

Synthèse Télécom et réseau 2023-2024

Tom Deneyer

Table des matières

Généralités	4
Unités de mesures	4
Rôles d'un administrateur réseau	4
Types de menaces	5
Généralité sur les réseaux de données de nos jours...	5
Utilisation	5
Fonctionnement	5
Types de réseaux selon l'étendue de ceux-ci	5
Types de réseaux selon la technologie	5
Topologies	6
Modes d'accès aux réseaux	6
Modes de connectivités client	6
Composants d'un réseau :	7
Symboles réseaux	7
Thème réseaux	7
Accès Internet	8
Réseau dédié/convergent	8
Communications simultanées	8
Généralité sur l'Architecture réseau	9
Nouvelles tendance	9
BYOD	9
Virtualisations	9
HYPERVISEUR DE TYPE 1 :	10
HYPERVISEUR DE TYPE 2 :	10
Cloud computing	10
Communication en ligne	10
CPL (courants porteurs en ligne)	10
Réseau	11
DLNA	11

Utilité routeur domestique.....	11
Cisco IOS (Internet network operating system).....	11
Routeurs Cisco	11
Accès interface CLI (interface commande)	11
Fichier de configuration.....	11
Hiérarchie de l'IOS	11
Syntaxe de commandes.....	12
Adressage IP	12
Communication et protocoles réseaux	13
Eléments de communication	13
Codage du message.....	13
Formatage et encapsulation des messages.....	13
Synchronisation	13
Méthode d'accès	13
Contrôle de flux	13
Délai d'attente de la réponse.....	13
Options de remise des messages	14
Utilité protocole réseau.....	14
Modèle de protocole TCP/IP.....	14
Couche application	15
Couche transport.....	15
Couche Internet.....	15
Couche Accès Réseau	15
Exemple Model TCP/IP	16
PDU (Protocol data unit) du model TCP/IP	16
Modèle OSI (open systems interconnection)	17
Couches Application, Présentation, Session (5-6-7)	17
Couche Transport (4)	17
Couche Réseau (3).....	17
Passerelle par défaut	17
Nomenclature.....	17
En-tête du paquet IP.....	18
Couches Liaison de données (2)	18
LLC (sous-couche supérieure).....	18
MAC (sous-couche inférieure).....	18

Protocole ARP	18
En-tête de la trame	18
Couche physique(1)	19
NIC	19
Supports réseau.....	19
Composants physique (--1).....	19
Le codage (--2)	19
Codage NRZ	19
Codage Manchester.....	19
La signalisation (--3).....	19
Modulations de la signalisation	20
Bande passante	20
Perturbations électromagnétiques.....	20
Supports en cuivre.....	21
Connecteurs RJ-45	22
Fibre optique	23
Câbles sous-marins.....	24
PDU (Protocol data Unit) du modèle OSI	24
Normes IEEE dans couches liaisons de donnée et physique	24
Li-Fi	24
Comparaison OSI – TCP/IP	25
Organisme de normalisation	26
Internet society (ISOC).....	26
Internet Architecture Board (IAB).....	26
Internet Engineering Task Force (IETF)	26
Internet Research Task Force (IRTF)	26
Hiérarchisation de ces organismes	26
Institute of Electrical and Electronics Engineers (IEE)	26
Organisation internationale de normalisation (ISO).....	27
ICANN (Internet Corporation for Assigned Names and Numbers).....	27
Adressage IP	28
IPv4	28
Division ID.....	28
Classes IP	28
Adresse privées.....	28

Types d'adresses	28
Masque de sous-réseau variable	29
Calcul IPv4	29
Problème	29
IPv6	30
Notation	30
Ecriture simplifiée	30
Types d'adresses IPv6	30
Adresses publiques	30

Généralités

Unités de mesures

Longueur	m
masse	Kg
Intensité elec	A
Température	K
Longueur d'onde	M
Angle	Radian (x $360/2\pi$)
Surface	m ²
Volume	m ³
Force	N
Pression	Pa
Couple	Nm
Tension elec	V
Puissance elec	W
Resistance elec	Ω
Energie	J
Rotation	t/m
Fréquence	Hz
Temps	s

Capacité = Volume maximum

Volume = quantité donnée

Capacité \neq Volume

Informatique :

Bit = binary digit

octet(byte) ! 2⁸ valeur de binaire maximum (256)

pixel = Picture element

Definition = hauteur x largeur (en px)

fps = frame per second

bps= bit/s

Rôles d'un administrateur réseau

- Gestion des besoins/budget/priorités de l'entreprise
➔ Adaptation du matériels en fonction.
- Gestion des ordinateurs/périphériques du réseau
➔ Installation pour utilisateurs
- Gestion des utilisateurs/droits
- Gestion des fichiers du réseau

- Gestion des service
- Gestion des problèmes et de leurs résolutions
- Gestion des sauvegardes (backups...)
 - ➔ Sauvegarde physique en interne (+ société de sauvegarde de données, externe)
- Gestion du réseau et de sa sécurité
 - ➔ physique (armoires serveurs, salles verrouillées et technologie de surveillance)

Types de menaces

- Virus/cheval de Troie
- Logiciel espion
- Attaque zero-day
- Attaque pirate
- Déni de service
- Vol/interception de données
- Usurpation d'identité

Généralité sur les réseaux de données de nos jours...

Utilisation

- Messagerie instantanée
- Communication de connaissances
- Outils collaboratifs, wikis
- Réseau sociaux, blogs, podcasts,
- Partage de fichiers en P2P
- Jeux vidéo
- E-commerce

Fonctionnement

- Téléphone fixe/mobile (télécommunication)
- Télédistribution (Câble-opérateurs)
- Internet (informatique)

Types de réseaux selon l'étendue de ceux-ci

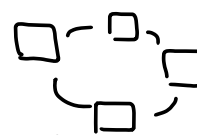
- PAN (Personal Area Network) = Réseau personnel
- LAN (Local Area Network) = Réseau local
- MAN (Metropolitan Area Network) = Réseau métropolitain
- WAN (Wide Area Network) = Réseau longue distance

Types de réseaux selon la technologie

- Par diffusion: Un seul support de transmission pour partager les données = BROADCAST (multi diffusion)



Topologie bus

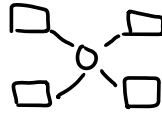


Topologie en anneau

- Point à Point : les éléments sont directement connectés entre eux par un support = UNICAST (diffusion individuelle)



Topologie point à point



Topologie en étoile



Topologie maillée

Topologies

- a) Topologie physique : Comment le réseau est formé, l'apparence, les périphériques, etc...
 - Son diagramme représente l'Emplacement des éléments, numéro de ports, etc...
- b) Topologie Logique : Comment les stations se partagent le support, en fonction du mode d'accès au réseau (voir ci-dessous, Ethernet, FDDI, etc...)
 - Son diagramme se focalise sur l'adressage ip des périphériques
 - Topologie Non Déterministe :
 - Aucun contrôle, accès basé sur le conflit → trames corumpues, nombreuses collisions,...
 - Utilisation du CSMA (Carrier Sense Multiple Access) : Detecte si un support véhicule un signal, collision etc
 - Topologie Déterministe :
 - Accès contrôlé, chaque noed utilise le support quand c'est son tour → pas de collisions, débit prévisible

Modes d'accès aux réseaux

- Ethernet : protocole d'accès CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*)
- Token ring : topologie en anneau avec un jeton d'accès. Requête envoyée uniquement quand le jeton est possédé.
- FDDI (*Fiber Distributed Data Interface*) : Ethernet utilisant fibre optique, constitué de deux anneaux servant de sécurité pour la perte de donnée.
- Comparatif Token ring / Ethernet

COMPARATIF	Token ring	Ethernet
Avantages	Pas de collision de donnée	Vitesse rapide
Inconvénients	Lenteur du débit, « dit prévisible »	Risque de collision de donnée si deux infos se lancent en même temps.

