



Introduction aux réseaux

Présentation : Ce module présente les éléments constituant un système de communication. Il permet d'associer les fonctionnalités aux divers sigles et acronymes communément utilisés dans le domaine des réseaux informatiques.

Prérequis : néant

Première version : 09/09/2015


Version actuelle : 1.31(E)-N du 11/01/2021

Auteur : Jean BUZIT

Société : I-S-I, 2 bis Rue Waldeck Rousseau, 29200 BREST

Propriété : Ce document est uniquement destiné aux formations assurées par la société I-S-I, et ne peut être reproduit pour aucun autre usage.





Cette page a été
laissée vierge
intentionnellement.

SOMMAIRE

Avant-propos

Présentation	i
Prérequis	i
Première version	i
Version actuelle	i
Auteur	i
Société	i
Propriété	i

1) Introduction	1
1.1) Bref historique	1
1.2) Un système de communication pour quoi faire ?	2
1.3) Périphériques finaux {end devices}	2
1.4) Périphériques intermédiaires {intermediary device}	2
1.5) Les supports {médium} de communication	2
1.6) Système de communication	2
1.7) Réseaux clients serveurs et pair à pair {égal à égal, poste à poste, peer to peer, P2P} ...	3
1.7.1) Réseaux clients serveur	3
1.7.2) Réseaux pair à pair {égal à égal, poste à poste, peer to peer, P2P}	3
1.8) LAN, WLAN, WAN, MAN, et PAN	4
1.9) Internet, intranet, extranet	5
1.10) Connexion à Internet des particuliers et des petites entreprises	5
1.11) Connexion à Internet des entreprises	5
1.12) Les réseaux convergents {converged network, converging network}	6
1.13) Les réseaux fiables {reliable network}	6
2) Les organismes de normalisation	7
2.1) Standards {de facto standard} et normes {de jure standard}	7
2.2) Les organismes de normalisation	7
3) Le modèle OSI {Open Systems Interconnection} ISO / IEC 7498 	8
3.1) Historique et objectifs	8
3.2) Les 7 couches OSI	9
3.3) La communication de niveau à niveau	10
3.4) La fragmentation ou segmentation	10
3.5) L'encapsulation	11
4) Modèle OSI : la couche physique {physical layer, L1}	13
4.1) Fonctionnalités de la couche physique	13
4.2) La structure physique du réseau ou topologie physique	14
4.3) Transmission Simplex, Half-duplex, Full-duplex	14
4.4) Structures et caractéristiques des médias {support}	15
4.4.1) Les câbles coaxiaux RG {Radio Grade} et les connectiques associées	15
4.4.2) Les paires torsadées {Twisted Pair} et les connectiques associées	17
4.4.3) Câbles à 4 paires torsadées à connectique 8P8C {RJ45}	18
4.4.4) Câbles à 1 ou 2 paires torsadées et connecteurs RJ11 et RJ14	22

4.4.5)	La fibre optique	23
4.4.6)	Les connecteurs de la famille SFP	25
4.5)	Câblage de raccordement, horizontal et vertical	27
4.6)	Recette d'un câblage	28
4.7)	Représentation des bits sur le support	30
4.8)	Transmission numérique {digital}, signal bande de base {Baseband}	30
4.8.1)	Principe : codage en ligne réalisé par un transcodeur	30
4.8.2)	Codages en ligne classiques (transcodage bit par bit)	30
4.8.3)	Codages en ligne plus récents (transcodage tertiaires et quaternaires)	32
4.8.4)	Codage complet ou en bloc nB/mB, avec $n < m$	33
4.8.5)	Encodage de trame	34
4.9)	Codage analogique : transmission large de base {broadband}	34
4.9.1)	Débit et rapidité de modulation	35
4.10)	Autres caractéristiques de la couche physique.....	35
4.10.1)	Transmission série et transmission parallèle.....	35
4.10.2)	Multiplexage	36
4.10.3)	Transmission série synchrone et asynchrone	36
4.10.4)	Equipements de traitements de données et de circuits de données	36
4.11)	Extension du réseau par la couche physique et matériels associés	37
4.11.1)	Pourquoi étendre un réseau par le niveau 1 ?	37
4.11.2)	Extension d'une topologie en bus : répéteur {repeater}.....	37
4.11.3)	Extension d'une topologie en étoile : concentrateur {hub}.....	38
4.11.4)	Concentrateur : Topologie physique en étoile, topologie logique en bus.....	38
5)	Modèle OSI : la couche liaison de données {data link layer, L2}.....	38
5.1)	Fonctionnalités de la couche liaison de données	38
5.2)	La sous-couche MAC {Media Access Control}	39
5.2.1)	Trame {frame}.....	39
5.2.2)	Adresse MAC / physique / BIA des protocoles de réseaux locaux	40
5.2.3)	Modification des adresses MAC en RAM	40
5.2.4)	Adresse MAC de diffusion {broadcast} et de multidiffusion {multicast}	42
5.2.5)	Adresse MAC de monodiffusion {unicast}	43
5.2.6)	Résumé adresses MAC de destination de type unicast, broadcast et multicast	43
5.3)	Contrôle d'accès au support/ média {media access control}	44
5.4)	La sous-couche LLC {Logical Link Control, IEEE 802.2}	45
5.5)	Protocoles LANs : 802.3 et Ethernet, 802.5 et Token Ring / 802.2.....	45
5.6)	Autres protocoles de liaison de données.....	46
5.7)	Choix d'un protocole de liaison de données	46
5.8)	Extension du réseau par la couche liaison de données et matériels associés	46
5.8.1)	Pourquoi étendre un réseau par le niveau 2 ?	46
5.8.2)	Extension d'une topologie en bus : pont {bridge}	47
5.8.3)	Avantages des ponts {bridge} sur les répéteurs {repeater}.....	48
5.8.4)	Extension d'une topologie physique en étoile : commutateur {switch}	48
5.8.5)	Commutateur : topologie physique en étoile, topologie logique point à point.....	48
5.8.6)	Avantages des commutateurs {switch} sur les concentrateurs {hub}	49
5.8.7)	Domaine de collision limités par les ponts et les commutateurs	49
5.8.8)	Micro-segment reliant 2 ports CSMA full-duplex : plus aucune collision.....	50
5.9)	Encapsulation et PDU de la couche liaison de données.....	50
6)	Protocole Ethernet ou 802.3.....	50
6.1)	Ethernet ou 802.3 ?	50
6.2)	Principes de base.....	50
6.3)	La topologie, le support, le codage, le temps bit.....	51
6.4)	La synchronisation	51
6.5)	La politique d'accès au médium CSMA/CD.....	51

6.6)	Les trames Ethernet DIX et 802.3.....	52
6.6.1)	Trame Ethernet/802.3 générique	52
6.6.2)	La trame Ethernet DIX (type I ou II)	53
6.7)	La trame IEEE 802.3	53
6.8)	Adresses des trames Ethernet et 802.3.....	54
6.9)	Ethernet 10 Mbit/s sur bus	54
6.9.1)	10Base5 : Yellow Ethernet {Ethernet jaune}	54
6.9.2)	10Base2 : Thin Ethernet {Thinnet, Cheapernet, Ethernet Fin}	54
6.10)	10Base-T : Ethernet 10 Mbps sur paires torsadées non blindées {UTP}	55
6.10.1)	Caractéristiques	55
6.11)	Ethernet 10Mbit/s sur fibre optique	55
6.12)	Passage à Ethernet 100 Mbit/s {Fast Ethernet}.....	55
6.13)	Ethernet 100 Mbit/s sur paires torsadées UTP {100Base-T}	55
6.13.1)	100Base-TX.....	56
6.13.2)	Autres technologies 100 Mbit/s sur paires torsadées.....	56
6.14)	Ethernet 100 Mbit/s sur fibre optique	56
6.14.1)	100Base-FX.....	56
6.14.2)	100Base-SX.....	56
6.14.3)	Autres technologies 100Mbit/s sur fibre optique	56
6.15)	Ethernet Gigabit {1 Gbit/s, 1000 Mbit/s} sur câbles en cuivre.....	56
6.15.1)	1000Base-TX : Ethernet Ggigabit sur paire torsdée UTP cat 6	56
6.15.2)	1000Base-T : Ethernet Gigabit sur paire torsadée UTP cat 5	57
6.15.3)	1000Base-CX : Giga Ethernet sur câble blindé en cuivre	57
6.16)	Ethernet Gigabit {1 Gbit/s, 1000 Mbit/s} sur fibre optique.....	57
6.16.1)	1000Base-SX : Giga Ethernet onde courte {Short wave}	57
6.16.2)	1000Base-LX : Giga Ethernet onde longue {Long wave}	57
6.16.3)	Autres technologies Giga Ethernet sur fibre optique	57
6.16.4)	1000Base-X	58
6.16.5)	10 Gb/s et au-delà	58
6.17)	Tableau récapitulatif de d'évolution d'Ethernet jusqu'au gigabit.....	58
6.18)	Du hub {concentrateur} au switch {commutateur} Ethernet.....	58
6.18.1)	De la topologie logique en bus à la topologie logique point à point.....	58
6.18.2)	Introduction du mode full-duplex : élimination totale des collisions.....	58
6.18.3)	Ports cuivre 8P8C {RJ45} MDI et MDI-X.....	59
6.18.4)	Câbles droits et croisés historiques 10 et 100 Mbps : paires 1-2 et 3-6.....	59
6.18.5)	Types de câbles après normalisation EIA/TIA et support du gigabit.....	60
6.18.6)	Cascade de commutateurs : port Uplink MDI, et auto MDI/MDI-X	62
6.18.7)	Connexion de commutateur à commutateur : cascades ou empilés ?.....	62
6.18.8)	Stack d'alimentations redondantes de commutateurs	64
6.18.9)	Auto négociation	64
6.18.10)	Les types de transmissions de trames {commutation}	64
6.18.11)	Commutation symétrique et asymétrique	65
6.18.12)	Mémoire tampon	65
6.18.13)	Commutateurs administrables/gérables {manageable}.....	65
6.18.14)	Réseaux Locaux Virtuels: {-, VLAN, Virtual Local Area Network}	65
7)	Réseaux locaux sans fil {Wireless Local Area network, WLAN}	65
7.1)	Les autres technologies sans fil	66
7.1.1)	Réseaux personnels sans fil {Wireless Personal Area Network, WPAN}	66
7.1.2)	Réseaux étendus sans fil {Wireless Wide Area Network, WMAN}.....	66
7.2)	Les ondes radio	66
7.3)	Bandes de fréquences utilisées par les protocoles sans-fil	68
7.4)	Les protocoles de réseaux locaux sans fils : 802.11	68
7.5)	Les organismes de normalisation concernés.....	69
7.5.1)	Bandes de fréquences utilisables : ITU-R, ETSI	69
7.5.2)	Comité IEEE 802.11	69
7.5.3)	Wi-Fi Alliance®.....	69

7.6)	Objectif des réseaux locaux sans fil.....	70
7.7)	Le point d'accès	70
7.8)	Politique d'accès au médium CSMA/CA et trames associées	70
7.9)	Problèmes caractéristiques associés aux WLANs	71
7.9.1)	La sécurité	71
7.9.2)	L'environnement	71
7.9.3)	Semi-duplex, support partagé	71
8)	Modèle OSI : la couche réseau {network layer, L3}	72
8.1)	Fonctionnalités de la couche réseau.....	72
8.2)	Attribution d'adresse réseau	72
8.2.1)	Attribution manuelle	72
8.2.2)	Attribution dynamique à partir d'un serveur	72
8.2.3)	Auto-configuration.....	72
8.2.4)	Adresse réseau des équipements sensibles	72
8.3)	Transmission d'un paquet sur le même réseau.....	72
8.3.1)	Principe	72
8.3.2)	Résolution d'adresse réseau (couche 3) en adresse liaison de données (couche 2) ..	73
8.4)	Routeurs {router} et passerelles {gateway}	73
8.5)	Paquet à destination d'un autre réseau appelé réseau distant.....	73
8.5.1)	Configuration des équipements	73
8.5.2)	Étapes de la transmission d'un paquet vers un réseau distant.....	74
8.6)	Encapsulation et PDU de la couche Réseau	74
9)	La couche transport {niveau 4}	75
9.1)	Fonctionnalités de la couche transport.....	75
9.2)	Encapsulation et PDU de la couche transport	75
10)	La couche session {niveau 5}.....	75
11)	La couche présentation {niveau 6}.....	75
12)	La couche application {niveau 7}	75
13)	Le modèle TCP/IP	76
13.1)	Objectif du modèle TCP/IP	76
13.2)	Description du modèle TCP/IP	76
13.3)	Les protocoles de la couche Internet	77
13.3.1)	IP {Internet Protocol}	77
13.3.2)	ICMP {Internet Control Message Protocol}	77
13.3.3)	ARP {Address resolution protocol}	77
13.3.4)	Les protocoles IPsec AH {Authentication Header} et ESP {Encapsulating Security Payload} ..	77
13.4)	Les protocoles de la couche transport.....	77
13.5)	Les applications	77
13.5.1)	Les ports réservés ou ports bien connus {well known port}	77
13.5.2)	Les ports inscrits {registered port}.....	78
13.5.3)	Les ports privés ou dynamiques {private or dynamic port}.....	78
13.5.4)	Port source dynamique	78
14)	Adressage IP	78
14.1)	Adresses IPv4	78
14.1.1)	Format des adresses IPv4.....	78
14.1.2)	Adresses IPv4 publiques et adresses IPv4 privées	79
14.1.3)	Adresse de réseau IPv4.....	79
14.1.4)	Adresse de broadcast dirigé IPv4 : tous les hôtes d'un réseau	79
14.1.5)	Adresse de broadcast (limité) : tous les hôtes de ce réseau	79
14.1.6)	Adresse locale de lien {link local} ou adresse APIPA.....	79
14.1.7)	Adresse de boucle {loopback}	79

14.1.8)	Adresse IPv4 du réseau en cours de configuration	80
14.1.9)	Adresses IPv4 attribuables aux hôtes	80
14.2)	Épuisement de la réserve d'adresses IPv4 encore disponibles	80
14.2.1)	Le problème	80
14.2.2)	Définition d'adresses IPv4 privées.....	80
14.2.3)	La traduction d'adresse réseau IPv4 et de port.....	80
14.3)	IPv6	82
14.3.1)	Adresses IPv6.....	82
15)	Résumé des niveaux OSI et TCP/IP.....	83
16)	Comparatif table de commutation, table ARP IPv4, table de routage	84
16.1)	Table de commutation : pas d'intervention humaine nécessaire	84
16.2)	Table ARP : pas d'intervention humaine nécessaire.....	85
16.3)	Table de routage : intervention d'un administrateur nécessaire.....	86



Cette page a été
laissée vierge
intentionnellement.

1) Introduction

1.1) Bref historique

Les premiers ordinateurs sont apparus dès les années 50. Ils possédaient peu de capacités d'**Entrées/Sorties** {**E/S**, Input/Output, **I/O**}. Les perforateurs de cartes, imprimantes, lecteurs de cartes et consoles opérateurs constituèrent les premiers périphériques d'E/S. Ils furent rejoints un peu plus tard par les unités de bandes magnétiques. Ainsi, les échanges de données entre ordinateurs ne pouvaient se réaliser que par ressaisie des informations, échange de cartes perforées ou dans le meilleur des cas, de bandes magnétiques. L'apparition de nouveaux systèmes d'exploitation permit à plusieurs utilisateurs à partir de terminaux de partager une **unité centrale de traitement** {-, **Central Processing Unit**, **CPU**}, et d'imprimer leurs travaux sur des périphériques distincts. Dans ce mode de fonctionnement, tous les utilisateurs se partagent la puissance de traitement de la même CPU, les capacités de stockages des mêmes disques, C'était l'**informatique centralisée**. Ces ordinateurs étaient appelés **mainframes** {**macroordinateur**}. Chaque constructeur d'ordinateurs possédait des **systèmes d'exploitation** {**SE**, **Operating System**, **OS**} qui lui étaient propres, et qui ne s'exécutaient que sur un type de matériel donné. C'était l'époque de l'informatique propriétaire. Les progrès de la téléphonie autorisèrent les connexions distantes de terminaux, via des lignes commutées ou dédiées.

De ce fait, l'ordinateur passait de plus en plus de temps à gérer les communications. Tout naturellement, des **calculateurs spécialisés**, appelés **contrôleurs**, furent créés pour décharger le processeur principal de ces tâches.

Bien évidemment, aucune standardisation n'existait entre fabricants, et les sociétés clientes demeuraient dépendantes de leur fournisseur informatique.

Les besoins de traitement des sociétés informatisées grandirent très vite, et il n'était pas rare de voir plusieurs ordinateurs dans la même société. Afin d'autoriser la communication entre ces mainframes, les constructeurs développèrent leurs réseaux "maison". Ainsi, **DEC** {**Digital Equipment Corporation**} élaborait **DECNET** {**Digital Equipment Corporation NETWORK**} et **IBM** {**International Business Machines**} créa **SNA** {**System Network Architecture**}. Ces premiers réseaux ont permis l'interconnexion des matériels des grands constructeurs et des matériels compatibles, le client restant prisonnier d'un environnement donné. En effet, seuls les ordinateurs d'une même marque pouvaient dialoguer entre eux.

Le gouvernement américain joua alors un rôle fédérateur dans la mise en œuvre du réseau **ARPAnet** {**Advanced Research Projects Agency network**} qui reliait les ordinateurs des différentes administrations gouvernementales américaines (éducation, armée, santé, recherche, etc.). Ces ordinateurs étaient implantés sur des sites géographiques disséminés sur l'ensemble du territoire des USA. ARPAnet constitua ainsi le premier réseau étendu {-, **Wide Area Network**, **WAN**}. Par ailleurs, plusieurs marques et modèles d'ordinateurs se côtoyaient dans ces administrations, rendant ainsi les communications impossibles. Il a donc fallu instaurer des règles de bonne conduite, appelées protocoles, entre ces ordinateurs. Les travaux des secteurs privés et publics sur la mise en œuvre de ces protocoles sont à l'origine de standards actuels comme **TCP/IP** {**Transmission Control Protocol / Internet Protocol**} qui contrairement aux réseaux propriétaires, permet de connecter des équipements de structures diverses par l'intermédiaire d'un réseau public : **Internet**.

Parallèlement, la miniaturisation permit l'arrivée des premiers micro-ordinateurs et du concept d'ordinateur personnel. Les sociétés ne pouvant investir dans une informatique lourde ont alors acquis plusieurs micro-ordinateurs, et décidèrent par la suite de les connecter. Ce fût la naissance du **réseau local d'entreprise** {**RLE**, **Local Area Network**, **LAN**}.

1.2) Un système de communication pour quoi faire ?

L'objectif principal d'un système de communication est de permettre le dialogue entre :

- ◆ des applications s'exécutant sur des équipements distants ;
- ◆ des utilisateurs utilisant des équipements différents ;
- ◆ un utilisateur utilisant un périphérique et une application s'exécutant sur un autre équipement.

1.3) Périphériques finaux {end devices}

Les périphériques finaux :

- ◆ initialisent la communication ;
- ◆ émettent les données originales. Ils constituent la source du flux de données ;
- ◆ constituent la destination finale du flux de données.

Les périphériques finaux les plus courants sont :

- ◆ les ordinateurs ;
- ◆ les imprimantes ;
- ◆ les téléphones IP ;
- ◆ les tablettes ;
- ◆ les mobiles multifonction { smartphone }.

1.4) Périphériques intermédiaires {intermediary device}

Le flux de données émis par un périphérique final traversera un ou plusieurs **périphériques intermédiaires** avant d'atteindre le(s) périphérique(s) final(aux) de destination. Les périphériques intermédiaires permettent de :

- ◆ transmettre le signal codant les données ;
- ◆ remettre en forme le signal codant les données ;
- ◆ gérer le flux de données.

Les périphériques intermédiaires les plus courants sont :

- ◆ les répéteurs {repeater} ;
- ◆ les concentrateurs {hub} ;
- ◆ les ponts {bridge} ;
- ◆ les commutateurs {switch} ;
- ◆ les points d'accès sans fil {wireless access point} ;
- ◆ les routeurs {router} ;
- ◆ les passerelles {gateway} ;
- ◆ les barrières de sécurité {pare-feu, firewall} ;

1.5) Les supports {médium} de communication

Les supports de communication permettent la connecter :

- ◆ les périphériques intermédiaires entre eux ;
- ◆ les périphériques finaux aux périphériques intermédiaires.

Les supports de communication les plus courants sont :

- ◆ les fils de cuivre ;
- ◆ la fibre optique ;
- ◆ les supports non filaires {wireless}.

1.6) Système de communication

Un système de communication est donc composé de :

- ◆ périphériques finaux ;
- ◆ périphériques intermédiaires ;
- ◆ supports {média} de communication.

1.7) Réseaux clients serveurs et pair à pair {égal à égal, poste à poste, peer to peer, P2P}

Les périphériques finaux peuvent jouer les rôles de clients et/ou de serveurs

1.7.1) Réseaux clients serveur

Dans un environnement client-serveur, un très petit nombre de périphériques finaux jouent le rôle de serveurs tandis que l'extrême majorité des périphériques finaux jouent eux le rôle de client.

Chaque serveur exécute un nombre limité de services serveur tels que le service de partage de fichiers et d'imprimantes, le service DHCP, le service DNS, le service d'authentification, le service de base de données etc. Ces services serveurs peuvent être "facilement" paramétrés afin de répliquer leurs données entre eux, garantissant ainsi la disponibilité des données. Ce sont les services de type serveur qui effectuent tous les traitements des données.

Chaque client exécute des services clients qui émettent des requêtes vers les serveurs. Les serveurs répondent à ces requêtes en réalisant tous les traitements nécessaires, puis renvoient les résultats au poste client. Ainsi, seules les données nécessaires transitent par le réseau.

Les logiciels exécutés en tant que service client sont bien évidemment beaucoup moins gourmands en ressources que les logiciels exécutés en tant que service serveur.

Un client web utilisant un logiciel client de navigation (Firefox, Opera, Brave, Chrome, Edge, Safari, ...) interroge un logiciel serveur Web (Apache, IIS, ...).

Les services clients ou serveurs sont très généralement lancés au démarrage du système, sous forme de **démon** {**daemon**} dans les environnements Linux et de **service** dans les environnements Microsoft Windows.

1.7.2) Réseaux pair à pair {égal à égal, poste à poste, peer to peer, P2P}

Dans un réseau pair à pair, un périphérique exécute à la fois des services clients et serveurs. Ne nécessitant pas de périphériques dédiés au rôle de serveur, leur déploiement est donc moins onéreux que celui des réseaux clients serveur. Les réseaux de type pair à pair sont généralement moins complexes à mettre en œuvre car ils sont utilisés pour des tâches simples.

Dans les environnements Microsoft Windows de type **groupe de travail** {**workgroup**}, les ordinateurs opèrent en mode pair à pair pour l'authentification durant les ouvertures de session et le partage de fichiers et d'imprimantes. Chaque ouverture de session est validée par la base SAM de l'ordinateur sur lequel l'ouverture de session est demandée.

Dans les environnements Microsoft Windows de type **domaine** {**domain**}, les ouvertures de session des utilisateurs sont validées par les contrôleurs de domaine. Un contrôleur de domaines est un ordinateur équipé d'un système d'exploitation Windows Server sur lequel les services d'annuaire Active Directory ont été installés et paramétrés.

Cette manière de définir les réseaux de type pair à pair est la définition historique. De nos jours, les réseaux de type pair à pair sont plutôt considérés comme des réseaux où chaque périphérique final dispose des mêmes droits. La définition donnée par le site **FranceTerme** est la suivante :

« pair à pair, loc.adj.inv.

Journal officiel du 23/05/2017

Synonyme :

poste à poste, loc.adj.inv.

Domaine :

TÉLÉCOMMUNICATIONS - INFORMATIQUE / Internet

Définition :

Se dit du mode d'utilisation d'un réseau dans lequel chacun des participants connectés dispose des mêmes droits et qui permet un échange direct de services sans recourir à un serveur central ; par extension, se dit d'un tel réseau.

Note :

Les échanges de fichiers, le calcul décentralisé et les transactions en cybermonnaie sont des exemples de services couramment assurés grâce à un réseau pair à pair.

Voir aussi :

appairage, cybermonnaie, internet clandestin

Équivalent étranger :

peer-to-peer (en), P2P (en), P-to-P (en)

Attention :

Cette publication annule et remplace celle du terme « poste à poste » publié au Journal officiel du 13 mai 2006. »

1.8) LAN, WLAN, WAN, MAN, et PAN

Un système de communication se décompose en réseaux de types différents, qui sont généralement classés suivant leur étendue.

Les réseaux locaux {**RLE**, **Local Area Network**, **LAN**} ne couvrent qu'un espace géographique limité. Ce sont des réseaux dont les équipements :

- ◆ sont regroupés sur un même lieu géographique qui correspond généralement à un bâtiment, ou un ensemble de bâtiments proches ;
- ◆ sont gérés par un même administrateur ;
- ◆ appartiennent à la même organisation / entreprise.

Les protocoles LAN bien connus sont **Ethernet [802.3]** et **Token-Ring [802.5]**.

Les réseaux locaux sans fil {**Wireless LAN**, **WLAN**} sont des réseaux de type LAN qui permettent de s'affranchir de l'usage des câbles pour connecter les périphériques. Ils sont, par abus de langage, souvent qualifiés de réseaux **Wi-Fi**, car ils se conforment aux normes édictées par la **Wi-Fi Alliance {Wireless- Fidelity}** dont l'adresse du site est <http://www.wi-fi.org/>.

Les protocoles réseaux locaux sans fils sont 802.11a, 802.11b, 802.11g , 802.11n et 802.11ac.

Par opposition aux LANs, les réseaux étendus {-, **Wide Area Network**, **WAN**} peuvent couvrir des zones bien plus vastes que ne le font les réseaux locaux. Les liens de type WAN permettent de relier les réseaux locaux entre eux. Ces liens WANs sont généralement déployés et gérés par des opérateurs télécom.

X25, **Frame Relay**, **PPP** {**Point to Point Protocol**} **PPPoE** {**Point to Point Protocol over Ethernet**} et **PPPoA** {**Point to Point Protocol over ATM**}.

Les réseaux **MANs** {**Metropolitan Area Network**} sont des réseaux dont l'étendue couvre des zones dont la taille varie de celle d'un campus à celle d'une communauté urbaine.

Les réseaux personnels {**Personal Area Network**, **PAN**} permettent de relier des équipements "très" proches entre eux. Bluetooth, portée 100 mètres, et ZigBee portée 10 mètres sont des PANs sans fil, tandis que **USB** {**Universal Serial Bus**} est un PAN filaire.

1.9) Internet, intranet, extranet

Il est possible de connecter des LANs, des MANs, des WANs pour constituer des **interréseaux** {**internetwork**}.

L'**Internet** est un interréseau **public mondial** qui peut connecter l'ensemble des réseaux exécutant la suite de protocoles **TCP/IP**. Le terme public implique l'existence d'organismes responsables de l'attribution d'identifiants uniques à chaque entité désirant se connecter. Il s'agit des adresses PI publiques, des noms de domaine, et des numéros de systèmes autonomes.

Un **Intranet** regroupe **les réseaux TCP/IP privés** d'un seul organisme à l'usage du personnel et des collaborateurs de la structure, voire de tiers sous réserve d'autorisation.

Un **extranet** est la structure qui autorise les personnels et collaborateurs de structures approuvées à accéder en toute sécurité via la suite de protocoles **TCP/IP**, à l'intranet d'un organisme.

1.10) Connexion à Internet des particuliers et des petites entreprises

Les accès à Internet des particuliers et des petites entreprises :

- ◆ **lignes commutées** : il s'agit des lignes utilisées par le bon vieux réseau téléphonique analogique {**RTC**, Réseau Téléphonique Commuté, **POST**, Plain Old Telephone Service}. Un modem est nécessaire. Le débit est très faible ;
- ◆ **ADSL** : ligne d'abonné numérique asymétrique {**Asynchronous Digital Subscriber Line**}. Cette technologie occupe les fréquences non utilisées par le RTC des lignes analogiques. Elle assure un débit beaucoup plus important **en descente** {**download**} (depuis Internet) qu'**en montée** {**upload**} (à destination d'Internet). Le débit est élevé mais non garanti ;
- ◆ **câble** : technologie déployée par les opérateurs de télévision. Il assure un débit élevé et une connexion permanente via un **câble coaxial** ;
- ◆ **cellulaire** : c'est l'accès à Internet via le réseau utilisé par les téléphones mobiles ;
- ◆ **satellite** : permet l'accès à Internet dans les zones blanches ou très mal desservies par les autres technologies.

1.11) Connexion à Internet des entreprises

- ◆ **lignes louées dédiées** ou {**lignes spécialisées**} : ces lignes cuivre assurent un débit garanti et généralement une **GTR** {**Garantie de Temps de Rétablissement**}. Elles mettent en **œuvre** des circuits réservés chez l'opérateur de télécommunications. Suivant leur débit elles sont nommées **T-carrier T1, T2, T3** aux États-Unis et **E-carrier E1, E2, E3** en Europe. Elles servaient à connecter deux LANs privés. La facturation était généralement mensuelle voire annuelle ;
- ◆ **ADSL** ;
- ◆ **SDSL** : ligne d'abonné numérique symétrique {**Synchronous Digital Subscriber Line**}. Cette technologie occupe les fréquences non utilisées par le RTC des lignes analogiques. Le **débit en descente** {**download**} et **en montée** {**upload**}. Cette offre s'appuie sur les lignes louées et est généralement associée à un débit garanti et une **GTR**. L'ensemble des offres d'un opérateur est connu sous le nom de **DSL d'entreprise** {**Business DSL**} ;
- ◆ Réseau Ethernet métropolitain/urbain {**Metro Ethernet**} : c'est l'adaptation du protocole de réseau local Ethernet aux réseaux métropolitains ;
- ◆ **Satellite**.

1.12) Les réseaux convergents {converged network, converging network}

Les réseaux convergents permettent d'utiliser la même architecture afin de transporter des informations qui jusqu' alors transitaient par des types de réseaux bien différents. À savoir :

- ◆ les **réseaux téléphoniques** {**telephones network**} ;
- ◆ les **réseaux de diffusion** {**broadcast network**} : ce sont les réseaux de diffusion des émissions de radio et de télévision. En France ce monopole était dévolu à l'**ORTF** {**Office de Radiodiffusion-Télévision Française**}, au Royaume-Uni la **BBC** {**British Broadcasting Corporation**} est toujours en service.
- ◆ les **réseaux informatiques** {**computers network**}.

Un réseau convergent doit donc être apte à transporter simultanément :

- ◆ des conversations téléphoniques ;
- ◆ des émissions de vidéos et de sons ;
- ◆ des données informatiques traditionnelles.

L'utilisation d'une architecture unifiée pour ces trois types de réseaux doit permettre une simplification de la mise en œuvre et de la maintenance ainsi qu'une réduction des coûts.

1.13) Les réseaux fiables {reliable network}

Les architectures de réseaux convergents doivent être des architectures **fiables** {**reliable**}. Ceci est réalisé en garantissant :

- ◆ la **tolérance de pannes** {**fault tolerance**}. La **redondance** des services, des équipements et des supports de communications assure la résilience du réseau ;
- ◆ l'**évolutivité** {**scalability**} permet d'assurer que les nouveaux besoins pourront être satisfaits sans pénaliser les utilisateurs. Pour cela il est conseillé de privilégier des équipements modulaires au détriment des équipements à configuration fixe, tant d'un point de vue matériel que logiciel.
- ◆ La **sécurité** {**security**}. Elle s'applique aux données et doit garantir :
 - la **confidentialité** {**confidentiality**} des données : seuls les utilisateurs légitimes doivent avoir accès aux données,
 - l'**intégrité** {**integrity**} des données : les données ne doivent pas être modifiées durant leur transit et leur stockage dans l'infrastructure.
 - la **disponibilité** {**availability**} des données : les données doivent être rapidement accessibles par les utilisateurs en respectant la **règle des cinq neufs** {**five nines rules, five 9s rule**} qui pérennise l'accès pendant au moins 99,999% du temps;
- ◆ La **qualité de service** {**QoS, Quality of Service**} : elle permet de gérer les encombrements en donnant la priorité à certains flux de données comme les flux téléphoniques et de vidéos interactives.

Les réseaux fiables permettent l'essor de nouvelles tendances :

- ◆ **AVEC** {**Apportez Votre Equipement personnel de Communication, BYOD, Bring Your Own Device**} : « *Se dit de l'utilisation, dans un cadre professionnel, d'un matériel personnel tel qu'un téléphone multifonction ou un ordinateur.* » Journal officiel du 24/03/2013 ;
- ◆ la **collaboration en ligne** {**travail coopératif, logiciel de groupe de travail, Online Collaboration, groupware**} : « *Logiciel permettant à un groupe d'utilisateurs de travailler en collaboration sur un même projet sans être nécessairement réunis.* » Journal officiel du 22/09/2000 ;
- ◆ la **communication vidéo interactive** : elle est nécessaire aux échanges à distance entre humains. Elle est bien évidemment employée par les outils de collaboration en ligne et de **visioconférence**.

2) Les organismes de normalisation

2.1) Standards {de facto standard} et normes {de jure standard}

Le terme anglo-saxon standard accepte deux sens différents :

- ◆ **standard {de facto standard}**. Les standards proviennent d'une mise en œuvre, généralement propriétaire, largement répandue, en dehors de tout organisme de régulation ;
- ◆ **norme {de jure standard}**. Les normes sont développées dans le but d'assurer l'interopérabilité de systèmes différents, en rendant public leurs spécifications. Ces spécifications sont avalisées par au moins un organisme de normalisation.

Le mot anglais standard se traduit en français, à la fois par standard et par norme. Malheureusement, en français ces deux termes n'ont pas exactement la même signification. Ceci explique que les traductions francophones d'ouvrages anglo-saxons ne sont pas toujours rigoureusement exactes.

2.2) Les organismes de normalisation

Les organismes de normalisation les plus connus sont :

- ◆ **ISO**. Le nom ISO provient du grec **isos**, signifiant égal, afin que le nom de cette organisation de normalisation soit le même dans toutes les langues. La consultation de vieux documents permet de constater que cette définition n'a pas toujours été respectée. Ainsi, en anglais l'ISO était tantôt défini comme International Standards Organization ou International Organization for Standardization. En français, l'ISO devenait jadis, OSI ou encore Organisme de Standardisation International. (http://www.iso.org/iso/fr/about/discover-iso_isos-name.htm, <http://www.iso.org/>, <http://www.iso.org/iso/fr>). L'ISO est un organisme non gouvernemental regroupant plus de 156 pays membres, selon le principe d'un membre par pays, dont le secrétariat central, situé en Suisse à Genève, assure la coordination d'ensemble. Il existe trois types de membres, dont les définitions ISO sont :
 - **Comités membres** : « Un comité membre de l'ISO est l'organisme national " le plus représentatif de la normalisation dans son pays ". Un seul organisme par pays peut être admis en qualité de membre de l'ISO. Les comités membres sont habilités à participer avec plein droit de vote à tout comité technique et à tout comité de politique générale de l'ISO »
 - **Membres correspondants** : « Un membre correspondant est en général une organisation dans un pays qui n'a pas encore entièrement développé son activité nationale en matière de normalisation. Les membres correspondants ne prennent pas une part active aux travaux techniques et d'élaboration de politiques mais ont le droit d'être tenus pleinement informés des travaux qui présentent pour eux un intérêt »
 - **Membres abonnés** : « La catégorie de membre abonné a été créée pour des pays à économie très limitée. Ces membres abonnés paient une cotisation réduite qui leur permet néanmoins de rester en contact avec la normalisation internationale »

<http://www.iso.org/iso/fr/aboutiso/isomembers/MemberCountryList.MemberCountryList>

◆ **IEC** {International Electrotechnical Commission, **CEI**, **Commission Electrotechnique Internationale**}. L'IEC est une organisation internationale fondée en 1906. Son siège initialement situé à Londres, a été transféré à Genève en 1948. L'IEC prépare et publie les standards internationaux pour l'ensemble des industries électriques, électroniques et apparentées. L'IEC et l'OSI sont complémentaires. <http://www.iec.ch/> ;

◆ **ITU** {International Telecommunication Union, **UIT**, **Union Internationale des Télécommunications**}. L'UIT dépend de l'ONU {Organisation des Nations Unies, **UN**, **United Nations**}. Son site <http://www.itu.int/home/index.html> en donne la définition suivante : « L'UIT dont le siège est à Genève (Suisse), est une organisation internationale du système des Nations Unies au sein de laquelle les Etats et le secteur privé coordonnent les réseaux et services mondiaux de télécommunication ». L'organisme de normalisation **ITU-T** {International Telecommunication Union - Telecommunication standardization sector} constitue l'organisme de normalisation de l'ITU. Il publie ses travaux tous les 4 ans. Ses recommandations sont classées par domaines : la **série V** concerne la téléphonie et les modems, la **série X** les réseaux, et la **série S** le réseau RNIS, (Cf : <http://www.itu.int/ITU-T/publications/recs.html>). L'ITU-T a succédé au

CCITT {Consultative Committee for International Telegraph and Telephone, **CCITT**, Comité Consultatif International Télégraphique et Téléphonique}.

◆ **IEEE** {Institute of Electrical and Electronics Engineers}. L'acronyme **IEEE** doit se prononcer I3E {ItripleE}. Cette organisation à but non lucratif, constitue la plus grande institution professionnelle mondiale. Elle a en particulier développé les normes **802** relatives aux **réseaux locaux** {-, Local Area Network, **LAN**}, aux **réseaux métropolitains** {-, Metropolitan Area Network, **MAN**) et aux **réseaux étendus** {-, Wide Area Network, **WAN**). Ces standards sont appelés **802** car la première réunion s'est tenue en février, mois **2**, 1980. Son site peut être consulté à l'adresse suivante : <http://www.ieee.org/> ;

◆ **IETF** {Internet Engineering Task Force}. Cet organisme constitue l'une des instances de normalisation de l'Internet. ;

◆ **Wi-Fi Alliance®** {Wireless-Fidelity Alliance}. Ce consortium, s'appelait à l'origine **WECA** {Wireless Ethernet Compatibility Alliance}. Son but est d'édicter des standards sans fil, compatibles avec Ethernet, le protocole de réseau local le plus répandu, et de garantir l'interopérabilité des matériels des différents constructeurs. La Wi-Fi Alliance® est propriétaire de la **marque Wi-Fi**, La Wi-Fi alliance certifie les divers équipements en leur attribuant le label **Wi-Fi CERTIFIED**. Ce label est une marque déposée, et est symbolisé par le logo bien connu. Il garantit que les équipements respectent les normes émises par le comité IEEE 802.11 ainsi que les standards édictés par la Wi-Fi Alliance®. Le terme Wi-Fi est souvent interprété comme Wireless-Fidelity, mais ne semble avoir aucune signification particulière, et ne constituer qu'un jeu de mot ;

◆ **EIA** {Electronic Industries Association}. C'est une organisation professionnelle nord-américaine qui a élaboré des normes connues comme des Recommended Standards, telles que RS 232 ; RS 422 etc. Elle travaille en association avec la Telecommunications Industry Association {TIA} ;

◆ **AFNOR** {Association Française de **NOR**malisation}. L'AFNOR est le correspondant français de l'ISO. L'URL de son site est <http://www.afnor.fr>.

Il existe bien d'autres organismes comme l'**ANSI** {American National Standards Institute}, correspondant états-unien de l'**AFNOR**. Les recommandations de ces organismes sont quelquefois redondantes, par exemple V24 de l'ITU-T et RS 232 de l'EIA.

Les logos des organismes les plus connus sont repris ci-dessous :



3) Le modèle OSI {Open Systems Interconnection} |ISO / IEC 7498|

3.1) Historique et objectifs

Dans les années 70, la plupart des constructeurs informatiques développèrent leurs réseaux propriétaires. Tous ces réseaux étaient incompatibles entre eux. En 1977, l'**ISO** décida d'étudier un modèle "universel", et le **15 novembre 1984**, cet organisme publia en collaboration avec IEC et l'ITU-T la norme **ISO / IEC 7498** ou **ITU-T Recommendation X.200**, connue en tant que modèle **OSI** {Open Systems Interconnection}. Ce modèle permet d'identifier et de localiser des objets dans un **environnement d'interconnexion de systèmes ouverts** {-, Open Systems Interconnection Environment, **OSIE**} pour leur permettre de communiquer. Le problème initial consistait à faire dialoguer des applications qui s'exécutaient :

- ◆ avec des codages de caractères différents ;
- ◆ sur des systèmes d'exploitation différents ;
- ◆ sur des ordinateurs de modèles et de marques différentes ;
- ◆ sur des systèmes de câblage différents.

Le modèle OSI de l'ISO n'est pas unique. Le modèle TCP/IP constitue un autre modèle de système de communication. Le modèle TCP/IP s'avère plus restrictif mais plus simple que le modèle ISO.

Les modèles OSI et TCP/IP décomposent les systèmes de communication en plusieurs **niveaux** {couche, layer} de fonctionnalités. Chacune de ces couches correspond à un concept particulier et à des compétences spécifiques. Par exemple, les connaissances nécessaires au développement d'une IHM {Interface Homme Machine} sont radicalement différentes de celles mises en œuvre pour transporter les signaux sur une fibre optique. Le découpage en niveaux permet de représenter et donc de mettre en évidence les diverses compétences nécessaires. Les **modèles par couches** {layered model} fournissent un cadre pour expliquer et comprendre les tâches élémentaires mise en œuvre, ainsi que les interactions entre ces tâches élémentaires.

Les avantages de toute normalisation par couche sont les suivants :

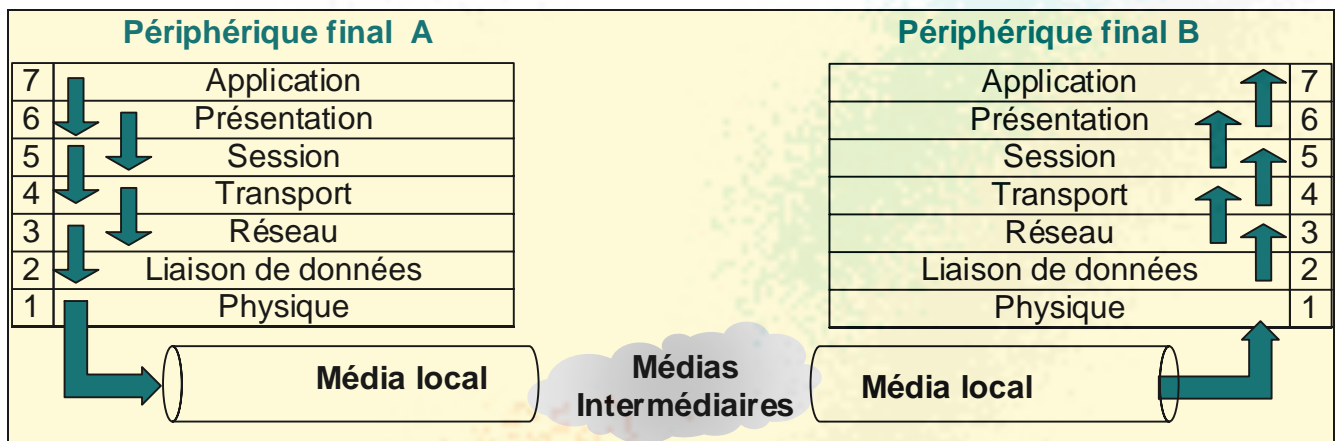
- ◆ réduction de la complexité ;
- ◆ uniformisation des interfaces entre les niveaux ;
- ◆ garantie de l'interopérabilité ;
- ◆ conception modulaire facilitée ;
- ◆ simplification de l'apprentissage.

