

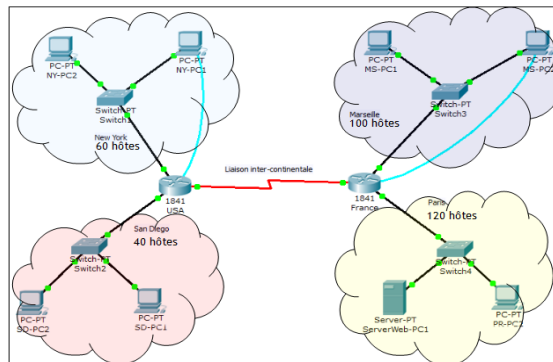


Formation STS SN Académie d'Aix-Marseille

Découverte des réseaux informatiques

Durée : 6 h

Détail du module : A la fin de ce module, vous serez en mesure de mettre en œuvre et de configurer un réseau informatique étendu.



Savoir S7.2. :

- Concepts fondamentaux des réseaux
- Types de réseaux : du PAN au WAN
- Topologies (bus, étoile, etc.)
- Équipements réseau : connecteur, carte réseau, commutateur, pont, routeur, etc.
- Modèles de référence (OSI, etc.)
- Classification et critères déterminants de choix
- Modèle en couches et protocoles de l'Internet : IP, ICMP, ARP, UDP, TCP, etc.

Compétences :

- C4.1 : câbler et/ou intégrer un matériel
- C4.2 : adapter et/ou configurer un matériel

Moyens : Logiciels : Cisco Packet Tracer (téléchargeable : <http://www.silanus.fr/sin/cisco>)

Matériel : PC avec droits administrateur – Commutateurs – Routeurs – Câblage RJ45 – Caméra IP ...

Documents : <http://www.silanus.fr/sin> Menu BTS SN

Sommaire

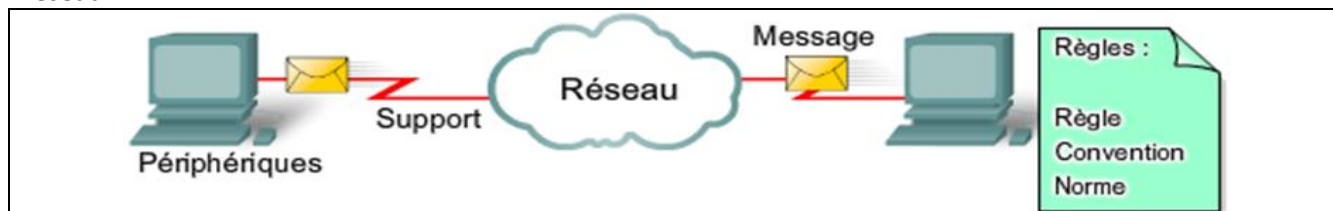
1	Caractéristiques des réseaux	1
1.1	Eléments d'un réseau	1
1.2	Architecture réseau	2
2	Connexion des périphériques	5
2.1	Les supports de transmission	5
2.2	Transmission longue distance sur cuivre	7
2.3	Classification des réseaux de données	8
2.4	Topologie des réseaux	10
3	Fonctionnement d'un réseau	11
3.1	Le modèle de référence OSI.....	11
3.2	Comparaison des modèles OSI et TCP/IP	11
3.3	Principe de l'adressage et de l'encapsulation	12
3.4	Adressage IPv4.....	13
3.4.1	Nécessité.....	13
3.4.2	Attribution	14
3.4.3	Passerelle par défaut	16
3.4.4	Constitution d'une adresse IPv4	16
3.4.5	Masque de sous-réseau	17
3.4.6	Les anciennes classes réseau	18
3.4.7	Plages d'adresse IPv4 exclues de l'adressage des hôtes	20
3.5	Exercices : Adressage IP	21
3.5.1	Définition de l'adresse réseau	21
3.5.2	Calcul du nombre d'hôtes disponible	22
3.5.3	Calcul des adresses réseau, d'hôte et de diffusion.....	22
3.5.4	Calcul de la plage d'adresse utilisable pour les hôtes et de l'adresse de diffusion.....	22
3.6	Principe du routage	23
3.7	Principe du nommage – Service DNS (Domaine Name System).....	24
3.8	Chemin suivi par l'information	25
3.8.1	La commande ping.....	25
3.8.2	La commande traceroute (tracert)	26
3.9	Notions de base sur la création de sous-réseaux	28
3.9.1	Nombre de sous-réseaux.....	28
3.9.2	Le nombre d'hôtes.....	28
3.9.3	Exercice	29
3.9.4	Découpage des réseaux à des tailles appropriées.....	29