Modes de connectivités client







- Client-Serveur (98% du temps) :

- i. Client = demandeur d'une requête, machine équipé d'un logiciel pour y parvenir.
 - ii. Serveur= Hôte répondant au client (rôle dit passif, il « écoute »)
- Peer to Peer (P2P) :
 - i. Chaque « client », connecté au réseau est à la fois lui-même un serveur et un client. Ses données sont accessibles aux autres machines du serveur.
 - ii. Facile à configurer, faible coût, simple
 - iii. Peu sécurisé, pas de données centralisées, non évolutif, lent

Composants d'un réseau :

- Périphériques :
 - i. Finaux = Hôtes, Pc, etc... Disposants d'une interface utilisateur individuelle visible.
 - ii. Intermédiaires : Non visibles des utilisateurs, permettant le bon fonctionnement du réseau, ex : switch, etc...
- Supports de transmission (canaux qui permettent la transmission) :
 - i. Cable en cuivre
 - ii. Fibre optique
 - iii. Transmission sans fil (wireless)
- Services et processus :
 - i. Programmes exécutés sur le réseaux par les périphériques (intermédiaires et finaux)
 - ii. Fournissent les fonctionnalités aux utilisateurs

Symboles réseaux

1. Network media :
 - a. Wireless : 
 - b. Lan : 
 - c. WAN : 
2. Devices :
 - a. Switch : 
 - b. Router : 
 - c. Hub : 

Terme réseaux

- NIC (carte réseau) : Fournis la connexion au réseau à partir d'un ordinateur/périphérique hôte
- Port physique : Prise d'un périphérique
- Interface : Port spécifique pour se connecter à des réseaux individuels.
- Internet : Ensemble mondial de réseaux interconnectés
- Intranet : Réseau privé d'administration/entreprise avec accès uniquement sur place
- Extranet : Réseau privé d'administration/entreprise avec un accès sur place + certaines adresses spécifiques autorisées à la connexion.

Accès Internet

- FAI = Fournisseur d'accès internet, Ex : VOO, Proximus, Scarlet
- Via câble
- xDSL : DSL haut débit
- DSL (*Digital Subscriber Line*) : fonctionne sur ligne téléphonique comportant trois canaux :
 - i. Canal appel téléphonique
 - ii. Canal download
 - iii. Canal upload
- ADSL (*Asymmetric Digital Subscriber Line*) : DSL avec une asymétrie de débit sur les canaux
- VDSL (*Very-high-bit-rate DSL*) : Plus haut débit de donnée.
- VDSL2 : Encore plus rapide que le VDSL
- Par fibre, FTTx (x étant l'endroit ciblé par la fibre) :
 - i. FTTN = Fiber To The Neighborhood
 - ii. FTTC= " " curb (trottoir)
 - iii. FTTB= " " building
 - iv. FTTH= " " Home
- Satellite
- Cellulaire (ex: telephone portable)
- Par ligne commutée (ancêtre de l'ADSL)
- WiMax (*Worldwide Interoperability for Microwave Access*): Transmission via onde radio (maximum 70mbit/s à 50km)

Réseau dédié/convergent

a) Réseau dédié:

Infrastructure dédié par service/technologie (informatique,téléphone,diffusion)

b) Réseau convergent:

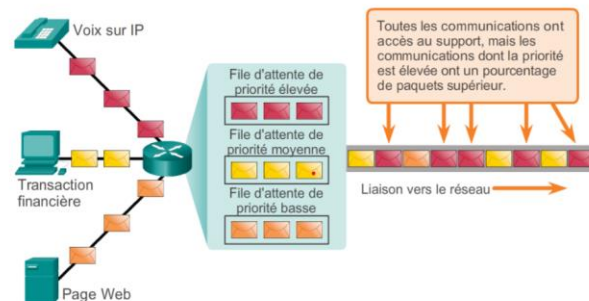
Toutes les lignes/services passent par la même infrastructure

Communications simultanées

- i. Segmentation :
Couper les paquets de donnée en petits morceaux/blocs
 - ii. Multiplexage :
Mélanger les données de différentes sources à la suite suivant leurs niveau de priorités. Entremêlage de plusieurs
« conversations »
- ➔ Niveau de fiabilité augmenter si crash d'une source et chemins de parcours optimisés.
 - ➔ Augmente la complexité de l'assemblage des données à leurs arrivages car en petits paquets.

Généralité sur l'Architecture réseau

- i. Comporte les technologies/ infrastructure/ services/ règles / protocoles...
- ii. Règle des cinq 9, fiabilité, disponibilité de 99,999% du temps. (5minutes par ans d'indisponibilité)
- iii. Tolérance aux pannes :
Limiter l'impact des pannes, utiliser de la redondance (plusieurs voix pour communiquer avec les éléments du réseaux.
- iv. Evolutivité :
Pouvoir ajouter des utilisateurs au réseau facilement, développer un réseau hiérarchisé en plusieurs couches
- v. La qualité du service (QoS) :
Service non interrompu, en continu. Utilisation de niveau de priorité sur l'utilisation du réseau.



- vi. La sécurité :
Utilisation de matériel de sécurité performant sur le réseau.

Nouvelles tendance

BYOD

Bring your own device (to work)

Virtualisations

Centraliser différents types de serveur sur un seul même plus gros serveur qui gère tous les services.

- a) Avantages :
 - Un seul serveur à acheter
 - Portabilité du serveur
 - Administration simplifiée
 - Réduction d'électricité
 - Accélération de la mise en place

b) Inconvénients :

- Coût de la machine plus importante
- Panne généralisée
- Vulnérabilité généralisée

HYPERVISEUR DE TYPE 1 :

Il est la base sur la machine, il pilote des OS qui sont installés

Ex : Microsoft Hyper-V, XEN, ...

HYPERVISEUR DE TYPE 2 :

« architecture hébergée », application installée sur un OS existant.

Ex : VirtualBox ; VmWare Workstation

EN GROS : Type 1 = OS //// type 2 = Application

Cloud computing

Utilisation des ressources d'une machine à distance, via le réseau.

Ex : cloud de stockage, privé(entreprise, gouvernement) ou hybride (personnalisé/publique)

(ex : Windows Azure, Amazon Web services, Icloud, Onedrive, etc)

Communication en ligne

Ex: teams

CPL (courants porteurs en ligne)

Faire passer le réseau via deux prises électriques connectée sur le même réseau câblé.



