routage consiste à définir comment sont échangées les informations de routage, et donc à :

- découvrir les autres routeurs du réseau.
- construire les tables de routage.
- maintenir les tables de routage à jour

Les principaux protocoles sont :

- RIP (Routing Information Protocol) : protocole à vecteur de distance.
- OSPF (Open Shortest Path First) : protocole de routage à état de lien.
- IS-IS ((Intermediate System to Intermediate System) : multi-protocole de routage à état de lien.
- IGRP/EIGRP : protocole propriétaire CISCO.

Le routage dynamique

Ex : protocole RIP

1. Chaque routeur annonce périodiquement (30s) tous ses réseaux et le nombre de sauts pour y aller.
2. Chaque machine écoute les annonces des passerelles et actualise sa table de routage.
3. Si au bout d'un certain temps (3mn=180s), un réseau n'est plus annoncé il est supprimé de la table de routage.

Quand un routeur reçoit l'information périodique, il ne met à jour sa table que si une distance plus courte vers une destination est trouvée ou si une nouvelle destination est annoncée.

Plan

V - TCP/IP

1 - Généralités
2 - Le Protocole TCP
3 - Le Protocole UDP
4 - Le protocole IP
5 - Le routage
6 - Les sous réseaux

Création d'un sous-réseau

Il existe 2 façons de créer des sous-réseaux :

1. A partir d'un changement du masque de sous-réseau.
2. Par l'intermédiaire d'un VLAN.

Changement de masque

L'idée consiste à changer un ou plusieurs bits du masque de sous réseau de façon à obtenir un champ d'identification du réseau plus grand.
Supposons que l'on désire que les deux premiers bits du troisième octet permettent de désigner également le réseau. Le masque à appliquer sera alors :

$$11111111.11111111.11000000.00000000 \Rightarrow 255.255.192.0$$

Si l'on applique ce masque sur l'adresse suivante : 139.199.53.7 (adresse de classe B)

Adresse IP :	10001011.11000111.00110101.00000111
Masque :	11111111.11111111.11000000.00000000

La machine est donc disponible sur le réseau 139.199.0.0.

Changement de masque

En réalité il y a 4 cas de figures possibles pour le résultat du masquage d'une adresse IP d'un ordinateur du réseau 139.199.0.0 :

- Si les deux premiers bits du troisième octet sont 00, le résultat du masquage est 34.199.0.0
- Si les deux premiers bits du troisième octet sont 01, le résultat du masquage est 34.199.64.0
- Si les deux premiers bits du troisième octet sont 10, le résultat du masquage est 34.199.128.0
- Si les deux premiers bits du troisième octet sont 11, le résultat du masquage est 34.199.192.0

Ce masquage divise donc un réseau de classe B (pouvant admettre 65 534 ordinateurs) en 4 sous-réseaux (d'où le nom de masque de sous-réseau) pouvant admettre 2^{14} ordinateurs, c'est-à-dire 16 384 ordinateurs.

Création de VLAN

Définition

- VLAN : **V**irtual **L**ocal **A**rea **N**etwork (Réseau local virtuel)
- Regroupement de machines de façon logique et non physique.

Il existe plusieurs types de VLAN :

- VLAN de niveau 1 : le réseau virtuel est défini en fonction des ports de raccordement sur le commutateur.
- VLAN de niveau 2 : le réseau virtuel est défini en fonction des adresses MAC.
- VLAN de niveau 3 :
  - ✓ VLAN par sous-réseau selon les IP.
  - ✓ VLAN par protocole.

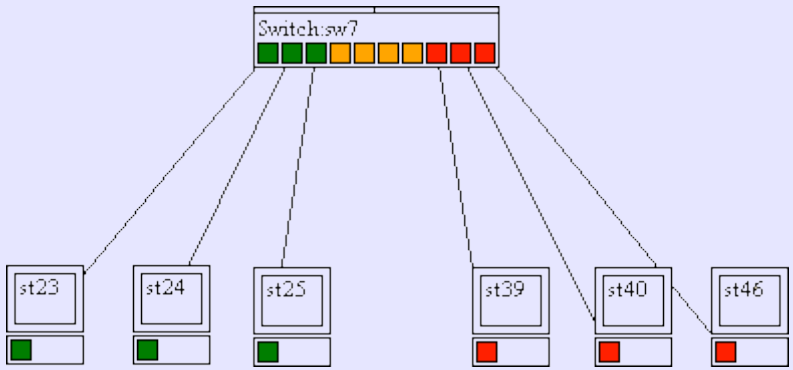
Création de VLAN

Intérêt des VLAN

L'intérêt est de séparer les ports d'un switch pour créer des réseaux différents. Ils ne pourront donc plus communiquer ensemble.

