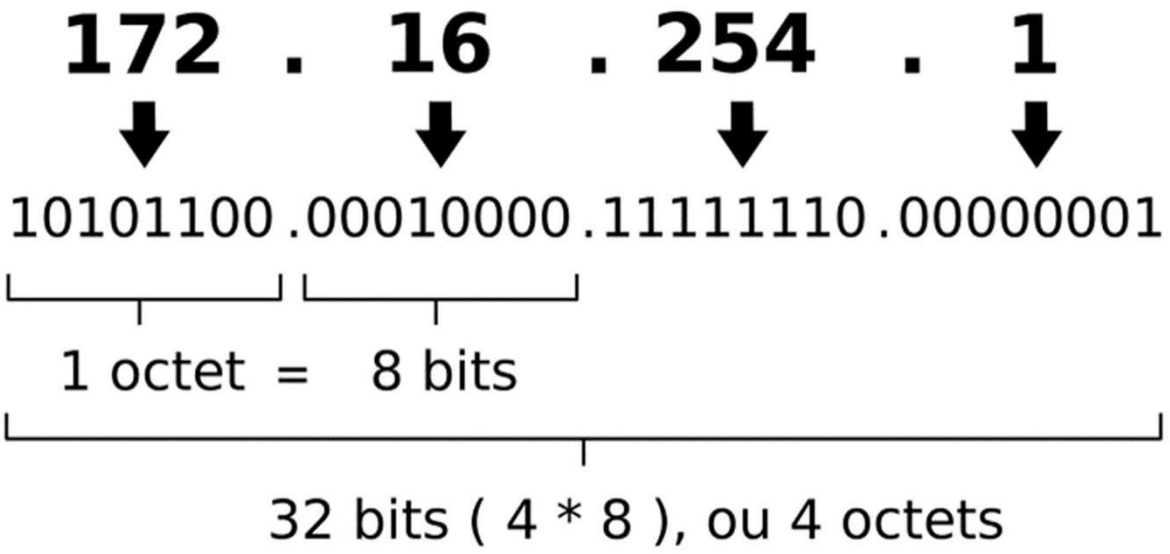
Introduction aux reseaux windows

I. Adressage IP

Une adresse IPv4 (notation décimale à point)



Adresse IP/IP Address

Une adresse IP (avec IP pour Internet Protocol) est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol.

L'adresse IP est à la base du système d'acheminement (le routage) des paquets de données sur Internet.

Il existe des adresses IP de version 4 sur 32 bits, et de version 6 sur 128 bits.

La version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points, ce qui donne par exemple « 172.16.254.1 ».

Utilisation des adresse IP

L'adresse IP est attribuée à chaque interface avec le réseau de tout matériel informatique (routeur, ordinateur, smartphone, modem ADSL ou modem câble, imprimante réseau, etc.) connecté à un réseau utilisant l'Internet Protocol comme protocole de communication entre ses nœuds.

Cette adresse est assignée soit individuellement par l'administrateur du réseau local dans le sous-réseau correspondant, soit automatiquement via le protocole DHCP.

Si l'ordinateur dispose de plusieurs interfaces, chacune dispose d'une adresse IP spécifique. Une interface peut également disposer de plusieurs adresses IP.

Chaque paquet transmis par le protocole IP contient l'adresse IP de l'émetteur ainsi que l'adresse IP du destinataire. Les routeurs IP acheminent les paquets vers la destination de proche en proche.

Certaines adresses IP sont utilisées pour la diffusion (multicast ou broadcast) et ne sont pas utilisables pour adresser des ordinateurs individuels. La technique anycast permet de faire correspondre une adresse IP à plusieurs ordinateurs répartis sur Internet.

Les adresses IPv4 sont dites publiques si elles sont enregistrées et routables sur Internet, elles sont donc uniques mondialement.

À l'inverse, les adresses privées ne sont utilisables que dans un réseau local, et ne doivent être uniques que dans ce réseau.

La traduction d'adresse réseau, réalisée notamment par les box internet, transforme des adresses privées en adresses publiques et permet d'accéder à Internet à partir d'un poste du réseau privé.

Classe d’adresse IP

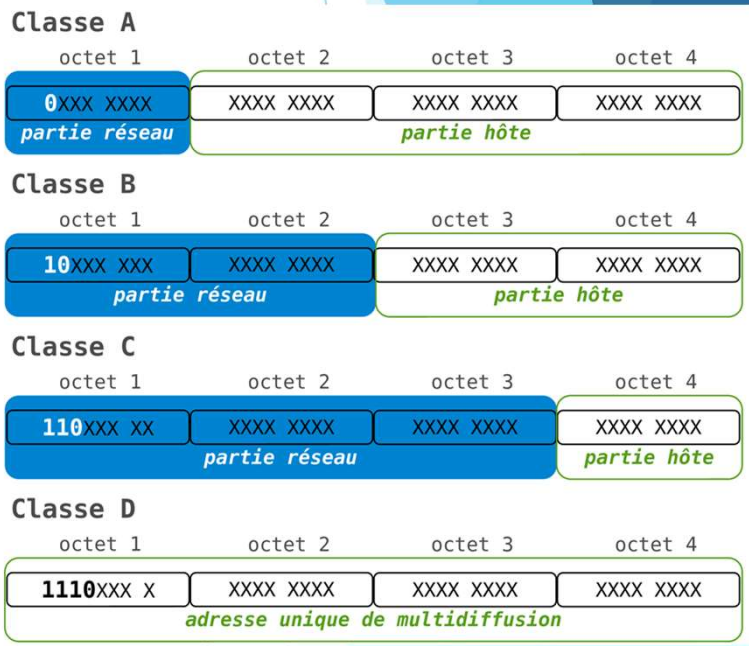
Chaque adresse IP appartient à une classe qui correspond à une plage d’adresses IP.

Au total 5 classes existent A, B, C, D et E, cela sert à adapter l’adressage selon la taille du réseau. Si l'ordinateur dispose de plusieurs interfaces, chacune dispose d'une adresse IP spécifique. Une interface peut également disposer de plusieurs adresses IP.

Les adresses IP des classes D sont des adresse multicast et E sont réservé réservées par IETF (Internet Engineering Task Force) donc non utilisable.

Voici les plages d’adresse selon les classes :

- La classe A de l’adresse IP 0.0.0.0 à 126.255.255.255
- La classe B de l’adresse IP 128.0.0.0 à 191.255.255.255
- La classe C de l’adresse IP 192.0.0.0 à 223.255.255.255
- La classe D de l’adresse IP 224.0.0.0 à 239.255.255.255 multicast
- La classe E de l’adresse IP 240.0.0.0 à 255.255.255.255 réservées par IETF



Adresse IP Private/privée

les adresse IP privées sont toutes les adresses IP qui ne sont pas utilisable sur internet, par exemple le réseau d'une entreprise ou le réseau domestique. Un réseau privé est un réseau qui utilise les plages d'adresses IP non accessibles depuis Internet.

Elles permettent de communiquer localement avec vos différents périphériques. Au total 3 classes existent A, B, et C.

Voici les plages d'adresse Privé selon les classes :

- Les adresses privées de la classe A: 10.0.0.0 à 10.255.255.255 (comprend 16 millions d'adresses)
- Les adresses privées de la classe B: 172.16.0.0 à 172.31.255.255 (comprend 65535 adresses)
- Les adresses privées de la classe C: 192.168.1.0 à 223.255.255.255 (comprend 256 adresses)

Adresse IP Public/publique

Les adresses IP publiques ne sont pas utilisées dans un réseau local mais uniquement sur internet.

Une adresse IP publique est unique dans le monde alors que pour une adresse IP privée c'est dans le réseau local qu'elle est unique.

Les adresses IP publiques représentent toutes les adresses IP des classes A, B et C qui ne font pas partie de la plage d'adresses privées de ces classes,

Il existe deux exceptions de la classe A qui sont le réseau 127.0.0.0 qui est réservé pour les tests de boucle locale et le réseau 0.0.0.0 qui est réservé pour définir une route par défaut sur un routeur.