Réseau

DLNA

(digital living network Alliance) → alliance +250 sociétés, définit un standard d'interopérabilité des appareils (finaux ; pc, smartphone, etc)

Utilité routeur domestique

Périphériques finaux sont connectés à un routeur domestique qui fait office de :

- Routeur → transfert paquets de données vers internet + recevoir
- Switch → connecte les périphériques finaux en câblés
- Par-feu → sécurise le trafic sortant/entrant

Cisco IOS (Internet network operating system)

Routeurs Cisco

1. Sécurité réseau
2. Adressage IP
3. Config les interfaces
4. Technologie de qualité de service (QoS)
5. Routage
6. Prise en charge des technologies du réseau

Accès interface CLI (interface commande)

Via :

1. Port console (appelée ligne CTY)
2. Telnet / SSH (accès aux sessions vty, Secure Shell = SSH)
(SSH>Telnet, via adresse IPv4)
3. Port AUX

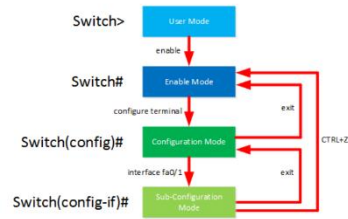
Fichier de configuration

1. Lors du démarrage, charge le « startup config » depuis la NVRAM (non volatile) et vient se charger dans la RAM
2. Si une modification est apportée, le fichier chargé dans la RAM s'appelle « Running config » et doit être sauvé dans la flash pour ne pas s'effacer au redémarrage.
3. Possible de sauver une copie à distance via FTP (sur serveur)

Hiérarchie de l'IOS

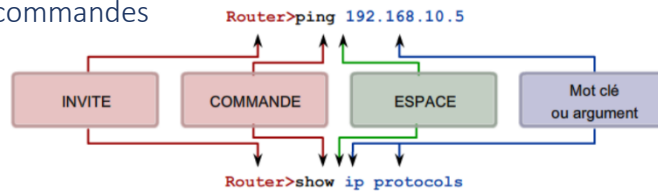
- | | |
|-------------------------------|--------------|
| 1. Mode exécution utilisateur | (restreint) |
| 2. Mode privilégié | (via enable) |

3. Mode configuration globale (via config t)
4. Mode configuration spécifique (via la spécification)
- 5.



Syntaxe de commandes

1.



2.

Convention	Description
boldface	Le texte en gras indique des commandes et des mots clés que l'utilisateur entre tels quels.
<i>italics</i>	Le texte en italique indique des arguments dans lesquels l'utilisateur fournit des valeurs.
[X]	Les crochets encadrent un élément facultatif (mot clé ou argument).
	Un trait vertical indique un choix dans un ensemble de mots clés ou d'arguments facultatifs ou obligatoires.
[X Y]	Les crochets encadrent un élément facultatif (mot clé ou argument).
{X Y}	Les accolades encadrent des mots clés ou des arguments séparés par un trait vertical indiquent un choix obligatoire.

3. Aide dans l'IOS via « ? »
4. Affectation des noms :
 - Commencent par une lettre
 - Ne contiennent pas d'espaces
 - Se terminent par une lettre ou un chiffre
 - Ne comportent que des lettres, des chiffres et des tirets
 - Comportent moins de 64 caractères

Adressage IP

- i. Attribution statique : IP manuelle (ipconfig/all)
- ii. Attribution dynamique : Ip automatique (DHCP = Dynamic Host Configuration Protocol)

Communication et protocoles réseaux

Éléments de communication

Émetteur

Récepteur

Support de transmission (canal)



Codage du message

Conversion des informations vers un format acceptable.

+Décodage qui permet de lire les informations

Données = transformées en **bits**

Formatage et encapsulation des messages

Placer les données dans une enveloppe, appelée **trame**

Destination (adresse matérielle/ physique)	Source (adresse matérielle/ physique)	Indicateur de début (indicateur de début du message)	Destinataire (identificateur de la destination)	Expéditeur (identificateur de la source)	Données encapsulées (bits)	Fin de la trame (indicateur de fin du message)
Adressage des trames		Message encapsulé				

Synchronisation

Méthode d'accès

Règles de synchronisation, savoir quand et comment les hôtes peuvent envoyer des messages, et comment réagir en cas d'erreurs, de collision etc

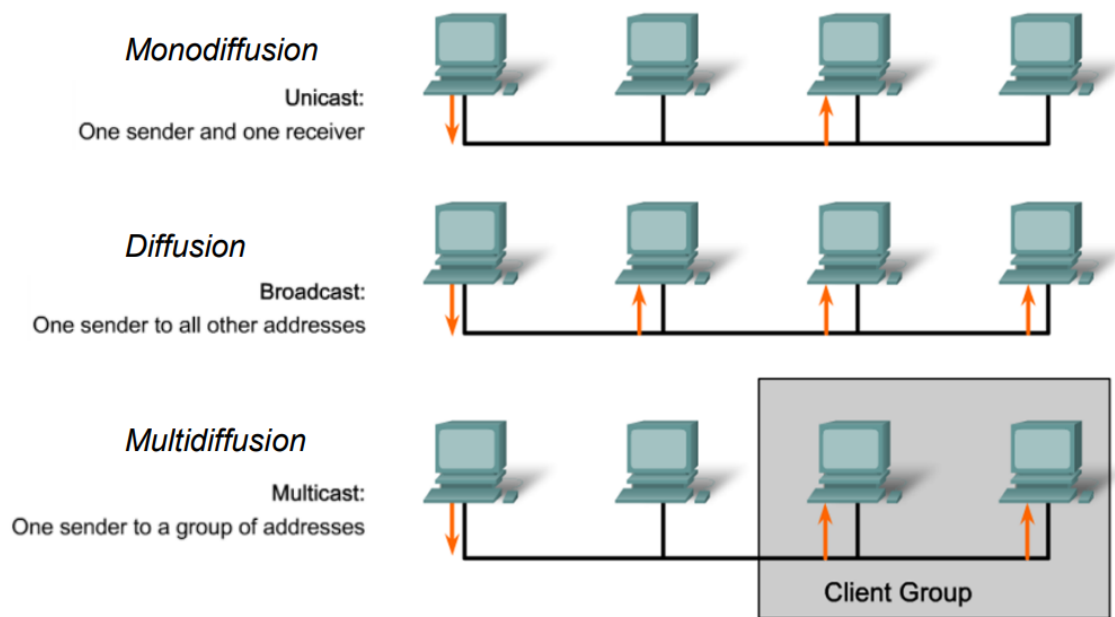
Contrôle de flux

Quantité d'information pouvant être envoyé et leur vitesse.

Délai d'attente de la réponse

Si pas de réponse rapide, supposition d'erreur d'acheminement des données

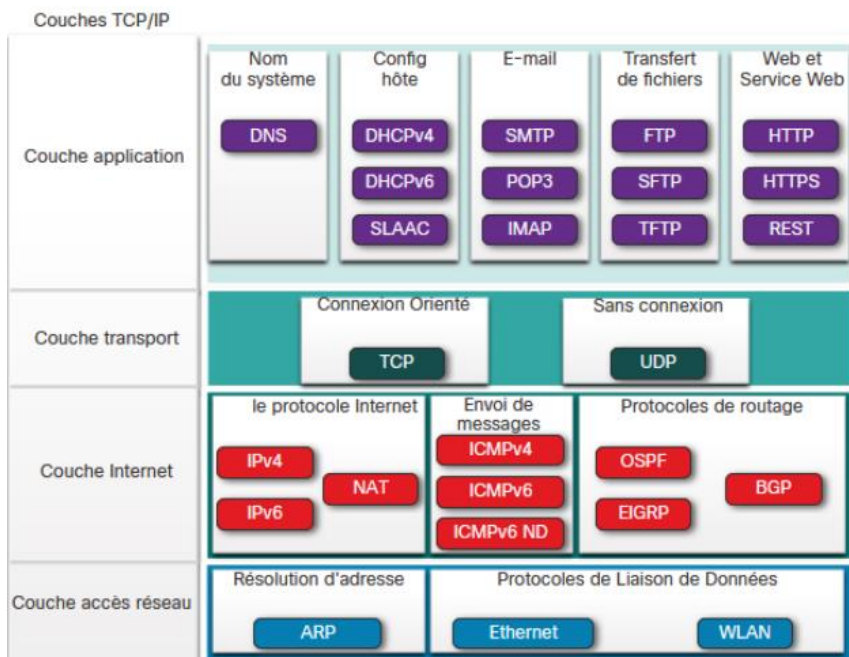
Options de remise des messages



Utilité protocole réseau

Afin que des périphériques puissent communiquer correctement, une suite de protocoles réseau doit décrire des exigences et des interactions précises. Les protocoles réseau définissent un format et un ensemble communs de règles d'échange des messages entre les périphériques.