3.2) Les 7 couches OSI

Pour ce faire, l'ISO a décomposé la tâche que doit remplir un système de communication en sept tâches élémentaires. Chacune de ces tâches est appelée **couche** ou **niveau** {layer}.

7	Application	{Application}	Couches orientées applications : Couches applicatives { Application layers }
6	Présentation	{Présentation}	
5	Session	{Session}	
4	Transport	{Transport}	Couches orientées réseau : Couches de flux de données { Data flow layers }
3	Réseau	{Network}	
2	Liaison de données	{Data link}	
1	Physique	{Physical}	

Si un utilisateur travaille physiquement sur le périphérique final A, et qu'il désire accéder à une application d'un périphérique final B, sa demande suivra le chemin suivant :



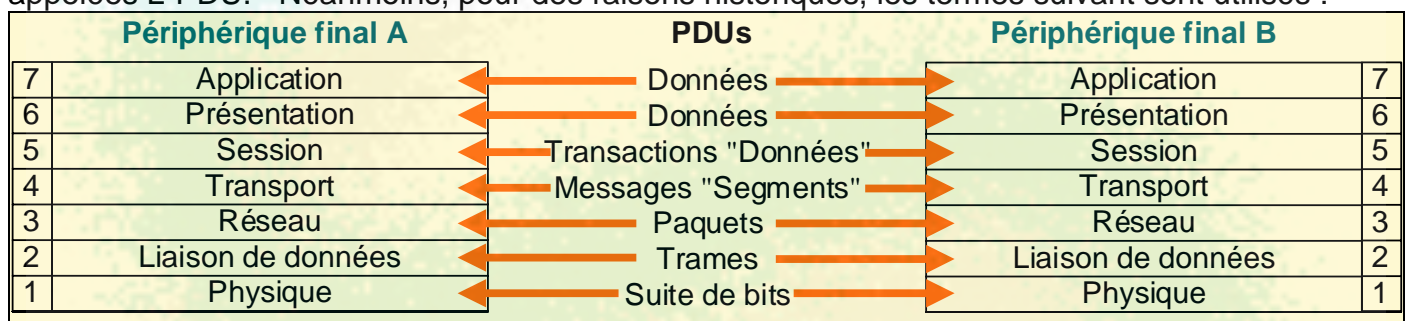
Les informations passent donc d'une couche à une autre. Néanmoins d'un point de vue logique, tout se passe comme si la couche N de l'hôte A, communiquait directement avec la couche N de l'hôte B grâce à un **protocole** commun de niveau N.



Le découpage en couches permet de décomposer un problème complexe en une suite de problèmes plus simples : les protocoles. Les protocoles réseaux permettent d'adapter plus facilement le modèle aux nouvelles technologies, et garantissent l'interopérabilité entre les constructeurs.

3.3) La communication de niveau à niveau

Bien que la transmission des données de niveau N d'un hôte A vers un hôte B, mette en œuvre les couches inférieures, tout se passe comme si les niveaux N des deux équipements dialoguaient directement, en s'échangeant des unités d'informations de niveau N. Ces unités d'informations spécifiques à un protocole sont appelées **PDUs {Protocol Data Unit}**. Le modèle OSI ne nomme pas les PDUs. Une PDU de niveau n est appelée Ln-PDU ou bien X-PDU, X représentant la première lettre du nom anglo-saxon du niveau, à l'exception de la couche 2 dont les PDUs sont appelées L-PDU. Néanmoins, pour des raisons historiques, les termes suivants sont utilisés :



Plusieurs protocoles peuvent avoir été définis dans une même couche. Chaque protocole possède une structure de PDU qui lui est propre, et définit ses interactions avec les niveaux supérieur et inférieur. Tout constructeur ou éditeur déployant un protocole particulier doit respecter la **structure de la PDU**, ainsi que les **interactions avec la couche inférieure et la couche supérieure**. Par contre, le constructeur ou l'éditeur a toute liberté pour mettre en œuvre le protocole.

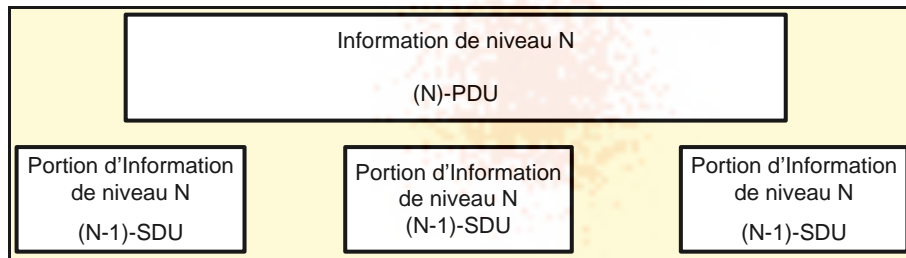
Un protocole :

- ◆ **définit ce qui doit être réalisé**, à savoir :
 - la structure de la PDU,
 - l'interaction avec la couche inférieure et la couche supérieure ;
- ◆ **ne définit pas comment cela doit être réalisé**.

Le transit de l'information par des couches différentes met en œuvre deux mécanismes : l'encapsulation et la fragmentation, encore appelée segmentation.

3.4) La fragmentation ou segmentation

Si nous considérons l'utilisateur de l'ordinateur A, qui désire connaître le catalogue des dossiers de l'ordinateur B, sa demande initiale relativement complexe va descendre successivement toutes les couches de l'ordinateur A jusqu'à être présentée au médium de communication. Ce support physique ne sait transmettre que des signaux codant des bits. Il faut donc que la demande de l'utilisateur soit, au fur et à mesure de son parcours descendant, fragmentée en unités d'informations de plus en plus petites appelées **SDUs {Service Data Unit}**.



Dans cet exemple, l'unité d'information de niveau N, a été fragmentée en trois unités d'informations de niveau N-1. En d'autres termes, la N-PDU a été décomposée en 3 (N-1)-SDUs.

Les PDUs sont générées par l'hôte source, transmises à l'hôte destination qui les réassemble.

3.5) L'encapsulation

L'hôte source a donc fragmenté l'information de niveau N en plusieurs informations de niveau N-1.

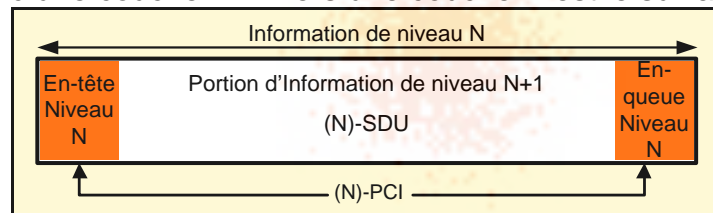
Pour que chacune de ces (N-1)-SDUs arrive à destination au niveau N-1, il faut rajouter une information de niveau N-1 caractérisant la destination. Afin de faciliter la réponse, une information identifiant au niveau N-1 l'émetteur, est également insérée.

Les identifiants de niveaux N-1 permettent au protocole de niveau N-1, de transporter les (N-1)-PDUs jusqu'à la destination. Ainsi les informations arriveront à destination, mais, pas forcément dans l'ordre d'émission. Pour y remédier, il faut, tout d'abord, que la couche N-1 de l'hôte de destination puisse s'assurer que toutes les (N-1)-SDUs sont arrivées. Ensuite, la couche N-1 de l'hôte de destination doit reconstituer l'information de niveau N, en réorganisant correctement les (N-1)-SDUs. Des informations de séquençement sont insérées par la couche N-1 de l'hôte source, afin que l'hôte de destination puisse assurer ces deux fonctionnalités.

La couche N-1 de l'hôte source peut, éventuellement, ajouter des informations, généralement appelées **informations de contrôle**, qui permettront au niveau N-1 de l'hôte de destination, de vérifier que les informations de la couche N n'ont pas été altérées durant la communication.

Une fois que la couche N-1 a reçu, éventuellement vérifié, puis réassemblé les informations de niveau N-1 en une information de niveau N, il faut que la couche N-1 sache à quel protocole de la couche N transmettre cette information. Pour se faire, la couche N-1 de destination lit une information insérée par la couche N-1 de l'hôte source : l'identifiant de protocole de niveau N auxquelles correspondent les informations en cours de traitement. Cet identifiant de niveau N, permet à la couche N-1 d'identifier, puis de regrouper les données d'un même protocole. La couche N-1 est ainsi en mesure de transporter différents protocoles de niveau N.

Le principe de passage d'une couche N+1 vers une couche N est le suivant :



Ce schéma montre que la couche N a rajouté deux types d'informations :

- ◆ **l'en-tête {header}** : il stocke en général :
 - les adresses destination et source de niveau N,
 - le protocole de niveau N+1 transporté,
 - la longueur des données de niveau N,
 - des bits de priorité,
 - des indications de **séquencements**
 - position dans l'information initiale de niveau N,
 - dernier octet de l'information initiale de niveau N,
- ◆ **l'en-queue {trailer}** : il transporte généralement un ou plusieurs **octets de contrôle**, afin de s'assurer que l'information n'a pas varié durant son transit par le réseau. Les termes **suffixe**, **terminaison** et **queue de bande** constituent des synonymes d'en-queue.

L'ensemble des informations d'encapsulation, en-tête et terminaison, est appelée **PCI** {Protocol Control Information}.

L'encapsulation :

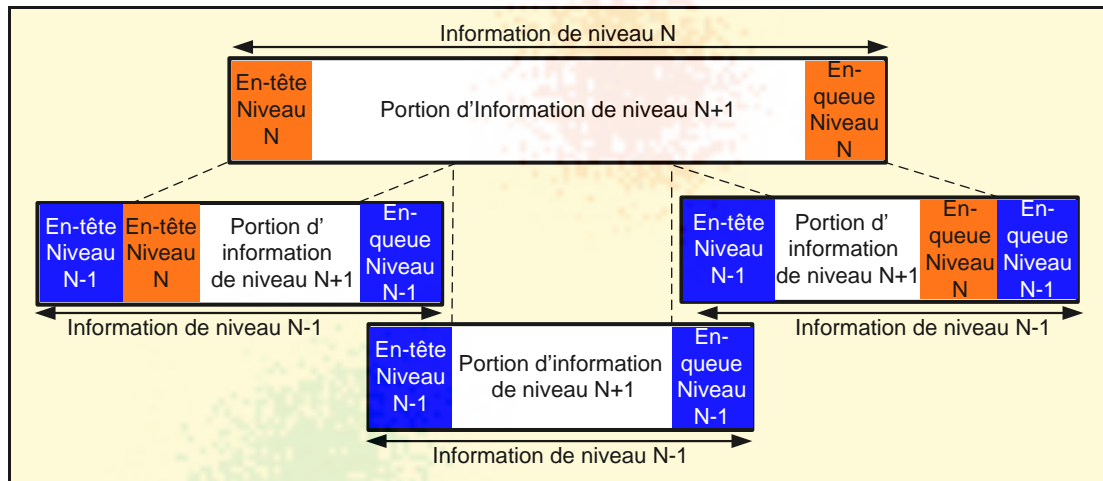
- ◆ identifie et regroupe les données d'une même communication, d'un même flux ;
- ◆ insère des informations permettant d'identifier la source et la destination ;
- ◆ garantit que les données seront adressées à la bonne destination ;
- ◆ réassemble les données sur la destination ;
- ◆ peut insérer une somme de contrôle.

La structure des N-PDUs détermine comment est réalisée l'encapsulation au niveau N. Comme ce sont les protocoles qui définissent la structure des PDUs, ce sont également les protocoles qui définissent les critères d'encapsulation.

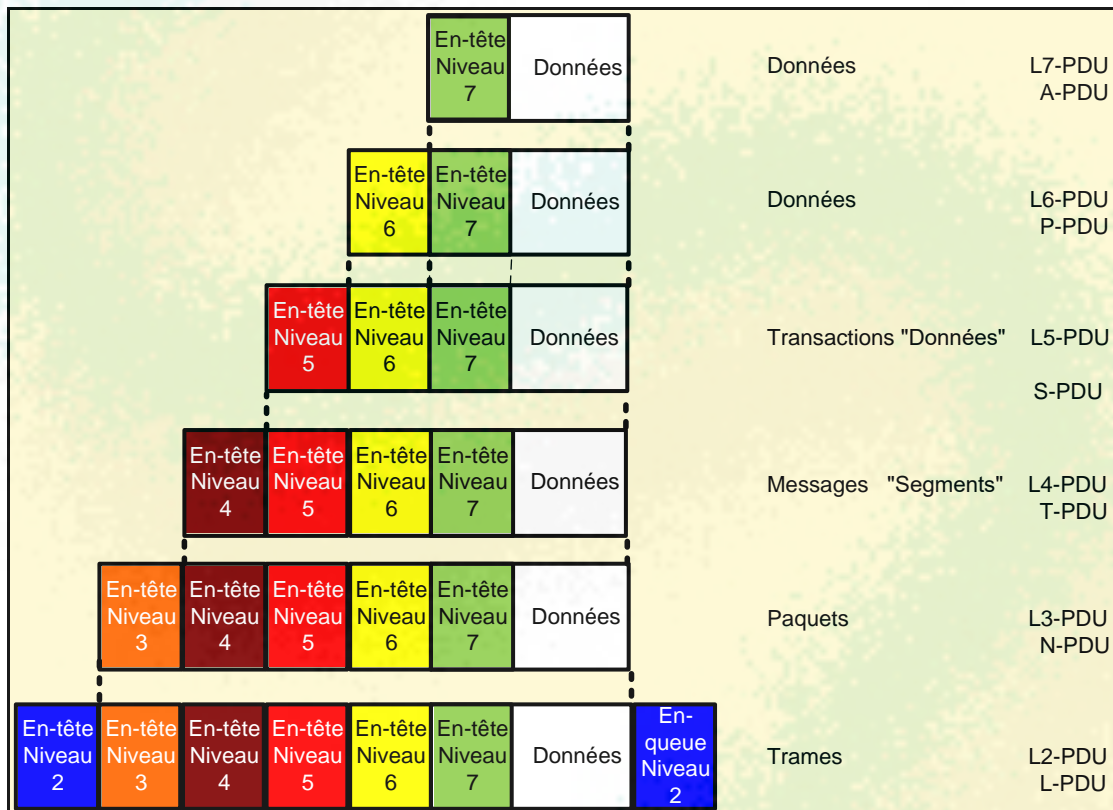
Rappel : un protocole :

- ◆ **définit ce qui doit être réalisé :**
 - **structure de la PDU qui correspond aux critères d'encapsulation,**
 - **interaction avec les couches voisines ;**
- ◆ **ne définit pas comment cela doit être réalisé.**

Pratiquement, seul le niveau 2 {liaison de données, data link}, gère les en-queues. Les autres niveaux utilisent un champ de l'en-tête pour le traitement des sommes de contrôle. La figure suivante illustre la combinaison des mécanismes de segmentation et d'encapsulation.



Ce procédé est gourmand en temps et en capacités de traitement. De plus, en insérant des informations de service dans les en-têtes et les en-queues, il contribue à diminuer le débit utile du réseau. C'est le phénomène de **surcharge {overhead}** dans le transport des données. Pour remédier à ces inconvénients, les couches hautes tentent de déterminer le nombre maximum d'octets que peut accepter une unité d'information de niveau 2. Ceci leur permet de générer des unités d'informations qui pourront "descendre" les niveaux jusqu'à la couche liaison de données, sans devoir être fragmentées.



4) Modèle OSI : la couche physique {physical layer, L1}

4.1) Fonctionnalités de la couche physique

Cette couche décrit les supports {média} ainsi que les connecteurs qui permettent de relier les périphériques entre eux, et comment les bits sont représentés sur les supports. Les fonctions principales assurées par la couche physique sont donc :

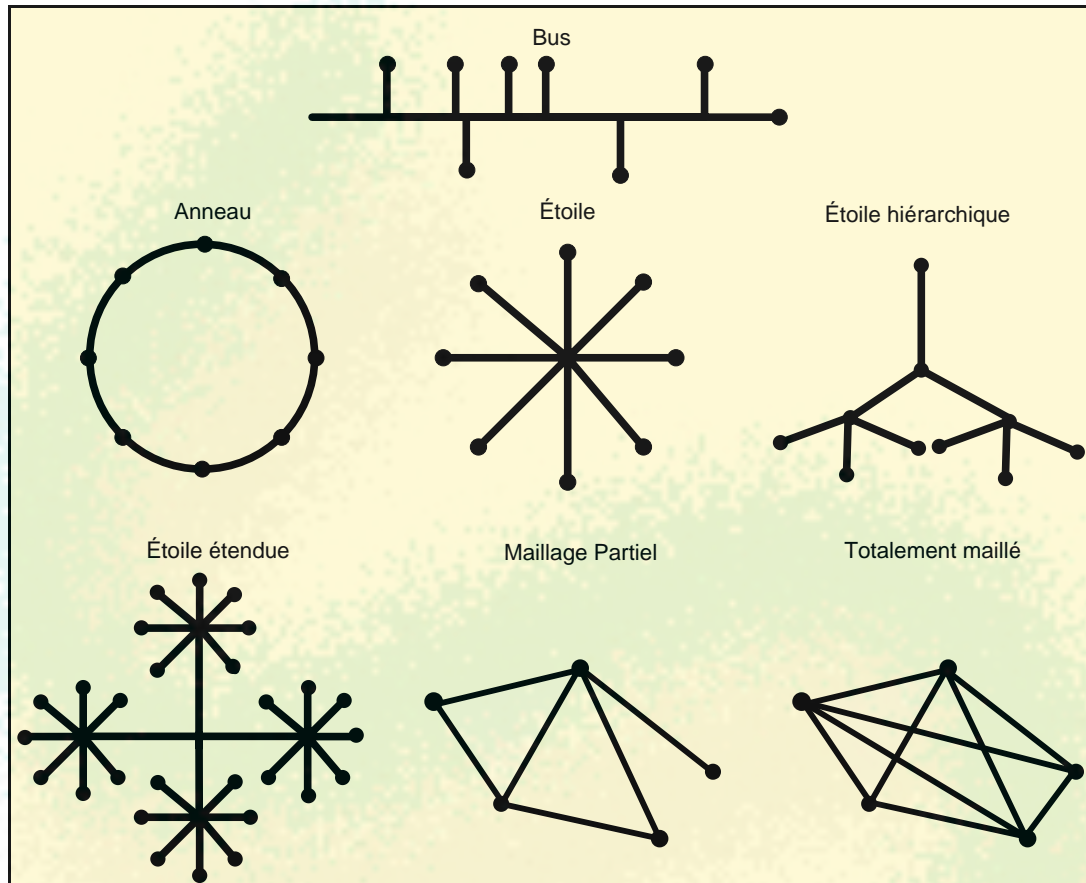
- ◆ la définition de la structure des médias {support} de communication et des connecteurs ;
- ◆ le codage et la représentation des bits ;
- ◆ l'émission et réception des signaux représentant les bits.

Pour que deux périphériques finaux puissent dialoguer au niveau 1, il faut que ces périphériques :

- ◆ représentent les bits de la même façon et utilisent des connecteurs compatibles;
- ◆ soient directement connectés, ou ne soient séparés que par des périphériques intermédiaires qui représentent les bits de la même façon, et qui utilisent des médias compatibles.

4.2) La structure physique du réseau ou topologie physique

Les topologies les plus courantes sont le **bus** {bus}, l'**étoile** {star}, l'**étoile étendue** {extended star}, l'**anneau** {ring}, la **topologie hiérarchique** {hierarchical, tree}, et le **maillage** {mesh}, avec ses deux variantes **maillage partiel** {partially meshed} et **totallement maillé** {full meshed}.



Les topologies LANs les plus utilisées sont :

- ◆ **bus** (ancienne technologie) ;
- ◆ **anneau** (ancienne technologie) ;
- ◆ **étoile** ;
- ◆ **étoile étendue**.

Les topologies WANs les plus utilisées sont :

- ◆ **point à point** ;
- ◆ **hub and spoke**. Il s'agit une topologie en étoile particulière, dans laquelle les nœuds périphériques ne peuvent pas échanger de données entre eux. Les seuls échanges possibles se font entre un nœud périphérique (**agence, branch office**) et le nœud central (site central) ;
- ◆ **maillée** : une topologie totalement maillé garantit la haute disponibilité mais peut s'avérer onéreuse.

4.3) Transmission Simplex, Half-duplex, Full-duplex

Une transmission **simplex** ne transmet les données que dans un sens {**unidirectionnel**}.

Une transmission **half-duplex** {à l'**alternat**} véhicule les données tantôt dans un sens tantôt dans l'autre sens {bidirectionnelle en alternance}.

Une transmission **full-duplex** constitue une communication **bidirectionnelle simultanée**.

4.4) Structures et caractéristiques des médias {support}

Il existe deux types de supports de transmission :

- ◆ Les supports visibles (câbles, fils) appelés supports limités. Les médias les plus répandus sont : les câbles coaxiaux, la paire torsadée, la fibre optique. ;
- ◆ Les supports invisibles ou supports non limités (non traités ici).

4.4.1) Les câbles coaxiaux RG {Radio Grade} et les connectiques associées

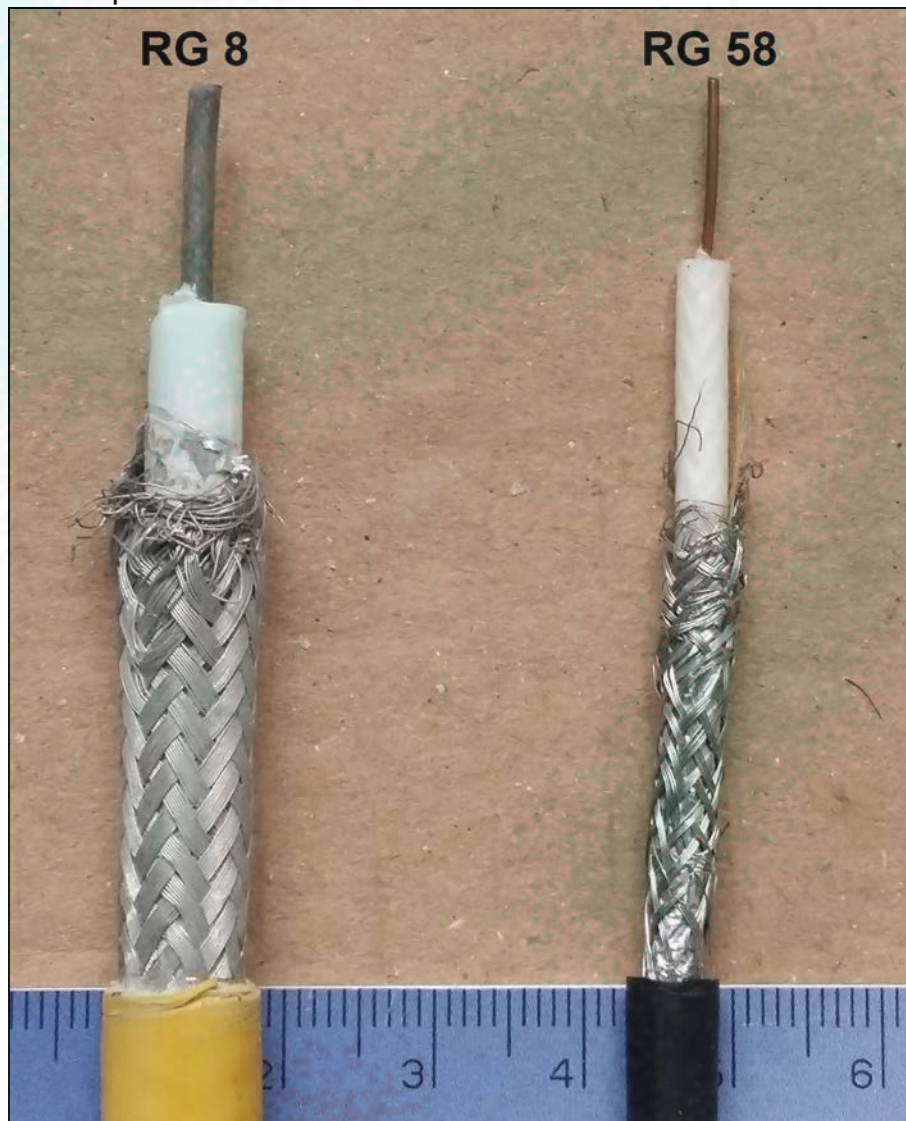
Les **câbles coaxiaux** sont constitués :

- ◆ d'une âme de **cuivre** qui constitue le conducteur central ;
- ◆ d'un diélectrique, isolant qui entoure l'âme ;
- ◆ d'un blindage en métal tressé qui enveloppe le diélectrique ;
- ◆ d'une gaine plastique qui recouvre l'ensemble.

Ces câbles sont connus sous le terme de générique **RG {Radio Grade}**. Les plus répandus sont :

- ◆ **RG 69** : ancien système ARCNET, impédance de **93 Ω** {Ohms} ;
- ◆ **RG 59** : câble d'antenne de télévision, impédance de **75 Ω** ;
- ◆ **RG 8** : coaxial épais {**Thick Ethernert**}, support originel d'Ethernet : impédance de **50 Ω** ;
- ◆ **RG 58** coaxial fin {**Thinnet**}, utilisé pour le câblage Ethernet, impédance de 50 Ω .

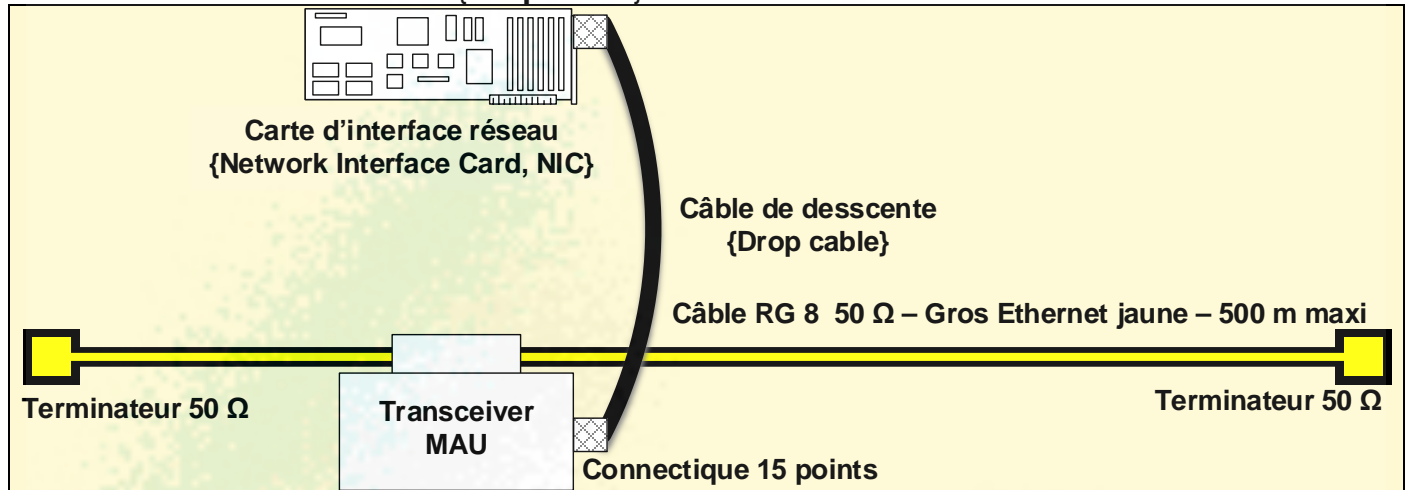
Les câbles coaxiaux les plus utilisés dans les réseaux locaux furent les câbles RG 8 et RG 58



Plus le diamètre de l'âme est important, plus le câble, est de qualité. Ainsi un segment **RG 58** est **restreint à 185 mètres**, tandis qu'un segment qu'un segment de **RG 8** peut **atteindre jusqu'à 500 mètres**.

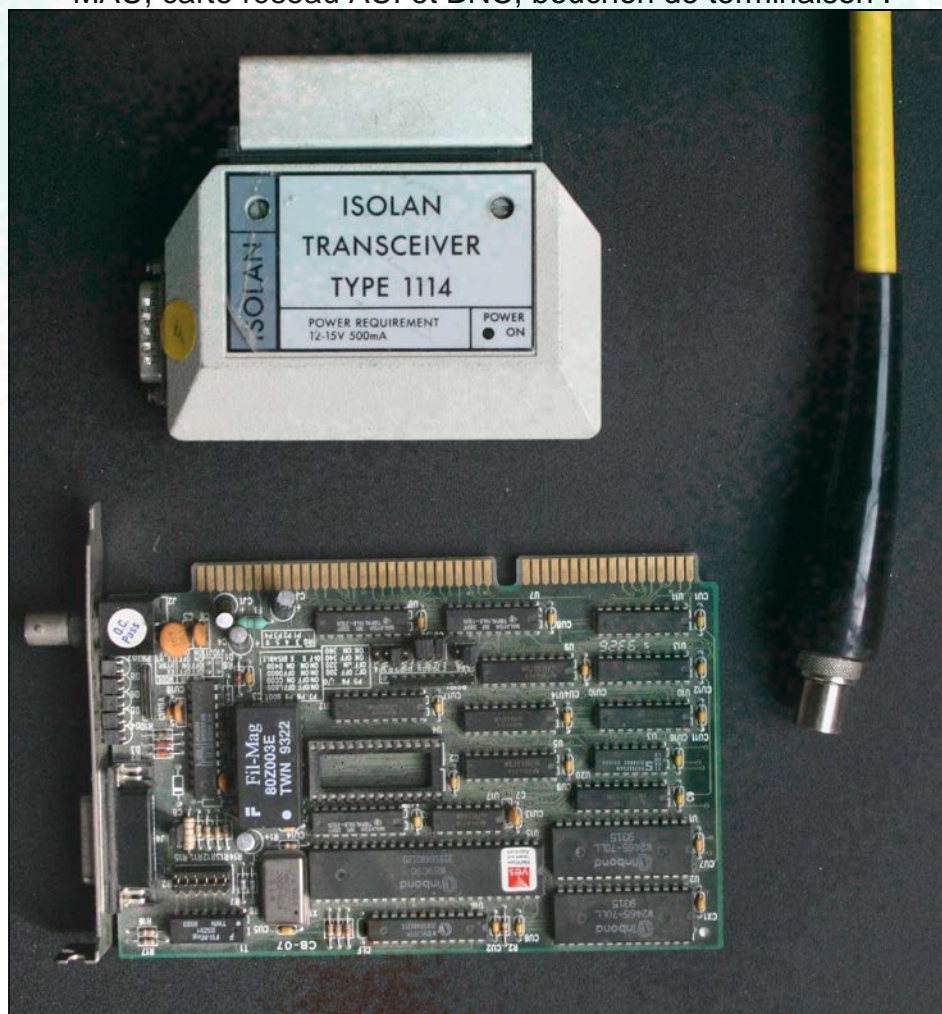
Un câblage **Thick Net {RG 8}** est connecté à une carte réseau **{Network Interface Card, NIC}** par l'intermédiaire :

- ◆ d'un **MAU {Media Attachment Unit}** appelé **transceiver** ou **prise vampire** ;
- ◆ d'un **câble de descente {Drop cable}**.

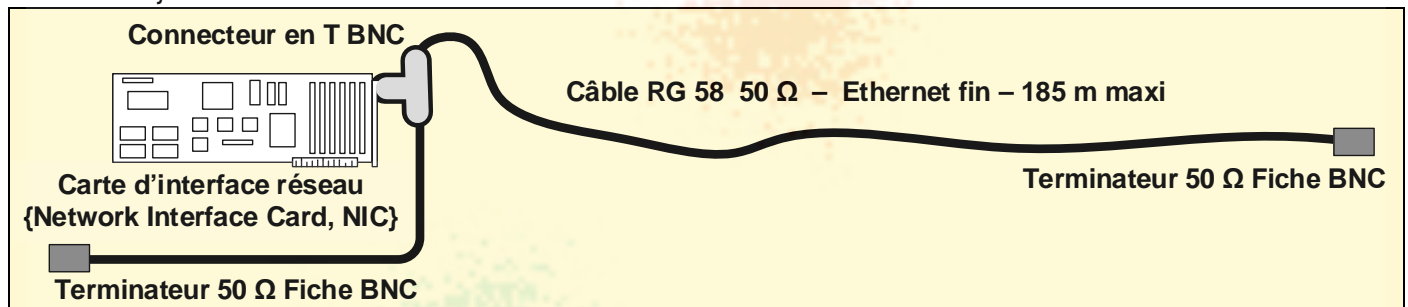


La connectique MAU / Drop cable et Drop cable / NIC est de type **AUI {Attachment Unit Interface}** 15 points.

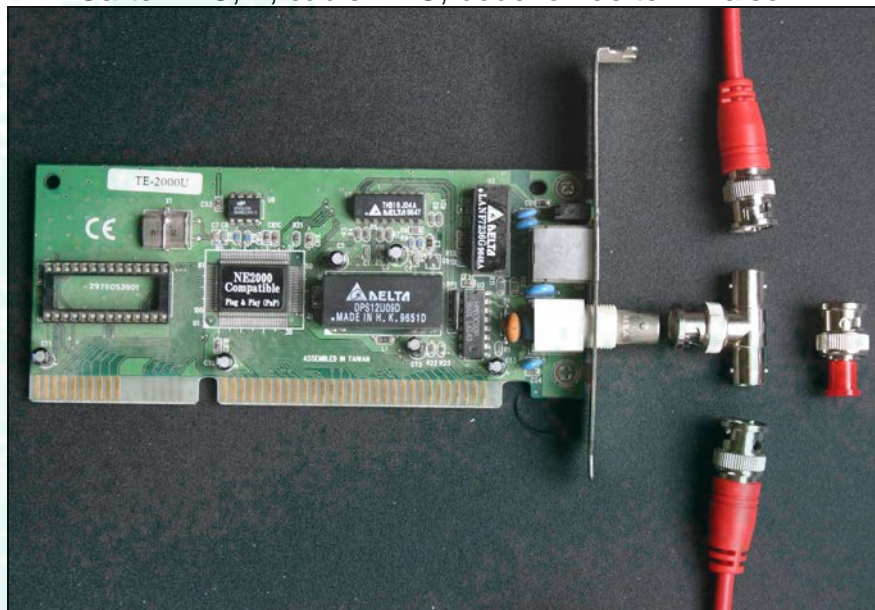
MAU, carte réseau AUI et BNC, bouchon de terminaison :



Le câble RG 58 est connecté à la carte réseau par l'intermédiaire d'une prise **BNC** {**British Naval Connector**} en forme de T.



Carte BNC, T, câble BNC, bouchon de terminaison :



Les bus à base de câbles coaxiaux doivent être munis à chaque extrémité d'un bouchon de terminaison {terminateur}.

Les principales caractéristiques associées aux câbles coaxiaux sont :

- ◆ l'**atténuation**. Elle s'exprime en décibel {dB} par unité de longueur. Plus sa valeur est petite plus le support est meilleur.
- ◆ le **temps de propagation** ou **coefficient de vélocité**. Il s'exprime en pourcentage de la vitesse de la lumière dans le vide ;
- ◆ l'**impédance** exprimée en **Ohm**, symbole Ω .

4.4.2) Les paires torsadées {Twisted Pair} et les connectiques associées

Un **câble à paire(s) torsadée(s)** est constitué d'un ensemble de fils conducteurs métalliques. Chacun de ces fils métalliques est entourés d'un isolant. Ces brins, fils métallique et isolants, sont torsadés par paires. Chaque conducteur transporte un signal électrique qui génère autour de ce brin un champ magnétique circulaire qui pourrait parasiter le signal d'un conducteur voisin. Dans une paire, les deux conducteurs, très proches, font transiter le courant électrique en sens inverse, créant ainsi deux champs magnétiques opposés qui ont tendance à s'annuler, évitant ainsi de parasiter les paires voisines. C'est le phénomène **d'annulation des champs magnétiques**. L'utilisation d'un nombre différent de torsades par unité de longueur pour chaque paire réduit encore les perturbations entre paires voisines.



Les conducteurs métalliques sont constitués de **cuivre {copper}** pur, ou d'un alliage cuivre aluminium. Cependant les câbles à paires torsadées sont presque toujours référencés comme de câbles de cuivre. L'**American Wire Gauge {AWG}** normalise le diamètre des fils conducteurs. Plus le nombre est important, plus le diamètre est faible.

Les principales caractéristiques associées aux paires torsadées sont :

- ◆ **l'affaiblissement linéique, ou atténuation.** Il s'exprime en décibel par unité de longueur ;
- ◆ **l'affaiblissement dû à la diaphonie.** La diaphonie caractérise les interférences créées par les paires voisines sur une paire, et se mesure en décibel (**dB**). Il existe plusieurs types de diaphonie.
 - la **paradiaphonie** {diaphonie locale, **NEXT, Near End crossTalk**} mesure les interférences créées localement, sur une paire, par une autre paire,
 - la **télédiaphonie** {diaphonie distante, **FEXT, Far End crossTalk**} mesure les interférences créées à l'autre extrémité d'une paire, par une autre paire,
 - la **diaphonie locale totale** {**PSNEXT, Power Sum Near End crossTalk**} mesure les interférences créées localement, sur une paire, par l'ensemble des autres paires,
 - la **diaphonie distante totale**, {**FSFEXT, Power Sum Far End crossTalk**} mesure les interférences créées, à l'autre extrémité d'une paire, par l'ensemble des autres paires ;
- ◆ la **vitesse de propagation** du signal;
- ◆ l'**impédance** des conducteurs exprimée en **Ohm**, symbole **Ω** .

4.4.3) Câbles à 4 paires torsadées à connectique 8P8C {RJ45}

Les câbles à paires torsadées les plus utilisés sont constitués de quatre paires différenciées par la couleur des isolants :

- ◆ paire blanc orange / orange ;
- ◆ paire blanc vert / vert ;
- ◆ paire bleu / blanc bleu ;
- ◆ paire blanc marron / marron.

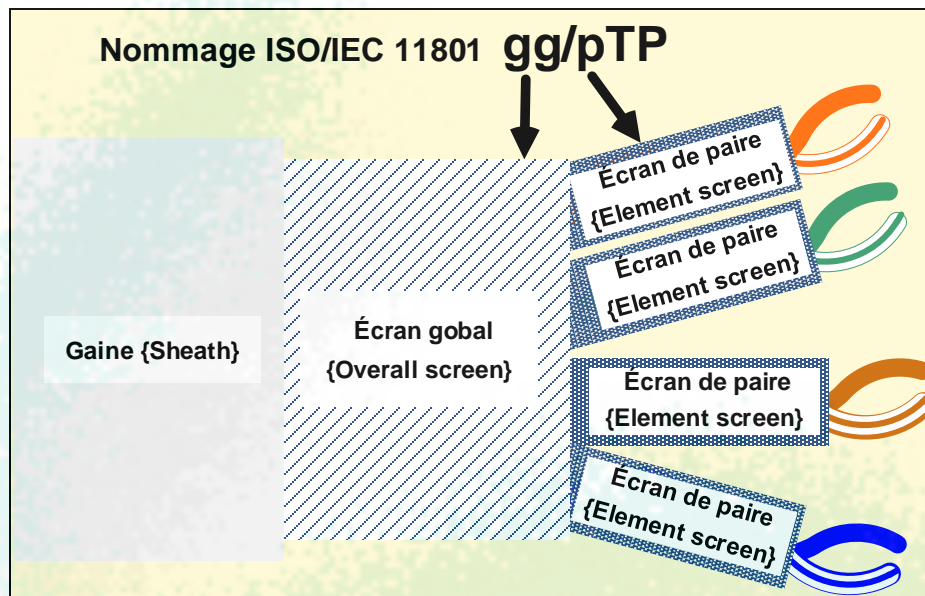
Cet ensemble de quatre paires :

- ◆ est maintenu ensemble par une gaine isolante ;
- ◆ **peut être écranté {screened}**. Dans ce cas, une protection située entre la gaine isolante et les quatre paires, joue le rôle d'écran et protège les paires des perturbations électromagnétiques de l'environnement. Cette protection globale de l'ensemble des paires est constituée d'une **feuille métallique** appelée **feuillard {foil}** et/ou d'une **trousse {braid}** **métallique**.

Chacune des paires **peut être** protégée des perturbations extérieures mais aussi des perturbations générées par les autres paires grâce à un **écran {screen}** constitué par une **feuille métallique** appelée **feuillard {foil}**.

Le standard international **ISO/IEC 11801** intitulé « *Information technology – Generic cabling for customer premises* » normalise, entre autre, les diverses dénominations des câbles à quatre paires torsadées. La convention de nommage ISO/IEC 11801 pour les câbles à quatre paires torsadées est du type **gg/pTP** :

- ◆ **gg** caractérise la protection globale de l'ensemble des paires :
 - **gg = U** {Unscreened} pas de protection (screen : écran, screened : filtré, blindé),
 - **gg = F** {Foil screened} protection par feuillard (foil : feuille, feuillard),
 - **gg = S** {Braid screen} protection par tresse (braid : tresse),
 - **gg = SF** {Braid and Foil screen} protection globale par une tresse qui entoure un feuillard;
- ◆ **p** caractérise la protection de chaque paire :
 - **p = U** {Unscreened} pas de protection sur aucune paire du câble,
 - **p = F** {Foil screened} protection par feuillard sur chaque paire du câble;
- ◆ **TP** signifie Twisted Pair [paire torsadée].



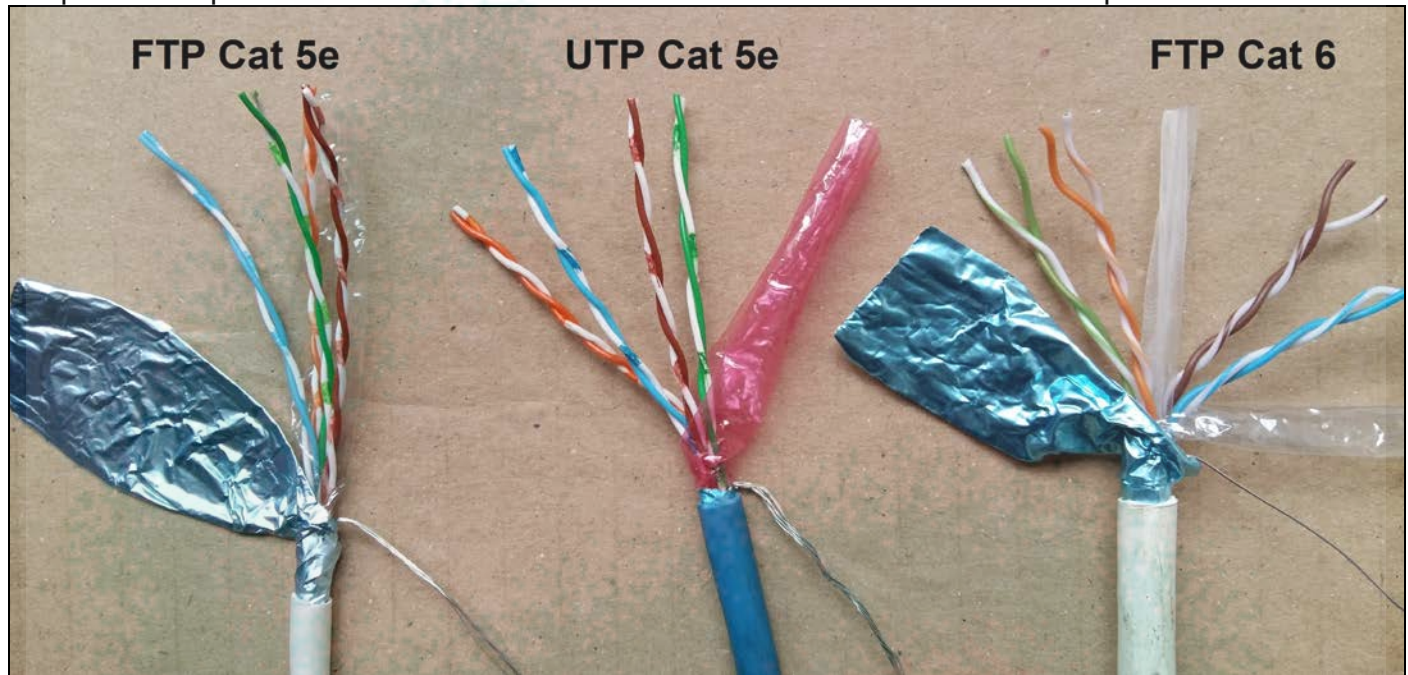
Les photographies ci-dessous représentent l'anatomie d'un câble S/FTP, ainsi que l'inscription figurant sur sa gaine externe. Les deux photographies ne sont pas à la même échelle.