3.10	TP Création d'un réseau étendu	31
3.10.1	Objectif du TP.....	31
3.10.2	Qu'allez-vous apprendre ?.....	31
3.10.3	A quoi cela va t-il vous servir ?.....	31
3.10.4	De quelles connaissances avez-vous besoin ?	31
3.10.5	Quel est le matériel dont vous avez besoin ?	31
3.10.6	Fichiers de TP	31
4	Architecture client/serveur.....	32
4.1	Définition	32
4.2	Serveurs	32
4.3	Principaux services et protocoles associés	33
4.3.1	Service de configuration TCP/IP automatique : protocole DHCP	33
4.3.2	Service de partage de fichiers : protocole SMB.....	34
4.3.3	Service web : protocole http.....	34
4.3.4	Service de transfert de fichier : protocole FTP	35
4.4	TP Services réseaux.....	36
4.4.1	Objectif du TP.....	36
4.4.2	Qu'allez-vous apprendre ?.....	36
4.4.3	A quoi cela va t-il vous servir ?.....	36
4.4.4	De quelles connaissances avez-vous besoin ?	36
4.4.5	Quel est le matériel dont vous avez besoin ?	36
4.4.6	Fichiers de TP	36
5	Références	37

1 Caractéristiques des réseaux

1.1 Éléments d'un réseau

Un réseau est constitué de périphériques, de supports et de services reliés par des règles et qui collaborent pour envoyer des messages. Le terme messages sert à désigner des pages Web, des courriels, des messages instantanés, des appels téléphoniques et toutes autres formes de communication prises en charge par le réseau.



L'étude des réseaux fait largement appel aux représentations graphiques et des symboles sont couramment employés pour représenter les périphériques réseau et leurs connexions.

On distingue deux types de périphériques :

Les périphériques terminaux :

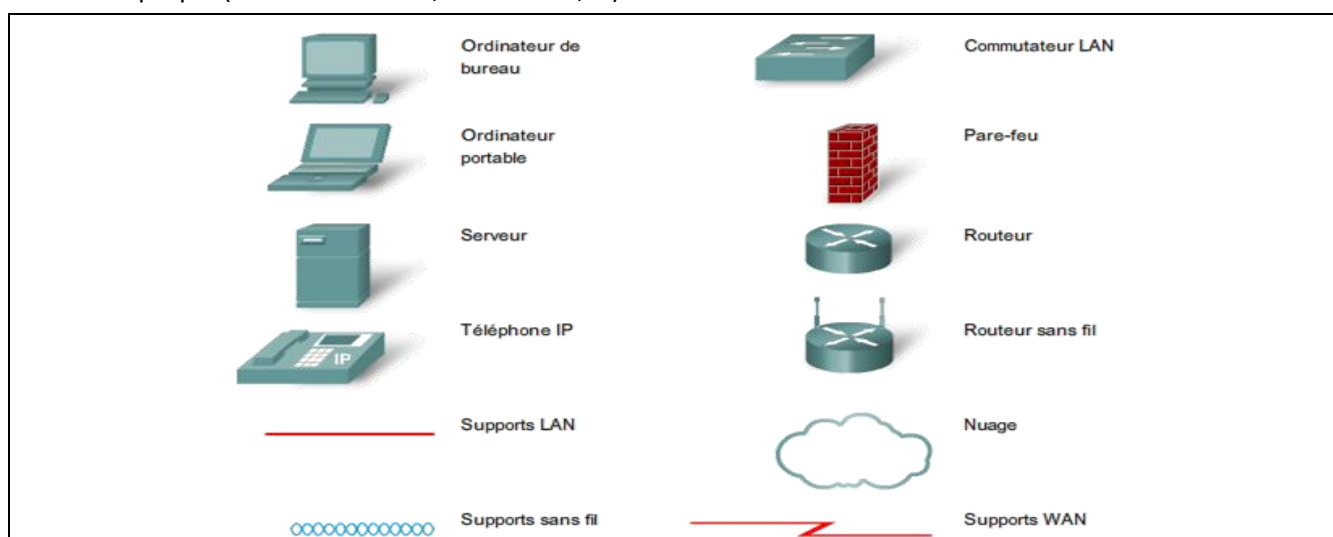
- Serveurs,
- Ordinateurs de bureau,
- Ordinateurs portables,
- Imprimantes,
- Téléphones IP,
- PDA, web phone,
- ...

Les périphériques intermédiaires :

- Commutateur (périphérique le plus couramment utilisé pour interconnecter des réseaux locaux),
- Pare-feu (assure la sécurité du réseau),
- Routeur (contribue à orienter les messages transitant sur un réseau),
- Routeur sans fil (type particulier de routeur souvent présent dans les réseaux familiaux),
- Nuage (sert à représenter un groupe de périphériques réseau et dont les détails ne présentent peut-être pas d'intérêt pour la discussion en cours)
- ...