Modèle de protocole TCP/IP



Model de protocole basé sur une norme ouverte, gratuite et utilisable par tous les constructeurs et développeurs.

Couche application

Informations depuis l'application utilisée pour sortir les données transportées, ex depuis un site internet http

- DNS (Domain Name System ou Domain Name Service) qui a pour rôle de traduire les noms de domaines. Par exemple www.cisco.com en adresse IP
- DHCP (Dynamic Host Configuration Protocol) qui attribue dynamiquement des adresses IP aux stations clientes au démarrage.
- POP (Post Office Protocol) et IMAP (Internet Message Access Protocol) qui permettent aux clients de récupérer des e-mails depuis un serveur de messagerie
- FTP (File Transfert Protocol), SFTP (Secure FTP) et TFTP (Trivial FTP) qui permettent à un utilisateur d'accéder à des fichiers sur un autre hôte du réseau.
- HTTP (HyperText Transfert Protocol) et HTTPS (HTTP Secure) qui permettent d'échanger du texte, des graphiques, des sons, des vidéos et autres fichiers multimédias sur le Web.

Couche transport

Fournit une méthode de transport des informations,

Segmentation et réorganisation via deux protocoles de transport :

- TCP (Transmission Control Protocol) Très fiable garantissant à toutes les données d'arriver
- UDP (User Datagram Protocol) Plus simple que le TCP mais moins fiable, permet l'envoi à un hôte sans connexion au préalable, mais sans confirmation de réussite de la transmission.

Couche Internet

Adressage des périphériques via protocoles IP (4 ou 6)

Encapsulation des données et routage de ceux-ci pour arriver à destination et procéder à la désencapsulation.

Protocoles de la couche internet :

- IP (Internet Protocol) qui permet de recevoir des segments de message de la couche transport. Il regroupe les messages en paquets et il indique l'adresse des paquets pour permettre leur acheminement de bout en bout sur un interréseau.
- NAT (Network Address Translation) qui permet de convertir les adresses IP d'un réseau privé en adresses IP globales et publiques. (CAR MANQUE D'ADRESSE IPv4)
- ICMP (Internet Control Message Protocol) qui permet à un hôte de destination de signaler à l'hôte source des erreurs liées aux transmissions de paquets.
- RIP (Routing Information Protocol) qui est un protocole de routage dynamique à vecteur de distance.

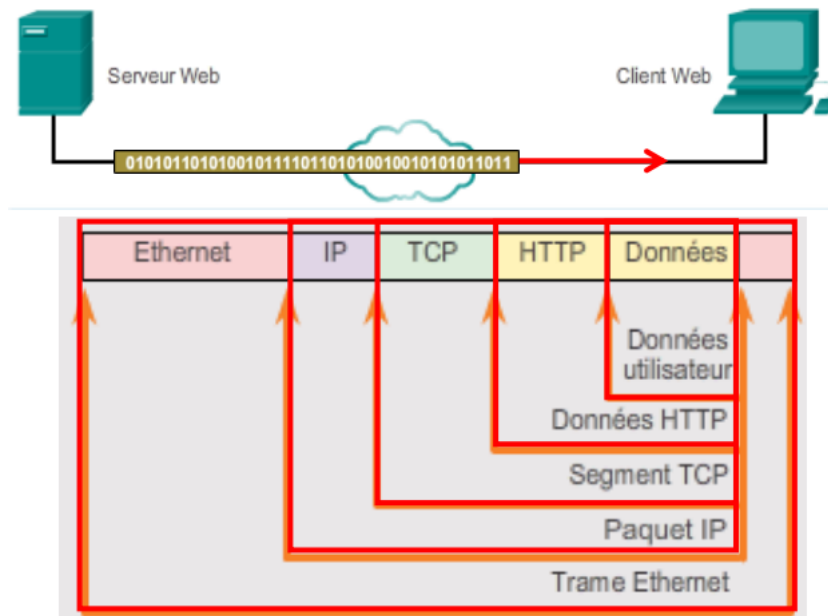
Couche Accès Réseau

- ARP (Address Resolution Protocol) Créer un lien entre l'adresse Ip et l'adresse MAC dans une table ARP

Table remplie soit dynamiquement avec l'analyse des messages passant, soit de manière statique

- Ethernet qui définit les règles de câblage et de signalisation de la couche d'accès réseau.
- WLAN (Wireless LAN) qui définit les règles de signalisation sans fil sur les fréquences radio 2,4 GHz et 5 GHz.

Exemple Model TCP/IP



PDU (Protocol data unit) du model TCP/IP

<u>PDU</u>		
Message	Application	Représente des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue.
Segment	Transport	Prend en charge la communication entre différents périphériques à travers divers réseaux.
Datagramme	Internet	Détermine le meilleur chemin à travers le réseau.
Trame	Accès réseau	Contrôle les périphériques matériels et les supports qui constituent le réseau.

Modèle OSI (open systems interconnection)

7. **application** La **couche application** contient les protocoles utilisés pour les processus communications.
6. **présentation** La **couche présentation** fournit une représentation commune des données transférées entre des services de couche application.
5. **session** La **couche session** fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.
4. **transport** La **couche transport** définit des services pour segmenter, transférer et réassembler les données de communications individuelles entre les périphériques finaux.
3. **réseau** La **couche réseau** fournit des services permettant d'échanger des parties de données sur le réseau entre des périphériques finaux identifiés.
2. **liaison de données** Les protocoles de **couche liaison de données** décrivent des méthodes d'échange de trames de données entre des périphériques sur un support commun.
1. **physique** Les protocoles de la **couche physique** décrivent l'ensemble des moyens permettant de gérer des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

Couches Application, Présentation, Session (5-6-7)

Fonctionnalités propres aux applications des utilisateurs. Ces couches sont égales à la couche Application du modèle TCP/IP, servent aux éditeurs de logiciels à faire fonctionner leurs produits sur les réseaux

Couche Transport (4)

Assure la fiabilité des données acheminées entre hôte et destination. Incluant un accusé de réception. Fonctionne via les protocoles [TCP ou UDP](#) de la suite TCP/IP

Couche Réseau (3)

Protocole IP utilisé pour l'acheminement des messages à travers le réseau.

Passerelle par défaut

Lorsqu'un hôte doit envoyer un message à un réseau distant, il doit obligatoirement passer par un routeur, également appelé « passerelle par défaut »

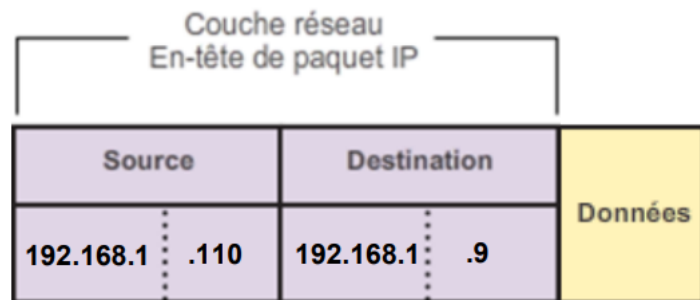
La passerelle par défaut est l'adresse IP d'une interface d'un routeur se trouvant sur le même réseau que l'hôte expéditeur.