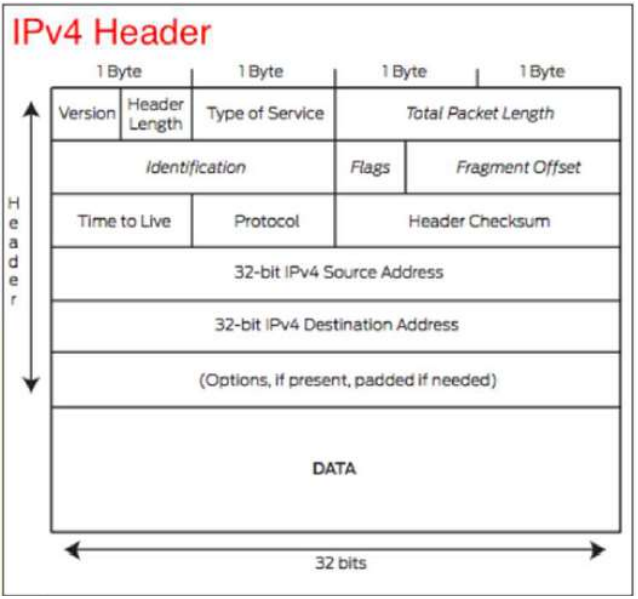
Adresse IPv4 et/ou IPv6

Même si IPv6 est destiné à remplacer un jour IPv4, ces deux protocoles sont actuellement étroitement mêlés : la plupart des ingénieurs les exécutent ensemble. La différence entre les deux version du protocol IP, ce trouvent dans le format de leurs adressages et dans leurs méthodes d'encapsulation.

Adresse IPV4

192.168.1.1

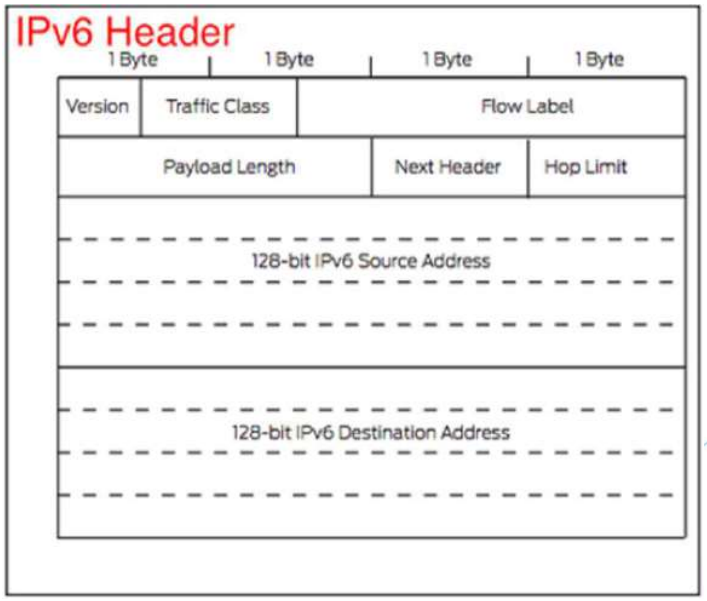
Format numérique de base à 32 caracthères



Adresse IPV6

00.08.45.ea.82.06.27

Format ASCII alphanumérique à 128 caracthères



IP Statique et Dynamique

Il existe deux types d'adresses IP : statiques et dynamiques.

Statiques : Une adresse IP statique est simplement une adresse qui ne change pas.

Une fois que votre appareil s'est vu attribuer une adresse IP statique, ce numéro reste généralement le même jusqu'à ce que l'appareil soit mis hors service ou que votre architecture réseau change.

Les adresses IP statiques sont généralement utilisées par des serveurs ou d'autres équipements importants.

Dynamique : les adresses IP dynamiques sont susceptibles de changer, parfois à tout moment.

Les adresses dynamiques sont attribuées, selon les besoins, par les serveurs **DHCP** (**Dynamic Host Configuration Protocol : protocole de configuration dynamique des hôtes**) ou par le Border Routeur (box FAI) si il n'y a pas de serveur DHCP.

Masque de sous-réseaux

Les adresses IP publiques ne sont pas utilisées dans un réseau local mais uniquement sur internet.

Un masque de sous-réseau (**désigné par subnet mask, netmask ou address mask en anglais**) est un masque distinguant les bits d'une adresse IPv4 utilisés pour identifier le sous-réseau de ceux utilisés pour identifier l'hôte.

From Wikipedia

On utilise les masques de sous-réseaux pour conditionner les communication entre adresse IP, une valeurs à 0 étant la plus permissive, une valeurs à 255 étant la plus restrictive.

Exemple:

192.168.001.001	255.255.255.000:	Toutes les adresses commençant par 192.168.1.X peuvent communiqué avec l'adresse 192.168.1.1
192.168.001.001	255.000.000.000:	Toutes les adresses commençant par 192.X.X.X peuvent communiqué avec l'adresse 192.168.1.1
192.168.001.001	255.255.255.254:	Seulement une adresse 192.168.1.254 pourras communiqué avec l'adresse 192.168.1.1

TP 1 changement de méthode d'adressage

- En invite de commande (CMD) identifiez l'adresse IP de votre carte ethernet.
- Via le centre réseaux et partage changez l'adresse IP dynamique de votre carte réseaux ethernet en adresse IP statique.
- Faite une requête ARP/ping vers l'adresse IP de votre machine hôte.

Commande de base

- Afficher les information d'adresse IP de la carte active de l'ordinateur

`ipconfig`

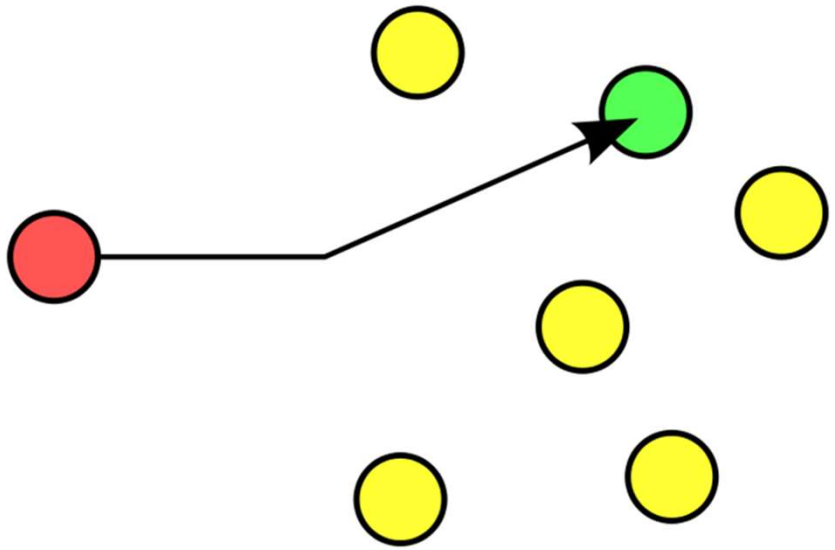
- Afficher les information d'adresse IP de toutes les carte de l'ordinateur

`Ipconfig /all`

- Vérifier si une carte réseau est bien présente sur le réseaux

`Ping ***.***.***.***` (les * corresponde à l'adresse ip de la carte réseaux recherché exemple 192.168.1.14)

II. Format de diffusion



UNICAST

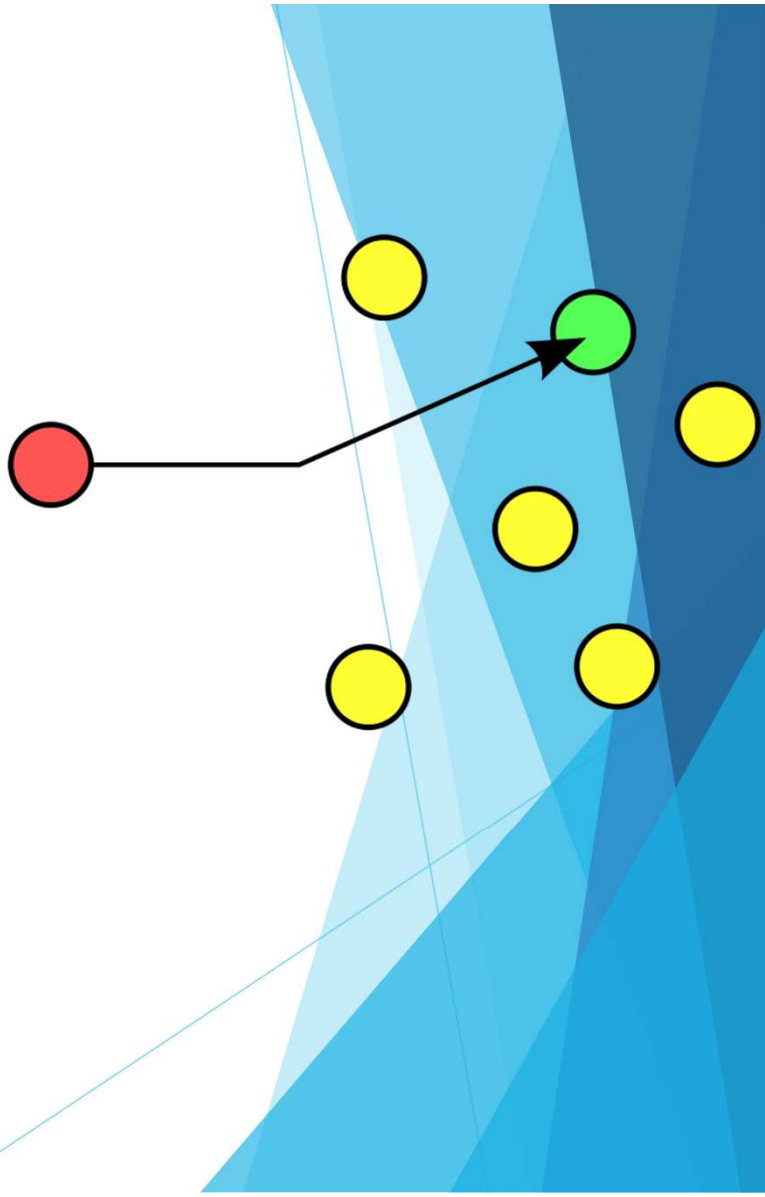
Le terme unicast définit une connexion réseau point à point, c'est-à-dire d'un hôte vers un (seul) autre hôte.