Avant que cette norme de nommage ne soit adoptée, de nombreux fabricants avaient conçu différents types de câbles à paires torsadées et référencé ces types de câbles par des acronymes plus ou moins standards. Ces acronymes ne devraient plus être utilisés.

Les "anciennes" dénominations les plus connues de câbles à paires torsadées sont :

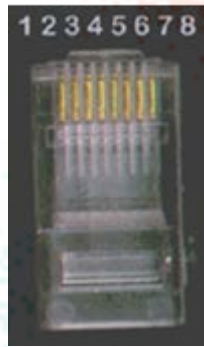
- ◆ **UTP** {**U**nshielded **T**wisted **P**air, paire torsadée non blindée} : correspond au câble U/UTP ;
- ◆ **FTP** {**F**oiled **T**wisted **P**air, paire torsadée écrantée} : correspond au câble F/UTP ;
- ◆ **STP** {**S**hielded **T**wisted **P**air, paire torsadée blindée} : correspond à un câble possédant au moins une protection autour de l'ensemble des paires et/ou autour de chacune des paires. La protection pouvant être une tresse ou un feuillard. FTP constitue un exemple de STP.



La norme TIA/EIA 568 définit les catégories de câbles à paires torsadées :

- ◆ catégorie 1 : transmission de la voix, fil téléphonique traditionnel ;
- ◆ catégorie 2 : transmission de données jusqu'à 4 Mbps ;
- ◆ catégorie 3 : transmission de données jusqu'à 10 Mbps ;
- ◆ catégorie 5 : transmission de données :
 - débit initialement limité à 100 Mbps,
 - supporte la technologie Gigabit développée par Intel,
- ◆ catégorie 5e : transmission de données :
 - amélioration de la catégorie 5, e pour enhanced {amélioré},
 - recommandée pour le Gigabit,
 - correspond à la **classe D ISO/IEC 11801** ;
- ◆ catégorie 6 : transmission de données :
 - un nouvel élément apparaît, il s'agit d'un isolant central qui sépare les paires, et qui permet d'augmenter le débit,
 - supporte le 10 Gigabit jusqu'à 56 mètres,
 - correspond à la **classe E ISO/IEC 11801** ;
- ◆ catégorie 6a :
 - category 6a pour **augmented category 6**,
 - supporte le 10 Gigabit jusqu'à 100 mètres,
 - correspond à la **classe Ea ISO/IEC 11801** ;
- ◆ catégorie 7 correspond à **classe F ISO/IEC 11801** ;
- ◆ catégorie 7a correspond à **classe Fa ISO/IEC 11801** ;

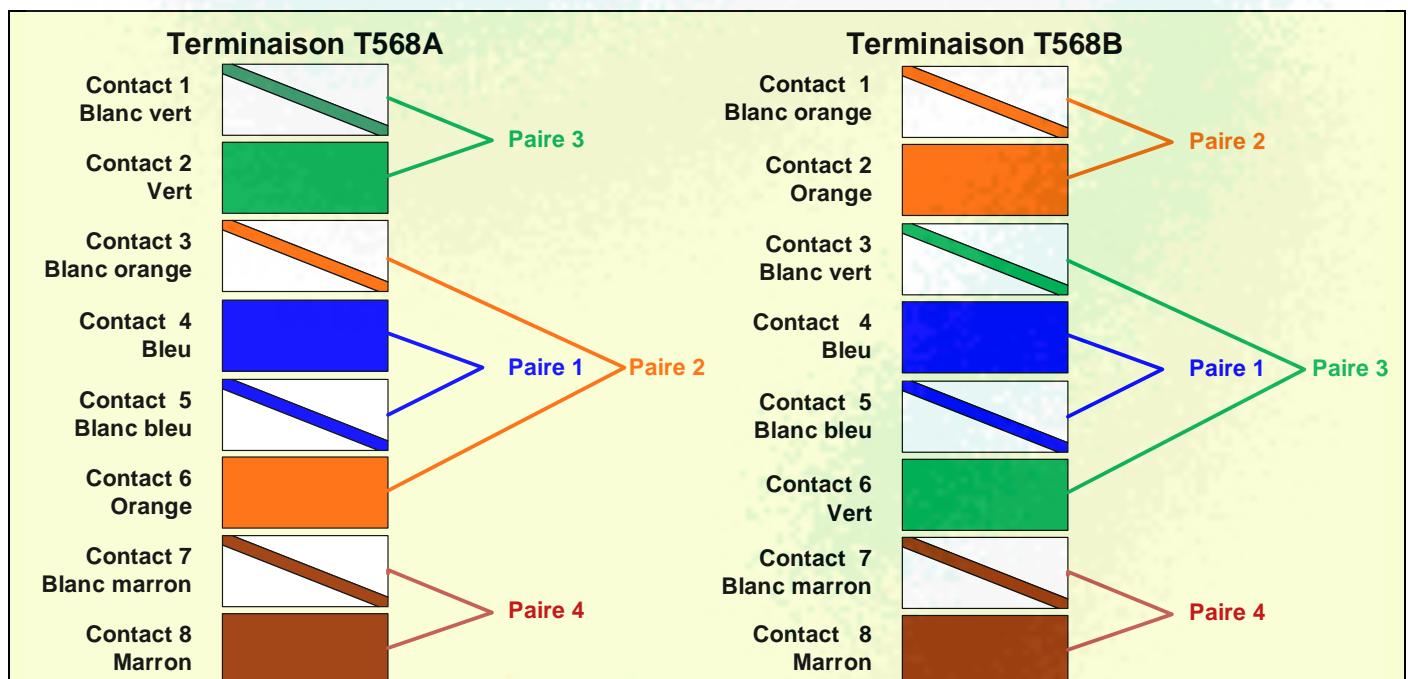
Les connecteurs associés aux câbles de la catégorie 3 à la catégorie 6a sont de type **RJ45** {Registered Jack 45} à 8 contacts numérotés de 1 à 8. Les contacts d'une prise RJ45 mâles sont numérotés de 1 à 8, à partir de la gauche, en regardant le connecteur par-dessus (clips en dessous).



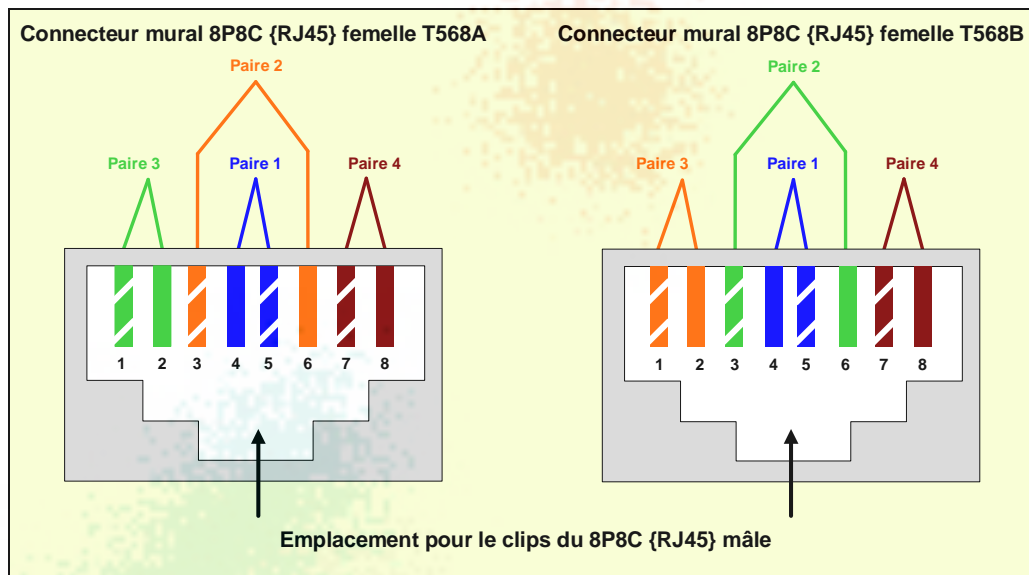
Les normalisations EIA/TIA 568 numérotent les paires, indiquent comment connecter les brins d'un câble à 4 paires torsadées dans une prise RJ45. Il existe deux terminaisons T568A et T568B. Les deux terminaisons utilisent les mêmes couples de contacts (1-2), (3-6), (4-5) et (7-8), et la même numérotation des paires. Par contre, les deux terminaisons n'associent pas les mêmes codes couleurs aux couples de contact et numéro de paires.

Les différences entre les terminaisons T568A et T568B sont :

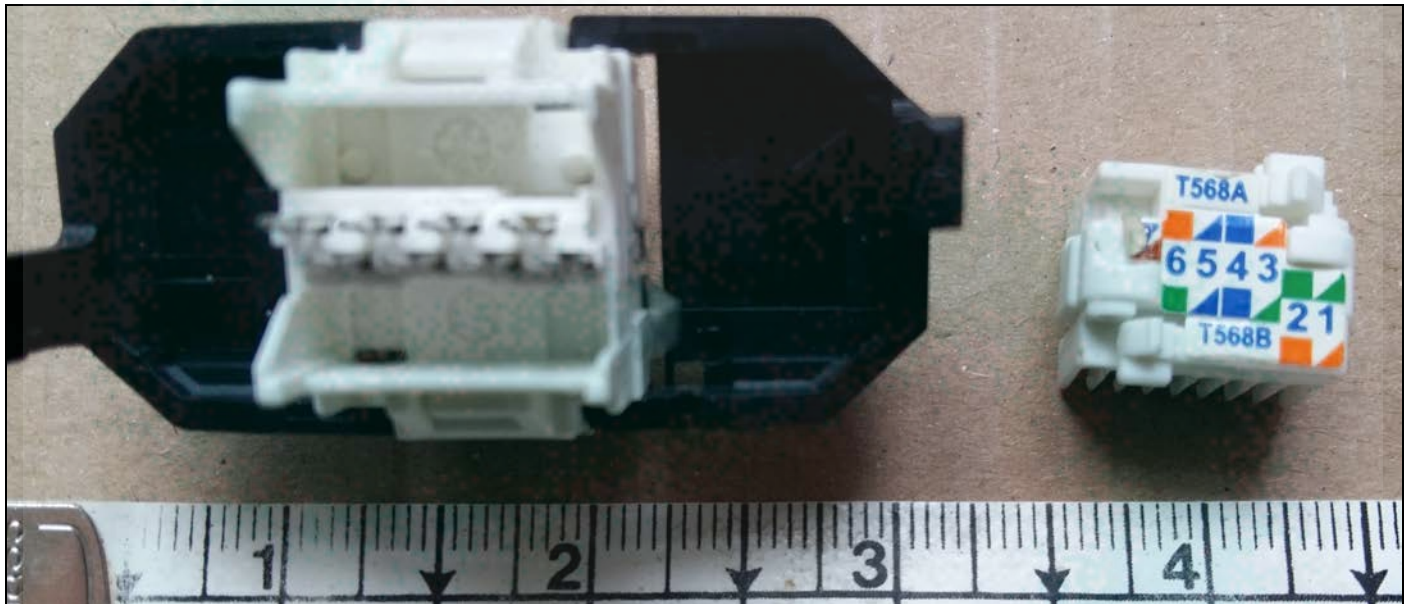
- ◆ **T568A :**
 - **Contacts (1-2)** = paire 3 associée aux couleurs **blanc vert / vert**,
 - **Contacts (3-6)** = paire 2 associée aux couleurs **blanc orange / orange**,
 - **Contacts (4-5)** = paire 1 associée aux couleurs **bleu / blanc bleu**,
 - **Contacts (7-8)** = paire 4 associée aux couleurs **blanc marron / marron** ;
- ◆ **T568B :**
 - **Contacts (1-2)** = paire 3 associée aux couleurs **blanc orange / orange**,
 - **Contacts (3-6)** = paire 2 associée aux couleurs **blanc vert / vert**,
 - **Contacts (4-5)** = paire 1 associée aux couleurs **bleu / blanc bleu**,
 - **Contacts (7-8)** = paire 4 associée aux couleurs **blanc marron / marron**.



Les connecteurs RJ45 mâles terminent les câbles reliant un terminal à une prise murale femelle qui respecte également le code des couleurs.



La photographie suivante montre la face arrière d'un connecteur mural femelle RJ45. Ces connecteurs utilisent un mécanisme auto-dénudant.



La terminaison T568A est employée en Amérique du nord, tandis que la terminaison T568B est employée en Europe.

Remarque : le terme RJ provient du vocabulaire utilisé pour décrire des connecteurs dédiés à la téléphonie, et son usage est "inapproprié" pour la transmission de données, et devrait donc être proscrit. Ainsi, il faudrait parler de :

- ◆ connecteur 8P8C ou connecteur modulaire 8/8 plutôt que de RJ45 ;
- ◆ connecteur 6P2C ou connecteur modulaire 6/2 plutôt que de RJ11.

8P8C signifiant 8 broches {position} et 8 contacts.

4.4.4) Câbles à 1 ou 2 paires torsadées et connecteurs RJ11 et RJ14

Tandis que les câbles à 4 paires torsadées sont utilisés pour la transmission de données, les câbles à une ou deux paires torsadées sont réservés aux transmissions analogiques de type voix de la téléphonie classique, non IP. Pour transmettre la voix, il suffit d'une paire. Les connectiques associées sont, normalement, de type RJ11. Un connecteur RJ11 possède six emplacements {positions} mais seuls les deux emplacements centraux sont munis de broches {contact} sont présents.

Il est de plus en plus courant que les connectiques RJ14 soient utilisées à la place des connecteurs RJ11. Un connecteur RJ14 possède six emplacements {positions} mais seuls les quatre emplacements centraux sont munis de broches {contact}.

Le terme RJ provient du vocabulaire utilisé pour décrire des connecteurs dédiés à la téléphonie, et son usage est "inapproprié" pour la transmission de données, et devrait donc être proscrit. Ainsi, il faudrait parler de connecteur :

- ◆ 8P8C ou encore connecteur modulaire 8 broches / 8 emplacements plutôt que de RJ45 ;
- ◆ 6P6C ou encore connecteur modulaire 6 broches / 6 emplacements plutôt que de RJ12 ;
- ◆ 6P4C ou encore connecteur modulaire 4 broches / 6 emplacements plutôt que de RJ14 ;
- ◆ 6P2C ou encore connecteur modulaire 2 broches / 6 emplacements plutôt que de RJ11.

Un connecteur mâle RJ11 {6P2C} peut être inséré dans une RJ45 {8P8C}, et la norme garantie que les deux contacts centraux du connecteur RJ11 mâle sont en contact avec les contacts centraux (4-5) de la prise RJ45 femelle.

Un connecteur mâle RJ14 {6P4C} peut être inséré dans une RJ45 {8P8C}, et la norme garantie que les quatre contacts centraux du connecteur RJ14 mâle sont en contact avec les contacts centraux (4-5 et 3-6) de la prise RJ45 femelle.

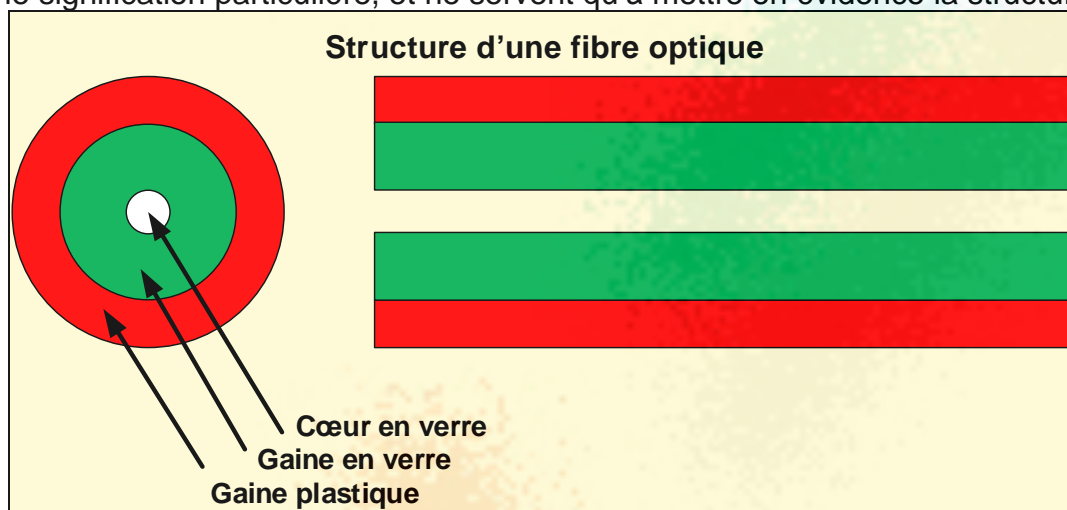
Il existe beaucoup d'autres connecteurs de type RJ, les connecteurs RJ9 {4P4C} par exemple, ce sont des connecteurs à quatre emplacements et quatre contacts. Ils sont utilisés pour connecter un combiné microphone-écouteur à un téléphone.

4.4.5) La fibre optique

Les câblages en fibres optiques sont déployés dans plusieurs domaines d'activité :

- ◆ les **réseaux d'entreprises** {Enterprise Networks} : la fibre est mise en œuvre dans le réseau fédérateur et pour raccorder les périphériques des centres de donnée {data-centers} ;
- ◆ la **fibre optique jusqu'au domicile** {FTTH, Fiber-To-The-Home} qui fournit le haut débit aux particuliers, aux **TPE** {Très Petites Entreprises} et aux **ETI** {Entreprise de Taille Intermédiaire} ;
- ◆ les **réseaux longue distance** {Long-Haul Networks} qui relient les villes ou les pays ;
- ◆ les **réseaux sous-marins** {Submarine Networks} qui nécessitent un medium très résistant et supportant de très hauts débits.

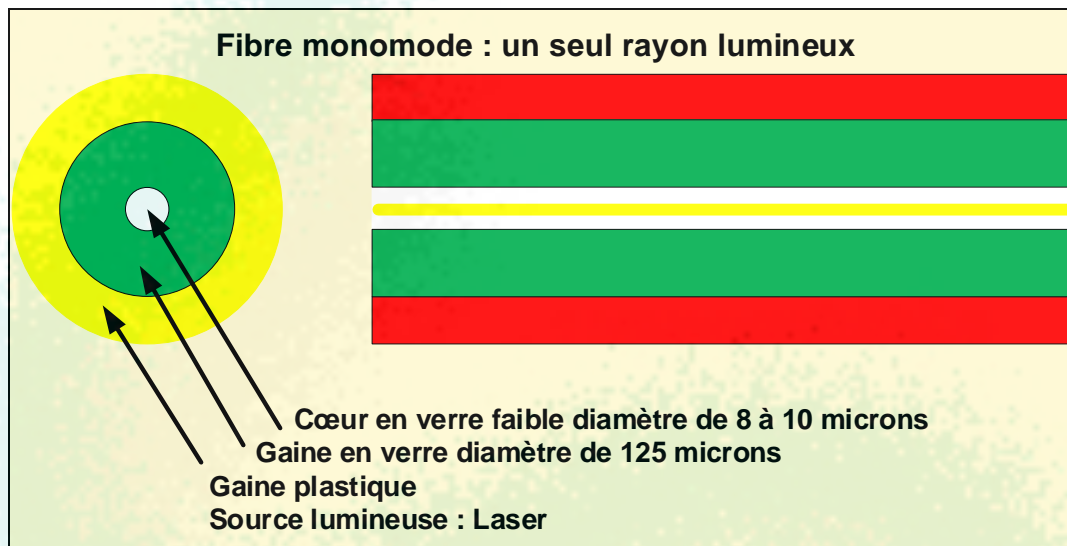
La **fibre optique** est un support qui véhicule les signaux lumineux. Une fibre optique est constituée d'un **conducteur lumineux**, généralement **en verre**, dans certains cas en plastique, appelé cœur. Celui-ci est entouré d'une **gaine optique en verre**, puis d'une enveloppe externe de protection. La figure suivante, représente la structure d'une fibre optique. Les couleurs utilisées n'ont aucune signification particulière, et ne servent qu'à mettre en évidence la structure du média.



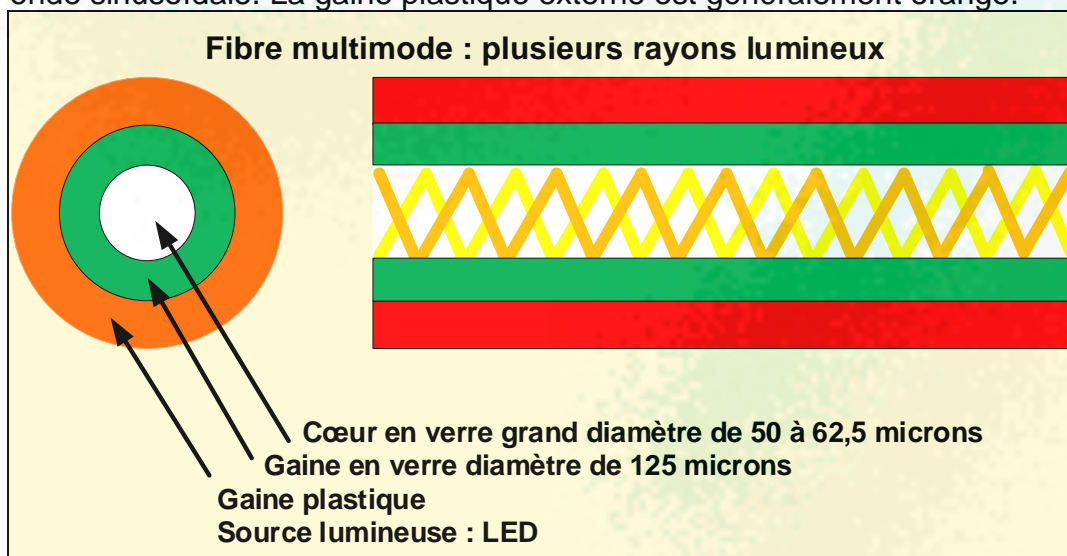
Contrairement aux câbles en cuivre, les fibres optiques ne sont sensibles ni aux **perturbations électromagnétiques** {ElectroMagnetic Interference, **EMI**}, ni aux **perturbations radioélectriques** {Radio Frequency Interference, **RFI**}. Mais c'est malheureusement le support le plus coûteux.

Une fibre optique est caractérisée par les diamètres, exprimés en **micron** { μm , 10^{-6}m }, de la gaine optique en verre et le du cœur en verre. Par exemple, 125 / 62,5 μm . La longueur d'onde de la source lumineuse est exprimée en nanomètre {nm, 10^{-9} mètre}.

Une fibre **monomode** {Single Mode Fiber, **SMF**} ne véhicule qu'un **seul signal**, habituellement généré par un **laser**, et transmis **sans réflexion**, en ligne "droite" dans un cœur de **faible diamètre**. Dans les réseaux d'entreprise, la gaine plastique externe est généralement jaune, plus rarement bleu eau (aqua).



Dans une fibre **multimode** {Multi Mode Fiber, **MMF**}, **plusieurs rayons** se propagent par **réflexion** d'angles différents dans un **cœur de grand diamètre**. La source lumineuse est généralement à base de **DEL** {Diode Electro- Luminescente, **LED**, Light-Emitting Diode}. La fibre à saut d'indice utilise la réfraction à angle droit, tandis que la fibre à gradient d'indice met en œuvre une onde sinusoïdale. La gaine plastique externe est généralement orange.



Une fibre monomode est plus onéreuse qu'une fibre multimode, et son utilisation se justifie sur les longues distances. Les fibres multimodes peuvent véhiculer un signal jusqu'à environ cinq cents mètres, tandis que les fibres monomodes peuvent s'étendre sur plusieurs dizaines de kilomètres.

Les normes de fibre développées pour les réseaux locaux font qu'une fibre ne peut transmettre un signal que dans un sens (unidirectionnel, simplex). Il faut donc deux fibres pour assurer la communication.

Par contre, pour les réseaux étendus, certaines normes sont bidirectionnelles {duplex}, et une seule fibre suffit.

Dans le cas des réseaux de type WAN, lorsqu'une fibre est installée mais pas encore utilisée, elle est qualifiée de **fibre morte** ou de **fibre noire** car, n'étant alimentée par aucune source lumineuse, aucune lumière ne la parcourt.

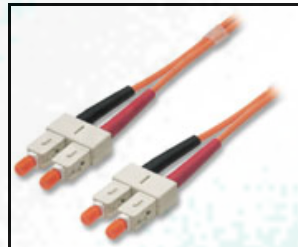
La vérification d'un câblage en fibre optique nécessite un **réflectomètre optique** {Optical Time-Domain Reflectometer, **OTDR**}.

Les connectiques les plus couramment utilisées sont de types :

ST
{Straight-Tip}



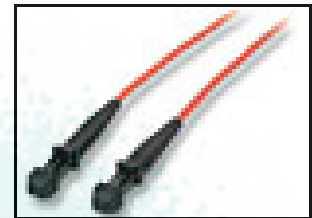
SC
{Subscriber Connector}
{Square Connector}



LC
{Lucent Connector}
{Little Connector}



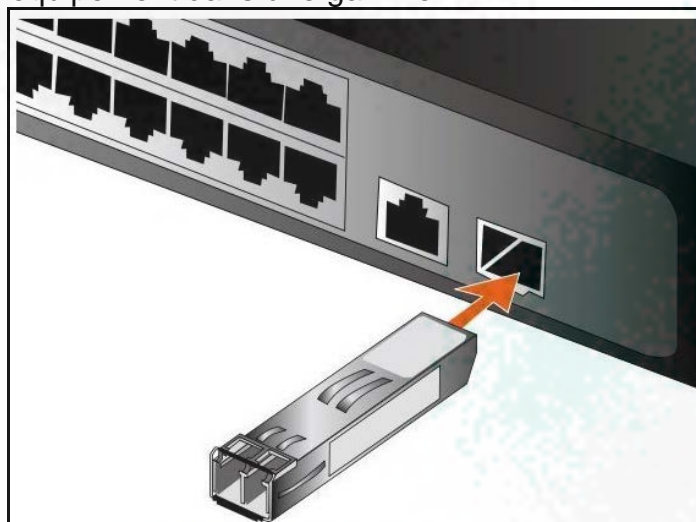
MT-RJ
{Mechanical Transfer-Registered Jack}

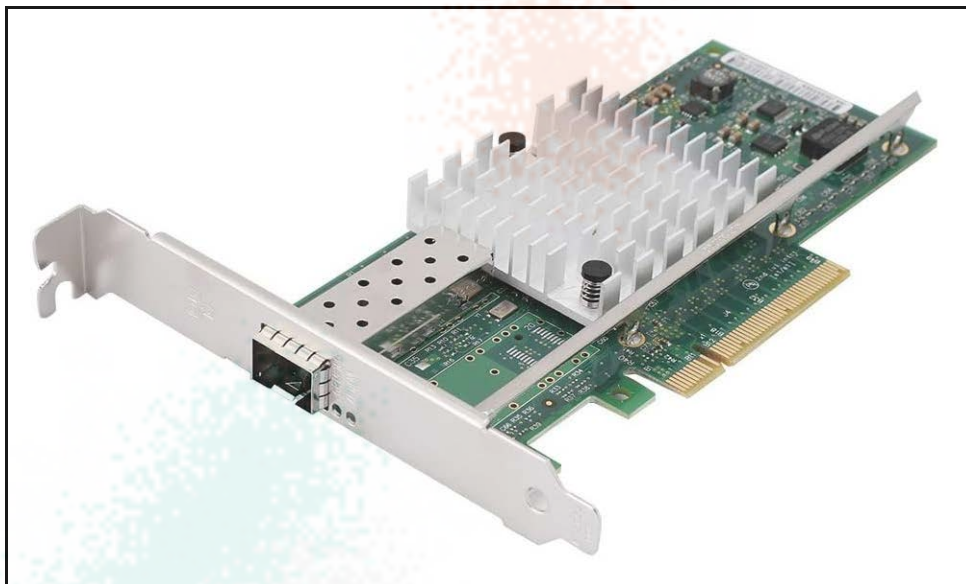


Le cœur des connecteurs ST et SC n'est pas visible sur les photographies, car il est recouvert d'une protection.

4.4.6) Les connecteurs de la famille SFP

Compte-tenu de la multitude des connecteurs fibre, les équipements auxquels ils sont connectés sont généralement équipés de ports "universels" femelles: les ports **Small form-factor pluggable transceiver** {**SFP**} initialement connus sous le nom de ports **Mini-GBIC**. Un port SFP permet d'apparier la carte mère à un connecteur particulier d'un support donné. Ceci permet de limiter le nombre de modèles d'équipement dans une gamme.





L'évolution **SFP+** {enhanced small form-factor pluggable} assure des débits jusqu'à 16 Gb/s tandis que le **Quad Small Form-factor Pluggable** {QSFP} monte jusqu'à 40 Gb/s. La récente évolution **QSFP56** supporte les 100 Gb/s.

Les adaptateurs des diverses familles SFP sont équipés d'un système d'extraction qui renseigne sur le connecteur et le type de medium supporté.

Remarque : Les modules de type SFP ne sont pas dédiés à la fibre optique. Il existe des modules pour supports cuivre.

Modules bidirectionnels fonctionnant par paire



Module de deux fibres unidirectionnelles



Module pour RJ-45 sur paires torsadée cuivre.



4.5) Câblage de raccordement, horizontal et vertical

Le **câble de raccordement** {patch cable} s'installe entre :

- ♦ un hôte et la prise murale RJ45 femelle ;
- ♦ un commutateur et le **tableau de connexions** {panneau de brassage, patch panel} dans une **armoire de répartition** {répartiteur, distribution facility, telecommunications room} ;

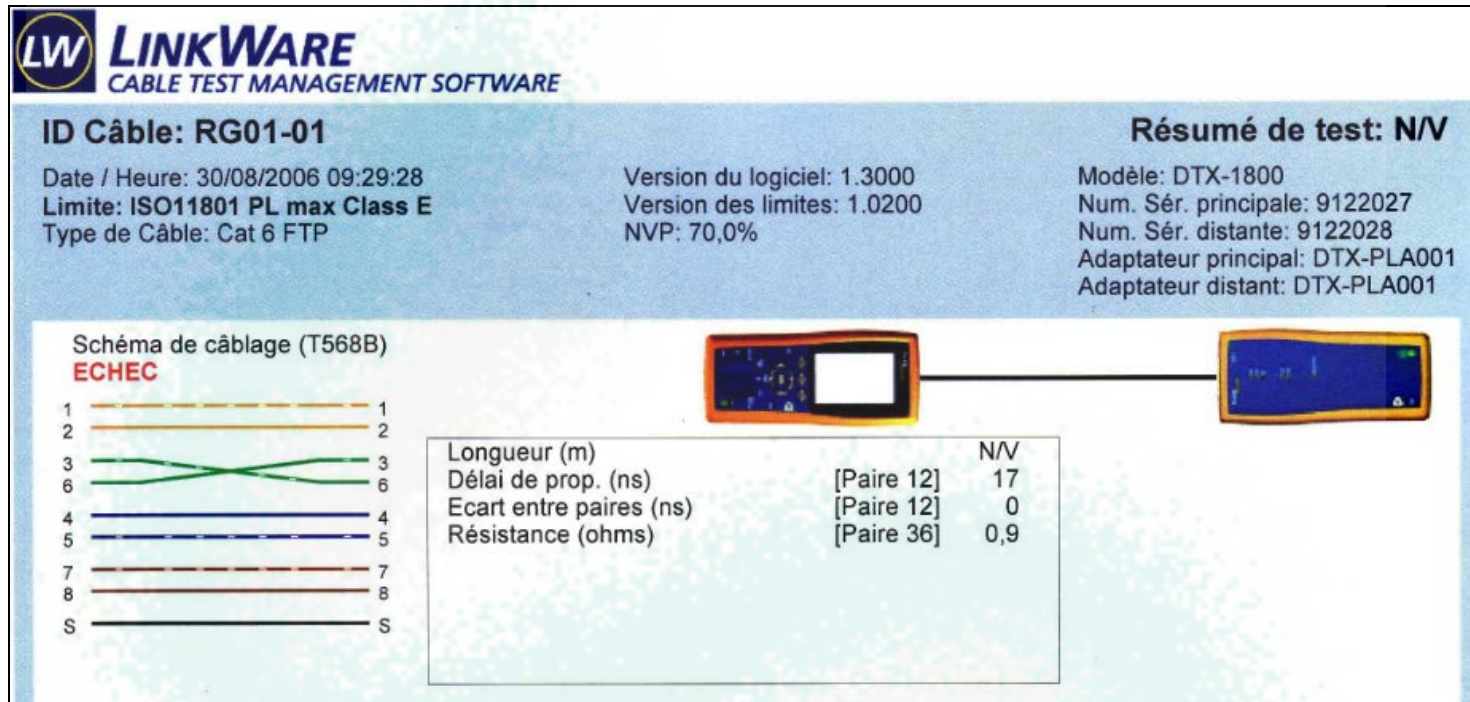
La norme ANSI/EIA/TIA-568-B appliquée aux câbles UTP spécifie que la longueur maximale d'un câble de raccordement est de cinq mètres.

Le **câblage horizontal** {horizontal cabling, distribution cabling} relie une prise RJ45 murale à un tableau de connexions dans une armoire de répartition. La norme ANSI/EIA/TIA-568-B appliquée au câble UTP spécifie que la longueur maximale d'un câblage horizontal est de quatre-vingt-dix mètres.

Le **câblage vertical** {**rocade**, **vertical cabling**, **backbone**} relie deux répartiteurs. Ce câblage peut être en fibre optique, ou assuré par un opérateur télécom si les répartiteurs sont sur des sites géographiquement distants.

4.6) Recette d'un câblage

Vous devez toujours demander à consulter le livre de recette du système de câblage sur lequel vous intervenez indirectement (ajout d'ordinateur, modifications de cartes réseaux, installation d'applications lourdes). En effet, un câble défectueux peut provoquer des phénomènes totalement aléatoires. Vous trouverez à suivre deux extraits d'un livre de recette. Le premier correspond à un câblage défectueux. Le dernier représente un câblage aux normes.



**ID Câble: RG01-02**

Date / Heure: 30/08/2006 09:22:27

Marge de Sécurité: 0,5 dB (NEXT 45-78)

Limite: ISO11801 PL max Class E

Type de Câble: Cat 6 FTP

Version du logiciel: 1.3000

Version des limites: 1.0200

NVP: 70,0%

Résumé de test: CORRECT

Modèle: DTX-1800

Num. Sér. principale: 9122027

Num. Sér. distante: 9122028

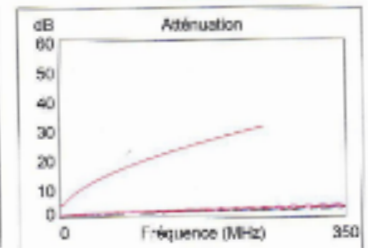
Adaptateur principal: DTX-PLA001

Adaptateur distant: DTX-PLA001

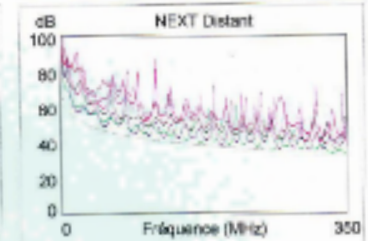
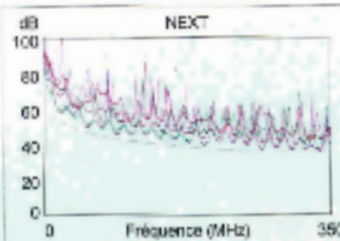
Schéma de câblage (T568B)**CORRECT**

Longueur (m)	[Paire 12]	6,1
Délai de prop. (ns), Lim. 498	[Paire 36]	30
Ecart entre paires (ns), Lim. 44	[Paire 36]	1
Résistance (ohms), Lim. 21,0	[Paire 36]	1,3

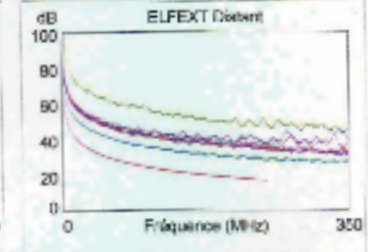
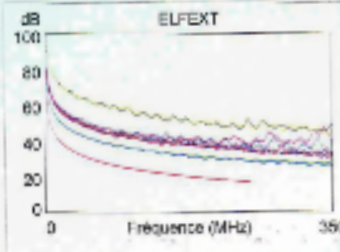
Atténuation Marge (dB)	[Paire 36]	27,7
Fréquence (MHz)	[Paire 36]	250,0
Limite (dB)	[Paire 36]	30,7



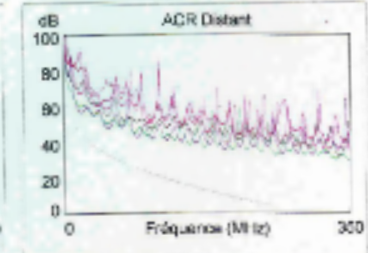
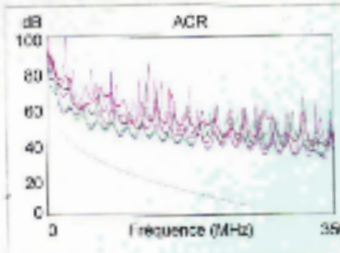
N/V	Pire marge		Pire valeur	
	MAIN	SR	MAIN	SR
Pire paire	45-78	45-78	12-36	36-45
NEXT (dB)	1,8	0,5	3,1	1,2
Fréq. (MHz)	195,5	195,5	248,0	240,0
Limite (dB)	37,1	37,1	35,4	35,6
Pire paire	45	78	12	78
PSNEXT (dB)	2,3	1,5	4,1	1,5
Fréq. (MHz)	177,0	196,0	249,0	196,0
Limite (dB)	35,2	34,5	32,7	34,5



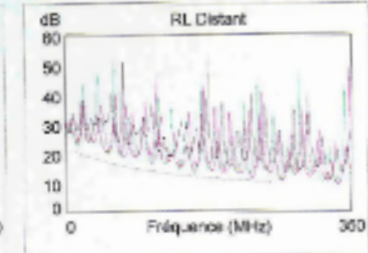
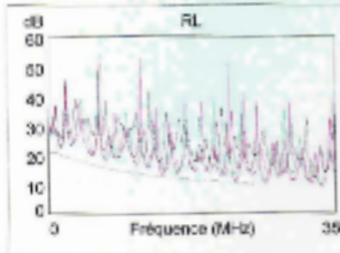
N/V	Pire marge		Pire valeur	
	MAIN	SR	MAIN	SR
Pire paire	45-36	36-45	45-36	45-36
ELFEXT (dB)	10,0	10,1	11,2	11,5
Fréq. (MHz)	1,0	1,0	248,5	248,5
Limite (dB)	64,2	64,2	16,3	16,3
Pire paire	36	36	36	45
PSELFEXT (dB)	11,2	11,4	12,7	12,8
Fréq. (MHz)	1,0	1,0	248,5	248,5
Limite (dB)	61,2	61,2	13,3	13,3



N/V	Pire marge		Pire valeur	
	MAIN	SR	MAIN	SR
Pire paire	45-78	45-78	12-36	36-45
ACR (dB)	11,3	10,8	30,7	28,8
Fréq. (MHz)	17,1	17,5	248,0	240,0
Limite (dB)	46,8	46,6	4,9	5,7
Pire paire	45	45	36	36
PSACR (dB)	11,3	11,0	31,8	30,5
Fréq. (MHz)	17,9	17,9	248,5	239,5
Limite (dB)	44,0	44,0	2,2	3,1



N/V	Pire marge		Pire valeur	
	MAIN	SR	MAIN	SR
Pire paire	36	36	45	45
RL (dB)	10,3	9,3	0,7	1,2
Fréq. (MHz)	250,0	250,0	227,5	227,5
Limite (dB)	10,0	10,0	10,4	10,4



Conforme aux normes de réseaux:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

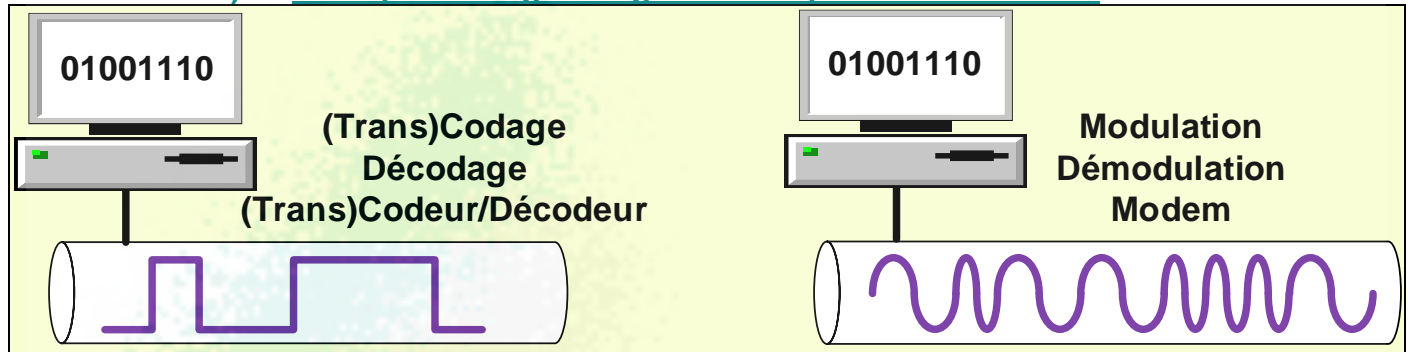
4.7) Représentation des bits sur le support

Les bits peuvent être représentés sous forme :

- ♦ **numérique {digital}**. Dans une transmission numérique, un **nombre fini de valeurs discontinues** est transmis,
- ♦ **analogique {analog}**. Une transmission analogique met en œuvre **une suite continue de valeurs** par intervalle de temps.

4.8) Transmission numérique {digital}, signal bande de base {Baseband}

4.8.1) Principe : codage en ligne réalisé par un transcodeur



Le signal **bande de base**, encore appelé **signal carré**, est constitué de créneaux caractérisant deux ou trois niveaux de tension sur un câble à base de cuivre, et deux intensités lumineuses sur une fibre optique. Les signaux bande de base sont générés par un **transcodeur** qui réalise un **codage en ligne**. Le codage en ligne associe à une suite donnée de bits à transmettre une suite caractéristique d'états du signal.