Nomenclature

- Adresse IP source
- Adresse IP de destination

En-tête du paquet IP

- Préfixe réseau
- Préfixe hôte

*Couches Liaison de données (2)*

Couche liaison de données divisé en deux parties :

LLC (sous-couche supérieure)

Gère la communication entre les couches supérieurs/inférieurs, extrait les données et ajoute informations de contrôle.

MAC (sous-couche inférieure)

Encapsulation des données + contrôle d'accès au support.

➔ en tête de trame + données + code de fin de **trame**

Adresse MAC :

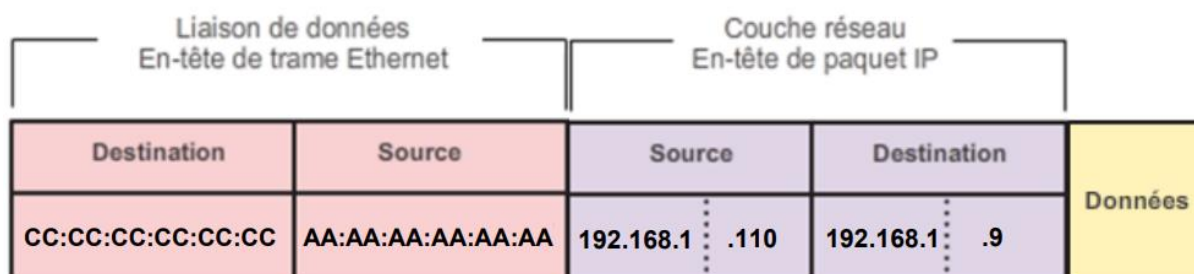
- 48bits, 12chiffres hexadécimaux
- Exemple d'adresse MAC Ethernet : AA :B1 :34 :2F :18 :0E (soit « : » soit «-»)
- Toutes les adresses MAC sont uniques (norme IEEE)

Protocole ARP

Faire le lien entre adresse IPv4 et adresse MAC

Charge table ARP (liste adresses) dans la RAM

Il complète la table ARP dynamiquement en analysant les flux avec le temps (ou de façon statique)

En-tête de la trame

Couche physique(1)

NIC

Les NIC sont les cartes réseau, qui connectent un périphérique au réseau.
Carte Ethernet en filaire, Carte WLAN en sans-fil local.

Supports réseau

Pour un support à câble de cuivre, les signaux sont des variations d'impulsions électriques.



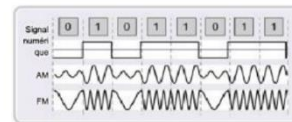
➤ Fibre optique

Pour la fibre optique, les signaux sont des variations lumineuses.



➤ Sans fil

Pour les supports sans fil, les signaux sont des variations de transmissions radio.



➤ Câble de cuivre

Composants physique (--1)

Support électroniques, support et connecteurs qui transportent et transmettent les signaux (bits)

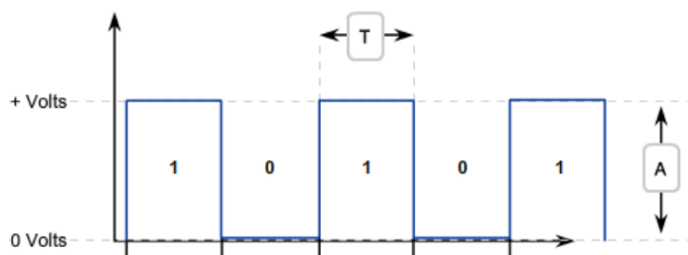
Le codage (--2)

Convertir un flux de bits de données en code prédéfini...

Codage NRZ

Non Return to Zero

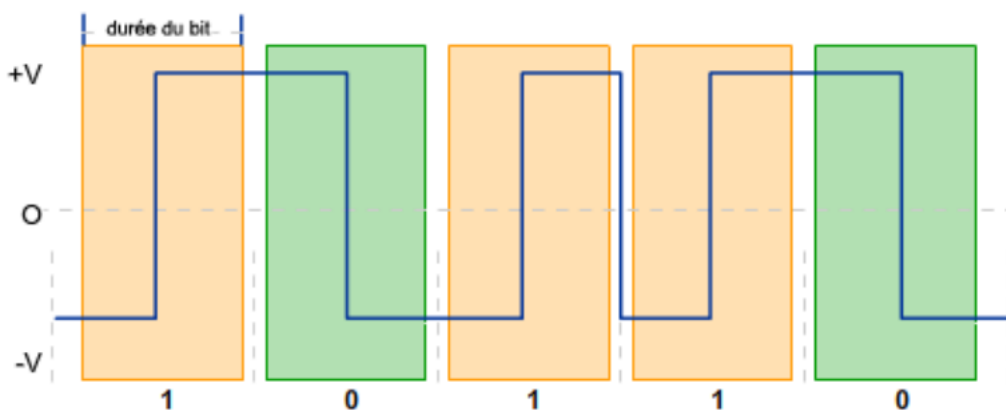
Bits sous une valeur de tension



T = durée du bit
A = Amplitude (hauteur des impulsions)

Codage Manchester

Transitions de tension, au milieu de chaque durée de bit



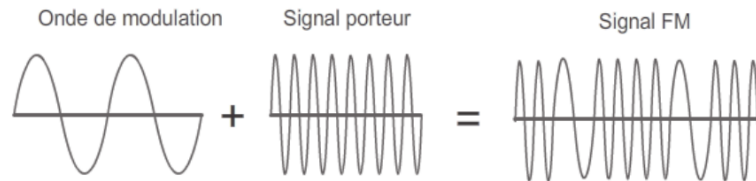
La signalisation (--3)

- Asynchrone : L'intervalle de temps entre les caractères ou les blocs de données peut être défini arbitrairement, ce qui signifie qu'il n'est pas normalisé. → les trames doivent comporter des indicateurs de début et de fin.

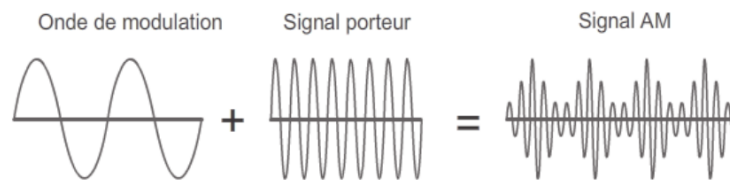
- Synchrones : les signaux de données sont envoyés synchronisés (c-à-d qu'ils se produisent à des intervalles réguliers appelés temps bits). Cette synchronisation se fait à l'aide d'un signal d'horloge échangé entre les deux périphériques qui doivent communiquer.

Modulations de la signalisation

- **Modulation de fréquence (FM)** : méthode de communication dans laquelle la fréquence porteuse varie selon le signal.



- **Modulation d'amplitude (AM)** : technique de transmission dans laquelle l'amplitude de la porteuse varie selon le signal.