On entend par unicast le fait de communiquer entre deux ordinateurs identifiés chacun par une adresse réseau unique.

Les paquets de données sont acheminés sur le réseau suivant l'adresse du destinataire « encapsulée » dans la trame transmise.

Normalement, seul le destinataire intercepte et décode le paquet qui lui est adressé.

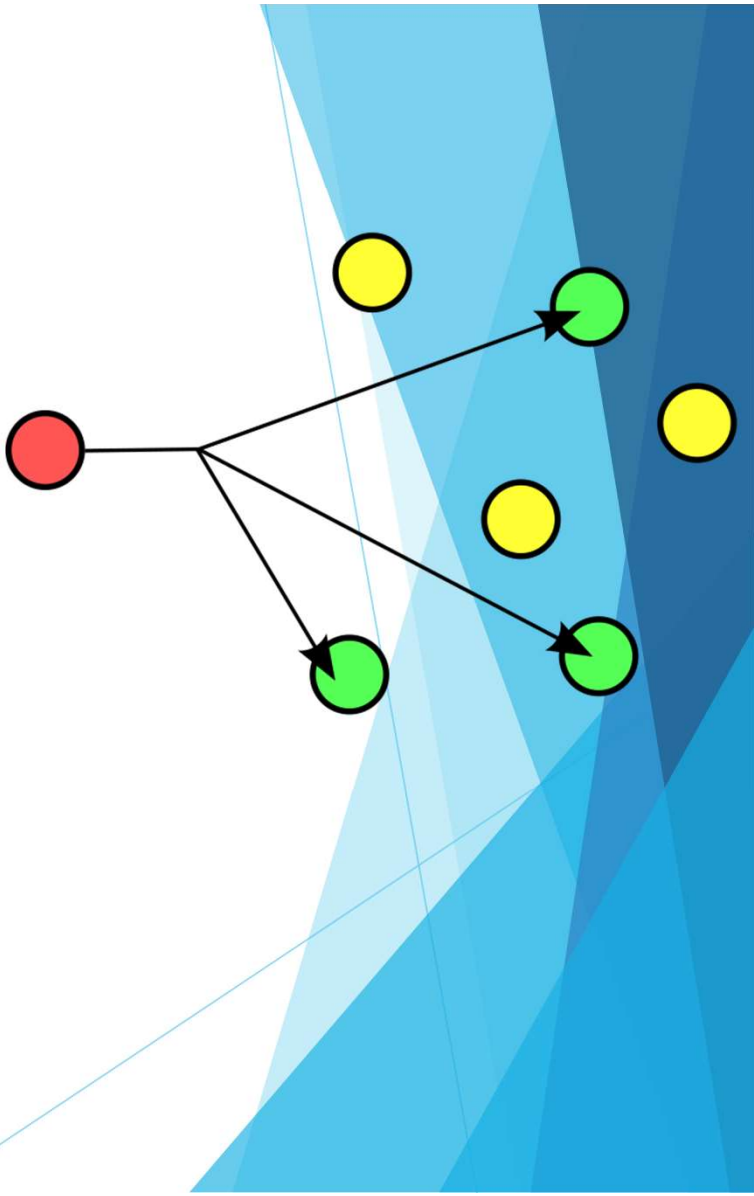
Dans le protocole IP, les adresses doivent être uniques dans la mesure où les paquets sont acheminés au niveau du LAN (Local Area Network) ou du WAN (Wide Area Network).



Multicast

Le multicast (multidiffusion) est une forme de diffusion d'un émetteur (source unique) vers un groupe de récepteurs. Les termes « diffusion multipoint » ou « diffusion de groupe » sont également employés.

Les récepteurs intéressés par les messages adressés à ce groupe doivent s'inscrire à ce groupe. Ces abonnements permettent aux switchs et routeurs intermédiaires d'établir une route depuis le ou les émetteurs de ce groupe vers les récepteurs de ce groupe.



Avantages

Ce système est plus efficace que l'unicast pour diffuser des contenus simultanément vers une large audience. En streaming unicast, on enverrait l'information autant de fois qu'il y a de connexions, d'où gaspillage de temps, de ressources du serveur et surtout de bande passante. Au contraire, en multicast, chaque paquet n'est émis qu'une seule fois et sera routé vers toutes les machines du groupe de diffusion sans que le contenu ne soit dupliqué sur une quelconque ligne physique ; c'est donc le réseau qui se charge de reproduire les données.

Le multicast permet de développer des applications interactives de groupe, comme la visioconférence, le partage de tableau, etc.

Inconvénients

Le multicast ne permet cependant en aucune façon le contrôle de la participation au groupe par la source : la source ne peut déterminer ni qui participe, ni qui peut participer ou non au groupe.

L'identification et l'authentification des participants doivent être prises en charge au niveau applicatif si elles sont souhaitées.

Broadcat

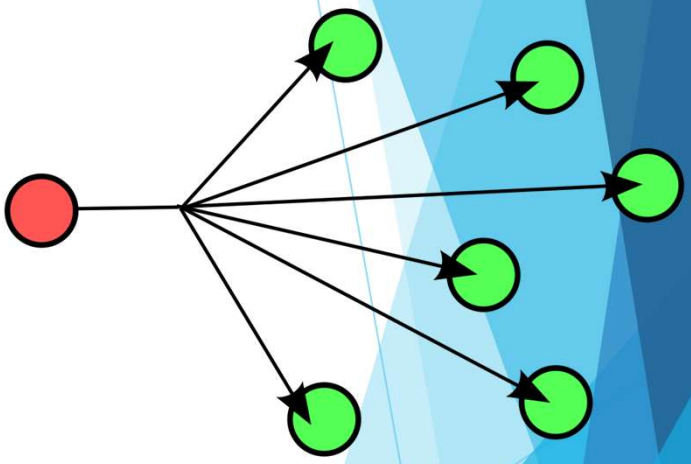
Le principe de base est le même que la télédiffusion, étant donné que l'on diffuse des paquets de données à de nombreux clients éventuellement sans discrimination.

Les protocoles de communications réseau prévoient une méthode simple pour diffuser des données à plusieurs machines en même temps (multicast). Au contraire d'une communication « Point à Point » (unicast), il est possible d'adresser des paquets de données à un ensemble de machines d'un même réseau uniquement par des adresses spécifiques qui seront interceptées par toutes les machines du réseau ou sous-réseau.

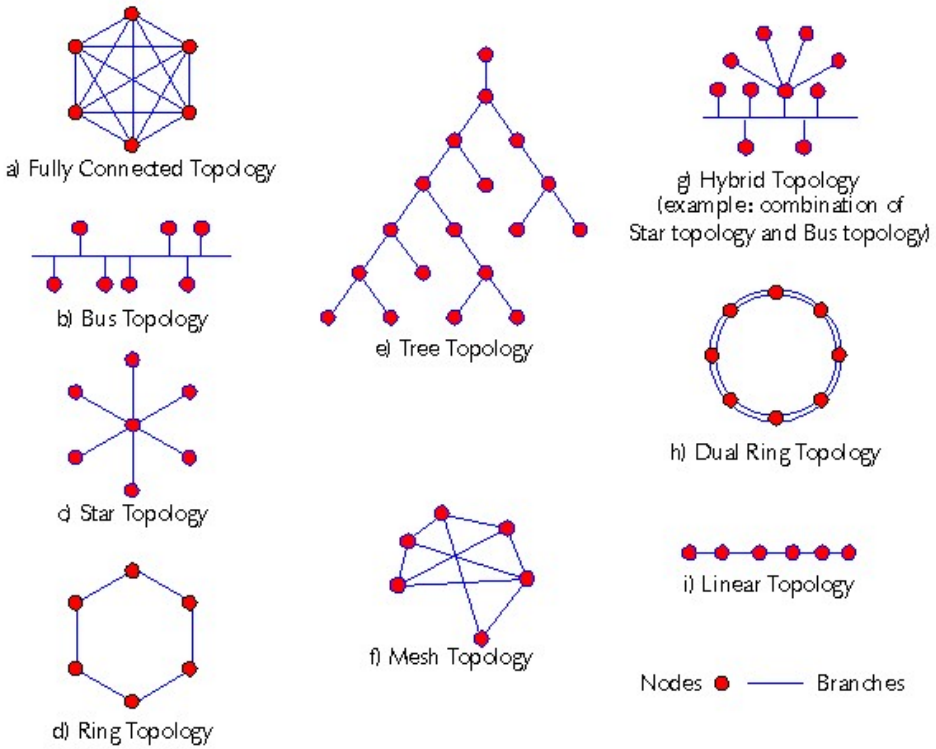
Ces paquets sont en général utilisés dans un environnement LAN pour atteindre une machine dont on ne connaît pas l'adresse MAC (protocole ARP pour le protocole IP version 4) ou pour des annonces faites aux clients potentiels par des machines pouvant offrir des services (comme les protocoles SSDP , NetBeui, ou d'interopérabilité comme DLNA).