Ce type de signal est facile à réaliser et ne nécessite donc pas de matériel onéreux. En contrepartie, ce signal possède une faible distance de propagation, et à un instant, un seul signal peut être présent sur le support. La transmission bande de base était essentiellement utilisée dans les réseaux locaux.

La transmission bande de base découpe l'échelle du temps en **temps-bit**, qui représente le temps nécessaire à l'émission d'un bit pour l'émetteur, et également le temps nécessaire à la reconnaissance de la valeur du bit pour le récepteur.

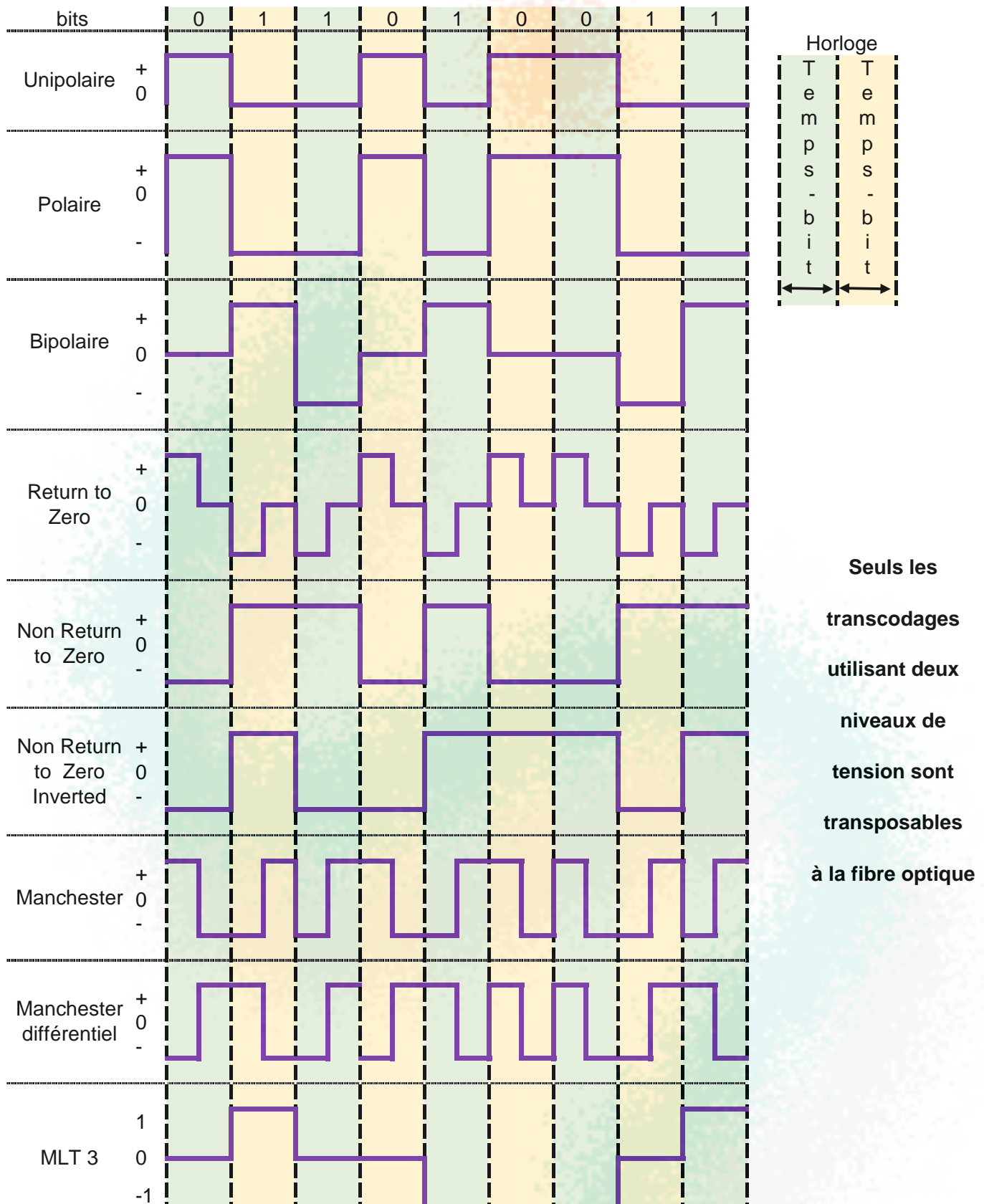
L'un des principaux problèmes de la transmission bande de base réside dans la **synchronisation de l'émetteur et du récepteur**. Pour que le(s) destinataire(s) remarque(nt) qu'une émission de données débute, **le niveau 2 {couche liaison de données} génère, en plus des données, des bits de synchronisation**. Ainsi la trame Ethernet est précédée d'un **préambule** {preamble} et éventuellement d'un **délimiteur de début de trame** {-, **Start Frame Delimiter, SFD**}, tandis que la trame Token-Ring inclut un champ appelé **délimiteur de début** {-, **Start Delimiter, SD**}. Une fois qu'un destinataire a détecté un début d'émission, il faut qu'il reste synchronisé avec l'émetteur.

4.8.2) Codages en ligne classiques (transcodage bit par bit)

Les **codes en ligne** classiques traitent les bits un par un. Sur un support de cuivre, les principaux types de transcodage bande de base historiques sont :

- ♦ **unipolaire**. Ce transcodage utilise une tension nulle et une tension positive ou négative (pas les deux). Par exemple : +3volts représentent le 0, et 0 volt représente le 1 ;
- ♦ **polaire**. Une tension positive et une tension négative sont utilisées. Par exemple : +3 volts représentent le 0, et -3 volts représentent le 1 ;
- ♦ **bipolaire**. Le signal varie entre 3 états significatifs, en général une tension positive, une tension nulle et une tension négative. Par exemple : les 1 seront successivement représentés par une tension positive, puis négative ; tandis qu'un zéro sera représenté par une tension nulle ;

- ◆ **Return to Zero {RZ}**. Le signal **transite** par le niveau zéro au milieu de l'élément à transmettre. Pendant un demi-temps bit, la tension est donc nulle. Par exemple : le passage d'une tension positive à une tension nulle, représente un 0, et le passage d'une tension nulle à une tension négative représente un 1. Le passage par 0 du signal au milieu du temps-bit permet au récepteur de rester synchroniser ;
 - ◆ **Non Return to Zero {NRZ}**. C'est un transcodage polaire très simple dans lequel une tension positive représente un 1, et une tension négative représente un 0 ;
 - ◆ **Non Return to Zero Inverted {NRZI}**. Le 1 est représenté par une inversion du signal au début du temps bit. L'inversion du signal correspond à une **transition** (passage d'une tension positive à une tension négative ou inversement) au début du temps bit. Le zéro est lui représenté par **l'absence de transition**. La transition du signal au début du temps-bit, lors de l'émission d'un 1, contribue à la synchronisation ;
 - ◆ **Biphase**. Un transcodage biphase réalise au moins une transition (passage d'une tension positive à une tension négative ou inversement) pendant le temps bit. Les transcodages biphases garantissent ainsi la synchronisation. Manchester et Manchester Différentiels appartiennent à cette catégorie.
 - **Manchester** (utilisé pour ETHERNET 10 Mb/s). Un 1 est représenté par une transition montante au milieu du temps bit, tandis qu'un 0 est représenté par une transition descendante au milieu du temps bit,
 - **Manchester différentiel** (utilisé pour TOKEN RING) : Le 0 est codé par une transition au début de chaque temps bit, le 1 est représenté par une absence de transition au début du temps-bit. Une transition est générée au milieu du temps bit.
- L'avantage du Manchester différentiel par rapport au Manchester réside dans le fait que c'est la transition, ou la non transition au début du temps-bit qui détermine la valeur du bit transmis, rendant ainsi Manchester différentiel insensible aux problèmes de polarité dus, par exemple, à un défaut de branchement ;
- ◆ **Multi-Level Threshold {MLT3}** (utilisé pour Fast Ethernet 100B-Tx). Le signal peut prendre les valeurs -1V, 0V, +1V. Le 0 est codé par une « non transition », et le 1 est représenté par une transition vers le niveau suivant.



4.8.3) Codages en ligne plus récents (transcodage tertiaires et quaternaires)

Les codages en ligne tertiaires et quaternaires constituent des transcodages plus récents que les codages en ligne historiques, mais ce ne sont pas les seuls.

Les codages tertiaires associent à une suite donnée de bits une combinaison d'états du signal générés à partir de trois états possibles. Ainsi, le codage **4B3T** associe à une suite donnée de quatre bits une suite de trois états trivalents du signal, à savoir, tension négative, tension nulle et tension positive. Il établit donc une correspondance non équivoque (bijection) entre l'ensemble

des 16 (2^4) suites de 4 bits et un sous-ensemble des 27 (3^3) combinaisons possible de 3 états du signal.

Les codages quaternaires associent à une suite donnée de bits une combinaison d'états du signal générés à partir de quatre états possibles. Par exemple, le codage **2B1Q**, associe à un groupe de deux bits, un symbole quaternaire qui correspond à une tension prise dans un ensemble de 4 valeurs. Si p et q sont des entiers, une table 2B1Q peut être représentée sous la forme suivante :

Codage quaternaire 2B1Q	
2 bits	1 tension
00	$-q_v$
01	$-p_v$
10	$+p_v$
11	$+q_v$

Les codages 4B3T et 2B1Q sont mis en œuvre par le protocole **RNIS** {Réseau Numérique à Intégration de Services, **ISDN**, Integrated Services Digital Network}.

4.8.4) Codage complet ou en bloc nB/mB, avec $n < m$

Le **codage complet**, encore appelé **codage en bloc** consiste à regrouper les bits à transmettre en blocs. Chacun de ces blocs est ensuite associé à une autre suite binaire qui constitue son codage. Le codage ne s'applique donc plus à un seul bit, mais à un bloc de bits qui codé, sous forme d'un groupe, généralement, plus important de bits, est ensuite transmis par l'un des codes en ligne précédents.

Les codages complets de type **nB/mB, avec $n < m$** , regroupent les bits à transmettre en blocs de n bits. Une table de correspondance permet de coder chacun de ces groupes par un bloc de m bits, comportant plus de bits que le bloc avant codage. A première vue, ceci paraît curieux car il faut transmettre plus de bits que la séquence originale de bits. La table de codage **4B/5B** permet de comprendre l'intérêt de cette opération.

Codage complet (en bloc) 4B/5B				
Nom du bloc de données	4 bits	5 bits	Séquence de contrôle Caractère de commande	5 bits
0	0000	11110	Q (Quiet – Silencieux)	00000
1	0001	01001	I (Idle – Occupé)	11111
2	0010	10100	J (Start delimiter #1 – Début #1)	11000
3	0011	10101	K (Start delimiter #2 – Début #2)	10001
4	0100	01010	T (End delimiter – Fin)	01101
5	0101	01011	S (Set)	11001
6	0110	01110	R (Reset)	00111
7	0111	01111	H (Halt – Arrêt)	00100
8	1000	10010		
9	1001	10011		
A	1010	10110		
B	1011	10111		
C	1100	11010		
D	1101	11011		
E	1110	11100		
F	1111	11101		

Chaque bloc de 5 bits, résultant du codage d'un bloc de 4 bits, **est transmis, bit à bit, par un codage en ligne de type NRZI sur de la fibre, et de type MLT-3 sur du cuivre**. Ors, aucun de ces codes en ligne ne génère de transition lors de l'émission du bit 0. Les blocs de 5 bits, résultant du **codage 4B/5B ne renferment aucune séquence de plus de 2 bits 0 consécutifs, évitant ainsi les problèmes de synchronisation lors de l'émission de longues suite de bits à 0**. De plus, il reste des blocs de 5 bits inutilisés. Ces blocs permettent :

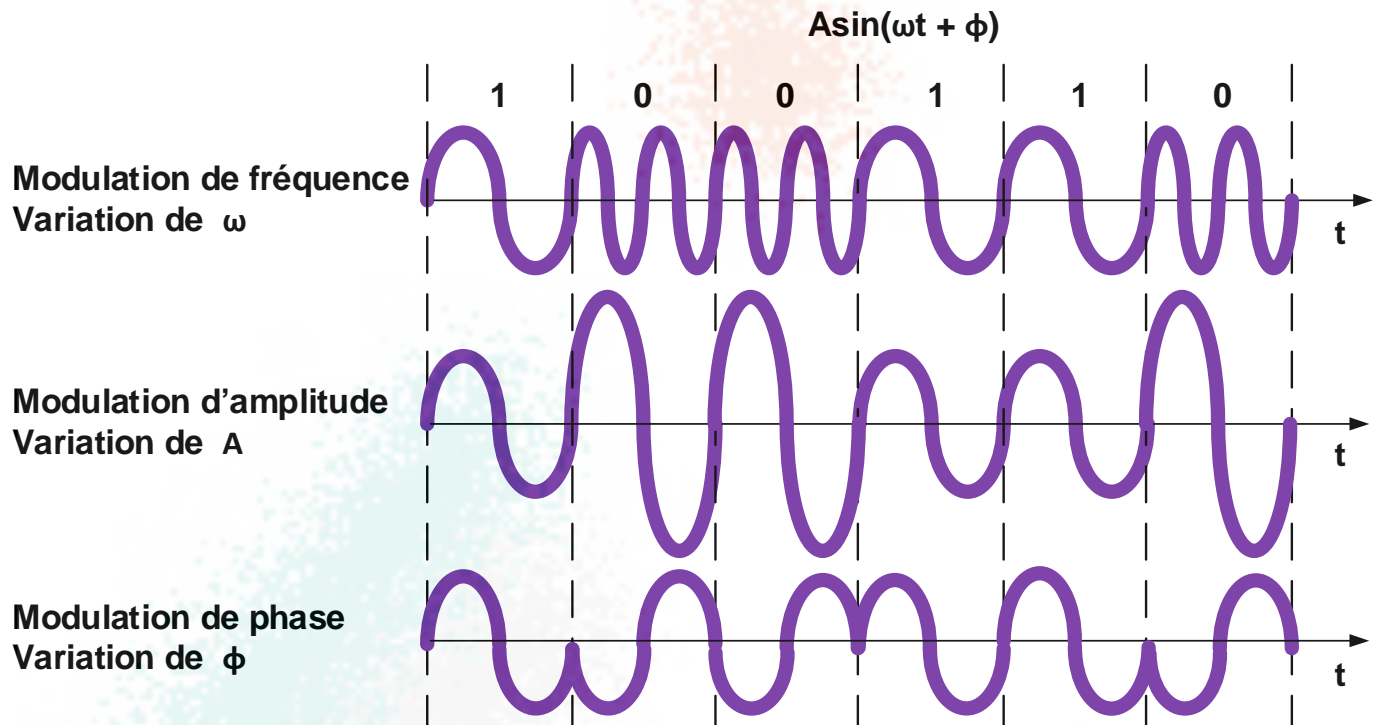
- ◆ **soit de représenter les opérations d'un langage de commande**. 4B/5B définit 8 séquences de contrôle encore appelés caractères de commande. Par exemple :
 - Ethernet 100 BASE-TX et FFDI utilisent « **JK** », soit « 11000 10001 », pour annoncer le début d'une trame,
 - Ethernet 100 BASE-TX utilise « **TR** », soit « 01101 00111 », pour délimiter la fin d'une trame,
 - FFDI utilise « **TT** », soit « 01101 01100 » pour délimiter la fin d'une trame ;
- ◆ **soit de mettre en évidence une erreur de transmission** : une des 8 séquences de 5 bits non répertoriée.

4.8.5) Encodage de trame

L'encodage de trame consiste en un code codage en bloc, suivi d'un codage en ligne. Le codage en bloc est facultatif, mais permet la détection d'erreur et la délimitation de trames.

4.9) Codage analogique : transmission large de base {broadband}

Le codage **large bande {Broadband}** utilise les diverses possibilités de modulations d'une onde. Le modulateur génère une porteuse à partir des informations binaires des systèmes informatiques. Le signal modulé possède une **grande portée**, il est représenté par une sinusoïde exprimée sous la forme $A \cdot \sin(\omega \cdot t + \varphi)$, et est caractérisée par son amplitude A, sa fréquence ω et sa phase φ .



Outre la grande portée assurée par les transmissions analogiques, un autre intérêt de ces transmissions réside dans la possibilité **de transmettre, à un instant t , plusieurs signaux**. Il devient ainsi possible de transmettre un **signal de synchronisation appelé horloge {clock} en même temps que les données**.

4.9.1) Débit et rapidité de modulation

Le débit binaire est exprimé en bit par seconde (bit/s, bps, bs^{-1}). La rapidité de modulation représente le nombre d'états du signal, encore appelés symboles, émis par seconde et s'exprime en **baud** ; en référence au code **baudot** mis au point par Emile Baudot, et utilisé en télégraphie.

Dans un système utilisant le code Manchester, et dont le débit binaire est de 10 Mbps, la rapidité de modulation est de 20 Mbps.

Remarque : 1 Kbps = 10^3 bps et non 2^{10} bps

4.10) Autres caractéristiques de la couche physique

4.10.1) Transmission série et transmission parallèle

La **transmission parallèle** permet l'émission de N signaux simultanément. Ce mode de transmission nécessite un support possédant plus de N conducteurs. Cette méthode possède l'avantage de la rapidité, mais pose plusieurs problèmes :

- ◆ interférence entre les divers conducteurs d'un support (diaphonie) ;
- ◆ différence possible de vitesse de propagation entre les divers conducteurs

Ceci impose la mise en œuvre de dispositifs complexes donc onéreux, et restreint l'utilisation de la transmission parallèle à de courtes distances. Elle est généralement réservée, à la communication entre éléments très proches (processeurs et périphériques à l'intérieur d'une unité centrale) ou proches (ordinateurs et grappe de disques externes, ordinateurs et imprimantes).

Les exemples de connexion parallèle les plus connus pour la connexion de périphériques sont :

- ◆ le bus **PATA** {**P**arallèle **A**dvanced **T**echnology **A**ttachment} résultant de l'évolution du bus **IDE** {**I**ntegrated **D**rive **E**lectronics} développé par la société **Western Digital** ;
- ◆ la famille de bus **SCSI** {**S**mall **C**omputer **S**ystem **I**nterface}.

La **transmission série** transmet les bits d'une entité (mots, messages) l'un après l'autre, sur un support commun. Comme les processeurs opèrent sur des mots, il faut que l'émetteur transforme

ces mots en une suite de bits, et que le récepteur reconstruise les mots à partir des bits reçus. Des contrôleurs spécialisés ont été développés à cet effet. C'est en particulier le rôle de l'**Universal Asynchronous Receiver Transmitter {UART}**. Une transmission série ne transmet qu'un seul bit à la fois, mais est beaucoup plus simple à gérer qu'une transmission parallèle et requiert des câbles plus simples.

Les exemples de connexion série les plus connus pour la connexion sont :

- ◆ le bus **SATA** {**S**erial **A**dvanced **T**echnology **A**ttachment} qui a supplanté le bus PATA ;
- ◆ le bus **SAS** {**S**erial **A**ttached **S**CSI} qui a supplanté le bus SCSI ;
- ◆ le bus **USB** {**U**niversal **S**erial **B**us}.

4.10.2) Multiplexage

Le multiplexage permet de véhiculer sur un support commun des informations différentes. Ceci est réalisé par la mise en place de multiplexeurs/démultiplexeurs.

4.10.3) Transmission série synchrone et asynchrone

Dans une liaison série, les bits sont émis successivement par l'émetteur. Un émetteur peut rester muet durant des périodes plus ou moins longues, puis transmettre une séquence de bits plus ou moins importante. Il faut donc que le récepteur détecte les bits émis et se synchronise avec l'émetteur.

Une **liaison asynchrone** fait précéder les bits à transmettre par un signal de début de transmission. Ceci permet au récepteur de synchroniser son horloge sur celle de l'émetteur. Certaines méthodes de transmission asynchrone encadrent les données par un **Start Bit** et un **Stop Bit**. Ces informations de synchronisation correspondent à la mise sur le support d'un signal particulier, pendant un temps donné. Celui-ci n'est pas forcément un multiple entier du temps bit.

Une liaison **synchrone** véhicule en même temps que les données, un signal de synchronisation, parfois appelé horloge, Ce signal permet au récepteur de se synchroniser sur le cadencement de l'émetteur.

4.10.4) Équipements de traitements de données et de circuits de données

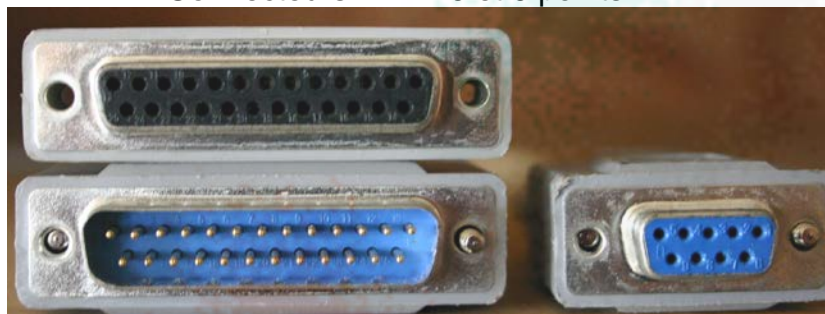
Les équipements constituant un réseau local constituent typiquement des **Équipements Terminaux de Traitement de Données {ETTD, Data Terminal Equipment, DTE}**. Ce sont les ordinateurs, imprimantes, routeurs, etc.

Les équipements mis en place par les opérateurs de télécommunication sont des équipements de circuits de données. Ils sont appelés **ETCD {Équipement Terminal de Circuit de Données, DCE, Data Circuit-Terminating Equipment}**. Les modems entrent dans cette catégorie. L'ETCD fournit le **signal de synchronisation {horloge, clock}** à l'ETTD auquel il est directement connecté.

Par abus de langage, les expressions **Data Circuit Equipment, Data Communication Equipment et Data Carrier Equipment** sont employés à la place de **Data Circuit-Terminating Equipment**.

Les connecteurs V24, X21 et V35 permettent de connecter les ETTD aux ETCD.

Connecteurs V 24 25 et 9 points



Connecteurs X21



Connecteur V35 mâle



4.11) Extension du réseau par la couche physique et matériels associés

4.11.1) Pourquoi étendre un réseau par le niveau 1 ?

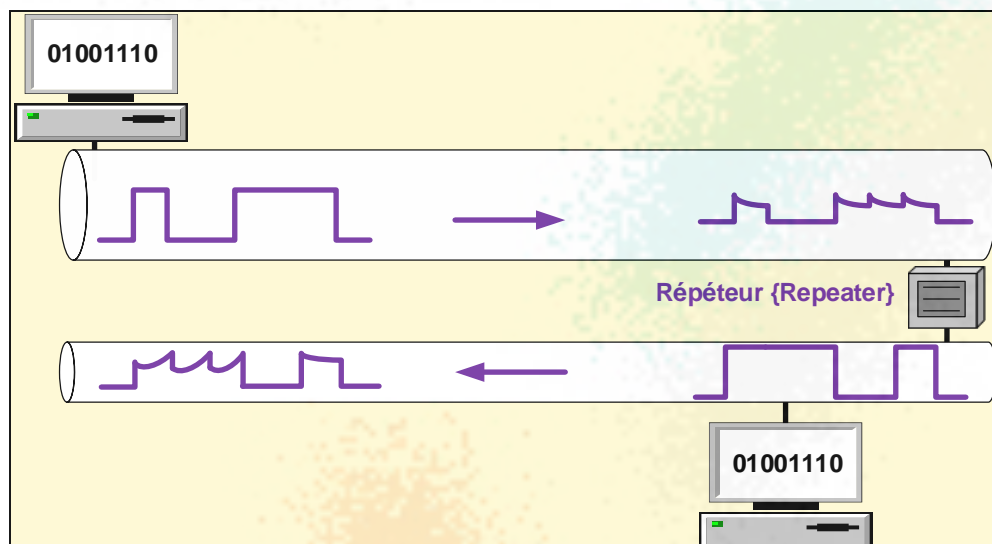
Tout au long du parcours du média, les signaux perdent en force et en qualité, si bien qu'à partir d'une certaine distance, le signal originel n'est plus reconnaissable. La couche physique qui définit la structure des médias, limite la longueur des segments en fonction de l'atténuation du support. Si deux équipements terminaux soit séparés par une distance plus grande que la taille maximale d'un segment, il faut employer deux segments et relier ces deux segments par un équipement qui est capable de :

- ◆ lire le signal atténué sur l'un des ports ;
- ◆ remettre le signal en forme, tel qu'il était à l'origine ;
- ◆ retransmettre le signal sur l'autre port.

Le périphérique intermédiaire situé entre les deux segments se "contente" de **remettre en forme le signal** qui représente des bits, mais cet équipement **ne connaît pas la signification des bits transportés**.

4.11.2) Extension d'une topologie en bus : répéteur {repeater}

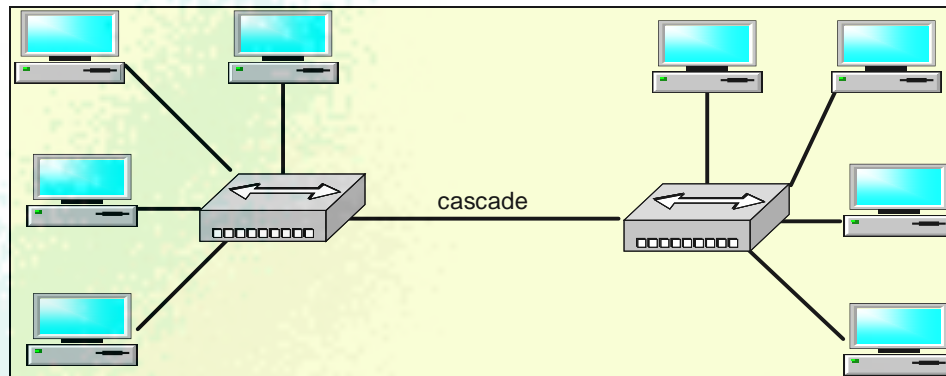
Les premiers réseaux locaux déployaient une topologie en bus, et le périphérique intermédiaire utilisé entre deux segments d'une même couche physique était appelé **répéteur {repeater}**.



4.11.3) Extension d'une topologie en étoile : concentrateur {hub}

Les topologies en bus ont été peu à peu abandonnées au profit des topologies en étoile. Le périphérique intermédiaire de la couche physique qui relie les segments d'une topologie en étoile constitue un **répéteur multiport** appelé **concentrateur {hub}**.

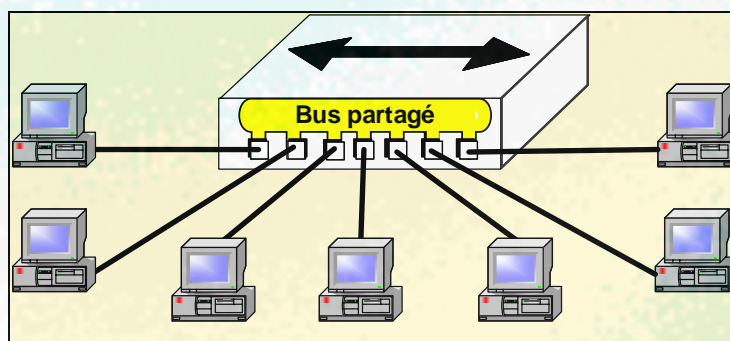
L'intérêt de migrer d'une topologie **physique en bus**, vers une topologie **physique en étoile** basée sur des concentrateurs, réside dans la plus grande robustesse de l'architecture. Dans une **topologie physique en bus**, la **dégradation du support sur un segment impacte directement l'ensemble des équipements** connectés à ce segment, tandis que, dans une topologie physique en étoile, la **dégradation d'un segment n'influe pas sur les autres équipements car ils sont connectés à d'autres segments**.



Un concentrateur {hub} retransmet un signal entrant par l'un de ses ports sur tous ses autres ports.

4.11.4) Concentrateur : Topologie physique en étoile, topologie logique en bus

Un concentrateur {hub} interconnecte tous les segments branchés sur chacun de ses ports par l'intermédiaire d'un bus interne commun partagé. D'un point de vue logique, tout se passe comme si les équipements étaient connectés à un bus commun partagé, avec tous les inconvénients que cela entraîne.

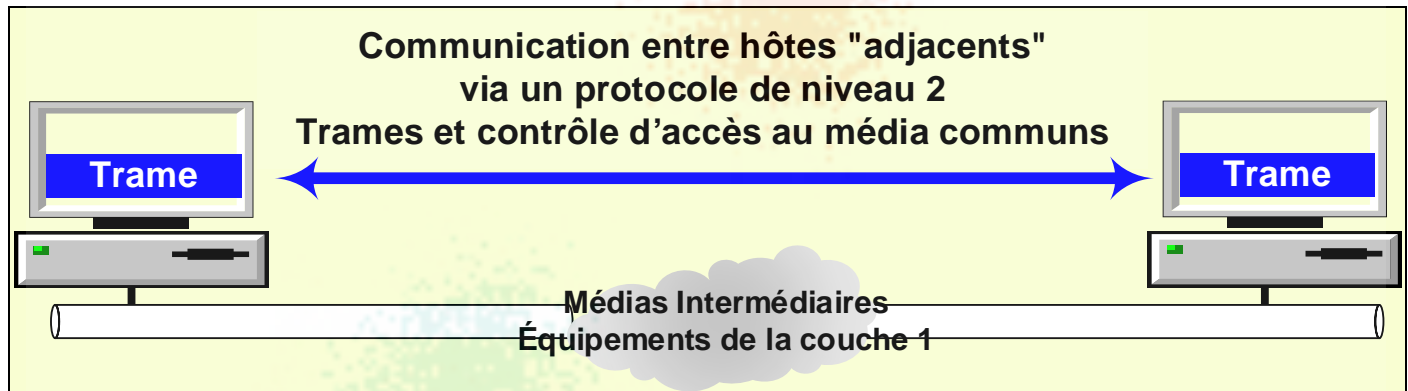


5) Modèle OSI : la couche liaison de données {data link layer, L2}

5.1) Fonctionnalités de la couche liaison de données

Tandis que la couche physique se "contente" de transporter une suite de bits sur le support. La couche liaison de données organise les bits en unités logiques d'informations, appelées **trames** et **contrôle l'accès au support** afin de s'assurer de la disponibilité et de la capacité du media à recevoir ces trames.

D'un point de vue logique, la couche liaison de données permet l'échange d'un **même type de trames** entre des hôtes "adjacents".



D'un point de vue physique, la carte réseau {Network Interface Card, NIC} de l'émetteur, encapsule les paquets en trames, et prépare la mise à disposition des données pour le niveau 1. Sur le récepteur, l'encapsulation de niveau 2 permet, la restitution, à la carte réseau des trames reconstruites à partir des représentations de bits transmises par la couche physique.



La couche liaison de données peut détecter, voire récupérer ou même corriger, les erreurs de transmission. La couche liaison est l'une des plus complexes du modèle OSI, car elle constitue l'interface avec le niveau physique qui met en œuvre des techniques très différentes sur les LANs et sur les WANs. Elle a donc été scindée en deux sous-couches.

5.2) La sous-couche MAC {Media Access Control}

5.2.1) Trame {frame}

La sous-couche MAC constitue la sous-couche la plus basse, c'est elle qui confectionne les trames, qui prépare leur insertion sur le média, et qui permet leur lecture à partir du support. Une trame est la **structure élémentaire de transport des informations sur le réseau**. A ce niveau, les informations ne peuvent transiter que par des systèmes informatiques reconnaissant les mêmes trames.

La sous-couche MAC est responsable de l'insertion des trames sur le média, elle doit donc garantir la **délimitation des trames**. Certains protocoles incluent dans la trame des séquences particulières de bits qui indiquent le début et la fin de la trame. D'autres protocoles, font précéder la trame d'un signal particulier, appelé préambule, et imposent un temps d'inactivité sur le support entre chaque trame. Ces mécanismes permettent la synchronisation de l'émetteur et du récepteur.

Si nous excluons les informations de synchronisation, la structure générale d'une trame est la suivante :

Adresse destination	Adresse source	Données	Information de contrôle
---------------------	----------------	---------	-------------------------

Le champ information de contrôle permet la détection/correction/récupération d'erreurs. Cette information de contrôle est :

- ◆ calculée par l'émetteur de niveau 2 ;
- ◆ insérée dans le champ information de contrôle de la trame par l'émetteur de niveau 2 ;
- ◆ recalculée par le destinataire de niveau 2, puis comparée avec le champ 'information de contrôle de la trame reçue.

Il existe plusieurs mécanismes de détection d'erreur. Les plus courants sont :

- ◆ la **parité paire** {even parity} qui est équivalente au **OU exclusif** {XOR, \oplus } ;
- ◆ la **parité impaire** {odd parity} ;
- ◆ la **somme de contrôle** {checksum} ;
- ◆ le **CRC** {Cyclic Redundancy Check, **CRC**, Code de Redondance Cyclique}.

5.2.2) Adresse MAC / physique / BIA des protocoles de réseaux locaux

Les adresses sources et destination des trames des protocoles de réseaux locaux sont appelés adresses MAC. Les adresses MAC sont attribuées par les constructeurs de cartes réseau {Network Interface Card, **NIC**}, et sont figées dans la **mémoire morte** {-Read Only Memory, **ROM**} **de la carte durant leur fabrication**. Les adresses MAC sont parfois appelées adresses physiques ou adresses **BIAs** {**B**urned-**I**n **A**ddress}. L'IEEE attribue à chaque constructeur un identifiant de fabricant, codé sur 24 bits, appelé **OUI** {Organizationally **U**nique **I**dentifier}. Le tableau suivant en donne des exemples exprimés en hexadécimal.

OUI	Propriétaire
00-00-0C	CISCO
00-AA-00	INTEL
00-80-C2	IEEE
00-A0-D2	Allied Telesyn
00-80-9F	Alcatel Business Systems
80-00-10	Att Bell Laboratories

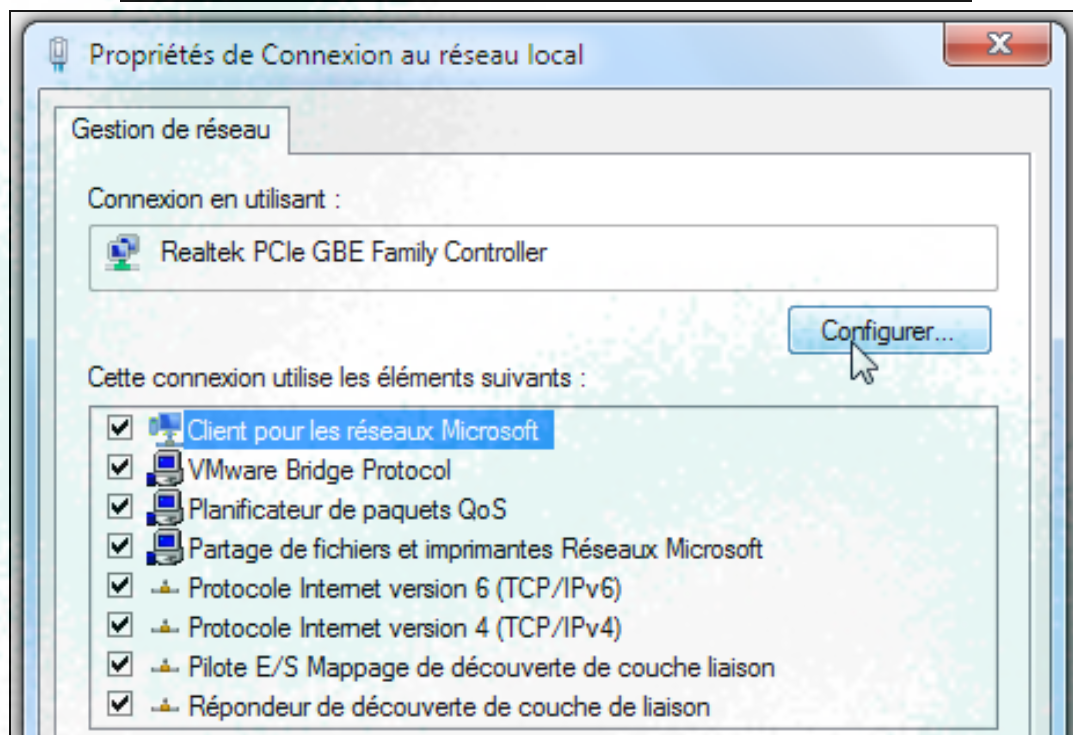
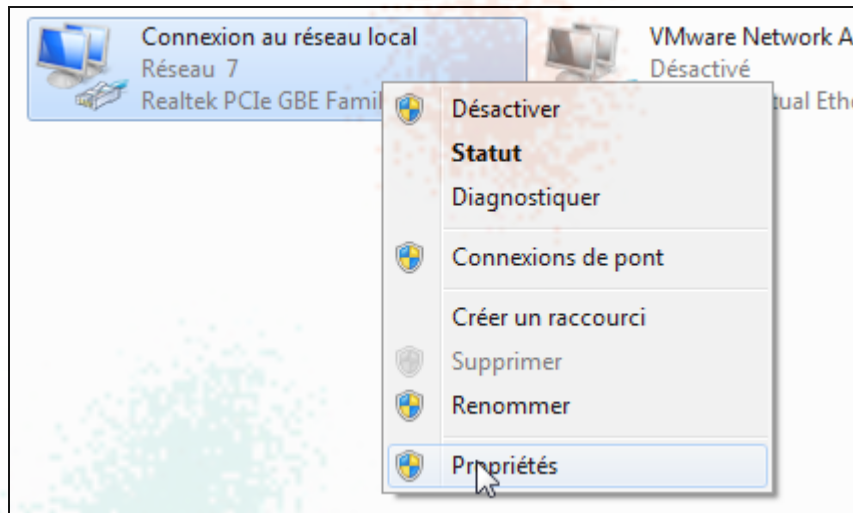
Pour chaque carte réseau, le fabricant génère une adresse MAC, **unique au monde**, par concaténation de son OUI avec une séquence de 24 bits dont il a la responsabilité. **La longueur totale d'une adresse MAC est donc de 48 bits, soit 6 octets**. Ce format d'adresse est appelé MAC-48. Une adresse MAC est représentée par six nombres hexadécimaux de deux chiffres habituellement séparés par le caractère '-'. Le lien suivant permet de retrouver le fabricant à qui un OUI particulier a été attribué, et de télécharger la liste des OUIs alloués par l'IEEE.

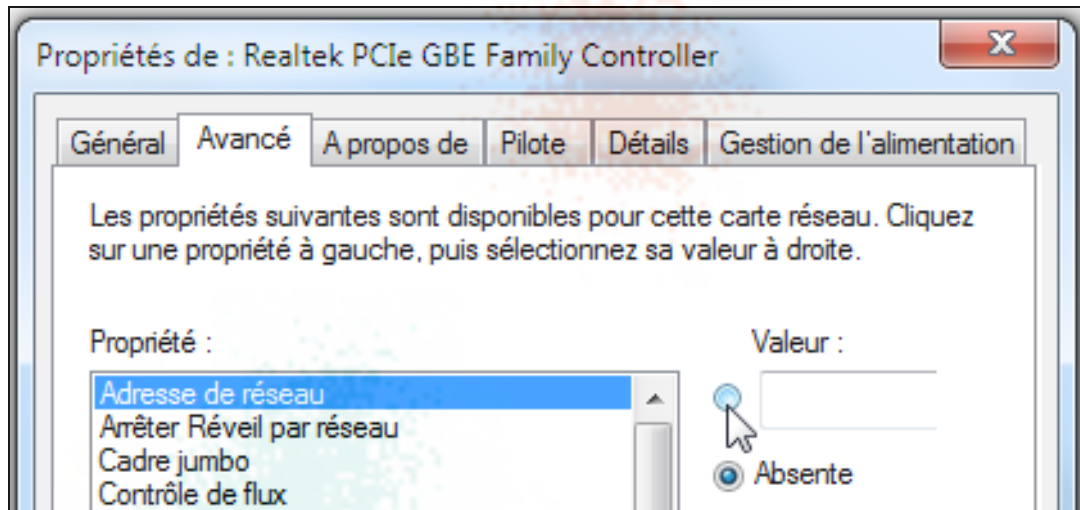
<http://standards.ieee.org/develop/regauth/oui/public.html>

Chaque NIC possède une adresse MAC unique gérée par le fabricant est stockée dans la ROM de la carte. Au démarrage les systèmes d'exploitation copie les adresses MAC en mémoire vive afin d'accélérer les traitements. Ce sont les adresses MAC copiées en RAM qui sont ensuite utilisées par les systèmes d'exploitation.

5.2.3) Modification des adresses MAC en RAM

Il est possible de **modifier la copie, en RAM, de l'adresse MAC**. Suivant les systèmes d'exploitation et les cartes réseau, cette opération est plus ou moins simple. Dans les environnements Windows, les pilotes logiciels, fournis par les fabricants de cartes réseau, permettent généralement de modifier l'adresse MAC stockée en RAM. La façon d'accéder à la modification de l'adresse MAC en RAM, dépend du driver. D'ordinaire cela est possible via l'une des propriétés affichées par l'onglet « **Avancé** » accessible par le bouton « **Configurer..** » des propriétés de la carte réseau.





Si le pilote de la carte réseau, ne fournit pas la possibilité de changer l'adresse MAC en RAM, il faut configurer manuellement la base de registre, ou passer par des utilitaires tierces.

Dans les environnements Linux, la commandes « **ifconfig** » et, suivant les distributions, la commande « **macchanger** » permettent la modification de l'adresse MAC en RAM.

Attention, la substitution d'une mauvaise adresse MAC à l'adresse MAC originale peut provoquer un véritable désastre. En effet, une adresse MAC ne doit jamais être dupliquée sur un même réseau. De plus, il existe des **adresses MAC réservées** appelées **adresses MAC de broadcast** et **adresses MAC de multicast**.

Il ne faut donc utiliser cette possibilité qu'en dernier recours et en cas d'extrême nécessité, comme par exemple pour pallier à la défection d'une carte réseau dont l'adresse MAC est utilisée par un programme particulier.

5.2.4) Adresse MAC de diffusion {broadcast} et de multidiffusion {multicast}

FF-FF-FF-FF-FF-FF représente une adresse MAC dont tous les bits sont égaux à 1, et est appelée **adresse MAC de Broadcast {diffusion}**. La diffusion permet à un périphérique d'adresser grâce à une seule trame, tous les équipements du réseau local, sans même devoir connaître les adresses MAC des autres équipements. Dans une trame, une adresse MAC de broadcast ne peut être utilisée que comme **adresse de destination**.

Une trame à **destination d'une adresse de broadcast** est :

- ◆ **lue par tous** les périphériques connectés au réseau local ;
- ◆ **traitée par tous** les périphériques du LAN.

Outre, la diffusion {broadcast}, la plupart des protocoles de réseaux locaux gèrent également la **multidiffusion {multicast}**. Une adresse MAC de multidiffusion représente un **groupe d'équipements du réseau local possédant une caractéristique particulière commune**, comme le fait d'exécuter une application ou un protocole particulier. Dans une trame, une adresse MAC de multicast ne peut être utilisée que comme **adresse de destination**.

Une trame à **destination d'une adresse de multicast** est :

- ◆ **lue par tous** les périphériques connectés au réseau local ;
- ◆ **traitée uniquement** par les périphériques du LAN possédant la **caractéristique désirée**.