Bande passante

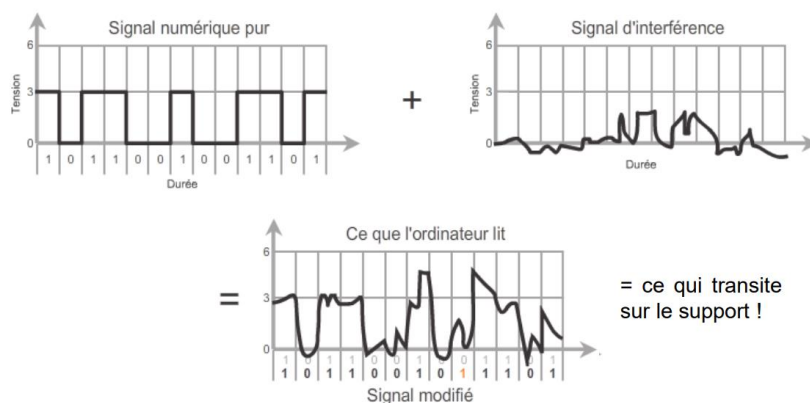
Quantité de donnée qui débite sur une période donnée, en kilobit par seconde (kbit/s) ou Mbit/s

Latence : Temps nécessaire d'un point A à un point B

Débit : Mesure de transfert de bit sur une période donnée

Débit applicatif : débit de donnée utilisable

Perturbations électromagnétiques

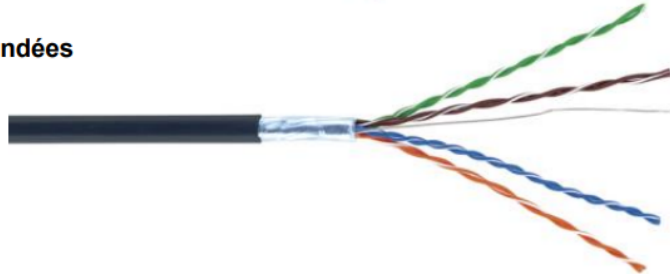


Supports en cuivre

➤ les câbles à paires torsadées non blindées



➤ les câbles à paires torsadées blindées



➤ les câbles coaxiaux



(pour câble coaxiaux,
connecteur BNC le plus
répandu)

Torsade= protection
interférences

Gaine= protection
physique

Plastique sur les fils=
protection électrique

Ces normes (établies conjointement par la TIA et l'EIA) concernant le câblage utilisé permettent de différencier ainsi plusieurs catégories de câbles :

- **Catégorie 5** : La catégorie 5 permet une bande passante de 100 MHz. Ce standard permet l'utilisation du 100BASE-TX et du 1000BASE-T, ainsi que diverses applications de téléphonie ou de réseaux (« Token Ring »).
- **Catégorie 5e** : cette catégorie de câble est une adaptation de la catégorie 5. Elle permet une vitesse allant jusqu'à 1000 Mbits/s pour une bande passante max de 100 MHz. Ce type de câblage peut être utilisé sur une distance max de 100m.
- **Catégorie 6** : ce type de câble permet une bande passante max de 250 MHz et un débit maximum de 10Gbit/s. Sa distance maximum d'utilisation est de 55m.
- **Catégorie 6a** : ce type de câble permet toujours un débit maximum de 10Gbit/s mais va permettre une bande passante plus haute (500MHz) et une distance maximum plus grande (100m).
- **Catégorie 7** : cette catégorie de câblage permet l'utilisation d'une bande passante de 600 MHz sur une distance courte (max 15m) et permet un débit allant jusqu'à 100 Gbit/s.
- **Catégorie 7a** : cette version permet l'utilisation d'une bande passante de 1GHz sur une distance max de 100m avec un débit max pouvant toujours atteindre les 100 Gbit/s.
- **Catégorie 8** : cette catégorie permet d'atteindre les 40Gbit/s sur une distance max de 30m avec une bande passante de 2GHz.

1) F/UTP (FTP) :

F= foil shield (feuille en aluminium de protection)

UTP = Unscreened twisted pairs (paires de câbles entremêlés non protégées)

2) S/UTP :

S= Braid screen (une gaine tressée de protection)

UTP...

3) SF/UTP :

SF= S + F (un tressage + une feuille de protection)

UTP...

4) S/FTP :

S= Braid Screen (Gaine tressée)

FTP = Foil Screened twisted pairs (les paires de cables sont protégées par une feuille de protection en aluminium)

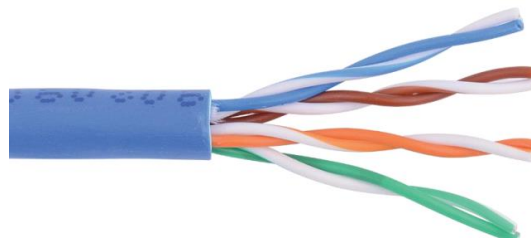
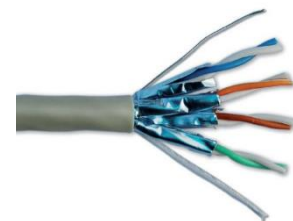
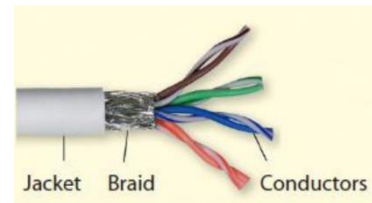
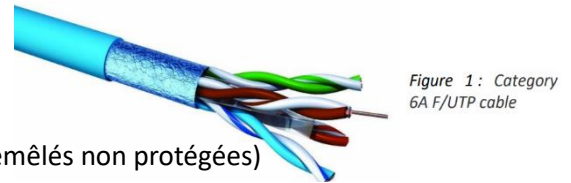
5) F/FTP :

6) U/FTP :

U= pas de feuille ni tressage de protection globale

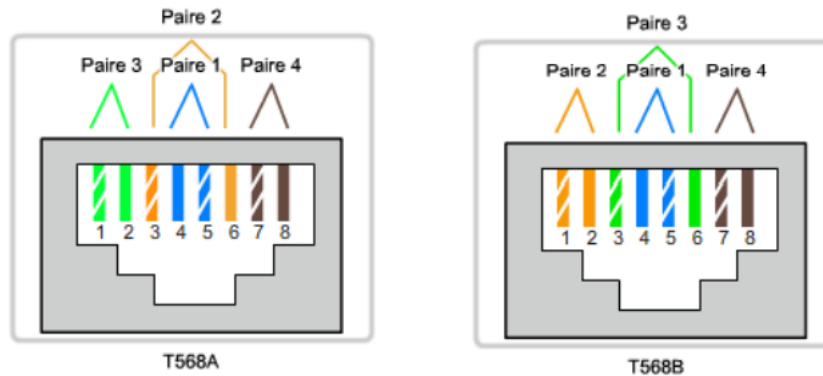
7) U/UTP :

Aucune protection du tout.



Connecteurs RJ-45

Type de câble	Standard	Application
Ethernet droit	Les deux extrémités T568A ou T568B	Connexion d'un hôte réseau à un périphérique réseau tel qu'un commutateur ou un concentrateur.
Ethernet croisé	Une extrémité T568A, l'autre T568B	Connexion de deux hôtes réseau. Connexion de deux périphériques intermédiaires réseau (un commutateur à un commutateur, ou un routeur à un routeur).
Renversement	Exclusif à Cisco	Connexion d'un port série de station de travail à un port console de routeur, à l'aide d'un adaptateur.



Fibre optique

Connecteurs :

Au niveau de la connectique, il existe beaucoup de connecteurs différents :

Un connecteur à fibre optique termine l'extrémité d'un câble à fibre optique. Un connecteur optique est constitué d'un raccord et de deux fiches.

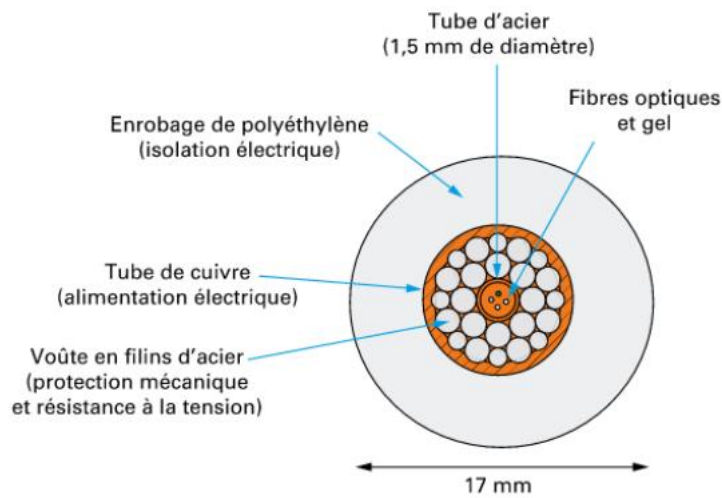
Les fiches optiques contiennent des férules (de 1,25 ou 2,5 mm) assurant le raccordement et le positionnement des deux extrémités de fibre avec précision. Ces fiches optiques sont raccordées via un raccord qui assure l'alignement.