L'étendue de diffusion sera restreinte au domaine de diffusion.

Un type de broadcast largement utilisé est la requête ARP ou PING



III. Les Topologie Réseaux



Topologie

Une topologie de réseau informatique correspond à l'architecture (physique ou logique) de celui-ci, définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle entre eux.

Elle peut définir la façon dont les équipements sont interconnectés et la représentation spatiale du réseau (topologie physique).

Elle peut aussi définir la façon dont les données transitent dans les lignes de communication (topologies logiques).

Mode de propagation

Il existe 2 modes de propagation classant ces topologies :

- Mode de diffusion (par exemple topologie en bus ou en anneau)

Ce mode de fonctionnement consiste à n'utiliser qu'un seul support de transmission. Le principe est que le message est envoyé sur le réseau, ainsi toute unité réseau est capable de voir le message et d'analyser selon l'adresse du destinataire si le message lui est destiné ou non.

- Mode point à point (par exemple topologie en étoile ou maillée)

Dans ce mode, le support physique ne relie qu'une paire d'unités seulement. Pour que deux unités réseaux communiquent, elles passent obligatoirement par un intermédiaire (le nœud).

Le réseau en anneau /Token Ring

Un réseau a une topologie en anneau quand toutes ses stations sont connectées en chaine les unes aux autres par une liaison bipoint de la dernière à la première.

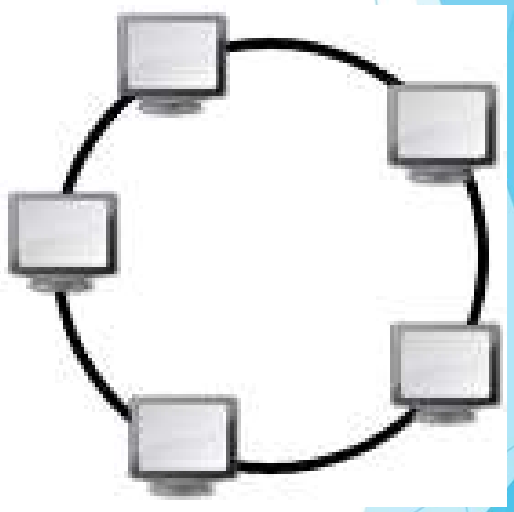
Chaque station joue le rôle de station intermédiaire.

Chaque station qui reçoit une trame, l'interprète et la ré-émet à la station suivante de la boucle si c'est nécessaire.

La défaillance d'un hôte rompt la structure d'un réseau en anneau si la communication est unidirectionnelle ; en pratique un réseau en anneau est souvent composé de 2 anneaux contra-rotatifs.

Note : les ordinateurs d'un réseau en anneau ne sont pas systématiquement reliés en boucle, mais peuvent être connectés à un répartiteur appelé « MAU », (pour Multistation Access Unit) qui va gérer la communication entre les ordinateurs reliés en allouant à chacun d'eux un « temps de parole ».

En cas de collision de deux messages, les deux seraient perdus, mais les règles d'accès à l'anneau (par exemple, la détention d'un jeton) sont censées éviter ce cas de figure.

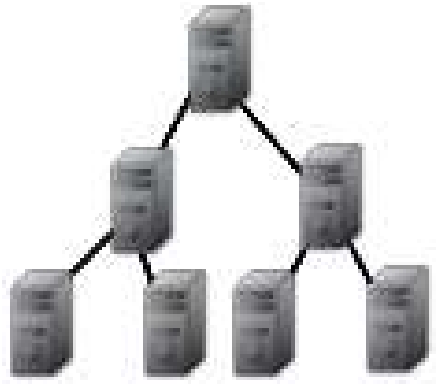


Le réseau hierarchies ou en arborescence

Le Réseau en arbre est divisé en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur, dans la hiérarchie.

Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

Le point faible de ce type de topologie réside dans l'ordinateur "père" de la hiérarchie qui, s'il tombe en panne, interdit alors toute communication entre les deux moitiés du réseau.



Le réseau en bus

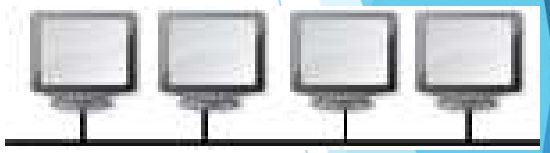
La topologie Réseau en bus est représentée par un câblage unique des unités réseaux.

Il a également un faible coût de déploiement et la défaillance d'un nœud (ordinateur) ne scinde pas le réseau en deux sous-réseaux.

Ces unités sont reliées de façon passive par dérivation électrique ou optique.

Les caractéristiques de cette topologie sont les suivantes :

- Lorsqu'une station est défectueuse et ne transmet plus sur le réseau, elle ne perturbe pas le réseau.
- Lorsque le support est en panne, c'est l'ensemble du réseau qui ne fonctionne plus.
- Le signal émis par une station se propage dans un seul sens ou dans les deux sens.
- Si la transmission est bidirectionnelle : toutes les stations connectées reçoivent les signaux émis sur le bus en même temps (au délai de propagation près).
- Le bus, dans le cas de câbles coaxiaux, est terminé à ses extrémités par des adaptateurs d'impédance (des « bouchons ») pour éliminer les réflexions du signal.



Le réseau en étoile / Hub and Spoke

La topologie Réseau en étoile la topologie la plus courante actuellement.

Omniprésente, elle est aussi très souple en matière de gestion et de dépannage d'un réseau :

la panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche, l'équipement central (un hub, un commutateur ou switch) qui relie tous les nœuds, constitue un point unique de défaillance (une panne à ce niveau rend le réseau totalement inutilisable).

Le réseau Ethernet est un exemple de topologie en étoile.

L'inconvénient principal de cette topologie réside dans la longueur des câbles utilisés (Déperdition).

Le réseau maillé

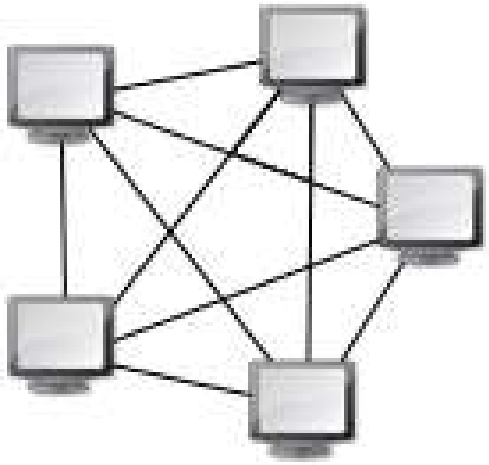
Une topologie maillée correspond à plusieurs liaisons point à point. (Une unité réseau peut avoir N connexions point à point vers plusieurs autres unités.) Chaque terminal est relié à tous les autres.

L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux l'est.

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet).

L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.

Elle existe aussi dans le cas de couverture Wi-Fi. On parle alors bien souvent de topologie mesh mais ne concerne que les routeurs Wi-Fi. Ceux-ci se relaient les paquets grâce au protocole OLSR.