Une adresse dont le **premier octet est impair** constitue une adresse de multidiffusion. Pour obtenir une adresse de multicast, il suffit de positionner le bit de poids faible du premier octet à 1. Ce bit est le bit le plus à droite de l'octet le plus à gauche.

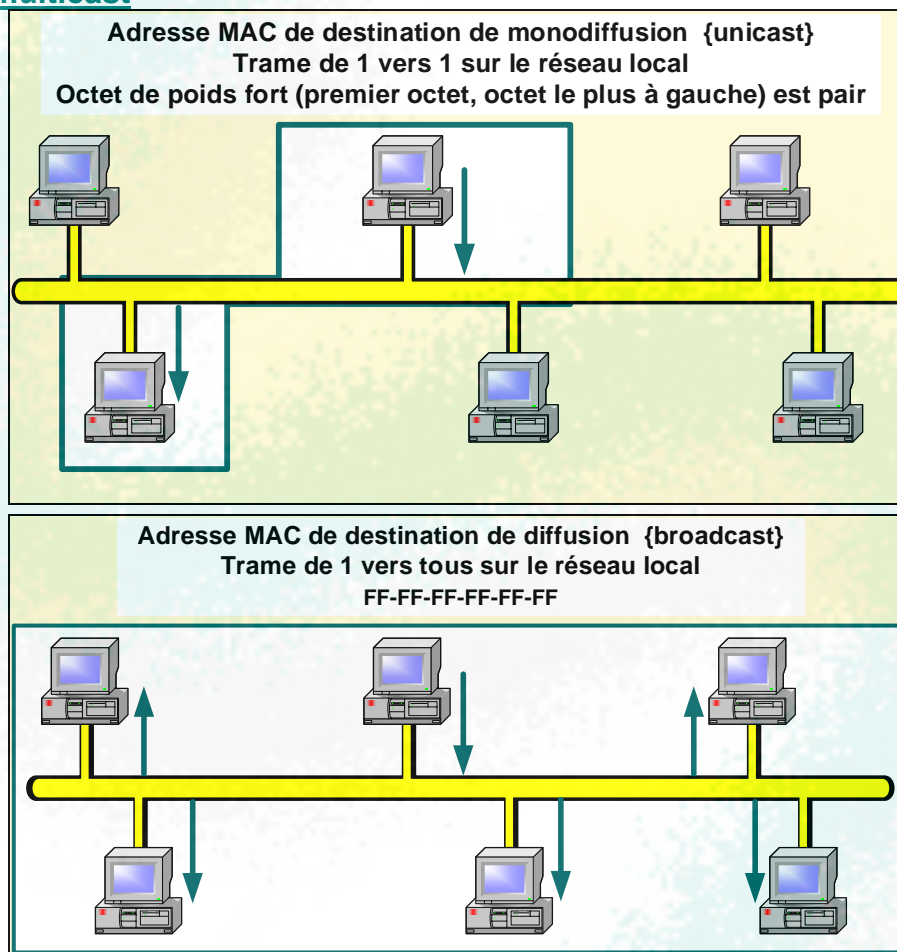
Des adresses de multidiffusion bien connues sont, par exemple :

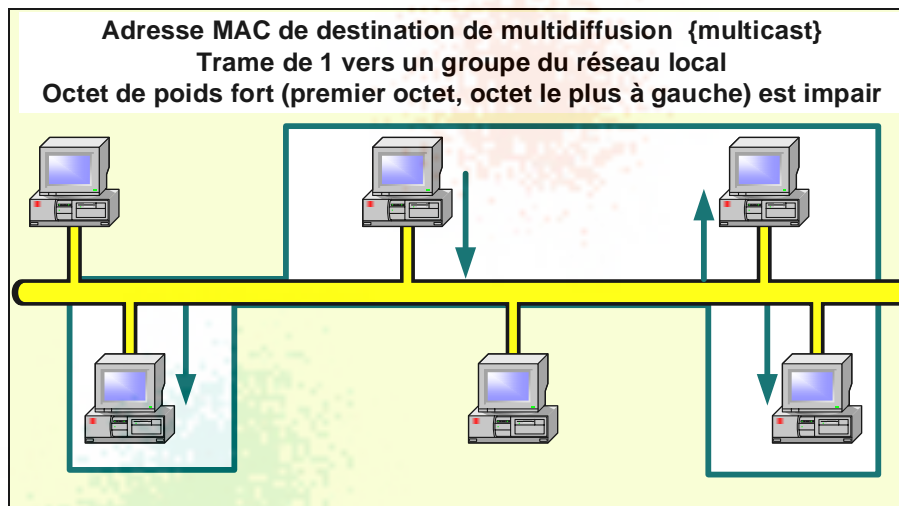
- ◆ 01-00-5E-00-00-05 {**O**pen **S**hortest **P**ath **F**irst ALLSPFRouters}
- ◆ 01-00-5E-00-00-06 {**O**pen **S**hortest **P**ath **F**irst ALLDRouters} ;
- ◆ 01-00-5E-00-00-16 {**I**nternet **G**roup **M**anagement **P**rotocol} ;
- ◆ 01-00-5E-00-00-FC {**L**ink-**L**ocal **M**ulticast **N**ame **R**esolution} ;
- ◆ 01-00-0C-CC-CC-CC pour le
 - multicast **CDP** {**C**isco **D**iscovery **P**rotocol},
 - multicast **VTP** {**V**irtual **T**runking **P**rotocol} ;
- ◆ 01-00-0C-DD-DD-DD pour le multicast **CGMP** {**C**isco **G**roup **M**anagement **P**rotocol}.

5.2.5) Adresse MAC de monodiffusion {unicast}

Une adresse de destination correspondant à l'adresse MAC d'une carte réseau est appelée adresse de monodiffusion {unicast}.

5.2.6) Résumé adresses MAC de destination de type unicast, broadcast et multicast



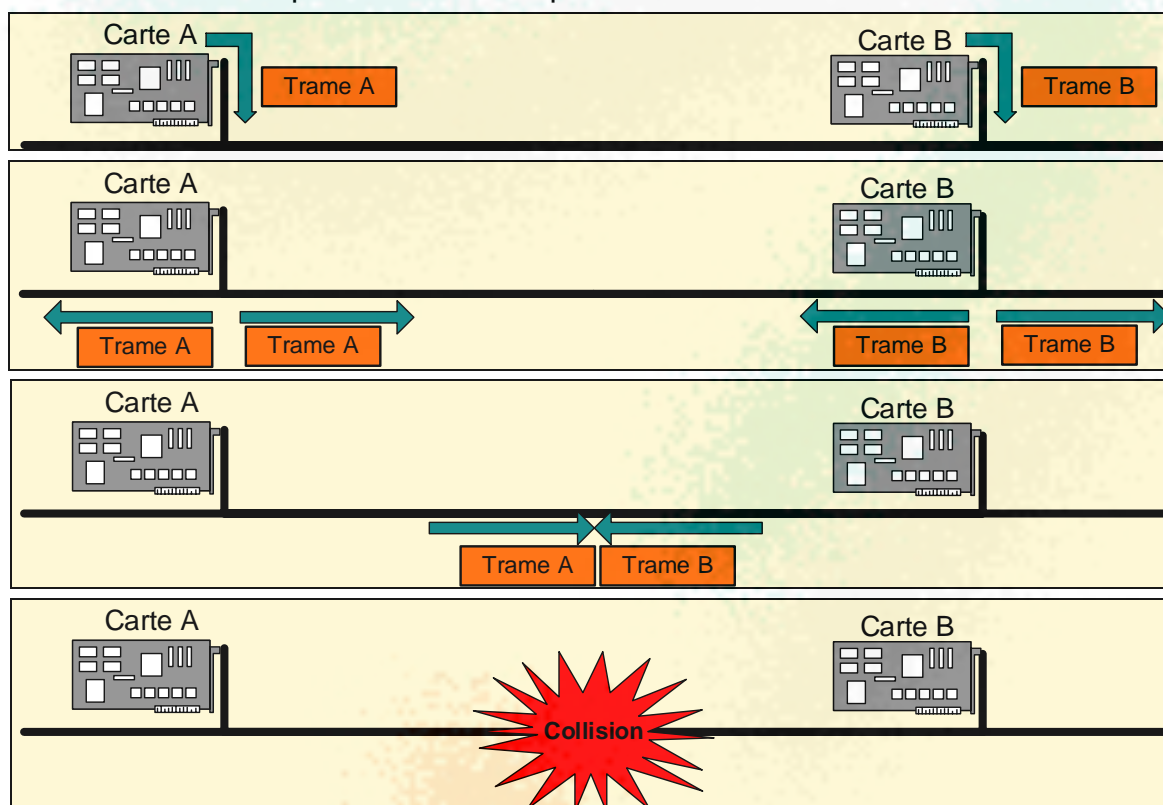


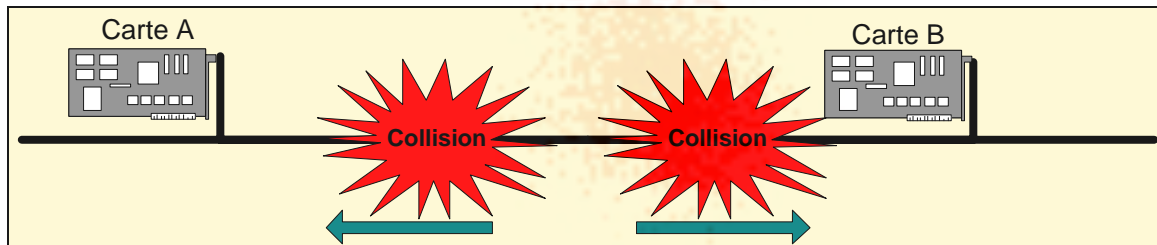
5.3) Contrôle d'accès au support/ média {media access control}

La sous-couche MAC permet également d'assurer le **contrôle d'accès au média** {-, Media Access Control, **MAC**}. Elle décrit le protocole d'accès à un média unique partagé par plusieurs éléments informatiques. Les politiques d'accès au média les plus utilisées sont :

♦ **CSMA/CD** {Carrier Sense Multiple Access Collision Detection}. En simplifiant, si une carte CSMA/CD a besoin d'émettre une trame sur le réseau

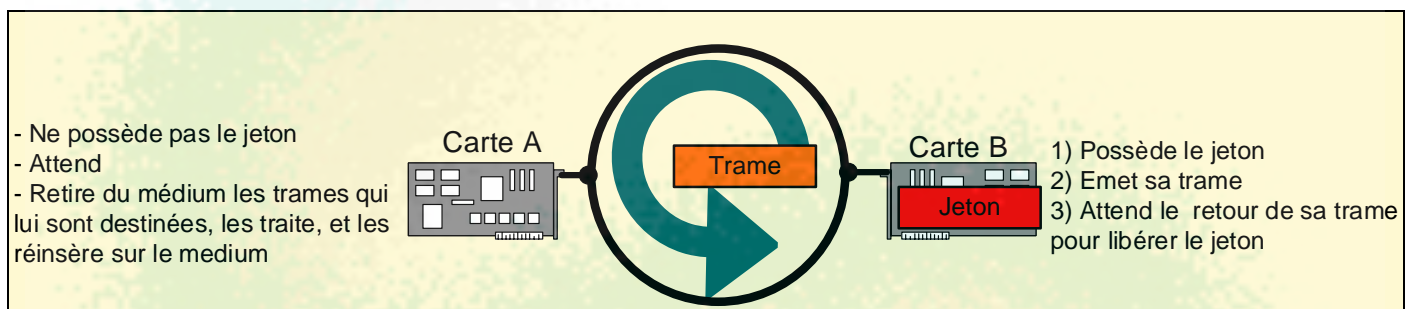
- elle écoute le média partagé, jusqu'à ce que le réseau soit silencieux,
- elle émet sa trame dans les deux sens sur le bus bidirectionnel,
- si pendant "un certain temps" aucune autre trame ne passe sur le média, la carte CSMA/CD considère que sa trame est arrivée à destination. Ce "certain temps", appelé **temps de retournement** {-, Round Trip Delay, **RTD**}, correspond en fait au temps maximum que met une trame pour parcourir deux fois l'ensemble du média (1 aller-retour). Dans le cas contraire, la carte réémettra sa trame plus tard. Cette politique d'accès au médium est décrite sous le terme d'accès au média avec contention. Lorsque deux cartes émettent presque simultanément, leurs trames se télescopent en créant une collision ou contention. Une trame n'est donc pas assurée d'arriver à destination. C'est pour cette raison que CSMA/CD est dit non déterministe.





♦ Token Ring {Jeton passant sur anneau}. Une carte ne pourra émettre sur le média que s'il possède une trame bien particulière appelée jeton {token}. Ce jeton caractérise donc le droit d'émettre. Une fois la transmission d'une trame terminée, la carte libère le jeton. En première approximation, le jeton peut être considéré comme une trame unique sur le média. Contrairement à CSMA/CD, plusieurs cartes réseau CSMA/CD ne peuvent donc pas émettre simultanément. Token Ring est déterministe. Schématiquement, une carte qui a besoin d'émettre une trame sur le réseau

- 1) attend le jeton,
- 2) garde le jeton,
- 3) émet sa trame,
- 4) attend que sa trame ait fait le tour de l'anneau,
- 5) libère le jeton, et le passe à son voisin.



Contrairement à CSMA/CD qui fonctionne sur un bus bidirectionnel, la plupart des systèmes basés sur le jeton passant sur anneau fonctionnent sur un anneau unidirectionnel. Bien évidemment, les trames CSMA/CD diffèrent des trames des systèmes basés sur le jeton passant.

5.4) La sous-couche LLC {Logical Link Control, IEEE 802.2}

La sous-couche **LLC {Logical Link Control}**, a été définie par le comité **IEEE 802.2**. Elle propose une interface unique à la couche 3 {réseau}, indépendante du type de trame MAC utilisée. Elle autorise des services avec ou sans connexion, avec ou sans acquittement, avec ou sans reprise d'erreur.

Lorsque la sous-couche LLC est mise en œuvre, elle confectionne une trame LLC qui encapsule le paquet. L'encapsulation LLC insère des informations permettant d'identifier les flux réseau véhiculés. La trame LLC est alors encapsulée dans une trame MAC. L'encapsulation MAC ajoute les adresses physiques source et destination, ainsi qu'un champ de vérification d'intégrité.

Certains systèmes ignorent cette sous-couche, et encapsulent directement le paquet dans la trame MAC. L'encapsulation MAC ajoute les adresses physiques source et destination, ainsi qu'un champ de vérification d'intégrité, mais également un champ permettant d'identifier le protocole réseau encapsulé.

5.5) Protocoles LANs : 802.3 et Ethernet, 802.5 et Token Ring / 802.2

Les réseaux existaient avant que l'**ISO** ne définisse le modèle **OSI**. En particulier, **Ethernet** et **Token Ring** avaient été respectivement développés par **Digital-Intel-Xerox {DIX}** d'une part et **IBM** d'autre part. Le modèle OSI a normalisé Ethernet en tant que **802.3** et Token Ring en tant que **802.5**.

Ethernet, 802.3 au sens du modèle **OSI**, occupe la couche 1, niveau physique : description des médias, topologie en bus ou en étoile, et la sous-couche **MAC** avec la politique d'accès au

médium **CSMA/CD**. Dans le cas d'Ethernet, la somme de contrôle est appelée **FCS** {**F**rame **C**heck **S**equences}.

Token Ringn, 802.5 du modèle **OSI**, occupe la couche 1, niveau physique : description des médias, topologie en anneau, et la sous-couche MAC avec la politique d'accès du jeton passant sur anneau. En schématisant :

Liaison	LLC	802.2	
	MAC	802.3 ou ETHERNET	802.5 ou TOKEN-RING
Physique			

5.6) Autres protocoles de liaison de données

Les autres protocoles de liaisons de données bien connus sont :

- ◆ **BSC** {**B**inary **S**ynchronous **C**ommunication} qui est un protocole orienté caractère, développé par IBM en 1960 ;
- ◆ **SDLC** {**S**ynchronous **D**ata **L**ink **C**ontrol} qui est un protocole orienté bit développé par IBM en 1970 pour remplacer BSC ;
- ◆ **HDLC** {**H**igh-Level **D**ata **L**ink **C**ontrol} qui résulte de l'amélioration et de la normalisation de SDLC par l'ISO fin des années 70. Bien que normalisé, beaucoup de constructeurs ont apporté à HDLC des fonctionnalités spécifiques, rendant par la même, les divers HDLC "propriétaires" non compatibles ;
- ◆ **PPP** {**P**oint to **P**oint **P**rotocol} qui d'inspire d'HDLC et qui est utilisé sur les liaisons point à point. PPP permet l'authentification des deux extrémités, ainsi que la compression des données.
- ◆ ...

5.7) Choix d'un protocole de liaison de données

Compte tenu, de tout ce qui précède, le choix d'un protocole de niveau 2 dépend :

- ◆ de l'étendue du réseau, LAN ou WAN ;
- ◆ du type de supports physiques déjà installés (couche physique) ;
- ◆ du nombre d'équipements à connecter.

5.8) Extension du réseau par la couche liaison de données et matériels associés

5.8.1) Pourquoi étendre un réseau par le niveau 2 ?

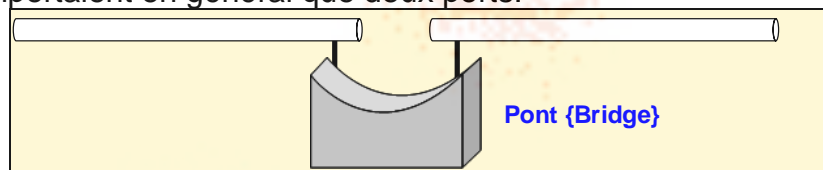
Les protocoles de niveau 2 mettent en œuvre des **délais d'attente** {**timeout**} qui définissent le temps maximum nécessaire à l'exécution de certaines tâches. Le temps de retournement {-, **Round Trip Delay, RTD**} d'Ethernet en est un exemple type. Il détermine le délai nécessaire pour réaliser un aller-retour sur le support. Ce délai maximal, implique **une longueur limite de segment** qu'il est facile de calculer à partir de la vitesse de propagation du signal sur le support. Les délais d'attente de ces protocoles induisent donc, pour chaque type de support, des longueurs maximales de segments de niveau 2. Il devient alors nécessaire de pouvoir prolonger un réseau de niveau 2 par un périphérique intermédiaire qui est capable de :

- ◆ **lire les trames entrantes sur chacun de ces ports ;**
- ◆ **reconnaitre les trames non conformes pour ne pas les retransmettre ;**
- ◆ **si nécessaire, retransmettre une trame entrée par un port sur un ou tous les autres ports, en respectant les règles de contrôle d'accès au support.**

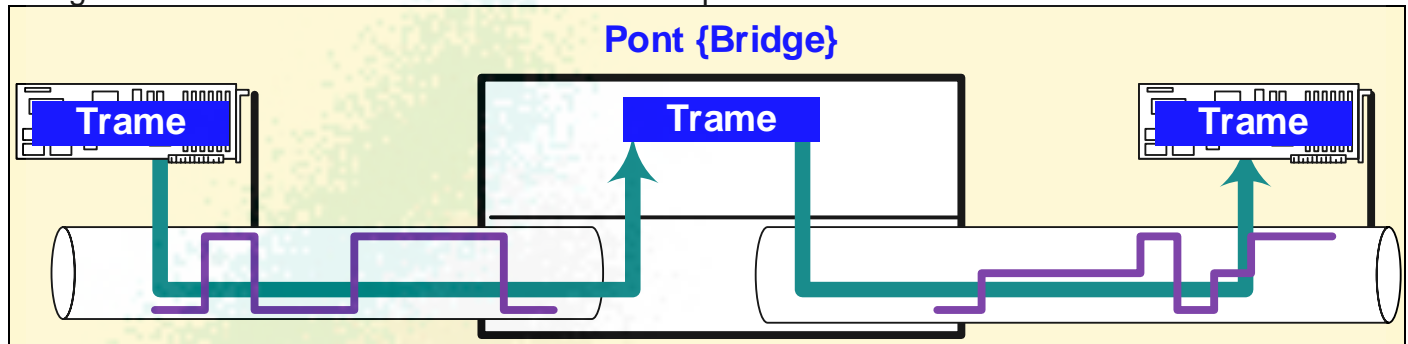
Contrairement aux répéteurs et aux concentrateurs, un périphérique intermédiaire de niveaux 2, **ne se "contente" pas de remettre en forme le signal** qui représente des bits, mais **agit suite à la lecture de trames dont il connaît la structure**. Les périphériques de niveaux 2 embarquent plus d' "intelligence" que les périphériques de niveaux 1, ils intègrent donc plus de matériel et de logiciel, et sont par conséquent plus onéreux.

5.8.2) Extension d'une topologie en bus : pont {bridge}

Les premiers réseaux locaux déployaient une topologie en bus, et le périphérique intermédiaire utilisé entre deux segments d'un même protocole de liaison de données était appelé **pont {bridge}**. Ils ne comportaient en général que deux ports.



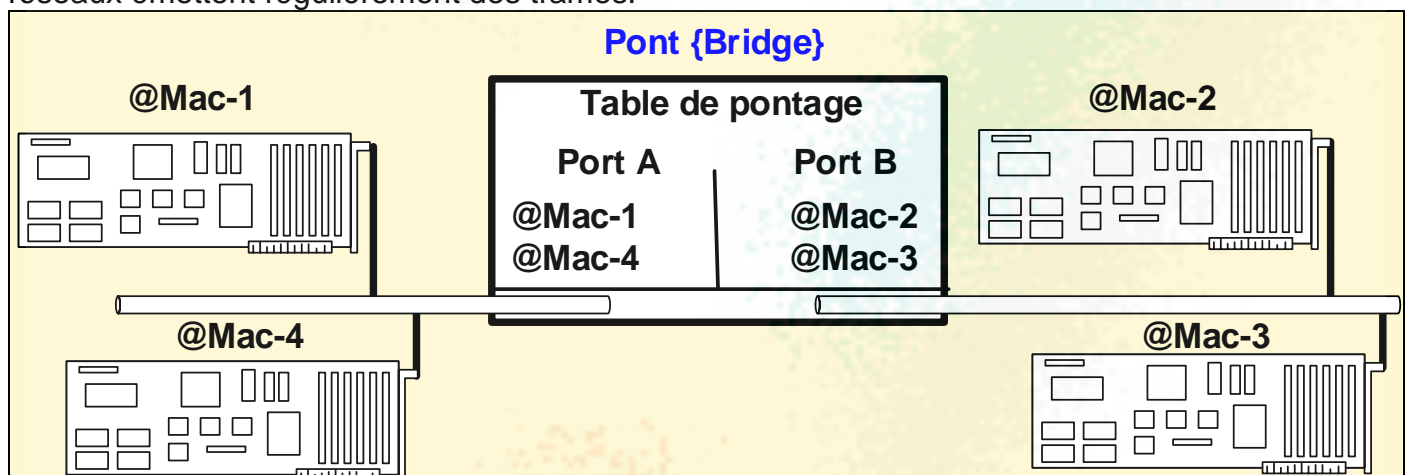
La figure suivante illustre le fonctionnement d'un pont.



Le pont :

- ◆ lit les représentations de bits qui entrent par l'un de ces ports ;
- ◆ essaie de réassembler ces bits en trame ;
- ◆ s'il ne peut pas réassembler les bits, les bits sont abandonnés ;
- ◆ si la trame est non conforme, la trame est abandonnée ;
- ◆ associe, dans sa **table de pontage**, l'**adresse MAC source** de la trame au **port d'entrée** ;
- ◆ si l'adresse de destination est une adresse de **broadcast** la trame est **réémise, sans modification, par les tous autres ports** ;
- ◆ si, dans sa table de pontage, le pont ne possède **aucune association** entre l'adresse MAC de destination et un de ses ports, la trame est **réémise, sans modification, par tous les autres ports** ;
- ◆ si, dans sa table de pontage, le pont possède **une association** entre l'adresse MAC de destination et un de ses ports, la trame est **réémise, sans modification, par ce port**.
- ◆ au bout d'un "**certain temps**" **sans trafic** provenant d'une adresse MAC présente dans la table de pontage, le pont **efface l'adresse MAC** de sa table de pontage.

La figure suivante, représente une table de pontage dans un environnement où toutes les cartes réseaux émettent régulièrement des trames.



5.8.3) Avantages des ponts {bridge} sur les répéteurs {repeater}

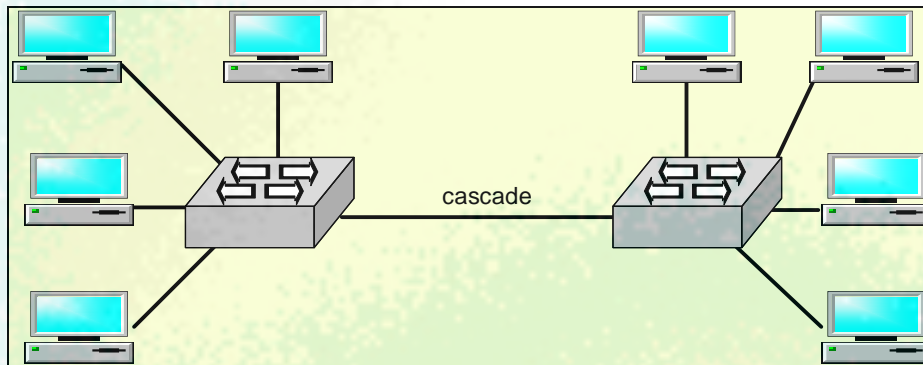
Alors que les ponts laissent passer tous les bits depuis un port vers tous leurs autres ports, les **ponts** réalisent, **automatiquement, sans aucune intervention extérieure**, les tâches suivantes :

- ◆ **maintenance de sa table de pontage,**
- ◆ **non retransmission des trames incorrectes ;**
- ◆ **non retransmission des collisions des protocoles de type CSMA ;**
- ◆ **filtrage du trafic.**

5.8.4) Extension d'une topologie physique en étoile : commutateur {switch}

Les topologies en bus ont été peu à peu abandonnées au profit des topologies en étoile. Le périphérique intermédiaire de liaison de données qui relie les segments d'une topologie en étoile constitue un **pont multiport** appelé **commutateur {switch}**.

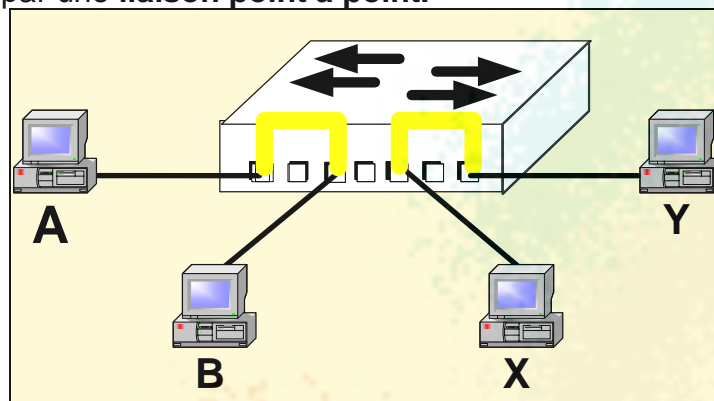
L'intérêt de migrer d'une topologie physique en bus, vers une topologie physique en étoile basée sur des commutateurs réside dans la plus grande robustesse de l'architecture. Dans une topologie physique en bus, la dégradation du support impacte l'ensemble des équipements connectés au bus, tandis que, dans une topologie physique en étoile, la dégradation d'un segment n'influe pas sur les autres équipements.



Le fonctionnement d'un commutateur est semblable à celui d'un pont, mais avec plus de ports. Il est préférable de parler de **table de commutation**, ou de **table d'adresses MAC**, plutôt que de table de pontage.

5.8.5) Commutateur : topologie physique en étoile, topologie logique point à point

Dans un commutateur {switch} tout se passe comme si le segment de l'équipement source était directement connecté au segment de l'équipement de destination. Ainsi, si A adresse une trame à B, cette trame empruntera, à l'intérieur du switch, un "chemin" qui lui est dédié, et elle ne pourra donc pas entrer en conflit avec une trame adressée par X à Y. Durant l'émission d'une trame, d'un point de vue **logique**, tout se passe comme si les équipements source et destination étaient directement connectés par une **liaison point à point**.



5.8.6) Avantages des commutateurs {switch} sur les concentrateurs {hub}

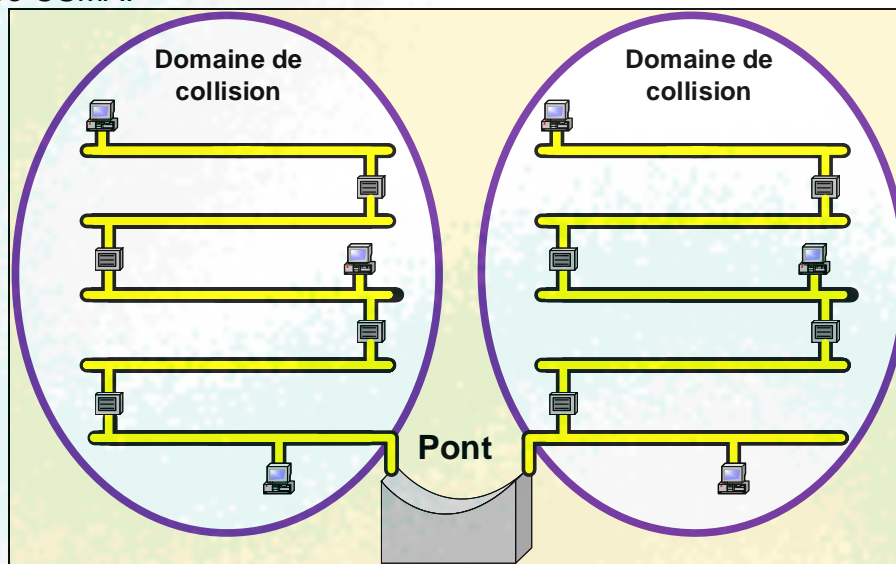
Alors que les concentrateurs laissent passer tous les bits depuis un port vers tous leurs autres ports, les **commutateurs** réalisent, **automatiquement, sans aucune intervention extérieure**, les tâches suivantes :

- ◆ **maintenance de sa table de commutation,**
- ◆ **non retransmission des trames incorrectes ;**
- ◆ **non retransmission des collisions des protocoles de type CSMA ;**
- ◆ **filtrage du trafic.**

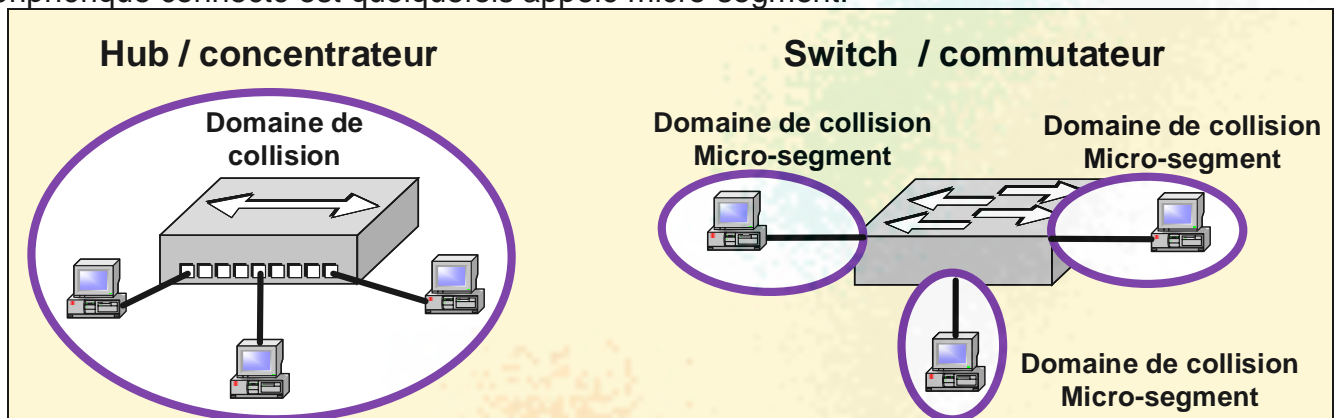
En éliminant le trafic inutile, les commutateurs permettent d'optimiser l'infrastructure réseau. En contrepartie, un périphérique final ne reçoit que les trames qui lui sont destinées. Dans sa configuration par défaut, **un commutateur, configuré par défaut, ne peut pas être utilisé pour analyser le trafic de l'ensemble du réseau**, car le dispositif d'analyse ne recevra qu'une partie des trames traversant le commutateur.

5.8.7) Domaine de collision limités par les ponts et les commutateurs

Contrairement aux répéteurs, les ponts limitent la propagation des collisions générées par les protocoles de type CSMA.



De la même façon, dans une topologie physique en étoile, contrairement aux concentrateurs, les commutateurs limitent la propagation des collisions générées par les protocoles de type CSMA. Les collisions ne peuvent pas se produire à l'intérieur d'un commutateur, sinon c'est un concentrateur. En revanche, sur le lien entre un port du commutateur et le périphérique connecté, une collision peut intervenir entre une trame émise par le commutateur vers le périphérique, et une trame émise par l'équipement vers le commutateur. Le lien entre un port du commutateur et le périphérique connecté est quelquefois appelé micro-segment.



Le remplacement d'un répéteur par un pont, ainsi que le remplacement d'un concentrateur par un commutateur :

- ◆ augmente le nombre de domaines de collision ;
- ◆ diminue la taille des domaines de collision.

5.8.8) Micro-segment reliant 2 ports CSMA full-duplex : plus aucune collision

L'établissement d'une communication bidirectionnelle simultanée {full-duplex} sur un micro-segment rend impossible, lors de l'utilisation des protocoles de type CSMA, l'apparition de collision. En effet, dans ce cas, un micro-segment ne possède que deux extrémités, dont chacune est équipé d'un port capable d'émettre et de recevoir simultanément.

Le protocole de réseau local le plus répandu est le protocole CSMA/CD Ethernet. Les commutateurs actuels Ethernet positionnent, par défaut, tous leurs ports en mode full-duplex.

5.9) Encapsulation et PDU de la couche liaison de données

Les principales **informations d'encapsulation** insérées par la **couche liaison de données** sont :

- ◆ l'adresse de niveau 2 de destination ;
- ◆ l'adresse de niveau 2 source ;
- ◆ un champ de vérification d'intégrité ;
- ◆ l'identifiant du protocole de niveau 3 encapsulé.

La PDU de niveau 2 est appelée **trame** {frame}.

6) Protocole Ethernet ou 802.3

6.1) Ethernet ou 802.3 ?

Ethernet représente le protocole de réseaux locaux le plus utilisé, la société **Xerox** en est à l'origine. Dans les années 1972-1973, un groupe de chercheurs dirigés par **Robert Metcalfe** mirent au point l'**Ethernet** original au Xerox **PARC** {Palo Alto Research Centre}. Robert Metcalfe quitta Xerox en 1979 et créa la société **3COM**. En septembre 1980, Xerox en partenariat avec **DEC** {Digital Equipment Corporation} et **Intel** publia « *The Blue Book* » intitulé : « *The Ethernet* ». Cet ouvrage posait les bases, méthode d'accès, support physique et topologie, de ce que nous connaissons aujourd'hui. Xerox déposa le nom Ethernet. En Novembre 1982, ces trois sociétés définirent la version 2.0 d'Ethernet. Ces premières versions sont désormais connues sous la dénomination **Ethernet DIX** {Digital Intel Xerox}.

Ethernet fut ensuite normalisé par l'ISO et l'IEE. La normalisation d'Ethernet est connue sous la référence 802.3, et a introduit des différences avec Ethernet DIX, en spécifiant cependant que 802.3 devait englober Ethernet DIX.

6.2) Principes de base

L'objectif initial d'Ethernet est la mise en œuvre d'un protocole simple. Les principes qui ont guidés la conception de ce protocole sont les suivants :

- ◆ le **support** doit être :
 - **peu onéreux**,
 - **facile à mettre en œuvre**,
 - **partagé** par tous les équipements.⇒ Ces critères ont conduit au choix de la topologie en **bus** ;
- ◆ chaque équipement doit pouvoir savoir s'il peut émettre, et ceci sans devoir communiquer avec un dispositif de droit à émettre ou de synchronisation ;
- ◆ **il doit être possible d'adresser** :
 - l'ensemble des équipements sur le support. C'est la **diffusion** {**broadcast**} ,
 - un sous-ensemble des équipements sur le support. C'est le **multicast** {**multidiffusion**, **diffusion multipoint**, **diffusion de groupe**}.

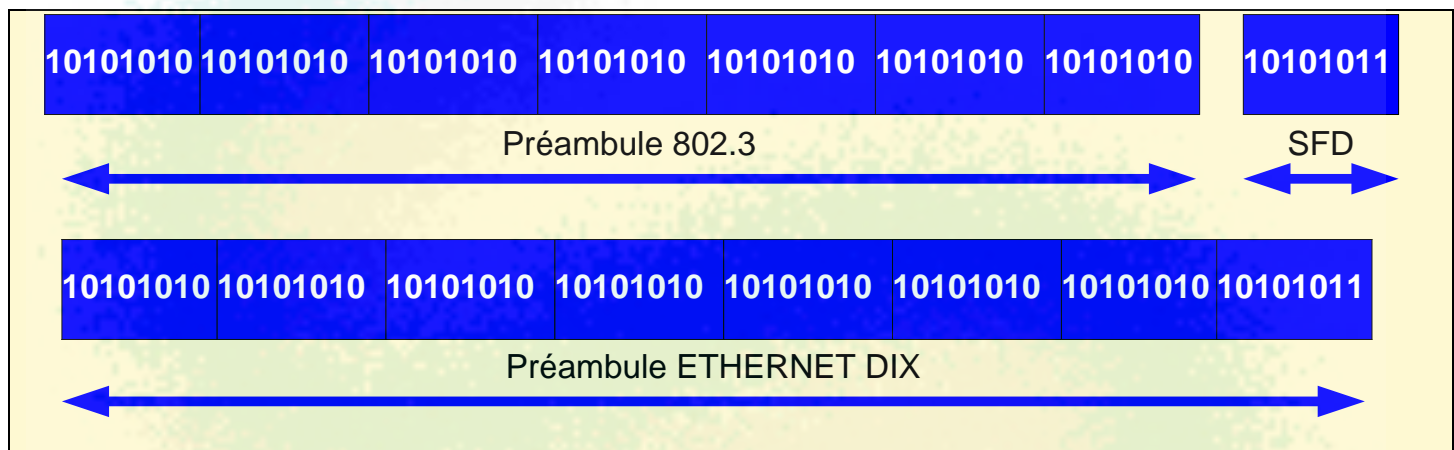
6.3) La topologie, le support, le codage, le temps bit.

La topologie est le bus. Le premier support réellement utilisé est le "gros" câble coaxial. Les transmissions se font en bande de base, par codage Manchester.

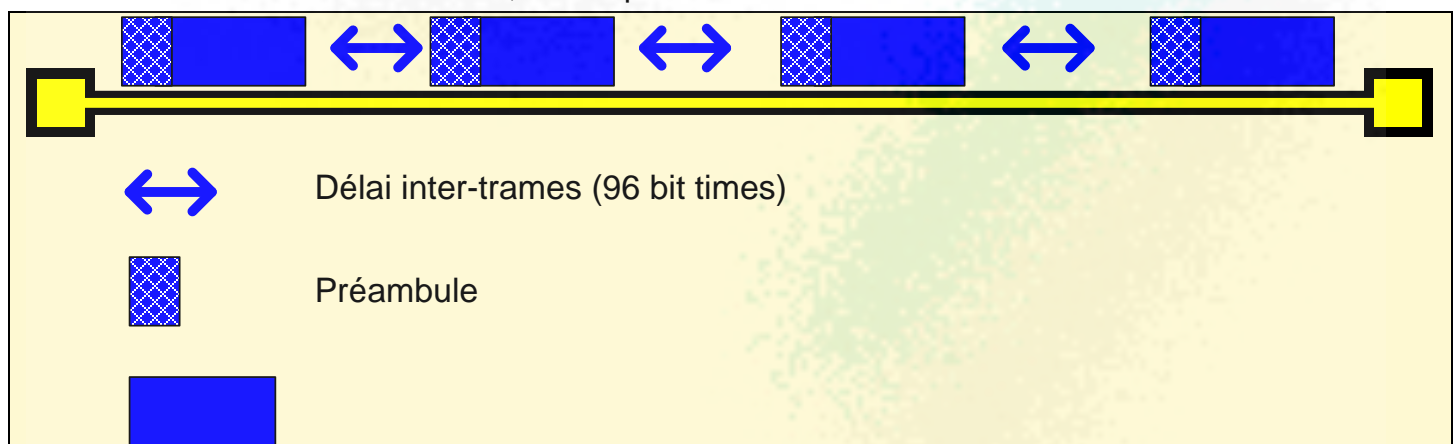
La durée du signal représentant un bit, appelé temps bit {bit time} temps était à l'origine de 0,1 μ s {micro seconde}. Cette valeur a évoluée de façon inversement proportionnelle au débit d'Ethernet.

6.4) La synchronisation

Comme il n'existe **pas d'équipement de centralisation**, et que la **transmission est asynchrone**, il faut que les données transmises permettent la synchronisation des équipements. Chaque **trame {frame}** qui constitue l'unité d'informations de niveau deux, est précédée d'un **préambule {preamble}**. Ainsi, avant qu'une trame ne soit transmise, la **carte réseau {-, Network Interface Card, NIC}** génère un préambule qui permet à l'horloge des récepteurs de se synchroniser avec celle de l'émetteur. Le préambule est constitué de huit octets pour la version DIX, et de sept octets plus un dans la version normalisée 802.3. Les sept premiers octets ont pour valeur **10101010** et le huitième est égal à **10101011**. Ce dernier octet est appelé **SFD {Starting Frame Delimiter,-, délimiteur de début de trame}**, car la rupture des séquences consécutives de bits 10 par la séquence 11 permet aux récepteurs de savoir que la transmission de la trame commence réellement.



Deux transmissions de trames successives doivent être séparées par un temps supérieur au **délai inter trames {Interframe Gap}** fixé à **96 bit times**. Ceci permet d'assurer un état neutre et stable du média pendant un temps minimum. Un hôte ne peut donc pas réémettre immédiatement une nouvelle trame. Par ailleurs, le délai inter trames laisse le temps aux hôtes surchargés de terminer le traitement des données en cours, avant qu'une nouvelle trame ne soit émise sur le média.



6.5) La politique d'accès au médium CSMA/CD

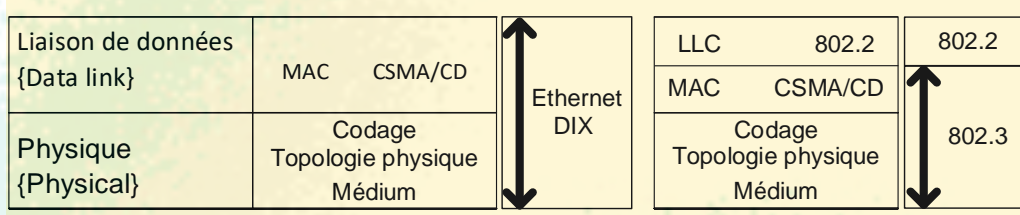
La politique d'accès au media est la politique non déterministe CSMA/CD.