Cela revient donc à "couper" le switch en plusieurs morceaux, comme si l'on avait plusieurs switchs.

En plus de la sécurité offerte par la séparation des réseaux, cela apporte de la facilité de configuration. Si on veut qu'un port passe d'un VLAN à un autre, il suffit de le configurer sur le switch.



Plan

VI - Wi-Fi

1 - Généralités
2 - Les normes 802.11x
3 - Structure des réseaux Wi-Fi
4 - Transmission en Wi-Fi
5 - Sécurité et Wi-Fi

Introduction

Les réseaux sans fils permettent de relier très facilement des équipements (ordinateur, routeur, smartphone, ...) distants de quelques dizaines de mètres, en évitant d'utiliser de lourds aménagements comme avec les réseaux filaires.

Wi-Fi signifie **Wi**reless **Fi**delity. La norme associée au Wi-Fi est la 802.11 et le type de réseau généralement associé est le WLAN (**W**ireless **L**ocal **A**rea **N**etwork).

Les matériels certifiés par la Wi-Fi Alliance bénéficie de la possibilité d'utiliser le logo.

Wi-Fi et OSI

La norme 802.11 définit les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques.

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique.

- La couche physique (couche 1) propose trois types de codages de l'information : DSSS, FHSS, Infrarouges.
- la couche liaison de données (couche 2) propose deux sous-couches :
  - ✓ le contrôle de la liaison logique (Logical Link Control, ou LLC) ;
  - ✓ le contrôle d'accès au support (Media Access Control, ou MAC).

Plan

VI - Wi-Fi

1 - Généralités
2 - Les normes 802.11x
3 - Structure des réseaux Wi-Fi
4 - Transmission en Wi-Fi
5 - Sécurité et Wi-Fi

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps.

Des révisions ont été apportées à la norme originale afin d'optimiser le débit ou de préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité (systèmes identiques).

Les principales révisions sont les suivantes :

Norme	Description
802.11a	▶ Débit : 54Mbps théoriques, 30Mbps réels. ▶ Bande de fréquence : 5GHz. ▶ 8 canaux disponibles.
802.11b	▶ Débit : 11Mbps théoriques, 6Mbps réels. ▶ Bande de fréquence : 2.4GHz. ▶ 3 canaux disponibles.

Norme	Description
802.11f	Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement.
802.11g	▶ Débit : 54Mbps théoriques, 30Mbps réels. ▶ Bande de fréquence : 2.4GHz. ▶ Compatibilité ascendente avec la 802.11b.
802.11i	Amélioration de la sécurité des transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11n	▶ Débit : 300Mbps théoriques, 100Mbps réels. ▶ Bande de fréquence : 2.4GHz ou 5GHz. ▶ Utilisation du MIMO.

Portée de la norme 802.11b

Débit théorique	Portée en intérieur	Portée en extérieur
11Mbps	50m	200m
5.5Mbps	75m	300m
2Mbps	100m	400m
1Mbps	150m	500m

Portée de la norme 802.11n

Débit théorique	Portée en intérieur	Portée en extérieur
300Mbps	70m	125m

Portée de la norme 802.11g

Débit théorique	Portée en intérieur	Portée en extérieur
54Mbps	27m	75m
48Mbps	29m	100m
36Mbps	30m	120m
24Mbps	42m	140m
18Mbps	55m	180m
12Mbps	64m	250m
9Mbps	75m	350m
6Mbps	90m	400m

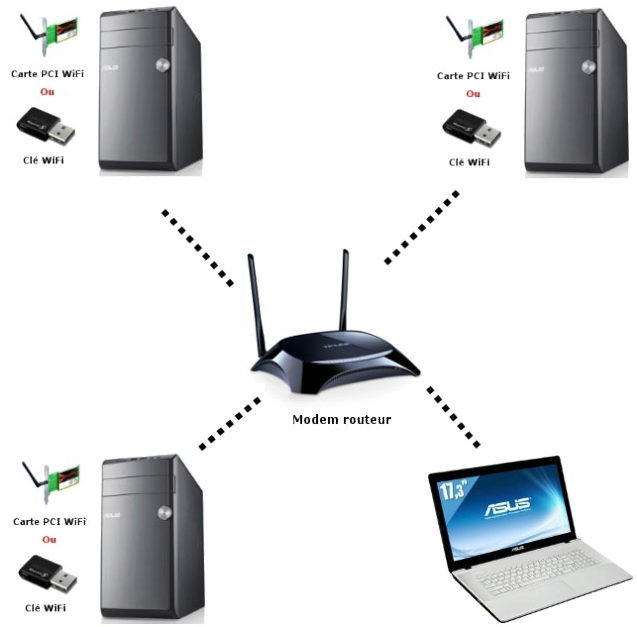
Plan

VI - Wi-Fi

1 - Généralités
2 - Les normes 802.11x
3 - Structure des réseaux Wi-Fi
4 - Transmission en Wi-Fi
5 - Sécurité et Wi-Fi

Le mode Infrastructure

En mode infrastructure chaque ordinateur se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé ensemble de services de base (BSS : **B**asic **S**ervice **S**et) et constitue une cellule.