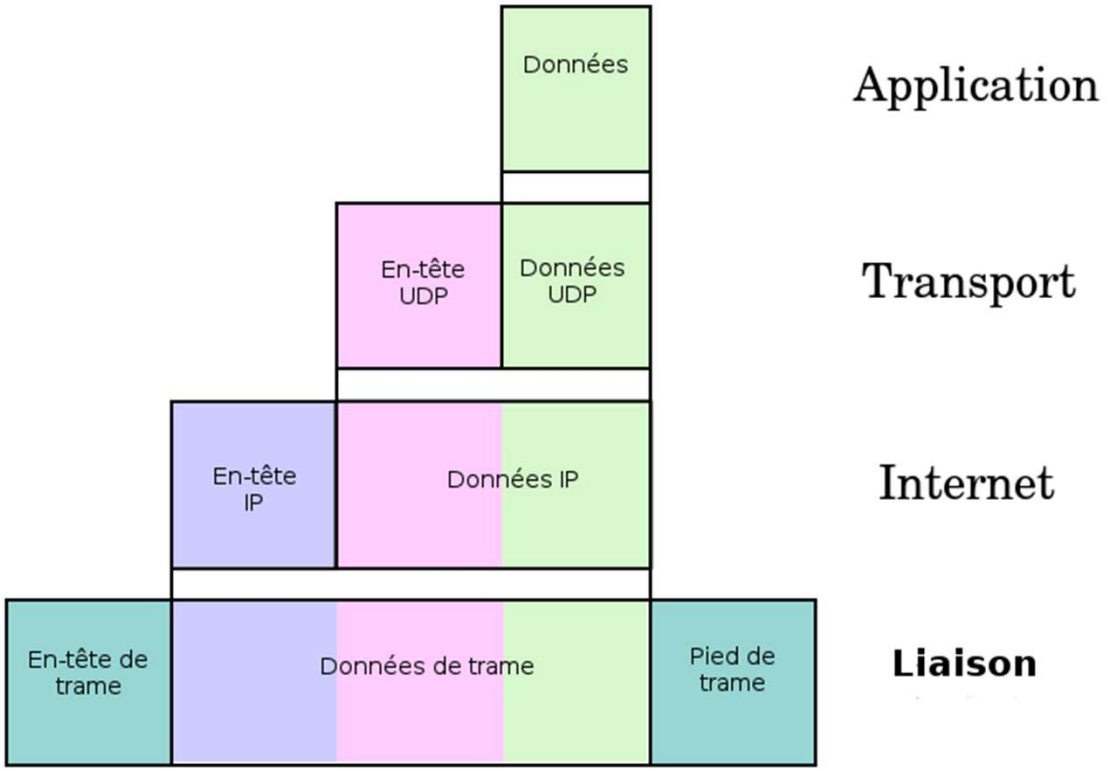


Internet

Internet est le nom donné à l'interconnexion de plusieurs réseaux, potentiellement de topologies différentes, l'unification n'en étant faite qu'au niveau du seul adressage IP (v4 ou v6) et d'un grand nombre de protocoles et règles définis par l'IETF.

De ce fait, aucun des cas particuliers de topologies citées ci-dessus ne s'applique; comme pour la plupart des grands réseaux, on dit d'Internet que sa topologie est quelconque, et de toute façon indépendante du plan d'adressage qui y est défini.

IV. Les Protocol Internet /Internet protocol (IP)



Suite des protocoles Internet

La suite des protocoles Internet est l'ensemble des protocoles utilisés pour le transfert des données sur Internet.

Elle est aussi appelée suite TCP/IPDoD, DoD Standard (DoD pour Department of Defense), DoD Model, DoD TCP/IP ou encore US DoD Model1.

Elle reste le plus souvent appelée TCP/IP, d'après le nom de ses deux premiers protocoles : TCP (Transmission Control Protocol) et IP (Internet Protocol). Ils ont été inventés par Vinton G. Cerf et Bob Kahn, travaillant alors pour la DARPA (Defense Advanced Research Projects Agency), d'après les travaux de Louis Pouzin.

Un peu d'histoire

TCP/IP fut créer lorsque la DARPA dut créer un protocol pour un réseau de commutation de paquet par radio.

Bob Kahn exposa sa publication de TCP/IP en 1973.

La première forme d'internet fut l' ARPANET (Advanced Research Projects Agency Network) en 1972, basées sur la communication par circuits électroniques, telle que celle utilisée par le réseau de téléphone, où un circuit dédié est activé lors de la communication avec un poste du réseau.

En 1982 ARPANET adopte le format TCP/IP, en 1984 le modèle théorique OSI (inventé en 1970), conditionnera la méthodologie de gestion des paquet pour donnée via sont format à 7 couches l'internet.

TCP / IP

Fonctionnement

Une session TCP fonctionne en trois phases :

1. l'établissement de la connexion ;
2. les transferts de données ;
3. la fin de la connexion.

L'établissement de la connexion se fait par un handshaking en trois temps. La rupture de connexion, elle, utilise un handshaking en quatre temps.

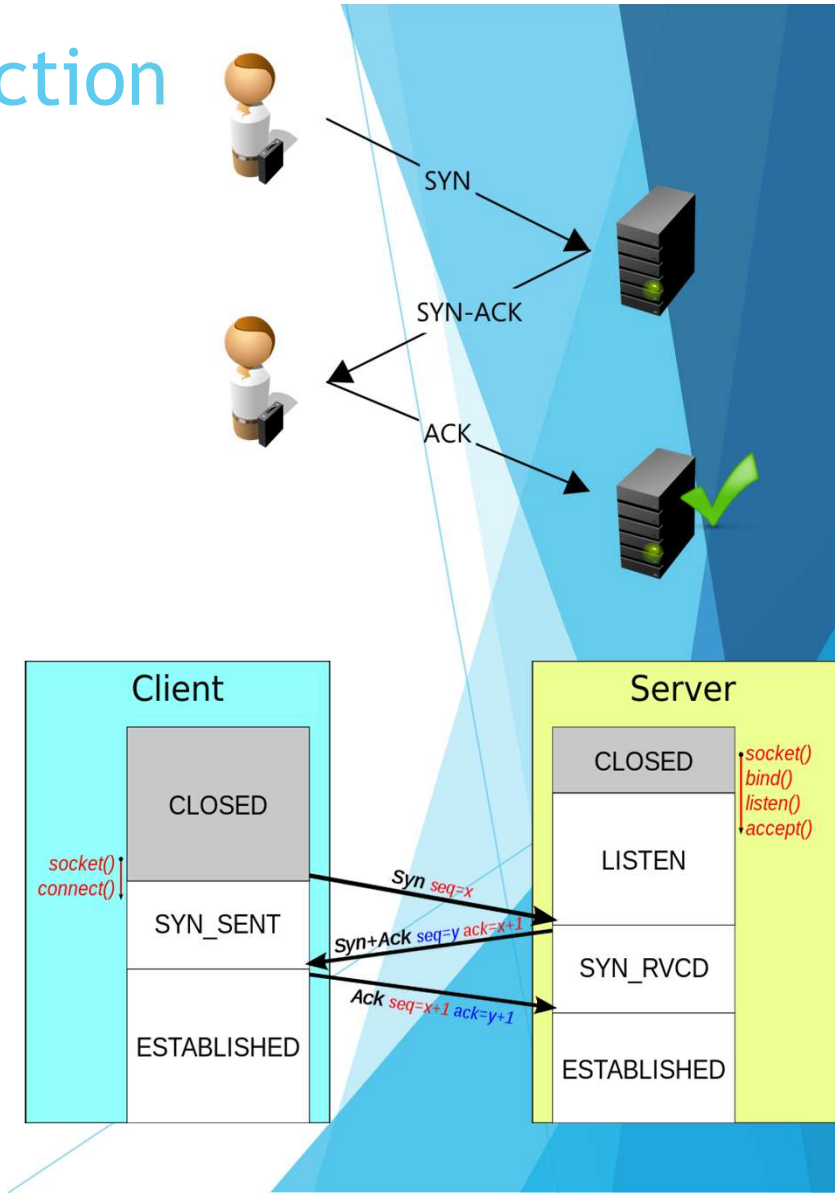
Pendant la phase d'établissement de la connexion, des paramètres comme le numéro de séquence sont initialisés afin d'assurer la transmission fiable (sans perte et dans l'ordre) des données.

TCP/ IP établissement de la connection (Handshaking)

Selon le protocole de communication TCP, une connexion entre deux hôtes s'établit en trois étapes : SYN, SYN-ACK et ACK,

Fonctionnement

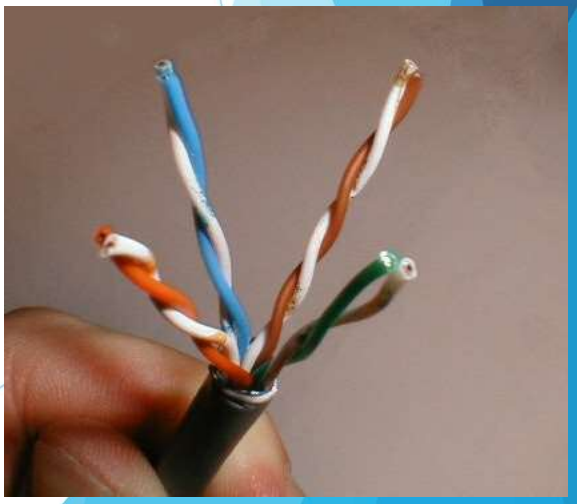
1. SYN : Le client qui désire établir une connexion avec un serveur va envoyer un premier paquet SYN (synchronized) au serveur. Le numéro de séquence de ce paquet est un nombre aléatoire A.
2. SYN-ACK : Le serveur va répondre au client à l'aide d'un paquet SYN-ACK (synchronize, acknowledge).Le numéro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



ETHERNET

Conçu au début des années 1970, pour relier entre eux des ordinateurs rattachés à un même câble coaxial, sur paire torsadée depuis les année 1990 (RJ45 par exemple suite à la création des switch) pour la connexion des postes clients et des versions sur fibre optique pour le cœur du réseau (équipement de tête de réseaux comme le Border routeur et Machine clé comme les serveur).