Les connexions :

- Filaires (câble droit, croisé, téléphonique, série, ...),
- Sans-fil (WiFi, GSM, GPRS, Bluetooth, ZigBee, ...),
- Optique (fibre monomode, multimode, ...).



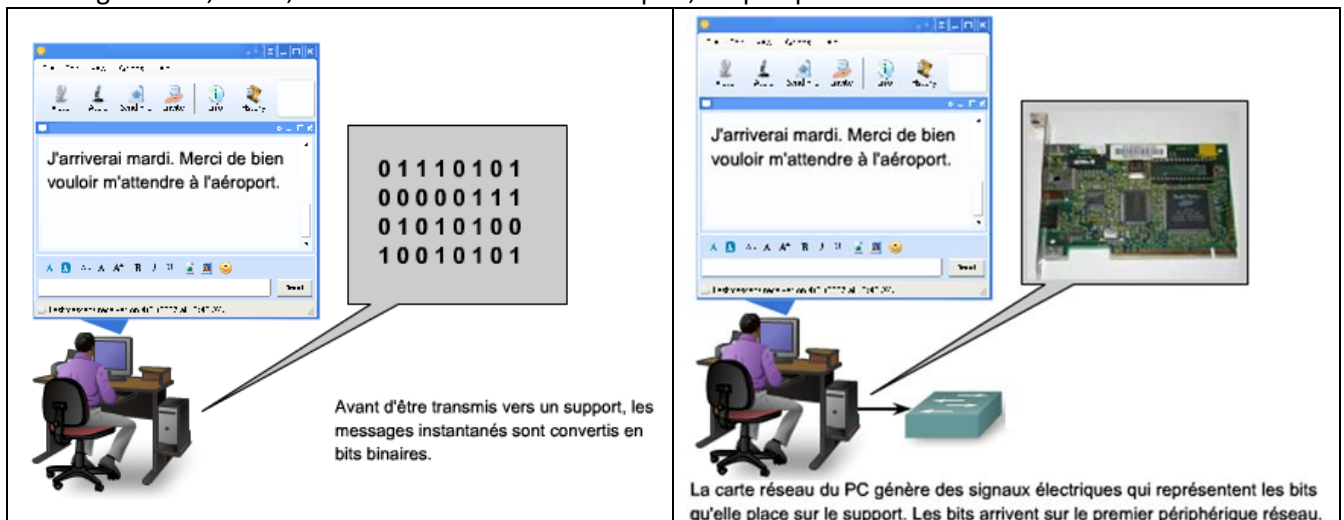
Pour envoyer et recevoir des messages divers et variés on utilise des applications informatiques qui ont besoin que le réseau leur fournisse certains services. Ces services sont régis par des règles, ou protocoles.

Aujourd’hui, la norme en matière de réseaux est un ensemble de protocoles appelé TCP/IP (Transmission Control Protocol/Internet Protocol). Le protocole TCP/IP est non seulement utilisé dans les réseaux privés et professionnels, mais il est aussi le principal protocole d’Internet. C’est en effet le protocole TCP/IP qui définit les règles de formatage, d’adressage et de routage utilisés pour veiller à ce que les messages soient livrés aux destinataires appropriés.

Les services de haut niveau tels que le World Wide Web, les messageries électroniques, les messageries instantanées et la téléphonie sur IP répondent à des protocoles normalisés.

Service	Protocole (« Règle »)
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
Courriel	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Message instantané (Jabber, AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
Téléphonie sur IP	SIP (Session Initiation Protocol)

Avant d’être envoyés vers leurs destinations, tous les types de messages doivent être convertis en bits, c’est-à-dire en signaux numériques codés en binaire. Ceci est obligatoire quel que soit le format d’origine du message : texte, vidéo, audio ou données informatiques, et quel que soit le service sollicité.