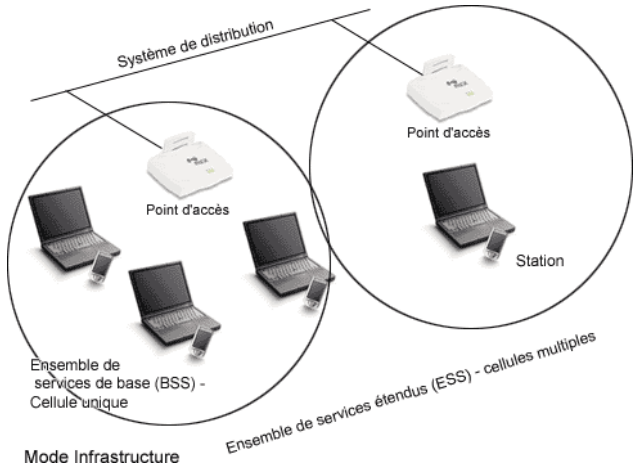


Chaque BSS est identifié par un BSSID. Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.

Le mode Infrastructure

Il est possible de relier plusieurs points d'accès entre eux par une liaison appelée système de distribution pour constituer un ensemble de services étendu (ESS : **E**xtended **S**ervice **S**et). Le système de distribution peut être aussi bien un réseau filaire, qu'un réseau sans fil. L'ESS est identifié par un ESSID.

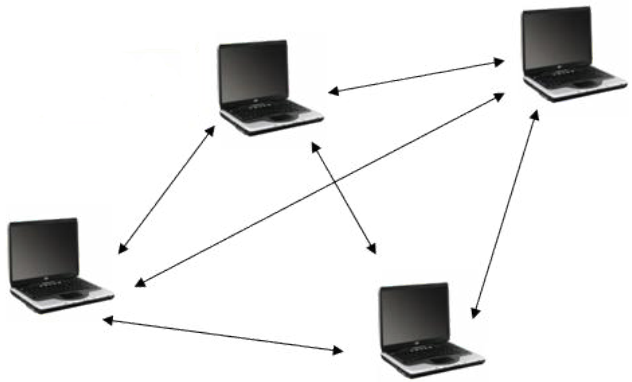
Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine change de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès s'échangent les machines de façon transparentes (roaming).



Le mode Ad-hoc

En mode ad hoc les machines sans fil se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès.

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (IBSS : **I**ndependant **B**asic **S**ervice **S**et). Il possède également un ID.



Plan

VI - Wi-Fi

1 - Généralités
2 - Les normes 802.11x
3 - Structure des réseaux Wi-Fi
4 - Transmission en Wi-Fi
5 - Sécurité et Wi-Fi

Dans un réseau local Ethernet classique, la méthode d'accès utilisée par les machines est le CSMA/CD (voir chapitre sur Ethernet).

Dans un environnement sans fil ce procédé n'est pas possible car deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée. Donc la norme 802.11 propose un protocole similaire appelé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Principe du CSMA/CA

Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusés de réception réciproques entre l'émetteur et le récepteur :

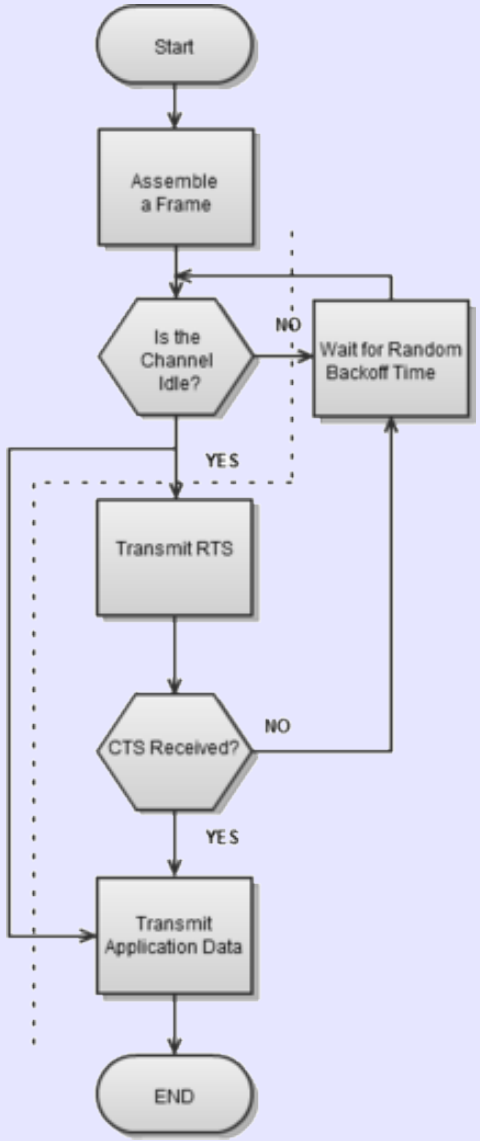
- La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée.