Le montage d'un connecteur sur une extrémité de fibre optique engendre une perte du signal optique, appelée la perte d'insertion (IL).

Une petite partie du signal transmis est également réfléchi par le connecteur directement vers la source lumineuse d'émission, ce qui engendre aussi des pertes (ORL).



Câbles sous-marins



vue en coupe d'un câble LW

PDU (Protocol data Unit) du modèle OSI



Normes IEEE dans couches liaisons de donnée et physique

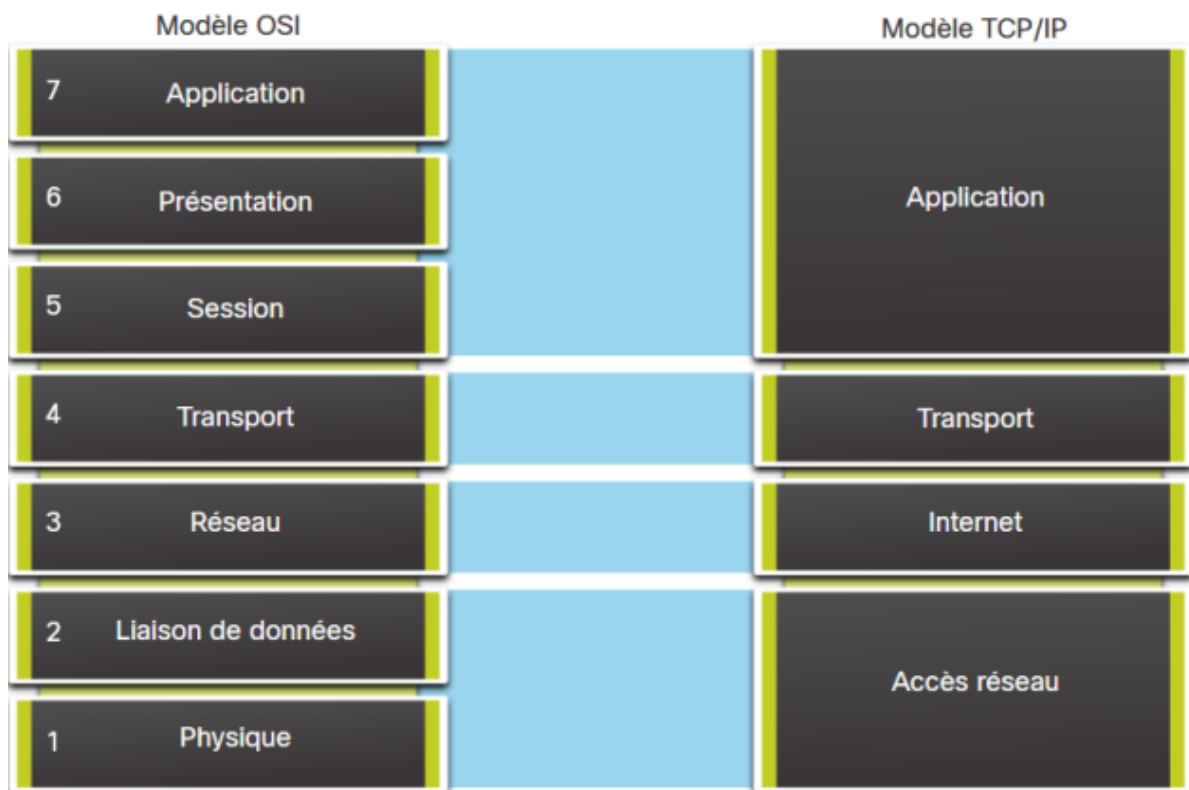
- IEEE 802.11 : Norme WLAN (Wifi)
- IEEE 802.15: Norme Bluetooth
- IEEE 802.16: Norme WiMAX (Worldwide Interoperability for Microwave Access)

Li-Fi

Transmission via le spectre optique (lumière)

Grace à une lumière Led, transfert de Bits 1/0 allumé/éteint

Comparaison OSI – TCP/IP



Organisme de normalisation

Internet society (ISOC)

chargée de promouvoir le développement, l'évolution et l'utilisation ouverts d'Internet dans le monde entier.

Internet Architecture Board (IAB)

S'occupe de la gestion et du développement généraux des normes Internet. Il assure la surveillance des protocoles et des procédures d'architecture utilisés par Internet. Les membres de l'IAB agissent en qualité de personne privée et ne représentent aucune entreprise, aucune institution ni aucune autre organisation.

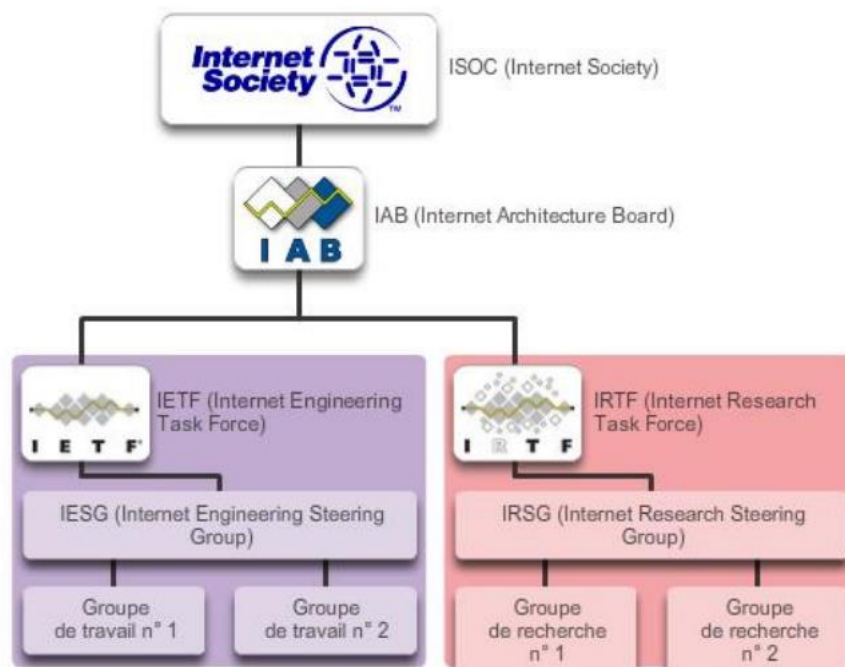
Internet Engineering Task Force (IETF)

A pour but de développer, de mettre à jour et d'assurer la maintenance d'Internet et les technologies TCP/IP. L'une des principales responsabilités de l'IETF est de produire des documents RFC (Request for Comments), c'est-à-dire des notes décrivant les protocoles, les processus et les technologies d'Internet.

Internet Research Task Force (IRTF)

Se concentre sur la recherche à long terme liée à Internet et aux protocoles TCP/IP (contrairement à l'IETF qui s'intéresse surtout aux besoins à court terme), aux applications, à l'architecture et aux technologies.

Hiérarchisation de ces organismes



Institute of Electrical and Electronics Engineers (IEEE)

L'IEEE est une association américaine professionnelle s'adressant aux spécialistes du génie électrique et de l'électronique qui souhaitent se consacrer à l'innovation technologique et à la création de normes.