6.6) Les trames Ethernet DIX et 802.3

Ethernet a été créé par XEROX en 1973. En 1983, le sous-comité **802.3 Working Group** du comité 802 de l'IEEE normalisa l'Ethernet DIX sous la référence 802.3. Malheureusement, avant la publication de la norme, plusieurs acteurs du marché des réseaux avaient déjà mis en œuvre ces technologies. Il existe donc aujourd'hui plusieurs types de trames dans la famille Ethernet/802.3. Ces trames sont, par ordre chronologique croissant :

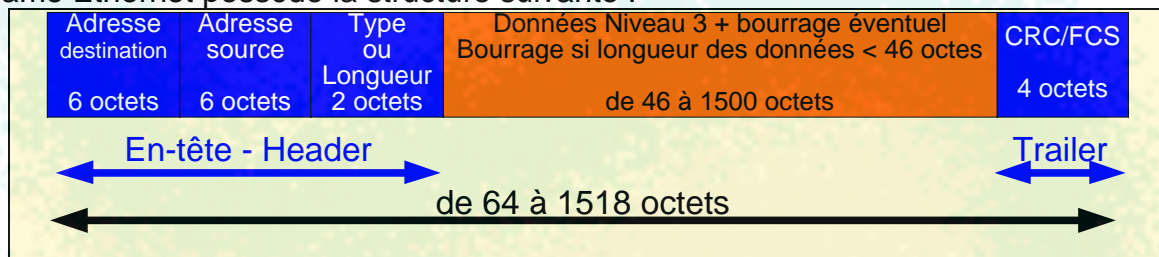
- ◆ La trame Ethernet DIX version, 1 puis 2, définie avant l'avènement de la sous-couche LLC ;
- ◆ La trame Ethernet NOVELL 802.3 (ou 802.3 RAW) développée pour véhiculer IPX ;
- ◆ La trame standardisée par l'IEEE qui encapsule l'en-tête d'une trame LLC ;
- ◆ La trame standardisée par l'IEEE **SNAP** {SubNetwork Access Protocol}.

Ces quatre types de trames peuvent être utilisés simultanément sur un même réseau "Ethernet". Leur normalisation fait que les interfaces réseaux sont capables de les reconnaître. Dans les descriptions suivantes, le préambule n'est plus mentionné, il ne faut néanmoins pas l'oublier avant chaque trame. Seules les trames DIX et IEEE 802.3 sont décrites dans ce support. Les deux schémas suivants résument la différence entre l'encapsulation Ethernet DIX et 802.3.



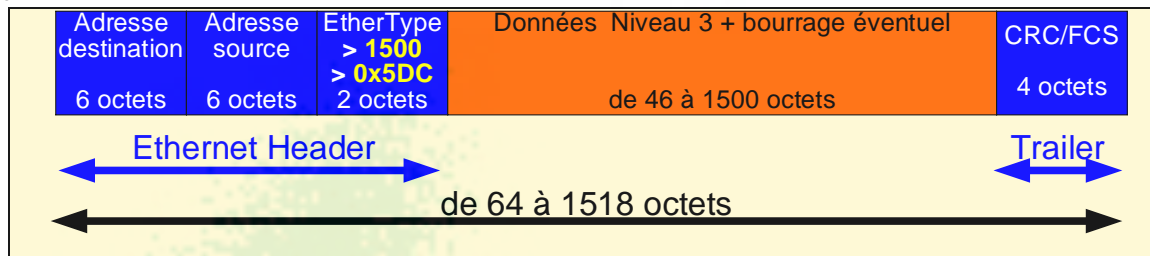
6.6.1) Trame Ethernet/802.3 générique

Toute trame Ethernet possède la structure suivante :



6.6.2) La trame Ethernet DIX (type I ou II)

La trame Ethernet DIX, type I ou II, utilise un champ type qui code sur 2 octets le protocole de niveau trois encapsulé, tandis que tous les autres types de trames utilisent ce champ pour coder le nombre d'octets utiles (à l'exclusion des octets de remplissage). Comme la zone de données comporte entre 46 {0x002E} et 1500 {0x05DC} octets, une valeur de ce champ strictement supérieure à 1500 {0x05DC} indique qu'il s'agit d'un numéro de protocole, et donc d'une trame Ethernet DIX.



Historiquement, c'est XEROX qui fixait la valeur des EtherTypes, mais depuis la normalisation c'est L'IEEE qui les attribue.

Décimal	Hexadécimal	Protocole
1536	0x0600	Xerox XNS
2048	0x0800	IP
2054	0x0806	ARP
2101	0x0835	Reverse ARP
33079	0x8137	Novell IPX
33080	0x8138	Novell
34525	0x86DD	IP Version 6

6.7) La trame IEEE 802.3

Le modèle OSI décompose la couche **liaison de données** {Data link} en deux sous-niveaux : le sous-niveau MAC, et le sous niveau **LLC** {Logical Link Control} [IEEE 802.2]. La sous-couche LLC permet de mettre à la disposition du niveau trois, une interface unique indépendante des protocoles inférieurs LAN, ou WAN. Elle communique avec la couche réseau par l'intermédiaire des **LSAPs** [Link Service Access Point]. Le **SSAP** est le **Source Service Access Point**, et le **DSAP** constitue le **Destination Service Access Point**. Le tableau suivant en donne quelques exemples.

Port (SAP)	Libellé
0X00	Null LSAP
0x42	IEEE Spanning tree
0x80	Xerox XNS
0x98	ARP
0xAA	Sub Network Access Protocol
0xE0	Novell IPX
0xF0	IBM Netbios
0xFE	ISO Protocole réseau en mode non connecté
0xFF	LSAP Global

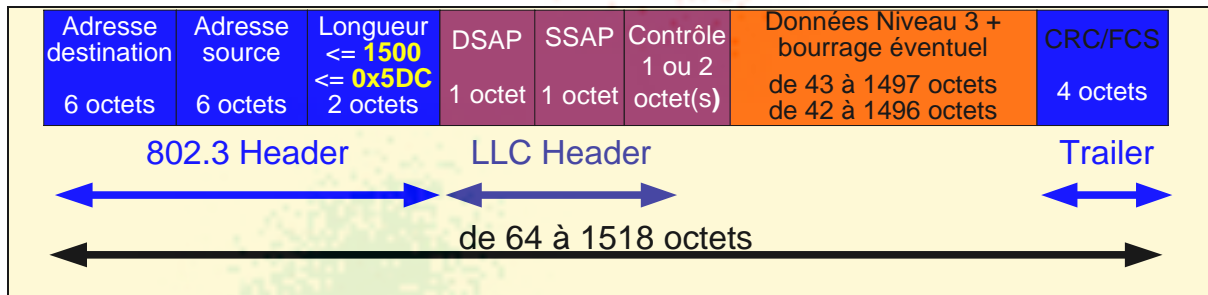
La sous-couche 802.2 {LLC} intègre trois types de service au niveau liaison :

- ◆ **type 1** : service sans connexion et sans acquittement ;
- ◆ **type 2** : service orienté connexion. Avec acquittement et contrôle de flux à "**fenêtre glissante**" ;
- ◆ **type 3** : service sans connexion, sans reprise sur erreur avec acquittement individuel de chaque trame. Ce contrôle de flux est dit "**stop and wait**".

La trame **IEEE 802.3** intègre un en-tête **LLC 802.2** dans la zone de données. Certains systèmes référencent cette trame sous le qualificatif d'Ethernet 802.2 (Novell Netware) ou Ethernet SAP (Cisco).

L'en-tête **LLC** est constitué de :

- ◆ un octet **DSAP** {**D**estination **S**ervice **A**ccess **P**oint} ;
- ◆ un octet **SSAP** {**S**ource **S**ervice **A**ccess **P**oint} ;
- ◆ un ou deux octets de contrôle LLC.



6.8) Adresses des trames Ethernet et 802.3

Les adresses des trames Ethernet et 802.3 sont les adresses MAC classiques. Les adresses de destination peuvent être des adresses de **monodiffusion** {**unicast**} de diffusion {**broadcast**} de multidiffusion {**multicast**}.

6.9) Ethernet 10 Mbit/s sur bus

Depuis sa création en 1972 ou en 1973, Ethernet a beaucoup évolué. Ce protocole s'est continuellement adapté aux nouveaux besoins et aux nouvelles technologies. L'Ethernet originel assurait un débit de 10 Mbit/s, utilisait un codage bande de Base, et s'appuyait sur une topologie en bus, réalisée grâce à des câbles coaxiaux de cuivre.

6.9.1) 10Base5 : Yellow Ethernet {Ethernet jaune}

La dénomination **10Base5** met en évidence :

- ◆ le débit : **10** Mbit/s ;
- ◆ le codage : bande de **Base** {**B**aseband} ;
- ◆ la longueur maximale d'un segment de câble : **500** m.

Les notation **10Base5** et **10BASE5** sont toutes deux d'emploi courant. Dans la suite, c'est la notation **Base** qui est employée, en raison de sa meilleure lisibilité.

C'est le standard historique Ethernet. Ces caractéristiques sont les suivantes :

- ◆ câble coaxial de 50 Ohm dont la gaine externe est jaune ;
- ◆ le segment comporte à chaque extrémité une charge {terminateur} de 50 Ohm ;
- ◆ respect d'un rayon de courbure de 30 centimètres minimum à la pose pour éviter que le câble ne perde ses caractéristiques électriques ;
- ◆ la longueur maximum d'un segment est de 500 mètres ;
- ◆ les stations se connectent suivant une topologie en bus, par l'intermédiaire d'un **transceiver** et d'un **câble de descente** {**drop cable**} ;
- ◆ le câble 10Base5 comporte un repère tous les 2,50 mètres indiquant où brancher le transceiver. Le nombre maximum d'équipements connectés est donc deux cent (500 / 2,5) ;
- ◆ la connectique utilisée avec le câble 10Base5 est de type N ;
- ◆ la longueur maximum d'un réseau Ethernet est 2 500 mètres. En effet, un réseau Ethernet peut comporter jusqu'à cinq segments, séparés par quatre répéteurs. Mais trois segments au plus peuvent comporter des équipements autres que des répéteurs. C'est la règle des 5, 4, 3 (5 segments, 4 répéteurs, 3 segments peuplés).

6.9.2) 10Base2 : Thin Ethernet {Thinnet, Cheapernet, Ethernet Fin}

La dénomination **10Base2** met en évidence :

- ◆ le débit : **10** Mbit/s ;
- ◆ le codage : bande de **Base** {**B**aseband} ;
- ◆ la longueur maximale d'un segment de câble : 185 m { ≈ 200 m}.

C'est le standard qui a popularisé Ethernet, grâce à sa facilité de mise en œuvre et à son faible coût. Ses principales caractéristiques sont :

- ◆ câble coaxial de 50 Ohm, écranté et blindé ;
- ◆ le segment comporte à chaque extrémité une charge de 50 Ohm ;
- ◆ rayon de courbure minimum 5 centimètres ;
- ◆ la longueur maximale de chaque segment est de 185 mètres ;
- ◆ le nombre maximum de segments est de cinq, connectés par quatre répéteurs, avec au plus trois segments peuplés. La longueur maximum d'un réseau 10Base2 est donc 925 mètres ;
- ◆ les stations se connectent suivant une topologie en bus grâce à un connecteur en T ;
- ◆ la connectique utilisée est de type BNC ;
- ◆ le câble est plus fin {**thinnet**} et plus économique {**cheapernet**} que le câble "jaune" ;
- ◆ Distance minimale entre les stations : de 0,5 mètres ;
- ◆ Nombre maximum de connexions par segment : 30.

6.10) 10Base-T : Ethernet 10 Mbps sur paires torsadées non blindées {UTP}

6.10.1) Caractéristiques

Le manque de fiabilité des deux systèmes en bus (si le bus est rompu, tout le réseau s'arrête) a conduit à définir un nouveau câblage s'appuyant sur un bus physique en étoile. La dénomination **10Base-T** met en évidence :

- ◆ le débit : **10** Mbit/s ;
- ◆ le codage : bande de **Base** {**Baseband**} ;
- ◆ le support : paire torsadée {**Twisted pair**}.

Les caractéristiques principales des réseaux 10Base-T sont les suivantes :

- ◆ câble à **paire**s torsadées non blindées {**UTP**} **catégorie 3** minimum ;
- ◆ les stations sont raccordées à un **concentrateur** {**hub**} ;
- ◆ la distance maximale entre un hub et une station ou entre deux hubs cascades est de 100 mètres ;
- ◆ la topologie du réseau : étoile ou cascade d'étoiles reliées entre elles. Les hubs peuvent être empilés {**stacked**} pour réaliser des concentrateurs composites et permettre la réalisation d'un réseau de plusieurs centaines de postes. L'empilement constitue un mécanisme propriétaire, tandis que la cascade est normalisée.
- ◆ la connectique est de type RJ45. Les **2 paires 1-2 et 3-6** sont utilisées pour l'émission et la réception ;
- ◆ une détérioration locale au niveau d'une station ne provoque pas de perturbation générale du réseau ;
- ◆ les hubs sont des répéteurs multiports au sens de la norme Ethernet. Il faut donc respecter la célèbre règle des 5, 4, 3.

6.11) Ethernet 10Mbit/s sur fibre optique

Plusieurs standards Ethernet 10 Mbit/s ont été définis. Celui qui a connu le plus grand succès est **10Base-FL**. Il permettait d'atteindre des distances de 2 km et utilisait une onde courte de 850 nm sur une paire de fibres multimodes 62.5 / 125 µm.

6.12) Passage à Ethernet 100 Mbit/s {Fast Ethernet}

Le passage à Ethernet 100 Mbit/s s'est fait au détriment des supports coaxiaux initiaux en cuivre de 50 Ohm, qui ne sont plus supportés dans les normes 100 Mbit/s. Le terme Fast Ethernet englobe tous les standards Ethernet 100 Mbit/s.

6.13) Ethernet 100 Mbit/s sur paires torsadées UTP {100Base-T}

100Base-T représente l'ensemble des standards Fast Ethernet sur paire torsadée.

6.13.1) 100Base-TX

100Base-TX est la technologie sur paire torsadée qui s'est imposée, car elle reste **compatible avec les technologies 10 Mbit/s**. Le passage à 100 Mbit/s impose un câblage à paires torsadées non blindées {UTP} catégorie 5. 100BaseTX n'utilise que **2 paires torsadées**.

Le codage, toujours bande de base, associe le **codage complet 4B/5B** et le **codage en ligne MLT-3**.

Les expressions 100Base-T et 100Base-TX ne sont pas synonymes, mais sont malheureusement souvent confondues.

6.13.2) Autres technologies 100 Mbit/s sur paires torsadées

D'autres technologies 100 Mbit/s sur paires torsadées ont été proposées, mais leur usage est resté très limité.

100Base-T4 nécessite un câblage à **4 paires torsadées** catégorie 3. 3 paires sont utilisées pour l'émission/réception et une permet la détection de collisions. 100Base-T4t utilise le codage complet **8B/6T** en association avec le codage en ligne **PAM-3 {Pulse Amplitude Modulation}**.

100Base-VG a normalisé le **100VG ANYLAN** propriétaire HP {Hewlett-Packard}. Il nécessitait un câblage de 4 paires torsadées catégorie 3. Ce standard n'est plus actif.

6.14) Ethernet 100 Mbit/s sur fibre optique

6.14.1) 100Base-FX

100Base-FX constitue la première mise en œuvre de Fast Ethernet sur fibre optique. Ses caractéristiques principales sont :

- ◆ longueur d'onde : de **1 300 nm** ;
- ◆ Support : fibre multimode **62.5 / 125 µm** ;
- ◆ étendue jusqu'à :
 - 400 m en mode half-duplex,
 - 2 km en mode full-duplex ;
- ◆ codage **bande de base**, code
- ◆ complet **4B/5B** associé au codage en ligne **NRZI**.

L'étendue de 2 km n'a pu être obtenue que grâce à l'utilisation d'ondes longues, peu sensibles aux phénomènes d'atténuation. Malheureusement, les équipements associés à ces longueurs d'ondes sont onéreux, et non compatible avec **10Base-FL**.

6.14.2) 100Base-SX

100Base-SX a été développé afin d'assurer la compatibilité avec 10Base-FL, et de rendre les solutions Fast Ethernet sur fibre optiques moins onéreuses. Ses caractéristiques principales sont :

- ◆ longueur d'onde : de **850 nm** ;
- ◆ Support : fibre multimode **62.5 / 125 µm** ;
- ◆ étendue : **2 km**.

6.14.3) Autres technologies 100Mbit/s sur fibre optique

100Base-LX10 et 100Base-BX10 constituent des standards propriétaires Fast Ethernet sur fibre optique. Ils permettent d'atteindre des distances de 10 km en utilisant de la fibre monomode.

6.15) Ethernet Gigabit {1 Gbit/s, 1000 Mbit/s} sur câbles en cuivre

6.15.1) 1000Base-TX : Ethernet Ggigabit sur paire torsdée UTP cat 6

1000Base-TX représente la première normalisation Ethernet Gigabit sur paire torsadée. Elle présente le très gros désavantage de nécessiter un **câblage catégorie 6**. A l'époque de sa standardisation, l'énorme majorité des câblages étaient réalisés en catégorie 5. Ceci a constitué un frein énorme, et 1000Base-TX n'a jamais été réellement déployé.

6.15.2) 1000Base-T : Ethernet Gigabit sur paire torsadée UTP cat 5

L'adoption de 1000Base-T a permis d'accélérer la transition de Fast Ethernet à Giga Ethernet. En effet 1000Base-T s'appuie sur un câblage catégorie 5. Il est cependant recommandé d'utiliser un câblage catégorie 5^e ou catégorie 6. Les caractéristiques principales de 1000Base-T sont :

- ◆ le débit : **1000** Mbit/s ;
- ◆ le codage : bande de **Base** {Baseband} ;
- ◆ le support : 4 paires torsadées {Twisted pair} UTP cat 5 minimum. Les **4 paires sont utilisées** ;
- ◆ codage : **PAM-5** {Pulse Amplitude Modulation}.

6.15.3) 1000Base-CX : Giga Ethernet sur câble blindé en cuivre

1000Base-CX a été introduit avant 1000Base-T. Il nécessite un câblage blindé dont la longueur maximale est de 25 mètres terminé par des connecteurs DB 9 ou HSSDC 8 contacts. Le codage mis en œuvre est le code **complet 8B/10B**. Ce standard est très peu employé

6.16) Ethernet Gigabit {1 Gbit/s, 1000 Mbit/s} sur fibre optique

6.16.1) 1000Base-SX : Giga Ethernet onde courte {Short wave}

Les caractéristiques principales de 1000Base-SX sont :

- ◆ longueur d'onde : de 770 nm à 860 nm (infra-rouge lointain),
- ◆ Support : fibre multimode,
- ◆ étendue :
 - 220 m sur fibre 62,5 / 125 µm,
 - 550 m sur fibre 50 / 125 µm ;
- ◆ Codage : bande de base, code **complet 8B/10B** associé au code **en ligne NRZ**.

1000Base-SX constitue une technologie **peu onéreuse**, mais limitée en étendue.

6.16.2) 1000Base-LX : Giga Ethernet onde longue {Long wave}

Les caractéristiques principales de 1000Base-LX sont :

- ◆ longueur d'onde : de 1 270 nm à 1 355 nm (technologie laser);
- ◆ Support : fibre multimode :
 - étendue : 550 m,
- ◆ Support : fibre monomode :
 - étendue : 5 km ;
- ◆ Codage : bande de base, code **complet 8B/10B** associé au code **en ligne NRZ**.

1000Base-LX constitue une technologie **onéreuse**, mais brise les limitations de distance de 1000Base-SX.

6.16.3) Autres technologies Giga Ethernet sur fibre optique

Les autres standards Giga Ethernet sur fibre optique, les plus répandus sont :

- ◆ 1000Base-LX10 ;
 - longueur d'onde : 1 315 nm ;
 - Support : fibre monomode ;
 - étendue : 10 km ;
- ◆ 1000Base-ZX ;
 - longueur d'onde : 1 550 nm ;
 - Support : fibre monomode ;
 - étendue : 70 km ;
- ◆ 1000Base-BX10 ;
 - longueur d'onde : 1 490 nm descendant – 1 390 montant ;
 - Support : fibre monomode ;
 - étendue : 10 km.

6.16.4) 1000Base-X

1000Base-X référence l'ensemble des standards Giga Ethernet qui utilisent le codage 8B/10B. 1000Base-T n'en fait pas partie car il emploie le codage PAM-5.

6.16.5) 10 Gb/s et au-delà

Les débits suivants sont désormais pris en charge par Ethernet :

- ◆ 10,000 Mb/s (10 Gb/s) : fibre et paires torsadées cat. 6a et 7 avec RJ-45 ;
- ◆ 40,000 Mb/s (40 Gb/s) : fibre et paires torsadées. catégorie 8 avec d'autres connecteurs que RJ-45. En paires torsadées la distance est limitée à 30 mètres ;
- ◆ 100,000 Mb/s (100 Gb/s) : fibre.

Au-delà des 100 Gbps, les choses ne sont pas figées, et les informations ci-dessus sont susceptibles de changer.

6.17) Tableau récapitulatif de d'évolution d'Ethernet jusqu'au gigabit

Liaison de données	LLC	802.3											802.2
	MAC	CSMA/CD Avec évolution pour prendre en compte le full-duplex et l'augmentation des débits, en restant compatible avec la norme originelle.											802.3
Physique		10	10	10	100	100	100	1000	1000	1000	1000	1000	
		Base	Base	Base	Base	Base	Base	Base	Base	Base	Base	Base	
		-5	-2	-T	-TX	-LX	-SX	-CX	-LX	-SX	-TX	-T	
		500m	185m	100m	100m			25m			100m	100m	
		Coax	Coax	UTP	UTP	FO	FO	2 paires-Blindées	FO	FO	UTP	UTP	
		gros	Fin	Cat 3	Cat 5						Cat 6	Cat 5	
		50Ω	50Ω	100Ω	100Ω			150Ω			100Ω	100Ω	
		N	BNC	RJ45	RJ45			*			8P8C	8P8C	
				2 TP	2 TP						4 TP	4 TP	
* connecteur High Speed Serial Data Connector et connecteur Sub-D 9 points													

6.18) Du hub {concentrateur} au switch {commutateur} Ethernet

6.18.1) De la topologie logique en bus à la topologie logique point à point

Un hub est un répéteur au sens Ethernet classique, il reconstitue en interne un bus logique à 10 Mbit/s. Le débit de 10 Mbit/s est donc partagé par toutes les cartes réseaux connectées en étoile via les câbles à paires torsadées. Le débit de 10 Mbit/s entre deux cartes réseau n'est jamais atteint, car il est bien rare que sur un réseau il n'y ait que deux cartes réseau actives. Afin de palier à cet inconvénient, les concentrateurs intelligents ont été mis en œuvre. Ils sont connus sous la dénomination de **commutateurs {switch}**.

Grâce à un dispositif de commutation interne, les commutateurs relient directement les ports connectés aux équipements en cours de communication. Dès lors, ces équipements ne partagent plus un bus commun avec d'autres équipements informatiques. Un commutateur travaille au niveau 2 {liaison de données}, il connaît donc l'adresse MAC des cartes réseau connectées à chacun de ses ports. C'est grâce à cela, qu'il peut réaliser la commutation. Un commutateur est un pont multiport au sens du modèle OSI, tandis que le concentrateur constitue un répéteur multiport, car il travaille au niveau 1 {couche physique}.

6.18.2) Introduction du mode full-duplex : élimination totale des collisions

Avec l'arrivée des commutateurs, les transmissions **full-duplex {bidirectionnelle simultanée}** ont été introduites. Un port de commutateur capable d'opérer simultanément sur les paires d'émission et de réception travaille en mode full-duplex. Il peut émettre et recevoir en même temps, à condition, que l'équipement qui lui est connecté supporte également le full-duplex. **La commutation Ethernet full-duplex élimine totalement les collisions.**

6.18.3) Ports cuivre 8P8C {RJ45} MDI et MDI-X

Au niveau de la couche physique, l'interface propre au médium {**MDI**, **M**edium **D**ependant **I**nterface} correspond à la description complète de l'interface (forme, nombre et disposition des connecteurs, signal, ...).

Ethernet **définit** dans la description des connecteurs 8P8C {RJ45} **les paires dédiées à l'émission et celles dédiées à la réception**. Pour Ethernet 10BaseT et 100BaseTx, qui n'utilisent que deux paires, les ports MDI sont des ports dont la paire 1-2 assure l'émission des données, tandis que la paire 3-6 prend en charge la réception des données.

Pour que deux équipements A et B puissent communiquer, il faut que ce qui est émis par la paire d'émission de A arrive sur la paire de réception de B, et, réciproquement, ce qui est émis par la paire d'émission de B arrive sur la paire de réception de A. Pour résoudre ce problème Ethernet a défini des ports MDI-X qui inversent la position des paires d'émission et de réception. Le X de MDI-X indique le croisement.

Tout périphérique, à l'exception des hubs et des commutateurs, pouvant se connecter à un réseau local Ethernet par câble à paires torsadées à connecteurs 8P8C {RJ45} est équipé d'une carte réseau de type **MDI**.

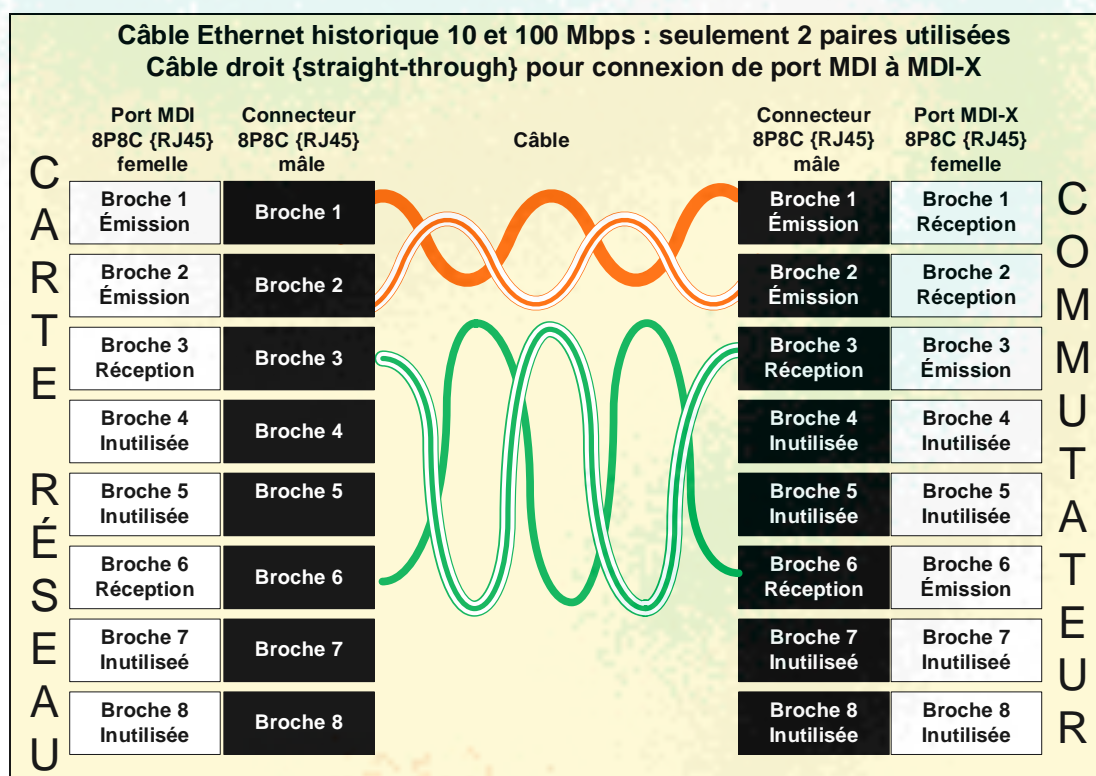
Les **hubs et les commutateurs** sont équipés de ports **MDI-X**.

6.18.4) Câbles droits et croisés historiques 10 et 100 Mbps : paires 1-2 et 3-6

La connexion d'un port MDI à un port MDI-X se fait par un **câble droit** {straight-through}.

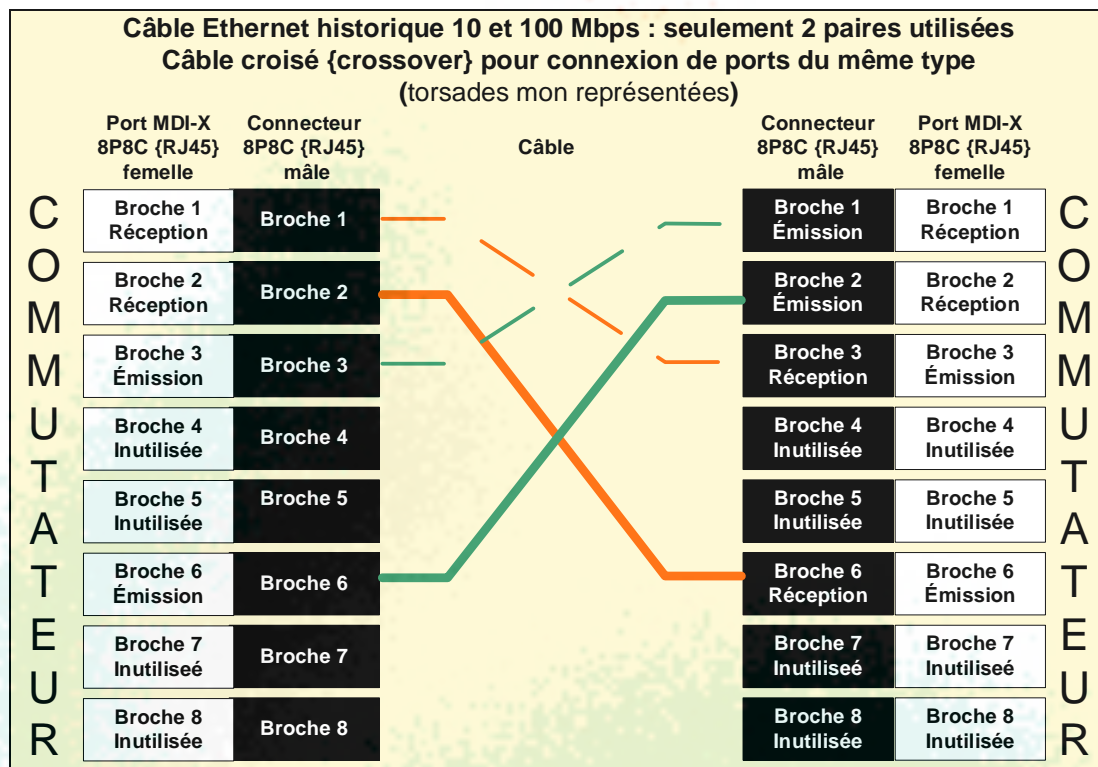
Un câble droit 100Base-TX, compatible 10BaseT, est un câble :

- ◆ respectant les paires 1-2 et 3-6 ;
- ◆ dont la broche 1 d'une extrémité est reliée à la broche 1 de l'autre extrémité ;
- ◆ dont la broche 2 d'une extrémité est reliée à la broche 2 de l'autre extrémité ;
- ◆ dont la broche 3 d'une extrémité est reliée à la broche 3 de l'autre extrémité ;
- ◆ dont la broche 6 d'une extrémité est reliée à la broche 6 de l'autre extrémité.



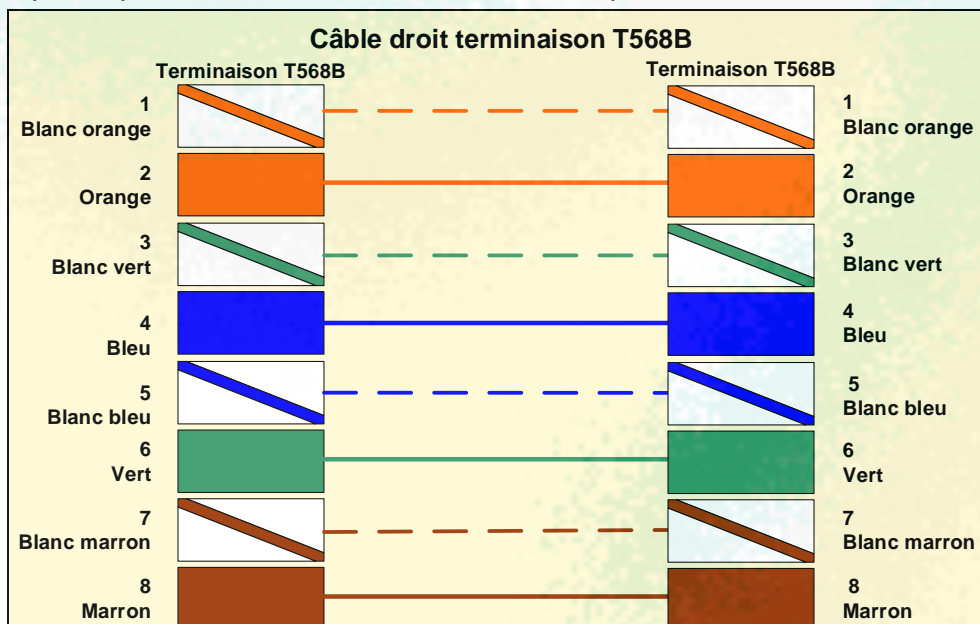
La connexion de deux ports du même type, MDI à MDI ou MDI-X à MDI-X, implique l'utilisation d'un **câble croisé** {crossover}. Un câble croisé 100Base-TX, compatible 10BaseT, est un câble :

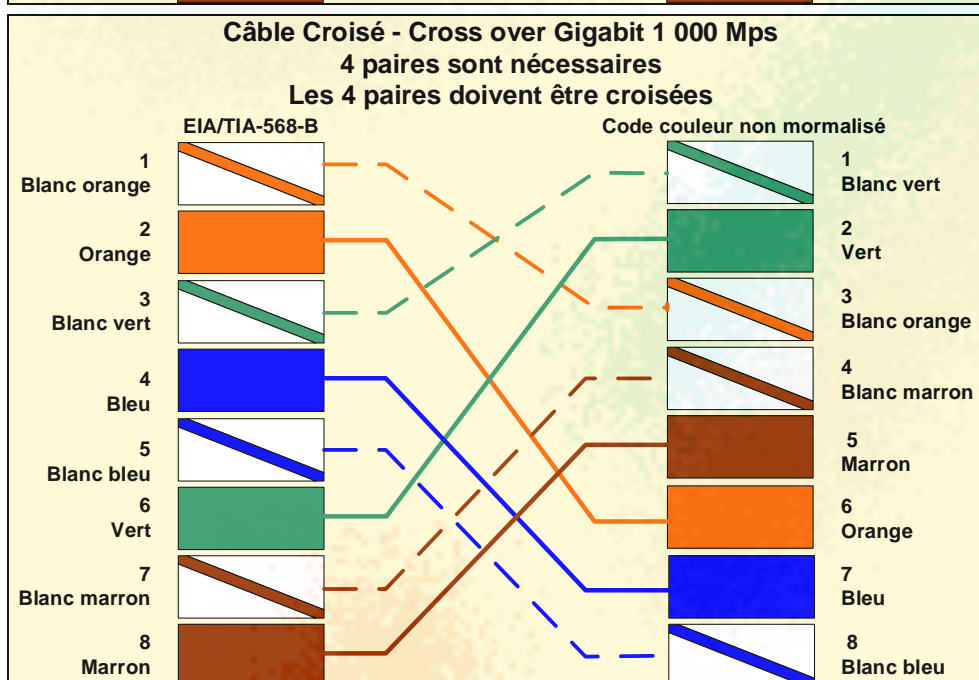
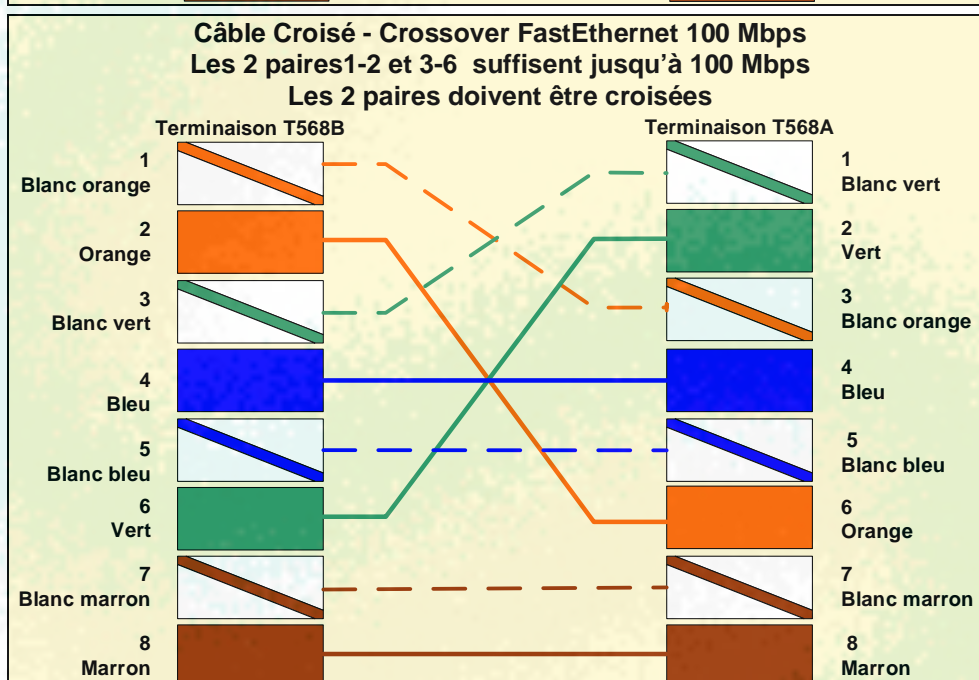
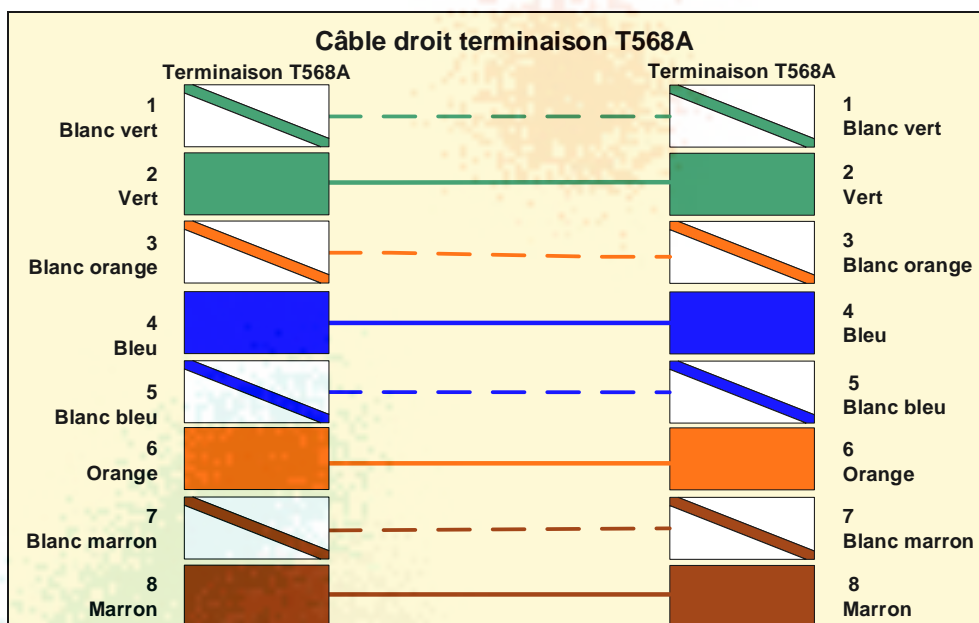
- ◆ respectant les paires 1-2 et 3-6 ;
- ◆ dont la broche 1 d'une extrémité est reliée à la broche 3 de l'autre extrémité ;
- ◆ dont la broche 2 d'une extrémité est reliée à la broche 6 de l'autre extrémité ;
- ◆ dont la broche 3 d'une extrémité est reliée à la broche 1 de l'autre extrémité ;
- ◆ dont la broche 6 d'une extrémité est reliée à la broche 2 de l'autre extrémité.



6.18.5) Types de câbles après normalisation EIA/TIA et support du gigabit

La normalisation du câblage par l'EIA/TIA, ainsi que l'augmentation des débits qui nécessitent l'utilisation des quatre paires ont conduit à l'utilisation de plusieurs modèles de câbles.





6.18.6) Cascade de commutateurs : port Uplink MDI, et auto MDI/MDI-X

Afin d'éviter l'emploi de câbles croisés lors de la connexion de deux commutateurs {cascading}, les commutateurs ont tout d'abord **intégré un port MDI**, appelé port **Uplink**, destiné à être connecté à un port standard, c'est à dire MDI-X d'un autre commutateur.

Sur certains swiths/hubs, il arrive qu'un port soit muni de deux connecteurs, non utilisables simultanément, l'un étant de type MDI, l'autre de type MDI-X. Dans d'autres cas, un bouton poussoir est associé à un port, suivant la position du bouton poussoir, le port opère en mode MDI ou MDI-X.

Plus intéressant, les commutateurs modernes possèdent la capacité de déterminer si leurs ports doivent fonctionner en mode MDI ou MDI-X. Suivant le constructeur, cette fonction est appelée **auto MDI**, ou **auto MDI-X**, ou encore **auto Uplink**.

6.18.7) Connexion de commutateur à commutateur : cascades ou empilés ?

Deux commutateurs sont **cascadés** {**cascaded**} lorsqu'ils sont reliés via des ports réseaux. Cette connexion est donc standardisée et permet d'associer des switchs de marques et de modèles différents. Des commutateurs connectés par cascade constituent une **étoile étendue**.

Deux commutateurs sont **empilés** {**stacked**} lorsque leurs bus systèmes sont directement interconnectés. Ceci n'est évidemment réalisable que si les deux switchs sont de la même marque et appartiennent à la même gamme. Le mécanisme de jonction des bus système n'est pas normalisé et varie, non seulement, suivant les fabricants, mais aussi suivant les diverses gammes de chaque constructeur. Historiquement l'empilement était assuré par des câbles propriétaires connectés à des ports de stack propriétaire situés à l'arrière des commutateurs.