IEEE 802.11 est la version sans fil d'Ethernet communément appelé WIFI (Wireless fiber),



Standardisation initiale d’ETHERNET

Ethernet est fondé sur le principe de membres (pairs) sur le réseau, envoyant des messages dans ce qui était essentiellement un système radio, captif à l'intérieur d'un fil ou d'un canal commun, parfois appelé l'éther.

Ainsi, Ethernet est conçu à l'origine pour une topologie physique et logique en bus (tous les signaux émis sont reçus par l'ensemble des machines connectées). Chaque pair est identifié par une clé globalement unique, appelée adresse MAC, pour s'assurer que tous les postes sur un réseau Ethernet aient des adresses distinctes sans configuration préalable.

Il incorpore le système d’anticplision CSMA/CD (Carrier Sense Multiple Access with Collision Detection / écoute de porteuse avec accès multiples et détection de collision) hérité de Token Ring, régit la façon dont les postes accèdent au média.

Fonctionnement

Deux procedure sont appliqué la principal et la gestion de collision.

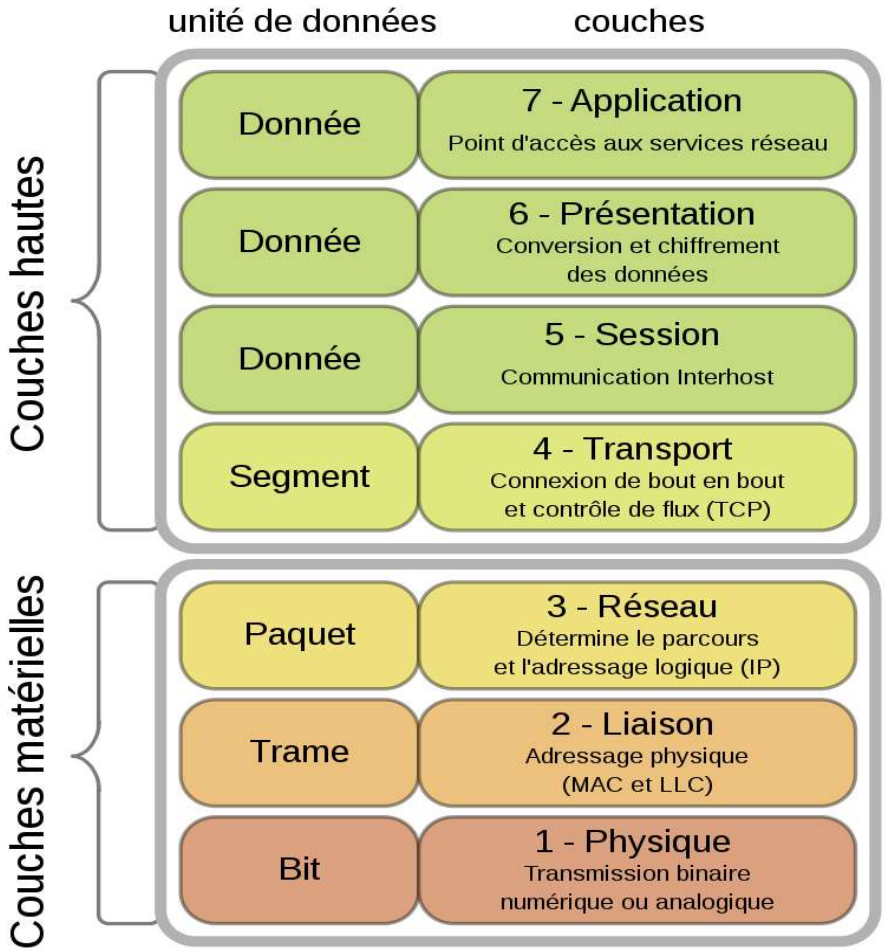
Procédure Principal:

1. Trame prête à être transmise.
2. Si le medium n'est pas libre, attendre jusqu'à ce qu'il le devienne puis attendre la durée intertrame (9,6 µs pour l'Ethernet 10 Mbit/s) et démarrer la transmission.
3. Si une collision est détectée, lancer la procédure de gestion des collisions. Sinon, la transmission est réussie.
4. Une station qui détecte une collision émet sur le média un signal de collision appelé « jam signal » (une séquence de 4 à 6 octets).

Procédure de gestion des collision:

1. Continuer la transmission à hauteur de la durée d'une trame de taille minimale (64 octets) pour s'assurer que toutes les stations détectent la collision.
2. Si le nombre maximal de transmissions (16) est atteint, annuler la transmission.
3. Attendre un temps aléatoire dépendant du nombre de tentatives de transmission.
4. Reprendre la procédure principale.

V. Model OSI (OPEN SYSTEM INTERCONNECTION)



v · m	Couches du modèle OSI [masquer]
7. Application	BGP · DHCP · DNS · FTP · FTPS · FXP · Gopher · H.323 · HTTP · HTTPS · IMAP · IPP · IRC · LDAP · LMTP · MODBUS · NFS · NNTP · POP · RDP · RTSP · SILC · SIMPLE · SIP · SMB-CIFS · SMTP · SNMP · SOAP · SSH · TCAP · Telnet · TFTP · VoIP · Web · WebDAV · XMPP
6. Présentation	AFP · ASCII · ASN.1 · HTML · MIME · NCP · TDI · TLS · TLV (en) · Unicode · UUCP · Vidéotex · XDR · XML
5. Session	AppleTalk · DTLS · NetBIOS · RPC · RSerPool · SOCKS
4. Transport	DCCP · RSVP · RTP · SCTP · SPX · TCP · UDP
3. Réseau	ARP · Babel · BOOTP · CLNP · ICMP · IGMP · IPv4 · IPv6 · IPX · IS-IS · NetBEUI · NDP · RIP · EIGRP · OSPF · RARP · X.25
2. Liaison	Anneau à jeton (token ring) · Anneau à jeton adressé (Token Bus) · ARINC 429 · AFDX · ATM · Bitnet · CAN · Ethernet · FDDI · Frame Relay · HDLC · I²C · IEEE 802.3ad (LACP) · IEEE 802.1aq (SPB) · LLC · LocalTalk · MIL-STD-1553 · PPP · STP · Wi-Fi · X.21
1. Physique	4B5B · ADSL · BHDn · Bluetooth · Câble coaxial · Codage bipolaire · CSMA/CA · CSMA/CD · DSSS · E-carrier · EIA-232 · EIA-422 · EIA-449 · EIA-485 · FHSS · HomeRF · IEEE 1394 (FireWire) · IrDA · ISDN · Manchester · Manchester différentiel · Miller · MLT-3 · NRZ · NRZI · NRZM · Paire torsadée · PDH · SDH · SDSL · SONET · T-carrier · USB · VDSL · VDSL2 · V.21-V.23 · V.42-V.90 · Wireless USB · 10BASE-T · 10BASE2 · 10BASE5 · 100BASE-TX · 1000BASE-T
Articles liés	Pile de protocoles · Modèle Internet · Couche 8

Description

Le modèle OSI est une norme de communication, en réseau, de tous les systèmes informatiques.

C'est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

L'OSI devient une norme en 1984 : la norme ISO 7498:1984 « Modèle basique de référence pour l'interconnexion des systèmes ouverts (OSI) »

La norme

L'objectif de cette norme est de spécifier un cadre général pour la création de normes ultérieures cohérentes. Le modèle lui-même ne définit pas de service particulier et encore moins de protocole.

La norme ISO 7498 et compose de 4 partie :

1. Le modèle de base (ref. 7498-1)
2. Architecture de sécurité (ref. 7498-2)
3. Dénomination et adressage (ref. 7498-3)
4. Cadre général de gestion (ref. 7498-4)

Concept et terminologie

Le modèle est essentiellement une architecture en couches définies et délimitées avec les notions de service, de protocole et d'interface.