Principe du CSMA/CA

- Si le réseau est libre pendant un temps donné, alors la station peut émettre. La station transmet un message appelé Ready To Send (RTS) contenant le volume des données qu'elle va émettre et sa vitesse de transmission. Le récepteur (point d'accès) répond un Clear To Send (CTS), puis la station commence l'émission des données.
- A la fin de la réception, le récepteur envoie un accusé de réception (ACK).

Par conséquent, toutes les stations voisines de celle qui émet patientent pendant un temps qu'elle considère être celui nécessaire à la transmission de son volume d'information à émettre à la vitesse annoncée $\Rightarrow$ **Les collisions sont donc évitées**.

Algorithme du CSMA/CA



Plan

VI - Wi-Fi

1 - Généralités

2 - Les normes 802.11x

3 - Structure des réseaux Wi-Fi

4 - Transmission en Wi-Fi

5 - Sécurité et Wi-Fi

Les ondes radio-électriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande (et en 3D ! ! !).

La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé. Cela facilite le piratage car on peut diposer d'une prise réseau "sur le trottoir".

$\Rightarrow$ **Il faut donc sécurisé le réseau à l'aide de clés de cryptage.**

La clé WEP

Caractéristiques

- **W**ired **E**quivalent **P**rivacy.
- Codage possible sur 64, 128 et 256 bits. Sur chaque codage, 24 bits sont réservés pour le vecteur d'initialisation.
- Algorithme de chiffrement par flot RC4.

Principe

Le protocole WEP utilise une clé d'une longueur de 64 à 256 bits dont 24 ne sont pas utilisés pour le chiffrement. Cela fait une clé, si on la compare à un mot, d'une longueur de 5 à 29 caractères. La majorité des clés est composée de 13 caractères.

La clé WEP

Principe

L'algorithme de chiffrement possède une grande faiblesse exploitable très facilement. En effet, ce dernier nécessite que les morceaux de la clé WEP circulent de temps à autres sur le réseau. La raison est que l'algorithme doit être initialisé à chaque échange pour ne pas utiliser deux fois la même clé. De fait une partie de la clé (les 24 bits en question) est utilisée comme élément d'initialisation (vecteur d'initialisation) et celui-ci n'est pas chiffré.

Au bout d'un moment, si quelqu'un écoute tous les échanges, il aura obtenu suffisamment d'éléments pour reconstruire la clé sans la connaître au préalable. Pour cette raison la clé WEP ne doit absolument plus être utilisée sur les équipements Wi-Fi aujourd'hui.

Il existe actuellement des logiciels capables de casser une clé WEP en quelques secondes

La clé WPA et WPA2

Caractéristiques

- **W**i-Fi **P**rotected **A**ccess.
- Basé sur le même algorithme que le WEP mais enrichi d'un algorithme de cryptage robuste : TKIP qui permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes.
- Nécessite une *passphrase* au départ d'au moins 32 caractères.

La clé WPA et WPA2

Principe

Le protocole WPA offre une protection d'un niveau bien supérieur à WEP. Il utilise pourtant le même algorithme de chiffrement et est basé sur le même principe de vecteur d'initialisation.

En revanche le TKIP (Temporal Key Integrity Protocol) a été ajouté, permettant ainsi une permutation plus importante des clés sans que le vecteur d'initialisation ne puisse être reconstitué de manière utile. Cela permet d'utiliser une clé alphanumérique normale d'une longueur d'au moins 32 caractères. Ce qui offre un niveau de protection tout à fait acceptable.

Le protocole WPA2 quant à lui utilise un algorithme de chiffrement beaucoup plus puissant, utilisé dans le cryptage des documents sensibles et possédant une clé très forte. Il s'agit de la dernière norme du protocole WPA permettant de protéger votre réseau WLAN.