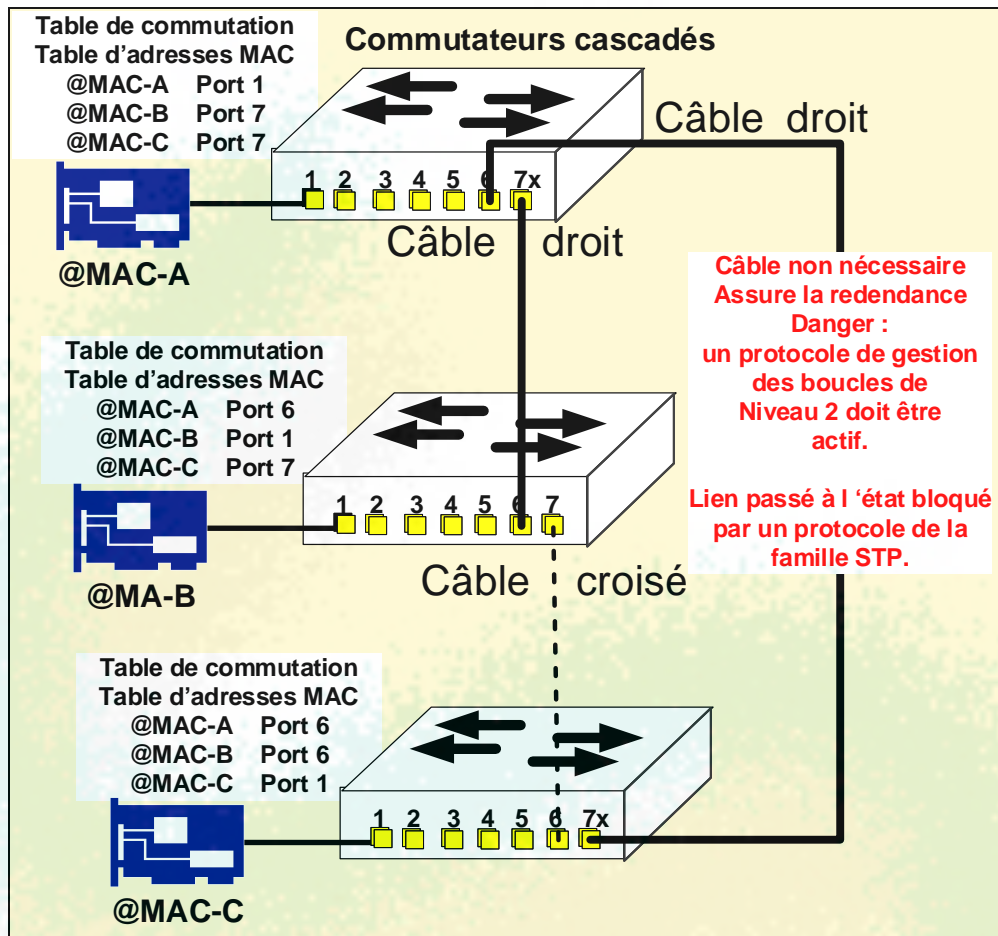


L'ensemble de ces trois commutateurs empilés via des câbles propriétaires se comporte comme un seul commutateur

Depuis qu'Ethernet supporte des débits supérieurs ou égaux au gigabit, il devient courant de voir des commutateurs qui utilisent des ports aux formats normalisés RJ45 ou SFP en tant que ports de stack. Attention, ces ports, bien que semblant parfaitement standards, ne permettent uniquement que de connecter des switchs du même fabricant et de la même gamme. Ils ne sont donc pas disponibles pour la connexion d'équipements terminaux. De plus la longueur des câbles de stack est très limitée et les commutateurs doivent être dans la même unité de brassage.

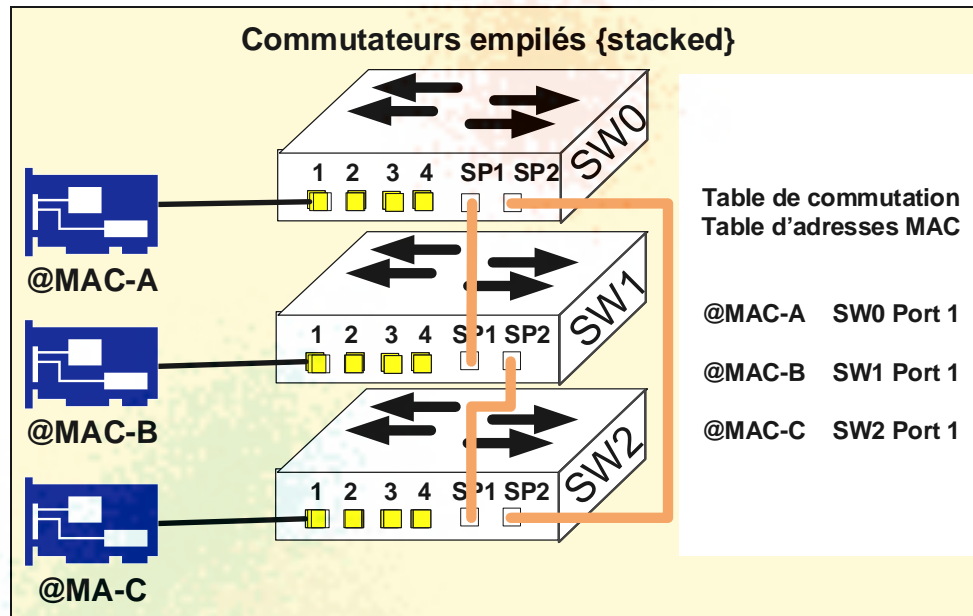
Un ensemble de commutateurs cascades :

- ◆ met en œuvre une table de commutation par commutateur ;
- ◆ est connecté par l'intermédiaire de ports Ethernet et de câbles droits ou croisés ;
- ◆ les échanges inter switch sont limités par le débit Ethernet ;
- ◆ peut être réparti entre plusieurs salles de brassage ;
- ◆ peut être constitué de commutateurs de la marque différentes.



Un ensemble de commutateurs empilés :

- ◆ ne maintient qu'une seule table de commutation ,
- ◆ est connecté par l'intermédiaire de ports de stack et de câbles très courts ;
- ◆ les débits inter switch sont limités par le débit Ethernet ;
- ◆ les échanges inter switch se font à la vitesse du bus système ;
- ◆ est situé dans la même unité de brassage ;
- ◆ nécessite un protocole Spanning Tree Procol en cas de redondance de liens ;
- ◆ est constitué de commutateurs de la même gamme chez un constructeur.



6.18.8) Stack d'alimentations redondantes de commutateurs

Afin d'assurer une alimentation électrique constante, certains commutateurs hauts de gamme sont équipés de deux blocs redondants d'alimentations, **échangeables à chaud {hotswap}** qui doivent être branchés sur des sources électriques différentes. Ainsi, en cas de défaillance d'une des sources d'alimentation ou d'un bloc d'alimentation le commutateur continue à fonctionner.

Afin de palier la défaillance de deux sources d'alimentation et/ou de deux blocs d'alimentation, certains constructeurs permettant d'interconnecter électriquement plusieurs commutateurs, afin que les commutateurs en manque d'alimentation électrique propre puissent s'alimenter via l'alimentation d'un autre commutateur.

La vulgarisation du **POE {Power Over Ethernet}** qui permet aux commutateurs d'alimenter les périphériques finaux favorise l'adoption du stack d'alimentations redondantes.

Cisco implémente le stack d'alimentations redondantes sous le nom de StackPower.

6.18.9) Auto négociation

Le mécanisme d'auto négociation permet aux équipements de se synchroniser (vitesse, mode half ou full-duplex) sans intervention de l'administrateur. Les équipements échangent des **NLPs {Normal Link Pulse, impulsion de liaison normale}**. Une rafale de NLPs est appelée **FLP {Fast Link Pulse, impulsion de liaison rapide}**. L'auto négociation est "obligatoire" en 1000BaseT, mais peut cependant être désactivée. L'auto négociation trouve son origine sur la paire torsadée, mais elle a été portée sur la fibre optique.

L'auto négociation cherche à établir les connexions dans l'ordre suivant :

- ◆ 1 – 1000BaseT full duplex ;
- ◆ 2 – 1000BaseT half duplex ;
- ◆ 3 – 100BaseTx full duplex ;
- ◆ 4 – 100BaseTx half duplex ;
- ◆ 5 – 10BaseT full duplex ;
- ◆ 6 – 10BaseT half duplex.

6.18.10) Les types de transmissions de trames {commutation}

La **latence** caractérise le temps qu'un signal met à aller de bout en bout d'un réseau. Chaque équipement réseau est caractérisé par sa latence. Plus un équipement réalise des tâches complexes, plus sa latence est élevée. Ainsi, un routeur possède une latence plus importante qu'un commutateur.

De la même manière, plus un commutateur isolera finement les segments, plus sa latence sera grande. Les commutateurs utilisent trois grands types de transmissions de trames :

- ◆ commutation **cut through** : latence la plus faible, et correction d'erreur minimale. Il existe deux modes cut through :
 - commutation **fast forward** {**early cut through**} : la trame est transmise immédiatement après la lecture de l'adresse MAC de destination. C'est le mode classique de fonctionnement **cut through**,
 - commutation **fragment free** {**runt free**} : le commutateur analyse les 64 premiers octets de données, afin de déterminer s'il s'agit d'un fragment de collision. Les fragments de collision représentent la grande majorité des erreurs de trames ;
- ◆ commutation par **stockage et retransmission** {**store and forward**} : le commutateur analyse toute la trame y compris le FCS. La latence est donc fonction de la taille de la trame ;

6.18.11) Commutation symétrique et asymétrique

La commutation symétrique assure le transfert des trames entre des ports de mêmes débits, tandis que la commutation asymétrique permet le transfert des trames entre des ports de débits différents.

6.18.12) Mémoire tampon

La mémoire est utilisée par le commutateur pour stocker les trames avant leur transmission. Les deux types de mémoires utilisées sont :

- ◆ la **mémoire tampon axée sur les ports d'entrée** {**in port based memory**} : les trames sont stockées dans des **files d'attentes FIFO** liées au port par lequel elles sont entrées dans le commutateur. Une trame destinée à un port dont le tampon de sortie est saturé bloque la file. Le terme entrée {in} est souvent omis dans le libellé ;
- ◆ la **mémoire partagée** {**shared memory**} : les trames sont stockées dans une mémoire commune partagée, allouée dynamiquement selon les besoins de chaque port.

6.18.13) Commutateurs administrables/gérables {manageable}

Les commutateurs d'entrée de gamme configurent automatiquement le mode half ou full-duplex, la vitesse ainsi que l'état NDI ou MDI-X de leurs ports sans laisser la possibilité aux utilisateurs de modifier le résultat de cette auto-configuration.

Les **commutateurs administrables**, encore appelés **gérables** {**manageable**} permettent aux utilisateurs de modifier ces trois paramètres. Certains modèles "offrent" des fonctionnalités supplémentaires, en particulier la gestion des Vlan.

6.18.14) Réseaux Locaux Virtuels: {-, VLAN, Virtual Local Area Network}

Un **VLAN** {**Virtual Local Area Network, réseau local virtuel, réseau virtuel**} constitue un réseau logique, de niveau 2, étanche, déployé sur un ensemble de **commutateurs** {**switch**}. Cette technologie permet

- ◆ le partage de commutateurs entre plusieurs entités/services ;
- ◆ la **séparation du trafic de niveau 2** entre ces entités/services :
 - garantit que les trames erronées d'une entité/services ne pollueront pas les autres entités/services,
 - limite les broadcasts dans l'entité/service où ils ont été générés,
 - rend plus difficiles les tentatives d'intrusion et d'espionnage depuis le réseau local.

7) Réseaux locaux sans fil {Wireless Local Area network, WLAN}

Les protocoles de réseaux locaux sans fil {Wireless Local Area network, WLAN}, également connus sous le nom de protocoles **Wi-Fi** {**Wireless Fidelity**} sont des protocoles normalisés par les différents comités IEEE 802.11. Ils couvrent les couches physiques et liaison de données OSI, sous-couche LLC {IEEE 802.2} comprise. Ils permettent d'échanger de données jusqu'à **300 mètres** avec des débits s'étalant de **11 Mb/s à plus de 1 Gb/s**. Ce ne sont pas les seuls réseaux sans fil.

7.1) Les autres technologies sans fil

Les technologies sans fil sont en perpétuelle évolution, il est néanmoins possible de les classer en fonction de leur portée.

7.1.1) Réseaux personnels sans fil {Wireless Personal Area Network, WPAN}

Ces technologies sont normalisées par le comité **IEEE 802.15** et fournissent des portées maximum comprises entre 10 et 100 mètres. Les protocoles WPAN les plus connus sont :

- ◆ **Bluetooth** qui apparie les périphériques jusqu'à **100 mètres** s'appuie sur la normalisation **IEEE 802.15.1**. Bluetooth est désormais normalisé par le « **Bluetooth Special Interest Group** », Bluetooth assure des débits jusqu'à **3 Mb/s** :
- ◆ **ZigBee** qui est un protocole de haut niveau dont la portée est limitée à **10 mètres** et le débit à **1 Mb/s**. Il s'appuie sur les spécifications **IEEE 802.15.4** pour la mise en œuvre de ses couches physiques et liaison de données. IEEE 802.2 {LLC} n'est pas supportée par ZigBee. C'est un protocole **radio à faible consommation électrique**, très simple, ne nécessitant donc que peu de code, par conséquent peu onéreux et est particulièrement adapté à l'**IoT {Internet des objets, Internet of Things}** et aux environnements industriels ;
- ◆ **Bluetooth Low Energy {BLE}**, anciennement connu sous le nom **Wibree**, s'appuie sur les spécifications **IEEE 802.15.1**. C'est un protocole **radio à faible consommation électrique**, de l'ordre de 10 fois moins que Bluetooth. Il constitue donc une technologie complémentaire au Bluetooth classique, mais ceci se fait au détriment du débit limité à **1 Mb/s** à une portée réduite à **10 mètres**.

7.1.2) Réseaux étendus sans fil {Wireless Wide Area Network, WMAN}

Les réseaux étendus sans fil possèdent des portées de plusieurs kilomètres. Ils peuvent donc couvrir l'étendue d'une ville, ou être déployés dans des liaisons interurbaines. Les protocoles de réseaux étendus sans fil les plus répandus sont :

- ◆ **WIMAX {Worldwide Interoperability for Microwave Access}**. Ce protocole est réglementé par les normes IEEE 802.16, et assure des débits élevés jusqu'à 50 kilomètres. Des options de mobilité ont été adjointes aux normes initiales afin de prendre en compte l'itinérance. WIMAX constitue une alternative sans fil à l'ADSL ;
- ◆ les **réseaux cellulaires à haut débit**. Ils correspondent aux réseaux bien connus de deuxième, troisième et quatrième génération, plus connus sous le nom de 2G, 3G et 4G ;
- ◆ les **réseaux satellites à haut débit**. Ces réseaux nécessitent l'installation d'une antenne parabolique bidirectionnelle pointant sur un satellite géostationnaire. Ces solutions ne peuvent pas être déployées partout, car aucun obstacle ne doit perturber le flux de données émis en ligne droite entre l'antenne et le satellite.

7.2) Les ondes radio

Les ondes radio sont des ondes électromagnétiques. Une onde électromagnétique est caractérisée par :

- ◆ sa **période**, notée **T**, qui est la plus petite durée qui sépare deux reproductions à l'identique du signal. La période est exprimée en **seconde** ;
- ◆ sa **fréquence**, notée **f** ou **v**, qui représente le nombre de répétitions du signal pendant 1 seconde. La fréquence est exprimée en **Herzt (Hz)** ;
- ◆ sa **longueur d'onde**, notée **λ** (lambda) qui mesure la distance parcourue par l'onde pendant une période. La longueur d'onde est exprimée en **mètres**.

Dans le vide, une onde électromagnétique, se propage à la vitesse de la lumière soit à 299 792 458 m/s. La vitesse d'une onde électromagnétique est appelée **célérité** et est notée **c**. Les relations entre période, fréquence et longueur d'onde sont les suivantes :

$$f = v = 1 / T$$

$$\lambda = c * T = c / f = c / v$$

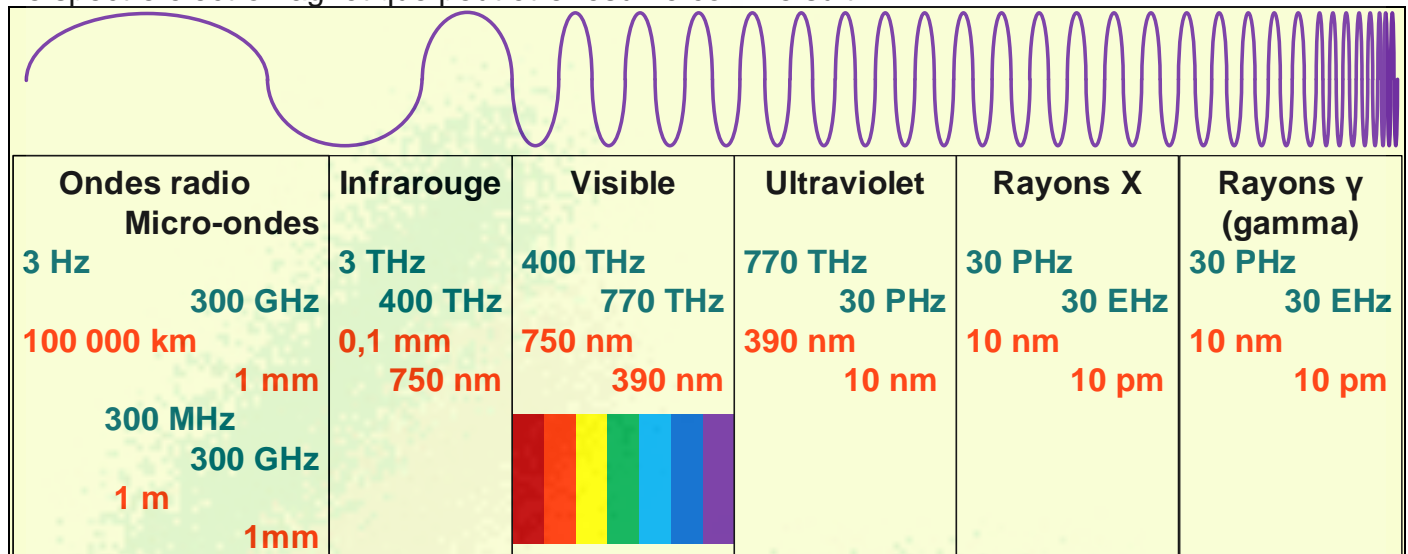
$$\text{avec } c = 299\,792\,458 \text{ m/s}$$

La période, et la longueur d'onde varient inversement à la fréquence.

Il est intéressant de noter que :

- ♦ plus une onde électromagnétique possède une fréquence élevée (plus sa longueur d'onde est petite), plus elle transporte d'énergie ;
- ♦ plus une onde électromagnétique possède une longueur d'onde élevée (plus sa fréquence est basse), plus sa portée est importante.

Le spectre électromagnétique peut être résumé comme suit :



Sur cette représentation il manque les deux gammes de fréquences extrêmes :

- ♦ les "très très" basses fréquences émises par les réseaux électriques et téléphoniques ;
- ♦ les "très très" hautes fréquences du rayonnement cosmique.

Le schéma suivant résume les bandes de fréquences des ondes radio, et resituent celles-ci dans le spectre électromagnétique.

Électricité Téléphonie	Ondes radio Micro-ondes	Infra rouge	Visible	Ultra violet	Rayons X	Rayons γ	Rayons cosmiques
Frequences radio 3 kHz 30 kHz 300 kHz 3 MHz 30 MHz 300 MHz					Frequences micro-ondes 3 GHz 30 GHz 300 GHz		
VLF Très basse fréquence Very Low Frequency	LF Basse fréquence Low Frequency	MF Moyenne fréquence Medium Frequency	HF Haute fréquence High Frequency	VHF Très haute fréquence Very High Frequency	UHF Ultra-haute fréquence Ultra High Frequency	SHF Supra-haute fréquence Supra High Frequency	EHF Extrêmement haute fréquence Extremely High Frequency

Chaque bande de fréquence est utilisées par des applications spécifiques :

- ◆ la bande des **très basses fréquences** {Very Low Frequency, **VLF**} :
 - radionavigation,
 - transmission sous-marine,
 - stimulateurs cardiaques,
 - **Courant Porteur Ligne {CPL}** ;
- ◆ la bande des **basses fréquences** {Low Frequency, **LF**} :
 - radionavigation,
 - radio AM,
 - stimulateurs cardiaques,
 - **Courant Porteur Ligne {CPL}**,
 - **Radio Frequency Identification, {RFID}** ;
- ◆ la bande des **moyennes fréquences** {Medium Frequency, **MF**} :
 - radio AM,
 - **Détecteurs de Victimes d'Avalanches {DVA}**,
 - **Courant Porteur Ligne {CPL}** USA ;
- ◆ la bande des **hautes fréquences** {High Frequency, **HF**} :
 - radio ondes courtes,
 - **Citizen Band {CB}**,
 - **Radio Frequency Identification, {RFID}** ;
- ◆ la bande des **très hautes fréquences** {Very High Frequency, **VHF**} :
 - radio FM,
 - télévision ;
- ◆ la bande des **ultra-hautes fréquences** {Ultra High Frequency, **UHF**} :
 - **WLAN (2,4 GHz)**,
 - **Bluetooth**,
 - **ZigBee**
 - **haut débit cellulaire**,
 - GPS,
 - fours micro-ondes,
 - télévision ;
- ◆ la bande des **supra-hautes fréquences** {Supra High Frequency, **SHF**} :
 - **WLAN (5 GHz)**,
 - transmissions satellites
 - transmissions micro-ondes,
 - radioastronomie ;
- ◆ la bande des **extrêmement hautes fréquences** {Extremely High Frequency, **EHF**} :
 - **WLAN (60 GHz)**,
 - guidage atterrissage par radar,
 - radioastronomie.

7.3) Bandes de fréquences utilisées par les protocoles sans-fil

Les protocoles de réseaux sans-fil, personnels, locaux et étendus utilisent tous **les ondes radio dans les fréquences micro-ondes**.

7.4) Les protocoles de réseaux locaux sans fils : 802.11

Les protocoles normalisés par le comité 802.11 de L'IEEE caractérisent les protocoles de réseaux locaux sans fils. Ces protocoles sont également connus sous le nom de protocoles Wi-Fi. Les divers réseaux locaux sans fil sont résumés dans le tableau suivant.

Normes	Frequences	Modulation	Utilisation simultanée de plusieurs antennes	Débit	Publication	Compatibilité	Remarques - Avantages inconvénients
802,11	2,4 GHz	FHSS - DSSS	Non	2 Mb/s	1997		Premier protocole Wi-Fi, Obsolète
802,11a	5 GHz	OFDM	Non	54 Mb/s	Septembre 1999		+ : Rapide peu sujet aux interférences - : Fréquence élevée => plus faible portée, sensibilité aux obstacles Coût
802,11b	2,4 GHz	DSSS	Non	11 Mb/s	Septembre 1999		+ : Portée, coût - : Lent, sujet aux interférences
802,11g	2,4 GHz	DSSS - OFDM	Non	11 Mb/s - 54 Mb/s DSSS - OFDM	Juin 2003	802,11b*	+ : Porté, Rapidité - : Sujet aux interférences
802,11n	2,4 GHz, 5 GHz	OFDM	Multiple-Input Multiple-Output	De 150 à 600 Mbps	Octobre 2009	802,11a/b/g*	+ : avec Mimo plusieurs antennes peuvent être utilisées simultanément (maximun 4 antennes)
802,11ac	5 GHz	OFDM	Multiple-Input Multiple-Output	De 450 Mb/s à 1,3 Gbps	2013	802,11a/n*	+ : avec Mimo plusieurs antennes peuvent être utilisées simultanément (maximun 8 antennes)
802,11ad WiGig	2,4 GHz, 5 GHz, 60 GHz	OFDM, simple porteuse, DSSS	Beamforming	Jusqu'à 7Gb/s		802,11a/b/g/n/ac*	- : Portée à débit maximum limitée à 10 mètres

FHSS : Frequency Hopping Spread Spectrum

DSSS : Direct-Sequence Spread Spectrum

OFDM : Orthogonal Frequency-Division Multiplexing

Ce tableau met en évidence que les normes 802.11 diffèrent non seulement par la bande de fréquence autorisée mais aussi par la modulation utilisée. A instant T, une puce radio ne peut utiliser qu'un seul type de modulation et une seule bande de fréquences. En conséquence, l'utilisation simultanée des protocoles rétro-compatibles réduit les débits espérés pour la dernière norme. C'est ce que rappelle le caractère '*' dans la colonne « **Compatibilité** ». C'est pour cette raison que certains points d'accès intègrent plusieurs puces radio.

7.5) Les organismes de normalisation concernés

7.5.1) Bandes de fréquences utilisables : ITU-R, ETSI

Le secteur des Radiocommunications de l'Union Internationale des Télécommunications {ITU-R, IUT-R} définit l'usage des bandes de radiofréquences et satellites. Des organismes locaux comme l'ETSI {European Telecommunications Standards Institute} précisent quels sont les canaux localement utilisables. Des réglementations nationales peuvent encore limiter l'utilisation des communications non filaires.

7.5.2) Comité IEEE 802.11

Le comité 802.11 édicte les normes que devraient respecter les protocoles de transmission par ondes radio. Il définit les couches physiques et liaison de données, et garantit ainsi la compatibilité avec les autres normes de protocoles de réseaux. Le comité IEEE ne produit que des spécifications techniques, mais aucune norme de construction d'équipements radio.

7.5.3) Wi-Fi Alliance®

La **Wi-Fi Alliance®** est une marque déposée qui identifie une association à but non lucratif d'acteurs du secteur des télécommunications. Son objectif est la promotion des réseaux locaux sans fil. Elle garantit la compatibilité des équipements radio aux normes et donc l'interopérabilité des équipements radio de marques diverses entre eux.

En plus de la certification des équipements par rapport aux normes 802.11a/b/g/n/ac/ad, la Wi-Fi Alliance® certifie la compatibilité des équipements radio par rapport aux applications et aux protocoles de sécurité suivants :

- ◆ **WPS** {**Wi-Fi Protected Setup**} qui permet de se connecter à un réseau Wi-Fi sans devoir saisir de mot de passe ;
- ◆ les protocoles de sécurité **WPA2™** et **EAP** (voir plus loin) ;
- ◆ le protocole **Wi-Fi Passpoint** qui permet de n'utiliser qu'une seule authentification lorsque le périphérique passe d'un point d'accès à un autre, même si ces points d'accès ne sont pas gérés par les mêmes entités ;
- ◆ le protocole **Wi-Fi Direct** qui permet l'échange de fichiers entre de périphériques radio même en l'absence de point d'accès ;
- ◆ le protocole **Wi-Fi Miracast** qui permet l'affichage déporté sur un autre périphérique radio ;
- ◆ etc.

<http://www.wi-fi.org/discover-wi-fi>

7.6) Objectif des réseaux locaux sans fil

L'objectif initial des réseaux locaux sans fil est de permettre à des périphériques finaux équipés d'un composant radio de se connecter au réseau classique filaire afin d'accéder à toutes les ressources disponibles à partir de celui-ci (imprimantes, serveurs, autres ordinateurs, Internet). Le réseau local sans fil devient ainsi une extension du réseau local Ethernet 802.3. Le nom de l'association qui garantissait, initialement, la compatibilité des équipements radio des réseaux locaux sans fil se passe de commentaire : **WECA** {**Wireless Ethernet Compatibility Alliance**}. Par abus de langage les réseaux locaux sans fil étaient appelés réseaux Ethernet sans fil.

7.7) Le point d'accès

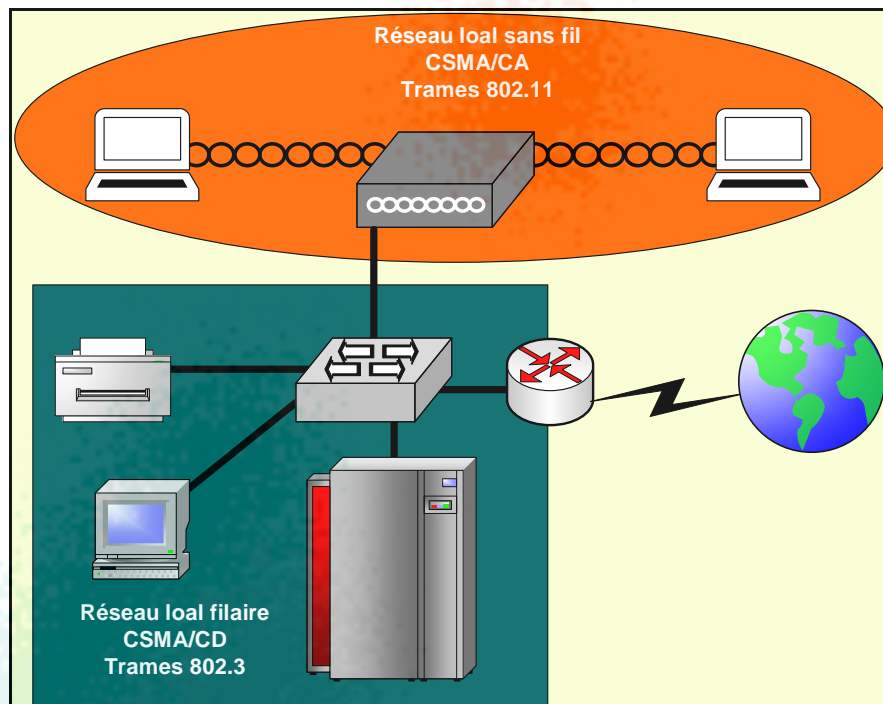
Le point d'accès constitue le périphérique intermédiaire des réseaux locaux sans fil. Un point d'accès est identifié par son **SSID** {**S**ervice **S**et **I**Dentifier}. Les équipements clients équipés du(es) composant(s) radio compatible(s) et du logiciel adéquat qui connaissent le SSID d'un point d'accès peuvent **s'associer** à ce point d'accès. En général les points d'accès diffusent continuellement leur SSID afin que tous les périphériques radio puissent les détecter. Pour des raisons de sécurité la diffusion du SSID peut être désactivée sur les points d'accès.

Si le périphérique présente les bonnes informations de sécurité (mots de passe, protocole correct d'authentification, etc.), alors le périphérique est **authentifié** par le point d'accès et la transmission de données peut commencer.

7.8) Politique d'accès au médium CSMA/CA et trames associées

La politique d'accès au médium des réseaux locaux sans fil est le **CSMA/CA** {**C**arrier **S**ense **M**ultiple **A**ccess **C**ollision **A**voidance}. Cette politique d'accès au médium se distingue du classique CSMA/CD d'Ethernet pour lequel un émetteur se contente de détecter les collisions puis de réémettre la trame, par le fait que CSMA/CA essaie **d'éviter {avoid} les collisions**. CSMA/CA s'avère donc plus complexe que CSMA/CD, et son étude n'est pas développée dans ce support. Les trames CSMA/CA traduisent cette complexité et sont différentes des trames 802.3. Les points d'accès doivent donc :

- ◆ extraire les informations des trames CSMA/CA et les insérer dans des trames CSMA/CD pour le trafic issu du réseau sans fil et à destination du réseau filaire ;
- ◆ extraire les informations des trames CSMA/CD et les insérer dans des trames CSMA/CA pour le trafic issu du réseau filaire et à destination du réseau sans fil.



7.9) Problèmes caractéristiques associés aux WLANs

7.9.1) La sécurité

Le problème principal associé aux réseaux locaux sans fil est la sécurité. En effet, tout équipement radio compatible peut lire le trafic émis et reçu par un autre équipement radio. Il faut donc **chiffrer** les données. Le premier protocole de chiffrement mis en œuvre était **WEP** {Wire Equivalent Privacy} qui comme son nom l'indique avait pour objectif de fournir un niveau de **confidentialité** {privacy} comparable à celui des réseaux locaux filaires. L'une des faiblesses de WEP provient du fait que la clé de chiffrement ne change jamais, faisant de ce protocole un protocole peu sécurisé, et facilement attaquant.

WPA™ {Wi-Fi Protected Access} qui a supplanté WEP, change régulièrement les clés de chiffrement durant les communications grâce au protocole **TKIP** {Temporal Key Integrity Protocol}. WPA existe en **version personnelle** et en **version entreprise**. Ces deux versions se différencient par la manière dont le client s'**authentifie** sur le point d'accès.

Avec **WPA™ version personnelle**, le client et le point d'accès doivent connaître la même clé secrète appelée **clé pré-partagée** {Pre-Shared Key}. Le **WPA™ entreprise** nécessite la mise en œuvre de serveur de type **AAA** {Authentication Autorisation Accounting/Auditing, authentification autorisation traçabilité}. **RADIUS** constitue un exemple de protocole AAA. Le protocole **EAP** {Extensible Authentication Protocol} permet l'authentification WPA™ entreprise.

WPA™ existe désormais en version **2**, et utilise un protocole de chiffrement plus sécurisé appelé **AES**, que celui de la version initiale à savoir **RC4**. De plus, les fonctionnalités de changement de clés assurées par **TKIP** {Temporal Key Integrity Protocol} ont été remplacées dans WPA2™ par celles, plus sûres, du protocole **CCMP** (Counter-Mode/CBC-Mac Protocol).

7.9.2) L'environnement

Les transmissions par ondes radio sont très dépendantes de l'environnement, et, il faut absolument réaliser une étude d'implantation en conditions réelles d'utilisation avant d'envisager de déployer une architecture de réseau local sans fil afin de déterminer la zone de couverture ainsi que les interférences présentes sur le site.

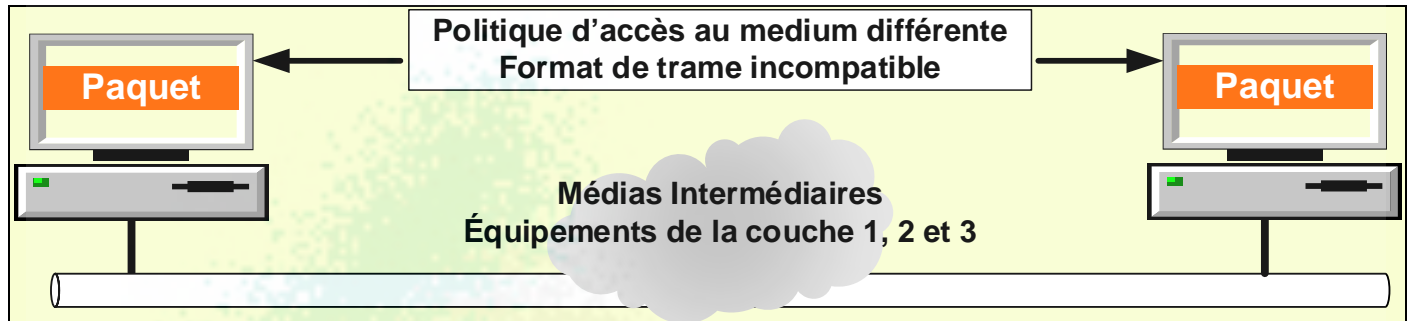
7.9.3) Semi-duplex, support partagé

Les communications sans fil partagent les mêmes fréquences et doivent donc fonctionner en mode duplex à l'alternat.

8) Modèle OSI : la couche réseau {network layer, L3}

8.1) Fonctionnalités de la couche réseau

La couche physique transmet une **suite de bits** sur un même type de média. La couche liaison transporte des **frames** de même type, entre plusieurs cartes réseau adjacentes qui reconnaissent la même politique d'accès au médium. La couche réseau permet de véhiculer des **paquets de l'hôte source à l'hôte de destination**, en **sélectionnant le meilleur chemin**, et en passant par des interfaces n'utilisant pas toutes le même type de trame.



La couche réseau permet un adressage hiérarchique. Les adresses de niveaux 3 sont composées d'au moins deux parties :

- ♦ l'identifiant de réseau qui détermine le réseau qui héberge l'hôte considéré ;
- ♦ l'identifiant d'hôte qui détermine sans ambiguïté l'hôte dans son réseau.

8.2) Attribution d'adresse réseau

Contrairement aux adresses de niveau 2 des réseaux locaux, qui sont fixées par le constructeur de la carte, les adresses de niveaux 3 sont très majoritairement définies par un administrateur.

8.2.1) Attribution manuelle

C'est la plus fastidieuse, il faut saisir les adresses sur chaque périphérique.

8.2.2) Attribution dynamique à partir d'un serveur

Un administrateur configure sur un serveur un ensemble d'adresses qui seront attribuées, pour une période donnée, aux périphériques qui en font la demande. C'est en particulier le rôle des serveurs **DHCP** {Dynamic Host Configuration Protocol} sur les réseaux IP.

Il est important de noter que l'attribution de l'adresse est une **attribution temporaire**, et qu'un équipement peut donc, changer d'adresse.

8.2.3) Auto-configuration

Si aucune adresse réseau n'est configurée manuellement, et si aucun serveur d'attribution dynamique n'est disponible, les nouvelles fonctionnalités de la couche réseau permettent aux périphériques de se générer une adresse réseau. Ces adresses sont connues sous le nom d'adresses de **locales de lien** {link local} sur les réseaux IP. Elles commencent par 169.254.

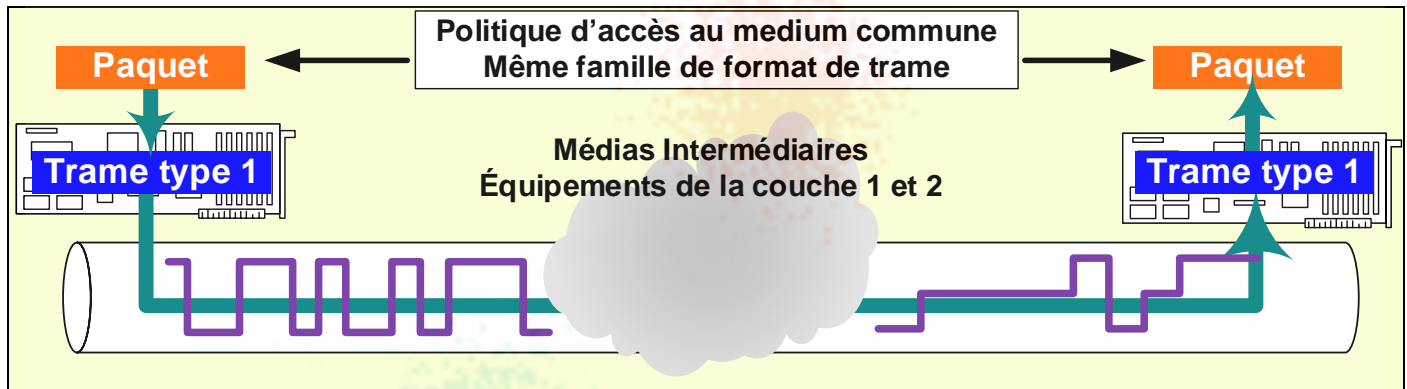
8.2.4) Adresse réseau des équipements sensibles

Les serveurs, les périphériques intermédiaires, les imprimantes réseaux constituent des équipements sensibles à qui il est fortement conseillé d'attribuer, manuellement, une adresse réseau fixe.

8.3) Transmission d'un paquet sur le même réseau

8.3.1) Principe

Si les équipements sources et destination partagent le même réseau, c'est-à-dire s'ils ne sont séparés que par des périphériques intermédiaires des couches Physiques et Liaison de données, il suffit d'insérer le paquet dans une trame qui est transmise sans modification jusqu'à la destination. Une fois la trame parvenue à destination le paquet en est extrait.



Cela semble simple, mais un problème sérieux se pose : quelle est l'adresse MAC de destination qui doit être insérée dans la trame qui encapsule et transporte le paquet jusqu'à l'équipement de niveau 2 de destination ?

8.3.2) Résolution d'adresse réseau (couche 3) en adresse liaison de données (couche 2)

Des protocoles ont été développés à cet effet, le plus connu est **ARP** {Address Resolution Protocol}. Ces protocoles font le **lien entre les couches Réseau et Liaison de données**. Ils permettent de trouver l'adresse de niveau 2 (MAC) d'une interface dont l'adresse de niveau 3 est connue. Les protocoles de résolution d'adresse de niveau 3 en adresse de niveau 2 agissent automatiquement, sans qu'aucun administrateur n'ait besoin d'intervenir.

Pour le **IPv6**, la résolution d'adresse réseau en adresse de liaison de données est réalisée par le Protocole **ICMPv6**. {Internet Control Message Protocol}.

8.4) Routeurs {router} et passerelles {gateway}

Les périphériques intermédiaires de la couche Réseau sont les **routeurs {router}**. Par abus de langage le terme **passerelle {gateway}** est aussi utilisé.

8.5) Paquet à destination d'un autre réseau appelé réseau distant

Si les équipements sources et destination ne partagent pas le même réseau, c'est-à-dire s'ils sont séparés par au moins un périphérique intermédiaire de la couche Réseau, la transmission doit se faire en plusieurs étapes et nécessite quelques prérequis.

8.5.1) Configuration des équipements

Bien évidemment les équipements source et destination doivent posséder une adresse de niveau 3, c'est-à-dire une adresse réseau.

De plus pour pouvoir communiquer avec les réseaux distants, tout périphérique doit connaître l'adresse réseau de **l'interface située sur le même réseau d'un routeur** connecté par ses autres interfaces à des réseaux distants.

Un routeur possède **autant d'adresses réseau** qu'il n'a **d'interfaces réseau opérationnelles**. Les identifiants de réseau de chacune des interfaces d'un routeur sont différents car un réseau ne peut être connecté à plusieurs interfaces d'un même routeur. C'est pour cette raison que les routeurs sont qualifiés de multi-domiciliés.

Chaque routeur doit connaître le **meilleur chemin afin d'atteindre tous les réseaux**. Ces chemins sont stockés dans la **table de routage**, et sont générés par le routeur à partir :

- ◆ des réseaux directement connectés ;
- ◆ des routes renseignées manuellement par un administrateur (routes statiques) ;
- ◆ des routes transmises par les autres routeurs grâce à des protocoles de routage dynamiques tels que RIP, OSPF et EIGRP.

Une **route/chemin vers un réseau** consiste en un **couple d'informations** composé de :

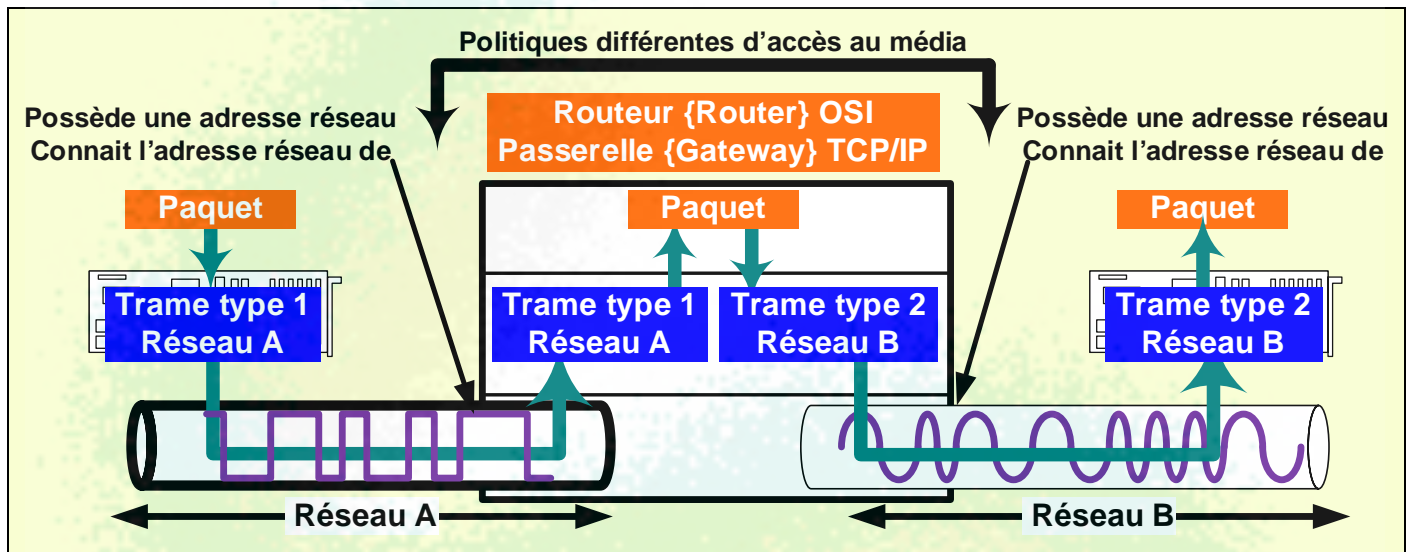
- ◆ l'identifiant du réseau à atteindre ;
- ◆ de l'adresse réseau de **l'interface la plus proche** du prochain routeur menant à ce réseau.