- Un service est une description abstraite de fonctionnalités à l'aide de primitives (commandes ou événements) telles que demande de connexion ou réception de données.
- Un protocole est un ensemble de messages et de règles d'échange réalisant un service.
- Une interface (« point d'accès au service » dans la norme) est le moyen concret d'utiliser le service. Dans un programme, c'est typiquement un ensemble de fonctions de bibliothèque ou d'appels systèmes. Dans une réalisation matérielle, c'est par exemple un jeu de registres à l'entrée d'un circuit.

Les détails d'un service varient bien sûr d'une architecture de réseau à l'autre. La classification la plus grossière se fait selon que le service fonctionne en mode connecté ou non. Malgré cette variabilité, les fonctions communes ont des noms conventionnellement constants. Ces noms ne proviennent toutefois pas directement de ISO 7498-1.

connection.request

est une demande de connexion sortante, i.e. à l'initiative d'une entité locale.

connection.indication

correspond à l'événement « Une demande de connexion entrante a été reçue. »

connection.response

est l'indication d'acceptation ou de rejet de la connexion

connection.confirmation

correspond à l'événement « La réponse du demandé a été reçue. » C'est un acquittement.

data.request, data.indication et data.confirm

sont le pendant pour les données.

Les données fournies à une primitive de service sont appelées (N)-SDU (« Service Data Unit ») où N est l'indication de la couche, son numéro dans la norme, parfois une lettre tirée du nom de la couche. Les messages d'un protocole sont appelés PDU (« Protocol Data Unit »).

*Les couches d'architectures

Note mémotechnique pour se rappeler des couches OSI:

Chaque 1ere lettre correspond à la couche correspondante -
Partout Le Roi Trouve Sa Place Assise
Partout=1 Physique
Le = 2 Liaison
Roi = 3 Réseau
Trouve = 4 Transport
Sa = 5 Session
Place = 6 Présentation
Assise = 7 Application

Modèle OSI

	PDU	Couche		Fonction
Couches hautes	Donnée	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5	Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment (en) / Datagramme	4	Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame	2	Liaison	Adressage physique (adresse MAC)
	Bit	1	Physique	Transmission des signaux sous forme numérique ou analogique

Les couches d’architectures: description

Caractérisation résumée des couches
La caractérisation donnée ici est tirée du chapitre 7 de ISO 7498-1. La description originelle donne en plus, pour chaque couche, les fonctions de manipulation de commandes ou de données significatives parmi celles décrites plus bas.

1. La couche « physique » est chargée de la transmission effective des signaux entre les interlocuteurs. Son service est limité à l'émission et la réception d'un bit ou d'un train de bits continu (notamment pour les supports synchrones (concentrateur)).
2. La couche « liaison de données » gère les communications entre deux machines directement connectées entre elles, ou connectées à un équipement qui émule une connexion directe (commutateur).
3. La couche « réseau » gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets (cf. note ci-dessous).
4. La couche « transport » gère les communications de bout en bout entre processus (programmes en cours d'exécution).
5. La couche « session » gère la synchronisation des échanges et les « transactions ».
6. La couche « présentation » est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises.
7. La couche « application » est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

Les fonctions : Communes

Fiabilisation des communications

L'un des rôles majeurs des couches 2 à 4, présentes dans nombre de piles protocolaires, est la construction d'une connexion exempte d'erreurs de transmission.

Cela signifie que les données transmises sont reçues sans corruption, perte, réordonnancement ni duplication. Cela implique qu'au moins une couche, et en pratique plusieurs, fasse de la détection d'erreur, de la correction d'erreur ou de la retransmission de données et du contrôle de flux.

Détection d'erreurs

repérage des PDU dont au moins un bit a changé de valeur lors du transfert.

Correction des erreurs

Compensation des erreurs soit par correction des données à l'aide de code correcteurs d'erreurs ou par destruction du PDU erroné et demande de retransmission.

Contrôle de flux

Synchronisation des communications destinée à empêcher qu'un interlocuteur reçoive plus de PDU qu'il ne peut en traiter.

Fonctions : de transformation

Fonctions de transformation

En plus de la structure en couche, le modèle définit aussi une série de mécanismes standards de manipulation de commandes ou de données, utilisées pour la réalisation d'un service. Cette section définit les plus courantes. Ces transformations sont décrites par paire d'opérations inverses l'une de l'autre.

Multiplexage et démultiplexage de connexion

Utilisation d'une connexion de niveau N pour transporter les PDU de plusieurs connexions de niveau N+1. Symétriquement, démultiplexer consiste à séparer les (N+1)-PDU entrants par connexion. Par exemple, ce mécanisme est prévu dans les réseaux ATM par la « couche » AAL 3/4.

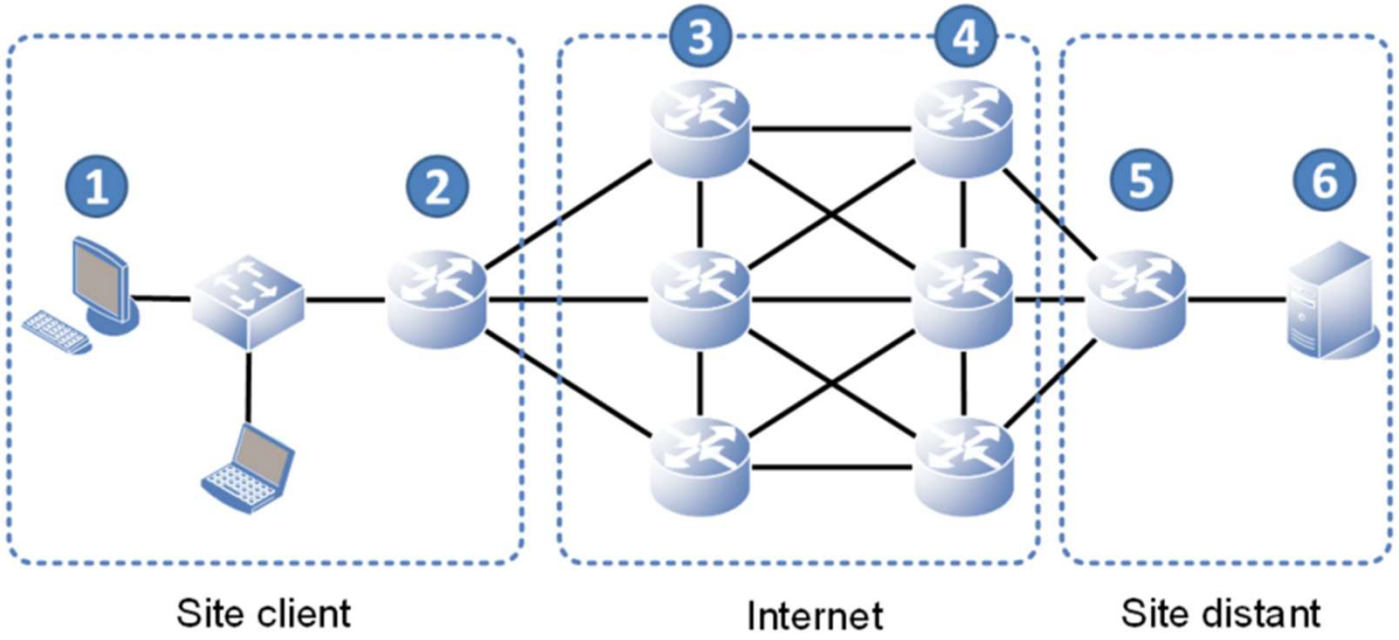
Éclatement et recombinaison

Opérations similaires dans lesquelles les (N+1)-PDU sont répartis sur plusieurs connexions de niveau N. Cela est utilisé en particulier par les utilisateurs d'accès RNIS pour augmenter le débit disponible.

Segmentation et réassemblage

Lorsque le service fourni par la couche (N) fixe une limite de taille sur les données trop petites par rapport au service de la couche (N+1), la couche (N+1) découpe les (N+1)-SDU en plusieurs fragments correspondant chacun à un (N+1)-PDU avant envoi. À la réception, la couche (N+1) concatène les fragments pour retrouver le (N+1)-SDU initial. Cela est massivement utilisé dans les réseaux ATM et dans SSL/TLS. Pour IP, cette fonction est traditionnellement appelée « fragmentation ».