Chaque norme IEEE correspond à un groupe de travail chargé de créer et d'améliorer des normes. Au niveau des groupes de travail des normes 802, on retrouve notamment :

- 802.1 qui est un groupe de travail sur les protocoles LAN de couche supérieure.
- 802.3 qui est un groupe de travail sur Ethernet. (MAC)
- 802.11 qui est un groupe de travail sur les LAN sans fil (WLAN).
- 802.15 qui est un groupe de travail sur les réseaux personnels sans fil (WPAN)

Organisation internationale de normalisation (ISO)

Il s'agit du plus grand concepteur de normes internationales pour une large gamme de produits et services. ISO n'est pas l'acronyme du nom de l'organisation.

Dans le domaine des réseaux, elle est surtout célèbre pour son modèle de référence OSI (Open Systems Interconnection)

ICANN (Internet Corporation for Assigned Names and Numbers)

Association à but non lucratif basée aux États-Unis qui coordonne l'attribution des adresses IP, la gestion des noms de domaine utilisés par le protocole DNS et les identificateurs de protocole ou numéros de ports utilisés par les protocoles TCP et UDP. L'ICANN crée des politiques et assume la responsabilité totale de ces attributions.

Adressage IP

IPv4

Division ID

IPv4 est codé sur 32bits (4 octets de 8 bits)

- Binaire : xxxx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
- Décimale : xxx.xxx.xxx.xxx (xxx = 0-255)

ID réseau (netID) = L'adresse réseau qui ne bouge pas, référence pour l'appartenance à un réseau

ID hôte (hostID) = Adresse du périphérique appartenant au réseau

Adresse IP :

ID réseau

ID machine

Classes IP

- Classe A :
netID = 8 premiers bits (/8) commençant par 0 (jusque 127)
0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
- Classe B :
NetID = 16 premiers bits (/16) commençant par 10 (de 128 à 191)
10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
- Classe C :
NetID = 24 premiers bits (/24) commençant par 110 (de 192 à 223)
110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
- Classe D :

Les 32bits sont l'ID réseau, adresse multicast (multidiffusion)

Exemple , vidéoconférence

- Classe E : Utilisation future

Adresse privées

- 10.0.0.0 à 10.255.255.255 (**10.0.0.0/8**)
- 172.16.0.0 à 172.31.255.255 (**172.16.0.0/12**)
- 192.168.0.0 à 192.168.255.255 (**192.168.0.0/16**)

Types d'adresses

- Adresse réseau (AR) : Première adresse du réseau , identité de celui-ci
- Adresse de diffusion (Broadcast) : Dernière adresse du réseau, vers tous les hôtes du réseau
- Adresse de bouclage : 127.0.0.1 (diriger le trafic vers l'hôte même)
- Adresse Link-local : APIPA (Automatic Private IP Addressing)
- Monodiffusion (Unicast) : Un hôte à un autre
- Multidiffusion (Multicast) : Envoyer à plusieurs hôtes en même réseau

Masque de sous-réseau variable

Pour mieux adapter le nombre d'adresse du hostID par rapport au nombre de périphériques utilisés.

⇒ /x (x= nombre de bits en partant de la gauche qui ne bougent pas, valant la partie netID)

Calcul IPv4

/n	Nbre hôtes
32	1
31	2
30	4
29	8
28	16
27	32
26	64
25	128

↑
 α_i

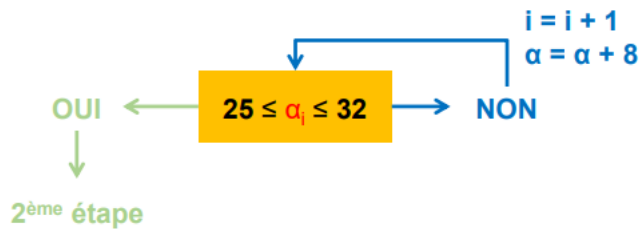
↑
 Q_i

Pour appliquer cette méthode, il suffit de connaître le tableau (ici à gauche) et puis de suivre 5 étapes :

Exemple précédent : $IP_i = 192.168.10.93 /28$

↑ ↑ ↑ ↑ ↑
 $i = 3 \quad 2 \quad 1 \quad 0 \quad \alpha_i$

1^{ère} étape : Initialisation → on démarre à $i = 0$



29

/n	Nbre hôtes
32	1
31	2
30	4
29	8
28	16
27	32
26	64
25	128

↑
 α_i

↑
 Q_i

2^{ème} étape : on regarde dans le tableau
 $Q_i = f(\alpha)$

3^{ème} étape : on trouve l'adresse réseau (AR)
 $AR = \text{PGM}(Q_i) \leq IP_i$

4^{ème} étape : on trouve l'adresse réseau suivant (ARS)
 $ARS = AR + Q_i$

5^{ème} étape : on trouve l'adresse de broadcast (BC)
 $BC = ARS - 1$

Problème

Manque d'adresse publiques pour toute la planète, donc besoin de solutions :

- NAT (toutes les adresses d'un réseau privé, sortent en une seule adresse publiques donnée) (via la correspondance entre une IP source et un numéro de port dans une table de routage NAT)
- créer un nouveau type d'adresse (IPv6) car al toile internet évolue beaucoup

IPv6

Notation

Sur 128bits, 8 groupes de 2octets écrits en hexadécimal, séparés par des « : »

Exemple : 2A01:EF35:2421:4BE0:CDBC:C04E:A7AB:ECF3

Couche de sous réseau = « longueur de préfixe » = 64bits = /64

Donc netID=64 hostID = 64

Ecriture simplifiée

- Les zéros à gauche de chaque groupes peuvent être retirés (ex : 01AB = 1AB)
- Les groupements de « 0000 » peuvent être remplacés par « :: » une seule fois dans l'adresses, comprenant le plus possible de groupements de « 0000 » à la fois pour optimiser la longueur (ex : 0000 : 0000 : 01AB : 0000 : 0001 : 5489 : AF12 : 0000 → :: 1AB : 0 : 1 : 5489 : AF12 : 0)

Types d'adresses IPv6

- Monodiffusion (toutes les adresses IPv6 sont uniques)
- Multidiffusion (envoyer vers plusieurs destinataires)
- Anycast (Adresse monodiffusion qui peut être adressé à plusieurs hôtes, paquet acheminé vers le plus proche)
- PAS D'ADRESSE DE DIFFUSION (Broadcast), mais équivalent avec une multidiffusion globalisée

Adresses publiques

Adresse de monodiffusion globale, comme avec IPv4 sauf que pas besoin de NAT car beaucoup d'adresse IPv6, attribuées soit dynamiquement soit statique

Attribué par L'ICANN, uniquement les 2000::/3 = 1/8eme de l'espace disponible

Une adresse de monodiffusion globale se compose de trois parties :

- **Préfixe de routage global** 48
- **ID de sous-réseau** 16
- **ID d'interface** 64

Le **préfixe de routage global** est le préfixe ou la partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un FAI) à un client ou à un site. Pour le moment, le préfixe global de routage attribué aux clients est /48. Ces clients incluent tous les clients potentiels, des réseaux d'entreprise aux réseaux particuliers. Cet espace d'adressage est plus que suffisant pour la plupart des clients.

L'**ID de sous-réseau** est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site.

L'**ID d'interface IPv6** est similaire à la partie hôte d'une adresse IPv4. Le terme ID d'interface est utilisé car un hôte unique peut avoir plusieurs interfaces, chacune dotée d'une ou de plusieurs adresses IPv6.