8.5.2) Étapes de la transmission d'un paquet vers un réseau distant

Sur le périphérique source, le paquet est encapsulé dans une trame qui est transmise à l'interface locale du routeur.

Une fois arrivée sur le routeur, le paquet est extrait de la trame.

Le routeur consulte sa table de routage, si un chemin présent dans la table de routage correspond à la destination à atteindre, le paquet est encapsulé dans une nouvelle trame à destination du prochain routeur. Si aucun chemin de la table de routage ne correspond au réseau de destination, le paquet est abandonné.



Il est important de noter qu'à chaque passage de routeur, les adresses de niveau 2 de la trame entrante sont perdues.

8.6) Encapsulation et PDU de la couche Réseau

Les principales **informations d'encapsulation** insérées par la **couche réseau** sont :

- ◆ l'adresse de niveau 3 de l'hôte de destination ;
- ◆ l'adresse de niveau 3 de l'hôte source ;
- ◆ l'identifiant du protocole de niveau 3 ou 4 encapsulé.

L'encapsulation d'un protocole dans un protocole de même niveau ou de niveau supérieur est appelé **tunelling**. Ce mécanisme est souvent employé lors de la mise en place de **réseaux privés virtuels** {RPV, Virtual Private Network, VPN}.

La PDU de niveau 3 est appelée **paquet** {packet}. Il existe bien évidemment plusieurs types de paquets, associés à des formats différents d'adresses de niveaux trois. Les plus connus sont les paquets **IP** {Internet Protocol}, et les paquets **IPX** {Internetwork Packet eXchange}.

9) La couche transport {niveau 4}

9.1) Fonctionnalités de la couche transport

La couche transport assure la **fiabilité (intégrité)** des informations transportées de **bout en bout** du réseau. C'est cette couche qui assure la qualité de service de la communication. Elle gère le mécanisme des accusés de réception, si l'expéditeur le désire. Il existe au-dessus d'**IP** deux protocoles principaux de niveau 4 :

- ♦ **TCP** {Transmission Control Protocol}. TCP assure une **liaison fiable** en mode connecté. Il établit une connexion entre les deux systèmes informatiques au début du dialogue. Il gère les accusés de réception, les reprises après erreur, la congestion de la connexion. A la fin du dialogue, TCP rompt la connexion.
- ♦ **UDP** {User Datagram Protocol}. UDP n'est pas orienté connexion, et n'accuse pas réception des données. C'est donc un protocole **non fiable**. Il appartient aux applications qui utilisent UDP de gérer la fiabilité. UDP possède deux avantages majeurs liés à son extrême simplicité : sa rapidité et le peu de surcharge relatif à son encapsulation.

Le niveau 4 constitue la **plus haute des couches de flux de données**. Il doit donc être à même de distinguer les processus sources et destination afin de restituer les flux de données au bon composant applicatif. La couche transport **identifie les composants applicatifs** grâce à leur **numéro de port**. Ceci permet au niveau 4 de multiplexer des données d'applicatifs différents dans une même connexion.

9.2) Encapsulation et PDU de la couche transport

Les principales informations rajoutées par l'**encapsulation de niveau 4** sont les **numéros de port source et destination**.

Au sens **OSI**, ce sont les **messages** qui sont véhiculés par la couche 4. Par abus de langage et analogie avec le modèle TCP/IP, le terme **segment** est également utilisé.

10) La couche session {niveau 5}

Elle est responsable de la mise en place et du contrôle du dialogue entre tâches distantes. Cette couche a pour objet d'activer, de synchroniser et de coordonner les tâches distantes. Par exemple, dans le cas de bases de données dupliquées en plusieurs points d'un réseau, il est important que des utilisateurs qui veulent faire des mises à jour sur le même enregistrement le fassent dans le même ordre sur l'ensemble des bases de données.

Au sens OSI, ce sont les **transactions** qui sont véhiculées par le niveau cinq. Par analogie au modèle en couches TCP/IP, le terme **donnée** est également utilisé.

11) La couche présentation {niveau 6}

Elle est responsable de la présentation des données échangées par les applications. C'est elle qui gère la compression, le chiffrement, et le transcodage des données (traduction du codage **ASCII** en **EBCDIC** par exemple).

La PDU de niveau 6 est la **donnée {data}**.

12) La couche application {niveau 7}

Elle remplit les fonctions nécessaires à l'exécution des applications réparties et des programmes qui y participent. Cette couche application assure également les fonctions de gestion de réseau qui peuvent être considérées comme des applications particulières. A ce niveau, les données sont traitées par des **applications** ou des **services**. Les applications bien connues comme FTP, Telnet occupent les trois derniers niveaux du modèle OSI. Ces applications sont identifiées par leur numéro de port. Les numéros de ports sont utilisés pour différencier les flux de données véhiculées dans une même connexion entre deux équipements.

La PDU de niveau 7 est la **donnée {data}**.

13) Le modèle TCP/IP

13.1) Objectif du modèle TCP/IP

Le modèle ISO ne constitue pas le seul modèle en couches. Le modèle TCP/IP, développé initialement par le ministère de la défense états-unien {**DoD**, **D**epartement **o**f **D**efense}.ne possède que quatre niveaux. Il décrit la famille des protocoles TCP/IP, dont l'objectif initial était, et reste, d'interconnecter, via un **réseau public commun**, des réseaux appartenant à des organisations différentes. Ces organisations pouvant être des administrations, des organismes de formation, des entreprises, des associations, etc. Un écosystème s'est donc développé afin de fournir :

- ◆ la spécification des protocoles et des applications. Ce rôle est tenu par l'**IETF** {**I**nternet **E**ngineering **T**ask **F**orce} par la publication de **RFCs** {**R**equest **F**or **C**omment}
- ◆ les identifiants publics attribués à chaque structure désirant joindre ses réseaux au réseau public commun. Ce rôle est dévolu à la Société pour l'attribution des noms de domaine et des numéros sur Internet {-,**ICANN**, **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers}. Par exemple, c'est l'ICANN qui gère la gestion des noms de domaine, tandis que c'est une de ses structures l'**IANA** {**I**nternet **A**ssigned **N**umbers **A**uthority} qui s'occupe de la gestion des adresses IP publiques.

13.2) Description du modèle TCP/IP

Ce modèle ne dispose que de quatre couches :

- ◆ la couche **Accès réseau** {**network access**}. Elle remplit les fonctions des deux premières couches, **Physique** et **Liaison de données** du modèle OSI :
- ◆ la couche **Internet**. Elle correspond exactement à la couche 3, **Réseau**, du modèle OSI. Autrefois ce niveau s'appelait la couche Internetwork ;
- ◆ la couche **Transport**. Elle correspond exactement à la couche 4, **Transport**, du modèle OSI. Autrefois ce niveau s'appelait la couche Host to host ;
- ◆ la couche **Application**. Elle correspond aux trois couches applicatives **Session**, **Présentation** et **Application**, du modèle OSI. Autrefois ce niveau s'appelait Process.

L'illustration suivante met en évidence la correspondance des niveaux OSI et TCP/IP. Les anciennes dénominations apparaissent entre parenthèses.

OSI ISO 7498			DoD TCP/IP							
Application	{Application}		Application (Process)	F T P	S M T P	H T T P	...	D N S	T F T P	N F S
Présentation	{Présentation}									
Session	{Session}									
Transport	{Transport}		Transport (Host to host)	TCP UDP						
Réseau	{Network}		Internet (Internetwork)	ICMP IP AH ESP ARP						
Liaison de données	{Data link}	LLC	Network acces	Pilote de carte						
		MAC								
Physique	{Physical}			Matériel réseau						

13.3) Les protocoles de la couche Internet

13.3.1) IP {Internet Protocol}

IP constitue le protocole le plus connu. C'est lui qui **transporte les paquets de l'hôte source à l'hôte de destination**. La version la plus courante est la version 4. La migration vers la version 6 est en cours. Elle a commencé chez les opérateurs de télécommunication, mais IPv4 restera encore longtemps en usage dans les entreprises, les administrations, les organismes de formation, et les associations.

13.3.2) ICMP {Internet Control Message Protocol}

ICMP permet de générer et de transporter les messages de gestion du réseau. C'est grâce à lui que nous pouvons utiliser les commandes **Ping** et **Traceroute**.

13.3.3) ARP {Address resolution protocol}

ARP est un protocole qui fait le **lien entre les couches Réseau et Liaison de données**. Il permet de trouver l'adresse de niveau 2 (MAC) d'une interface dont l'adresse IP est connue. C'est grâce à lui que l'adresse de destination d'une trame qui encapsule un paquet IP est déterminée.

Avec IPv6, ARP a disparu et a été remplacé par les fonctionnalités du protocole de découverte de voisin **NDP** {Neighbor Discovery Protocol} intégré à ICMPv6.

13.3.4) Les protocoles IPsec AH {Authentication Header} et ESP {Encapsulating Security Payload}

AH {Authentication Header} et **ESP** {Encapsulating Security Payload} sont deux protocoles de la famille **IPsec**. Les protocoles IPsec permettent de sécuriser les communications.

AH permet de **s'assurer de l'identité des correspondants** en garantissant qu'une extrémité du canal de communication est bien celle qu'elle prétend être.

ESP s'occupe du **chiffrement des paquets IP** en garantissant la **confidentialité** et l'**intégrité** des données {payload} des paquets.

IPsec constitue un ajout à IPv4, mais est directement intégré à IPv6.

13.4) Les protocoles de la couche transport

Les protocoles de la couche transport ont été traités dans le modèle OSI.

13.5) Les applications

Les applications sont identifiées par leur numéro de port. Il existe trois types de ports.

13.5.1) Les ports réservés ou ports bien connus {well known port}

Les numéros de ports correspondant aux ports réservés sont compris entre **0** et **1023**. Ils identifient les applications courantes bien connues ou des services de systèmes d'exploitation. Sous Linux, les privilèges de l'utilisateur root sont nécessaires pour lancer ces services. Ils ne peuvent pas être attribués dynamiquement en tant que port source. Ils sont attribués par l'**IANA** {Internet Assigned Numbers Authority}.

Les exemples classiques de ports réservés sont :

- ◆ transfert de fichiers sur TCP : **FTP ports 21 et 20** sur **TCP** ;
- ◆ ouverture de sessions distantes non chiffrées : **Telnet port 23** sur **TCP** ;
- ◆ ouverture de sessions distantes chiffrées : **SSH port 22** sur **TCP** et **UDP** ;
- ◆ mail sortant et entrant : **SMTP port 25** sur **TCP** ;
- ◆ gestion de noms : **DNS port 53** sur **UDP** et **TCP** ;
- ◆ configuration d'hôtes : **DHCP** sur **UDP** :
 - **port 67** pour le **client**,
 - **port 68** pour le **serveur** ;
- ◆ transfert de fichiers sur UDP : **TFTP port 69** sur **UDP** ;
- ◆ Web :

- **HTTP port 80** sur **TCP**,
- **HTTPS port 443** sur **TCP** avec chiffrement **TLS/SSL** ;
- ◆ mail entrant : **POP-3 port 110** sur **TCP** ;
- ◆ partage de fichiers en environnement Microsoft :
 - **ports 137, 138** sur **UDP** et **139** sur **TCP**,
 - **port 145** sur **TCP** pour **RPC** {Remote Procedure Call},
 - **port 445** sur **TCP** pour **SMB** {Server Message Block} ;

13.5.2) Les ports inscrits {registered port}

Les numéros de ports correspondant aux ports inscrits sont compris entre **1024** et **49151**. Ils sont attribués par l'**IANA**, et correspondent à des applications moins universelles que les ports bien connus. Ils sont aussi connus sous le nom de ports utilisateurs. En effet, sous Linux, les privilèges de l'utilisateur root ne sont pas nécessaires pour lancer ces services

13.5.3) Les ports privés ou dynamiques {private or dynamic port}

Les numéros de ports correspondant aux ports privés sont compris entre **49152** et **65535**.

13.5.4) Port source dynamique

Quand un client émet une requête vers un serveur, le client initialise le port de destination avec le port identifiant l'application désirée. Par contre le port source est configuré avec une valeur dynamique correspondant à un port disponible du poste client. Ceci permet, par exemple à deux navigateurs différents d'un même équipement, d'interroger, sans que leurs données ne se "mélangent", le même serveur Web.

14) Adressage IP

Une adresse IPv4 ou IPv6 est une adresse de niveau 3. Elle comporte donc une partie permettant d'identifier le réseau, et une partie permettant d'identifier l'équipement sur le réseau. De ce fait une adresse IP est toujours associée à un élément délimitant ces deux parties.

14.1) Adresses IPv4

14.1.1) Format des adresses IPv4

Les adresses IPv4 sont constituées de trente-deux bits et sont représentées sous **forme décimale pointée**, c'est à dire quatre octets exprimés en base dix et séparés par le caractère point. Un octet est constitué de huit bits.

La délimitation des parties réseau et hôte est assurée par un **masque de réseau**, lui aussi représenté sous forme décimale pointée, et dans lequel tous les bits égaux à 1 représentent une position binaire de la partie réseau.

Un octet dont tous les bits sont égaux à 0 à pour valeur décimale 0, tandis qu'un octet dont tous les bits sont égaux à 1 à pour valeur décimale 255.

L'adresse IPv4 10.1.2.3 associée au masque 255.0.0.0 représente l'hôte 1.2.3 sur le réseau 10.0.0.0.

L'adresse IPv4 10.1.2.3 associée au masque 255.255.0.0 représente l'hôte 2.3 sur le réseau 10.1.0.0.

L'adresse IPv4 10.1.2.3 associée au masque 255.255.255.0 représente l'hôte.3 sur le réseau 10.1.2.0.

De plus en plus, le masque réseau est remplacé par la notation représentant le nombre de bits utilisés pour représenter le réseau. Ainsi :

- ◆ 10.1.2.3 masque 255.0.0.0 est équivalent à 10.1.2.3 / 8
- ◆ 10.1.2.3 masque 255.255.0.0 est équivalent à 10.1.2.3 / 16
- ◆ 10.1.2.3 masque 255.255.255.0 est équivalent à 10.1.2.3 / 24

Sur un réseau donné, la partie réseau de l'adresse ainsi que le masque réseau attribués à chaque équipement doivent être identiques.

14.1.2) Adresses IPv4 publiques et adresses IPv4 privées

Les adresses commençant par **10**, et **192.168**, ainsi que les adresses dont le début est compris entre **172.16** et **172.31** sont des adresses qui ne sont jamais attribuées à des hôtes sur le réseau public Internet. Ce sont ces adresses qui **doivent être attribuées aux hôtes des réseaux privés**.

Aucun paquet avec une adresse, source ou destination, IPv4 privée ne doit circuler sur Internet. Les routeurs doivent, soit interdire l'accès vers Internet à ces paquets, ou mettre en œuvre la traduction d'adresses IPv4 afin de modifier les adresses IPv4 privées en adresses IPv4 publiques.

14.1.3) Adresse de réseau IPv4

Pour une adresse IPv4 donnée, l'adresse du réseau est obtenue en mettant tous les bits de la partie hôte à 0. L'adresse de réseau de :

- ◆ 10.1.2.3 masque 255.0.0.0 est 10.0.0.0
- ◆ 10.1.2.3 masque 255.255.0.0 est 10.1.0.0
- ◆ 10.1.2.3 masque 255.255.255.0 est 10.1.2.0

14.1.4) Adresse de broadcast dirigé IPv4 : tous les hôtes d'un réseau

L'adresse de broadcast dirigé représente tous les hôtes d'un réseau donné. Elle est obtenue en mettant tous les bits de la partie hôte à 1. L'adresse de broadcast dirigé de :

- ◆ 10.1.2.3 masque 255.0.0.0 est 10.255.255.255 (tous les hôtes du réseau 10.0.0.0)
- ◆ 10.1.2.3 masque 255.255.0.0 est 10.1.255.255 (tous les hôtes du réseau 10.1.0.0)
- ◆ 10.1.2.3 masque 255.255.255.0 est 10.1.2.255 (tous les hôtes du réseau 10.1.2.0)

Un paquet à destination d'une adresse IPv4 de broadcast dirigé, peut, sous certaines conditions passer les routeurs

14.1.5) Adresse de broadcast (limité) : tous les hôtes de ce réseau

Une adresse IPv4 dont tous les bits sont égaux à 1 constitue une adresse de broadcast, encore appelée broadcast limité car les paquets à destination de cette adresse ne "passent" pas les routeurs, et sont donc limités au réseau local. Elle représente tous les hôtes du réseau courant. Sa représentation décimale pointée est 255.255.255.255.

Un paquet à destination d'une adresse IPv4 **de broadcast (limité)** ne passe pas les routeurs. Les routeurs délimitent un interréseau en plusieurs réseaux qui constituent chacun un **domaine de broadcast**.

14.1.6) Adresse locale de lien {link local} ou adresse APIPA

Les adresses IPv4 qui commencent par **169.254** sont appelées adresses **locales de lien** ou encore adresse **APIPA** {Automatic Private IP Addressing}. Elles permettent, en l'absence de serveur DHCP, aux hôtes qui ne possèdent pas d'adresse fixe, de se générer une adresse IPv4. Si un serveur DHCP devient disponible, l'hôte doit abandonner son adresse APIPA et obtenir une configuration IPv4, adresse et masque, auprès du serveur DHCP.

Un paquet avec une adresse, source ou destination, locale de lien ne doit pas pouvoir accéder à Internet.

14.1.7) Adresse de boucle {loopback}

Les adresses IPv4 **débutant par 127** constituent des adresses de boucle. Elles représentent la **pile logicielle TCP/IP de l'ordinateur local**, et non pas l'adresse IPv4 de la carte réseau. L'adresse de boucle la plus connue est 127.0.0.1. La commande « **ping 127.0.0.1** » permet de savoir si la suite protocolaire TCP/IP est bien installée, mais pas de tester le fonctionnement de la carte réseau.

14.1.8) Adresse IPv4 du réseau en cours de configuration

Une adresse IPv4 commençant par 0 représente un équipement en cours de configuration sur le réseau local.

14.1.9) Adresses IPv4 attribuables aux hôtes

Il est interdit d'attribuer à un hôte, soit manuellement, soit par configuration de serveurs DHCP :

- ◆ une adresse de réseau ;
- ◆ une adresse de broadcast limité ou dirigé ;
- ◆ une adresse locale de lien ;
- ◆ une adresse de boucle ;
- ◆ une adresse du réseau en cours de configuration (réseau 0.0.0.0).

Les hôtes d'un réseau privé doivent se voir attribuer une adresse IPv4 privée appartenant à l'un des réseaux suivant :

- ◆ 10.0.0.0
- ◆ du réseau 172.16.0.0 au réseau 172.31.0.0
- ◆ 192.168.0.0

14.2) Épuisement de la réserve d'adresses IPv4 encore disponibles

14.2.1) Le problème

Les adresses IPv4 sont représentées par trente-deux bits. Il n'existe donc "que" 2^{32} adresses IPv4 différentes au monde à partager. Les adresses IPv4 sont attribuées depuis la fin des années 1960, et il n'en reste presque plus de libres. Afin de freiner l'épuisement de la réserve d'adresses IPv4 disponibles des mesures ont été prises.

14.2.2) Définition d'adresses IPv4 privées

Le fait d'imposer un ensemble d'adresses privées permet à de multiples organisations d'utiliser les mêmes adresses sur leurs réseaux privés, car la portée d'une adresse privée est confinée aux réseaux d'une organisation. Une adresse privée n'a aucune signification sur Internet Ceci pose quand même un problème : comment un hôte configuré avec une adresse privée peut-il accéder à Internet ?

14.2.3) La traduction d'adresse réseau IPv4 et de port

La **traduction d'adresse réseau** {-, **NAT**, **Network Address Translation**} et surtout sa version améliorée, la **traduction d'adresse et de port** {-, **PAT**, **Port Address Translation**} permettent aux hôtes configurés avec une adresse privée d'accéder à Internet.

Avec la NAT ou la PAT, l'adresse source d'un paquet est remplacée par l'adresse IP publique du routeur permettant l'accès à Internet.

La NAT ne travaille que des sur les adresses. Elle est utilisée lorsque qu'il y a autant d'adresses publiques (traduites) que d'adresses privées (à traduire).

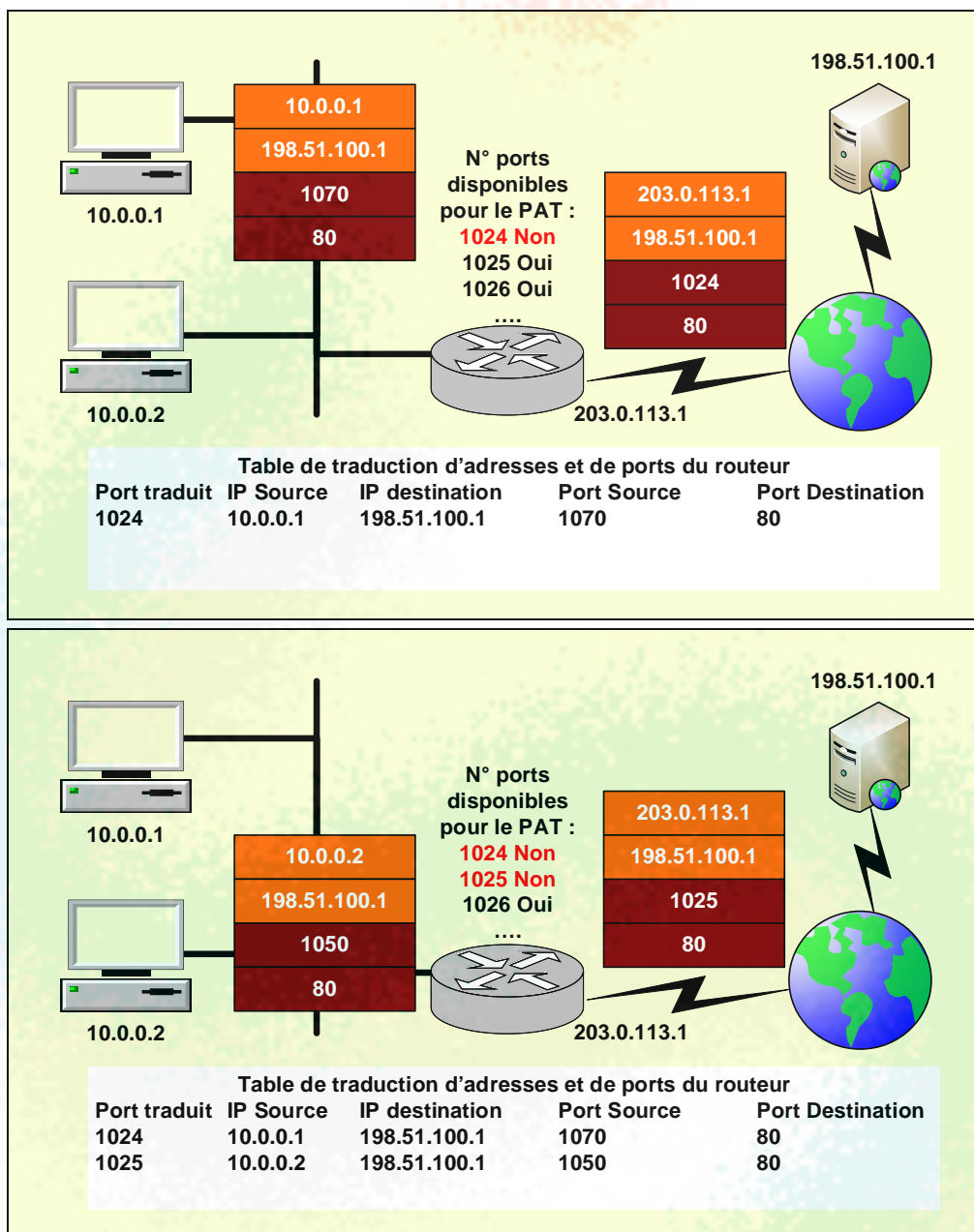
La PAT, en opérant également sur le numéro de port. Elle est utilisée lorsque qu'il y a moins d'adresses publiques (traduites) que d'adresses privées (à traduire).

Considérons les hôtes 10.0.0.1 et 10.0.0.2 qui doivent se connecter en HTTP à l'adresse 198.51.100.1 en accédant à Internet par le routeur dont l'adresse publique est 203.0.113.1.

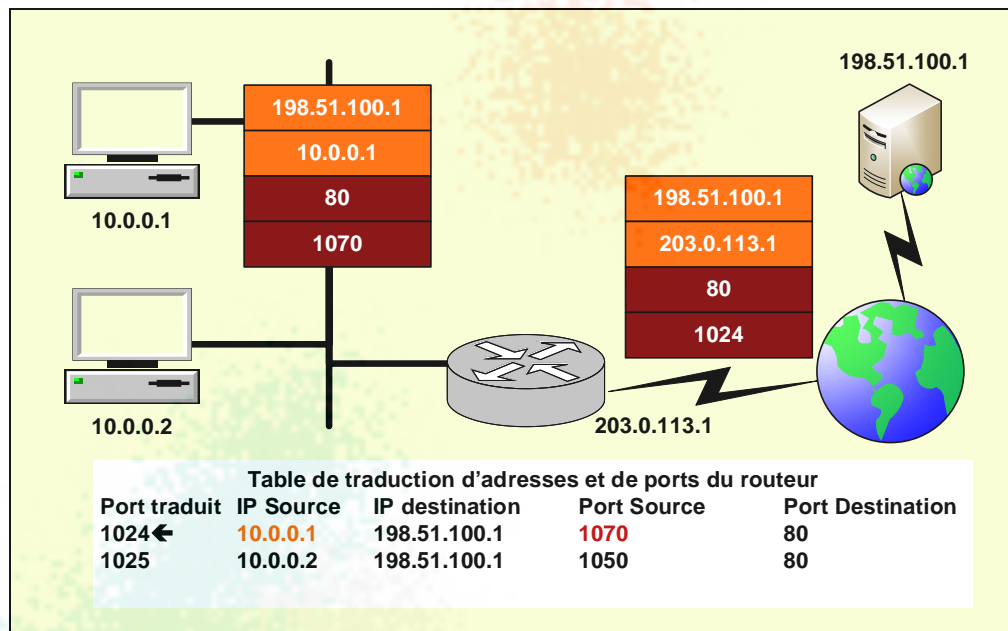
10.0.0.1 génère un paquet à destination de 198.51.100.1, port 80 à partir du port source dynamique 1070 (par exemple). Lorsque le paquet arrive au routeur, celui-ci remplace l'adresse source par son adresse publique, et le port destination par un numéro de port non encore utilisé par le PAT, ici 1024. Il insère dans sa table de suivi PAT à l'index 1024 les informations de la traduction, et indique que le port 1024 n'est plus disponible pour le PAT.

Ensuite, 10.0.0.2 génère un paquet à destination de 198.51.100.1, port 80 à partir du port source dynamique 1050 (par exemple). Lorsque le paquet arrive au routeur, celui-ci remplace l'adresse

source par son adresse publique, et le port destination par un numéro de port non encore utilisé par le PAT, ici 1025. Il insère dans sa table de suivi PAT à l'index 1025 les informations de la traduction, et indique que le port 1025 n'est plus disponible pour le PAT.



Une fois le premier paquet traité par le serveur web 198.51.100.1, celui-ci émet, en réponse un paquet à destination de 203.0.113.1 port 1024. Le routeur reçoit ce paquet, consulte sa table de suivi PAT, et constate que le port de destination correspond à un index valide. Le routeur remplace alors l'adresse et le port de destination du paquet par ceux qui correspondent dans la table PAT, ici 10.0.0.1 et 1070.



Dans cet exemple la plage de numéros de port utilisables par le PAT appartient aux ports bien connus (entre **1024** et **49151**). La RFC qui définit la traduction d'adresse n'est pas directive à ce niveau. Certaines mises en œuvre de PAT n'utilisent que les ports dynamiques (entre **49152** et **65535**).

Certains protocoles et certaines applications ne supportent pas la traduction d'adresse ou de port

14.3) IPv6

La raison majeure de l'introduction d'IPv6 est la pénurie d'adresse IPv4. IPv6 améliore la sécurité d'IPv4 en intégrant d'origine IPsec. IPv6 optimise également le traitement des paquets en limitant la fragmentation de ceux-ci.

14.3.1) Adresses IPv6

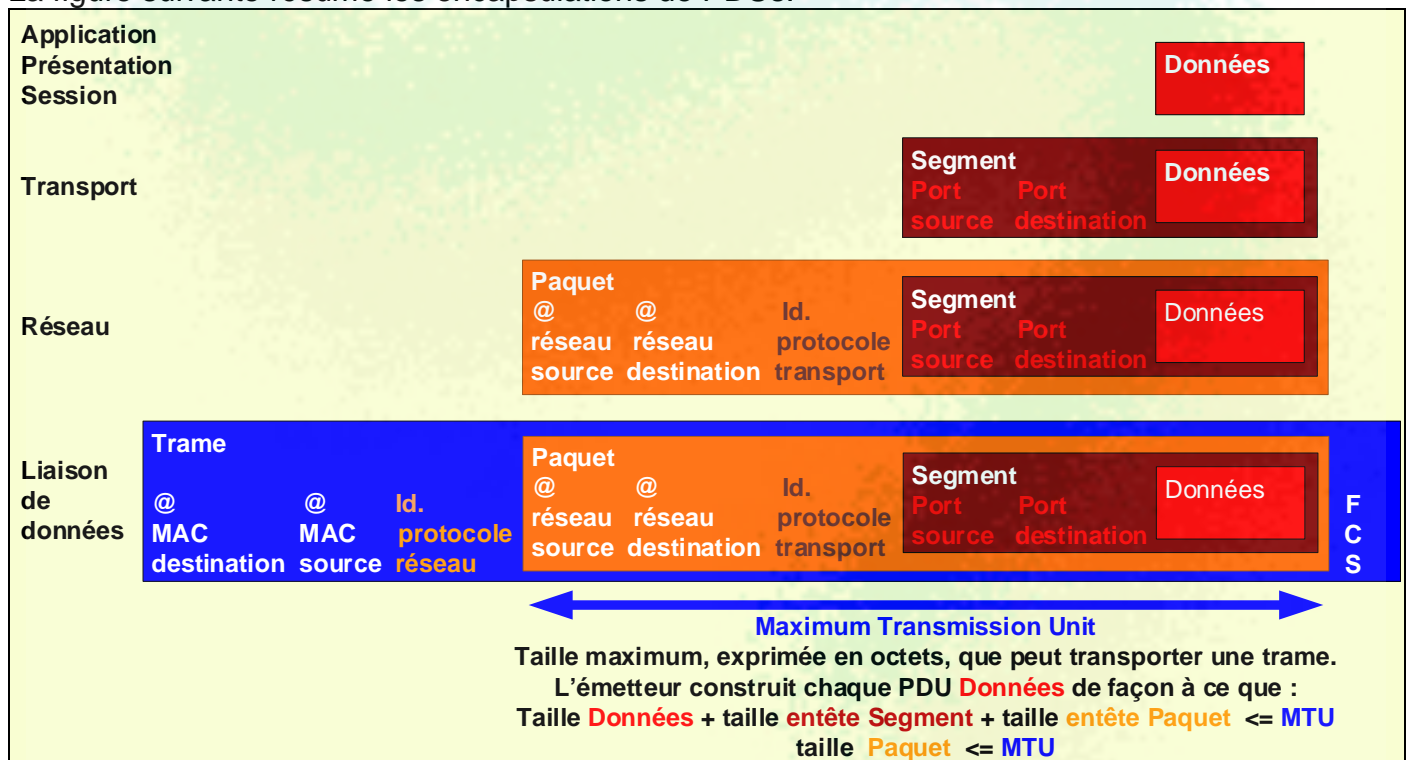
Les adresses IPv6 sont constituées de cent-vingt-huit bits, soit 2^{128} adresses différentes. Une adresse IPv6 est divisée en 2 parties délimitées par un préfixe qui indique combien de bits sont utilisés pour représenter le réseau. Une adresse IPv6 est représentée par une suite d'au maximum huit mots de seize bits séparés par le caractère ":".

15) Résumé des niveaux OSI et TCP/IP

Dans la réalité, il n'est pas rare de travailler avec un modèle qui utilise les couches basses d'OSI les couches hautes de du modèle TCP/IP.

Modèle « courant »	PDU - Unité d'information	Informations insérées par l'encapsulation	Matériel
Application	Données		
Transport {Transport}	Segment	N° de ports sources et destination	Passerelle
Réseau {Network}	Paquet	Identifiant du protocole transport encapsulé Adresses de niveau 3 source et destination	Routeur « Passerelle »
Liaison de données {Data link}	Trame	Identifiant du protocole réseau encapsulé Adresses de niveau 2 source et destination Suffixe (en-queue) de contrôle	Commutateur Pont
Physique {Physical}	Bit		Concentrateur Répéteurs

La figure suivante résume les encapsulations de PDUs.



La couche transport :

- ◆ Identifie les applications source et destination
- ◆ reçoit des données des applications ;
- ◆ restitue des données aux applications ;
- ◆ si besoin, assure le séquençement, le contrôle de flux, la gestion des acquittements, les ouvertures et clôtures de connexion.

=> L'encapsulation de la couche transport doit donc insérer les numéros de ports des applications sources et destination dans les segments. Si un protocole connecté et fiable comme TCP est utilisé, il faut en plus insérer dans les segments des informations de service relatives au séquençement, au contrôle de flux, aux accusés de réception, aux fermetures et ouvertures de session.

La couche réseau :

- ◆ permet d'aller de bout en bout de l'inter-réseau en empruntant le meilleur chemin ;
- ◆ reçoit les segments des protocoles de la couche transport ;
- ◆ restitue aux protocoles de la couche transport les segments ;
- ◆ transfère à l'hôte de destination les paquets en empruntant le meilleur chemin ;

=> L'encapsulation de la couche réseau insère donc dans le paquet l'identifiant du protocole transport encapsulé ainsi que les adresses IP source et destination.

La couche liaison de données :

- ◆ permet l'échange entre des hôtes adjacents (situés sur le même réseau) ;
- ◆ reçoit les paquets des protocoles de la couche réseau ;
- ◆ restitue les paquets aux protocoles de la couche réseau ;
- ◆ transfère les trames aux hôtes adjacents (sur le même réseau) ;

=> L'encapsulation de la couche liaison de données insère dans la trame l'identifiant du protocole de niveau 3 encapsulé ainsi que les adresses sources et destination de niveau 2.

En général l'encapsulation de niveau 2 ajoute également un suffixe permettant de s'assurer de l'intégrité des données.

La couche physique :

- ◆ insère les bits sur le média ;
- ◆ transfère les bits ;
- ◆ extrait les bits du média.

Bien que l'encodage de trame insère des bits de contrôle, il est généralement admis que la couche physique ne nettoie en œuvre aucune encapsulation.

16) Comparatif table de commutation, table ARP IPv4, table de routage

16.1) Table de commutation : pas d'intervention humaine nécessaire

Comme leur nom l'indique les tables de commutation sont gérées par les commutateurs. Elles établissent une correspondance entre l'adresse MAC source d'une trame entrante et le port par lequel cette trame est entrée dans le commutateur. Le commutateur connaît ainsi le port permettant d'atteindre l'adresse MAC source de la trame entrante. Cette information est ensuite utilisée afin de savoir sur quel port doit être transmise une trame à destination de cette adresse MAC.

Pour visualiser une table de commutation, il faut ouvrir une session d'administration sur un switch. Vous trouverez-ci-dessous une capture d'écran d'une table de commutation d'un switch Cisco.

```
ArmoireB-Position4#show mac-address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
All     0013.1a9f.bec0   STATIC    CPU
All     0100.0ccc.cccc   STATIC    CPU
All     0100.0ccc.cccd   STATIC    CPU
All     0100.0cdd.dddd   STATIC    CPU
1       0002.3f68.6502   DYNAMIC   Fa0/3
1       0021.910b.7cbe   DYNAMIC   Fa0/23
Total Mac Addresses for this criterion: 6
```

Cette capture d'écran met en évidence que :

- ◆ l'hôte équipé de la carte réseau d'adresse MAC 00-02-3F-68-65-02 est connecté au port Fast Ethernet 0/3 ;
- ◆ l'hôte équipé de la carte réseau d'adresse MAC 00-21-91-0B.7C-BE est connecté au port Fast Ethernet 0/23 ;
- ◆ certaines connexions sont référencées en tant qu'**associations statiques**. Une association statique peut être attribuée par l'administrateur, ou par le système. Les associations statiques référencent des adresses MAC réservées ou "bien connues", mais cela dépasse le cadre de ce support.

Dans les environnements Cisco, les tables de commutation sont connues sous le nom de tables d'adresses MAC « **mac-address-table** ».

Lorsqu'un switch constate qu'une adresse MAC apparaissant dans sa table de commutation n'a pas généré de trafic depuis "un certain temps", il retire cette adresse MAC de sa table de commutation. La notion de "un certain temps" dépend des fabricants. Elle est de l'ordre de cinq minutes.

Un switch travaille au niveau 2, il construit sa table de commutation et prend ses décisions de commutation à partir des informations contenues dans l'entête des trames, à savoir les adresses MAC source et destination. Il ne tient pas compte des adresses de niveau 3. L'attribution d'une adresse de niveau 3 (en général une adresse IP) à un commutateur permet l'administration du switch par le réseau. L'adresse de niveau 3 (en général une adresse IP) attribuée à un commutateur ne joue aucun rôle dans le processus de commutation.

Il existe des commutateurs de niveaux 3 possédant des fonctions de routage, mais ce sujet n'est pas couvert dans ce support. Le terme commutateur utilisé sans aucun qualificatif, indique qu'il s'agit d'un commutateur classique de niveau 2.

16.2) Table ARP : pas d'intervention humaine nécessaire

Lorsqu'un équipement a besoin de connaître l'adresse MAC correspondant à une adresse de niveau 3 distante, et que cette correspondance n'apparaît pas déjà dans sa table ARP, ARP génère une trame de diffusion {broadcast} à destination de ff-ff-ff-ff-ff-ff qui contient un message du type « **Qui possède cette adresse de niveau 3 ?** ». L'hôte du réseau local configuré avec l'adresse recherchée de niveau 3 répond par une trame de niveau 2 ayant pour adresse de destination l'adresse MAC de l'équipement demandeur (adresse source de la trame contenant la requête ARP initiale). L'équipement demandeur peut alors renseigner sa table ARP.

La table ARP permet de retrouver l'adresse **MAC, figée dans la carte réseau**, d'un hôte distant avec lequel une communication est établie et l'adresse de niveau 3 (en général une adresse **IP) attribuée** à cet équipement. La capture d'écran ci-dessus montre une table ARP dans un environnement Windows.

```
C:\>arp -a
```

Interface : 10.255.255.202 --- 0xb

Adresse Internet	Adresse physique	Type
10.0.0.208	9c-93-4e-2d-7d-75	dynamique
10.255.255.1	2c-e4-12-cb-b2-ff	dynamique
10.255.255.255	ff-ff-ff-ff-ff-ff	statique
224.0.0.22	01-00-5e-00-00-16	statique
224.0.0.252	01-00-5e-00-00-fc	statique
239.255.255.250	01-00-5e-7f-ff-fa	statique
255.255.255.255	ff-ff-ff-ff-ff-ff	statique

Cette capture d'écran met en évidence que :

- ◆ l'hôte local a pour adresse IP 10.255.255.202 ;
- ◆ l'hôte local est en communication avec les hôtes distants :
 - 10.0.0.208 dont l'adresse MAC est 9c-93-4e-2d-7d-75
 - 10.255.255.1 dont l'adresse MAC est 2c-e4-12-cb-b2-ff
- ◆ certaines connexions sont référencées en tant qu'**associations statiques**. Une association statique peut être attribuée par l'administrateur, ou par le système :
 - associations statiques attribuées manuellement par l'administrateur : elles permettent à l'administrateur de saisir directement les correspondances entre adresses de niveau 2 et adresses de niveau 3. Cela permet d'éviter les trames de diffusion {broadcast} ARP mais implique que l'administrateur connaisse très bien son parc,
 - associations statiques attribuées automatiquement par le système : elles référencent des adresses MAC "bien connues". Ce sont généralement des adresses de multicast identifiant des protocoles ou des applications. Ces adresses, permettent d'attribuer une adresse MAC ne référençant pas une carte réseau mais permettent d'adresser des trames à un hôte exécutant un protocole ou une application "normalisé". Il est à noter que la correspondance entre 10.255.255.255 (broadcast dirigé de niveau 3 du réseau local) et 255.255.255.255 (broadcast limité de niveau 3) avec l'adresse de broadcast de niveau 2 ff-ff-ff-ff-ff-ff apparaît également dans la table ARP.

En fonctionnement normal, le protocole ARP gère automatiquement, sans intervention humaine les correspondances adresses de niveau 3 / adresses de niveau 2.

Lorsque qu'ARP détecte qu'il n'y a plus de trafic avec un équipement distant figurant dans la table ARP locale, l'entrée dans la table ARP de cet équipement est effacée.

ARP n'est plus supporté par IPv6. De nouvelles fonctionnalités ont été ajoutées à ICMPv6 pour remplir ce rôle.

16.3) Table de routage : intervention d'un administrateur nécessaire

Le routage intervient au niveau 3. Le routeur compare l'adresse de destination de niveau 3 du paquet, avec les réseaux distants référencés dans sa table de routage. Ces réseaux distants apparaissent dans la table de routage parce qu'un administrateur les a renseignés, ou/et parce qu'un administrateur a configuré le routeur pour que ce routeur reçoive des informations de routage à partir d'autres routeurs.

Vous trouverez-ci-dessous une capture d'écran d'une table de routage d'un routeur Cisco.

```
Router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

172.31.0.0/24 is subnetted, 2 subnets
C 172.31.12.0 is directly connected, FastEthernet1/0
C 172.31.23.0 is directly connected, FastEthernet0/0
S 192.168.1.0/24 [1/0] via 172.31.12.1
C 192.168.2.0/24 is directly connected, FastEthernet9/0
S 192.168.3.0/24 [1/0] via 172.31.23.2
S* 0.0.0.0/0 [1/0] via 192.168.2.1
```

La partie supérieure de la table de routage "explique" les abréviations utilisées.

L'examen de la table de routage montre que ce routeur connaît les routes vers :

- ◆ 3 réseaux directement connectés dont chaque route est préfixée par « **C** » pour Connecté :
 - 172.31.12.0 réseau accessible localement par l'interface FastEthernet 1/0
 - 172.31.23.0 réseau accessible localement par l'interface FastEthernet 0/0
 - 192.168.2.0 réseau accessible localement par l'interface FastEthernet 9/0
- ◆ 3 routes saisies par un administrateur et préfixées par « **S** » pour Statique :
 - 192.168.1.0 : pour atteindre les adresses qui commencent par 192.168.1 il faut que le routeur transmette le paquet à 172.31.12.1
 - 192.168.2.0 : pour atteindre les adresses qui commencent par 192.168.2 il faut que le routeur transmette le paquet à 172.31.23.2
 - 0.0.0.0/0 qui représente toutes les destinations non référencées dans la table de routage. Pour atteindre un réseau absent de la table de routage le routeur transmet le paquet au routeur dont l'adresse est 192.168.2.1