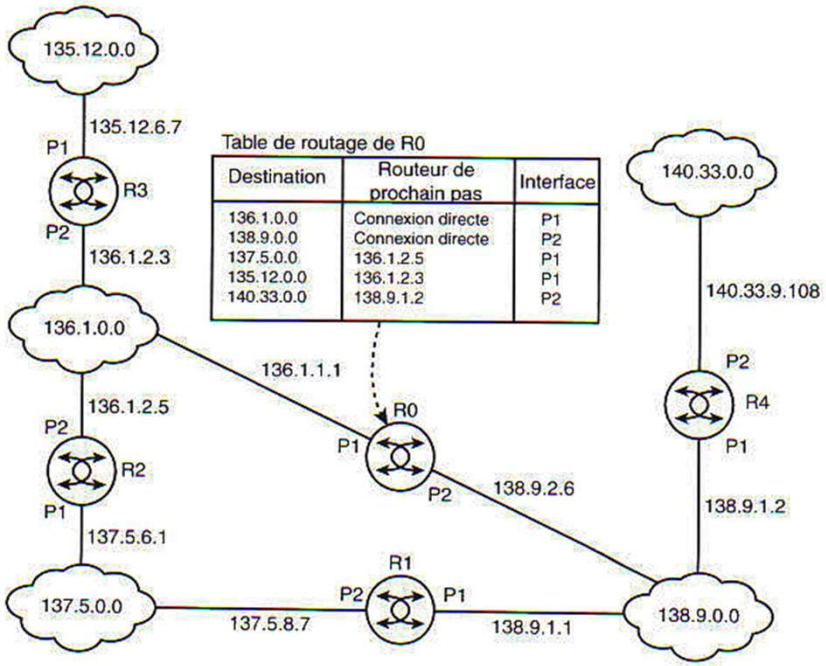
Routage



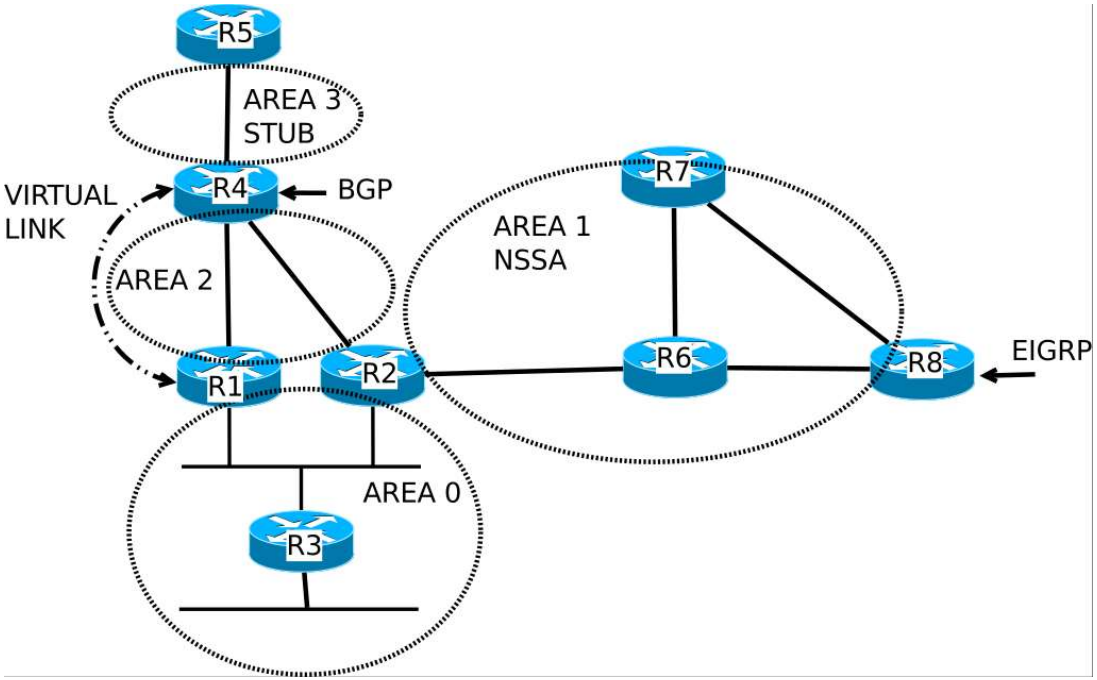
*Comment fonctionne un routeur

Un routeur à pour fonction de faire la passerelle entre deux sous réseaux en interfacage avec lui.

Il peu faire office d'intermediaire entre les deux réseaux si il possède les information de ses deux réseaux dans sa table de Rootage.



OSPF


R5
AREA 3
STUB
R4
BGP
VIRTUAL
LINK
AREA 2
R7
AREA 1
NSSA
R1
R2
R6
R8
EIGRP
AREA 0
R3

Protocol de Routage OSPF

Open Shortest Path First (OSPF) est un protocole de routage interne IP de type « à état de liens ». Il a été développé au sein de l'Internet Engineering Task Force (IETF) à partir de 1987.

Fonctionnement général

Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier.

Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (LSA) propagés de proche en proche à tous les routeurs du réseau.

L'ensemble des LSA forme une base de données de l'état des liens Link-State Database (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire.

Chaque routeur utilise ensuite l'algorithme de Dijkstra, Shortest Path First (SPF) pour déterminer la route la plus rapide vers chacun des réseaux connus dans la LSDB.

Le bon fonctionnement d'OSPF requiert donc une complète cohérence dans le calcul SPF, il n'est donc par exemple pas possible de filtrer des routes ou de les résumer à l'intérieur d'une aire.

En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur.

Routage OSPF AIRE

Afin d'éviter de propager la totalité de la base de données des liens et de limiter l'impact négatif du bagottement ou flapping (alternance rapide dans la disponibilité d'un lien), on segmente l'ensemble des routeurs en groupes connexes appelés aires, à la frontière desquels on peut procéder à des résumés.

Chaque aire est distinguée par un nombre entier positif ou nul variant de 0 à 4 294 967 295, ce nombre est parfois exprimé en notation décimale pointée, de la même manière qu'une adresse IP.Chaque sous-réseau appartient à une seule aire.

Il existe toujours une aire dorsale (backbone area), area 0 ou encore area 0.0.0.0 à laquelle toutes les autres aires sont connectées. Les aires sont logiquement contigües.

Si les routeurs qui constituent une aire ne sont pas physiquement contigus, alors des liens virtuels sont configurés entre les routeurs qui ont en commun une aire de transit.

Ces liens virtuels appartiennent à l'aire 0. Le protocole les traite comme des liens point-à-point non numérotés.

Chaque routeur est identifié à l'aide d'un router-id unique dans le réseau.

Le router-id est un nombre positif codé sur 32 bits, il est habituellement représenté sous la forme d'une adresse IP.

À défaut d'une configuration explicite, l'adresse IP locale la plus élevée sera utilisée, et s'il existe des interfaces de type loopback, l'adresse IP la plus élevée de celles-ci sera utilisée comme router-id.

La détermination du router-id a lieu uniquement à l'initialisation du processus OSPF et persiste ensuite, indépendamment de la reconfiguration ou du changement d'état des interfaces.

Routage OSPF Type de Routeur

On distingue les types de routeurs suivants :

1. Routeur interne: un routeur dont toutes les interfaces se trouvent dans la même aire ;
2. Area Border Router (ABR): un routeur qui dispose d'interfaces dans des aires différentes ;
3. Autonomous System Boundary Router (ASBR): un routeur qui injecte dans OSPF des routes qui proviennent d'autres protocoles de routage ou des routes statiques ;
4. Routeur backbone: un routeur dont au moins une interface appartient à l'aire 0. Tous les ABR sont des routeurs backbone.

Routage OSPF Les Paquet

OSPF fait usage du numéro de protocole 89 d'IP.

Le TTL des paquets est fixé à 1 pour éviter leur propagation au-delà du sous-réseau et le champ ToS (Type of Service)est fixé à 0. OSPF utilise des adresses multicast sur les réseaux de type broadcast et point à point.

Les paquets OSPF ont une taille qui peut aller jusqu'à 65535 octets et faire usage de la fragmentation IP si c'est nécessaire.

Il existe 5 types de paquets OSPF :

1. Hello (Type 1) : découverte des voisins et maintien des adjacences ;
2. Database Description (DBD, Type 2): description des LSA ;
3. Link State Request (Type 3): requête d'un LSA ;
4. Link State Update (LSU, Type 4) : mise à jour d'un LSA;
5. Link State Acknowledgement (Type 5) : acquittement d'un LSA..

TP 2 Installation de PACKET TRACEUR

1. Installé Packet Traceur
2. Créer un réseaux connécté avec 2 routeur 3 aire physique contenant chacune 2 PC.

Liens cours du packet Tracer

https://www.netacad.com/fr/courses/packet-tracer

TP 3 OSPF

1. Configuré OSPF sur vos routeur
2. Créez une aire 0 en 172.16.1.0,
3. Créez une aire 1 en 192.168.1.0,
4. Créez une aire 2 en 10.172.1.0,
5. Créez une aire 3 en 72.20.1.0,
6. Configuré les IP des deux pc de chacune des aire en X.X.1.3 et X.X.1.4
7. Configuré les IP des interface routeur en X.X.1.1 pour l'interface 1 et X.X.X.2 pour l'interface 2
8. Complété les table de routage de chaque routeur
9. Faite un ping avec les 6 PC et pingé les 5 autres