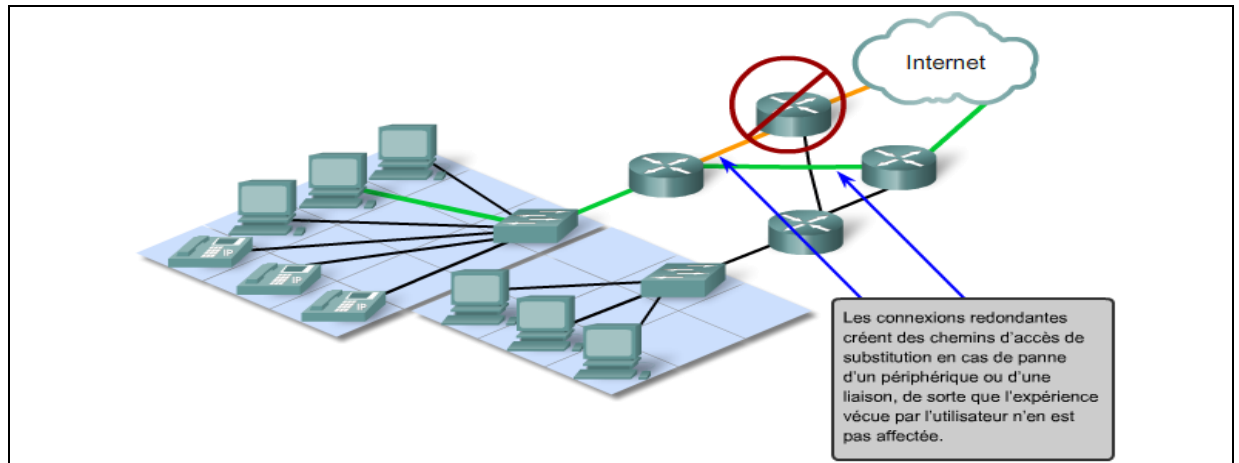


1.2 Architecture réseau

Les réseaux doivent d’une part prendre en charge une large gamme d’applications et de services et d’autre part fonctionner sur de nombreux types d’infrastructures physiques. Dans le contexte actuel, l’expression « architecture réseau » désigne aussi bien les technologies prenant en charge l’infrastructure que les services programmés et les protocoles qui déplacent les messages dans l’infrastructure. Alors qu’Internet, et les réseaux en général, évoluent, nous découvrons que les architectures sous-jacentes doivent prendre en considération quatre caractéristiques de base si elles veulent répondre aux attentes des utilisateurs : tolérance aux pannes, évolutivité, qualité de service et sécurité.

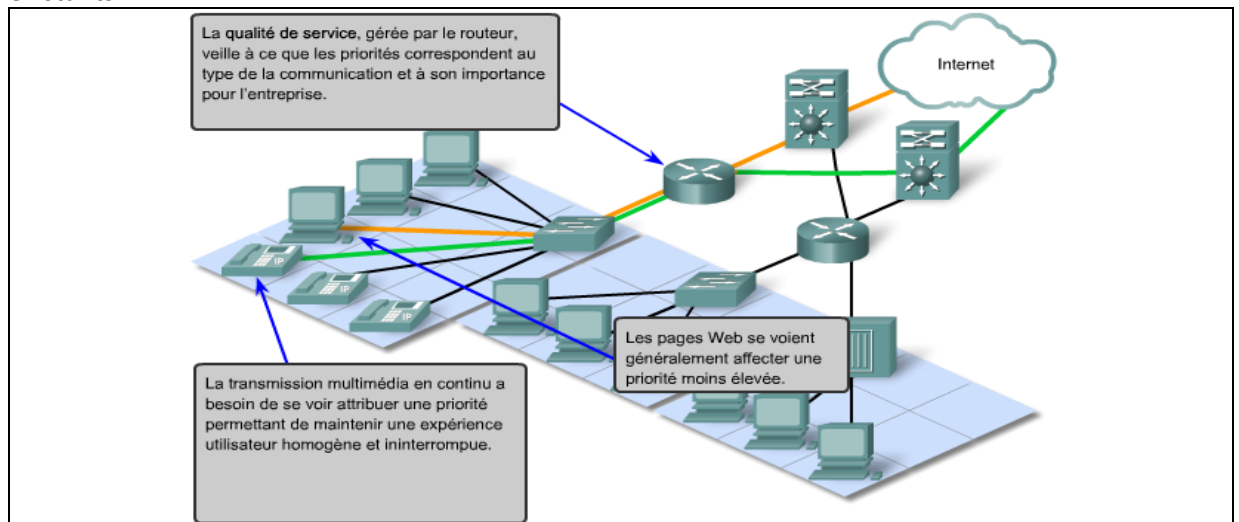
- **Tolérance aux pannes :**

Comme des millions d'utilisateurs attendent d'Internet qu'il soit constamment disponible, il faut une architecture réseau conçue et élaborée pour tolérer les pannes. Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes du matériel et des logiciels et qui peut être rétabli rapidement quand des pannes se produisent. De tels réseaux dépendent de liaisons, ou chemins, redondantes entre la source et la destination d'un message. En cas de défaillance d'une liaison (ou chemin), les processus s'assurent que les messages sont instantanément routés sur une autre liaison et ceci de manière totalement transparente pour les utilisateurs aux deux extrémités. Aussi bien les infrastructures physiques que les processus logiques qui dirigent les messages sur le réseau sont conçus pour prendre en charge cette redondance. Il s'agit d'une caractéristique essentielle des réseaux actuels.



- **Évolutivité :**

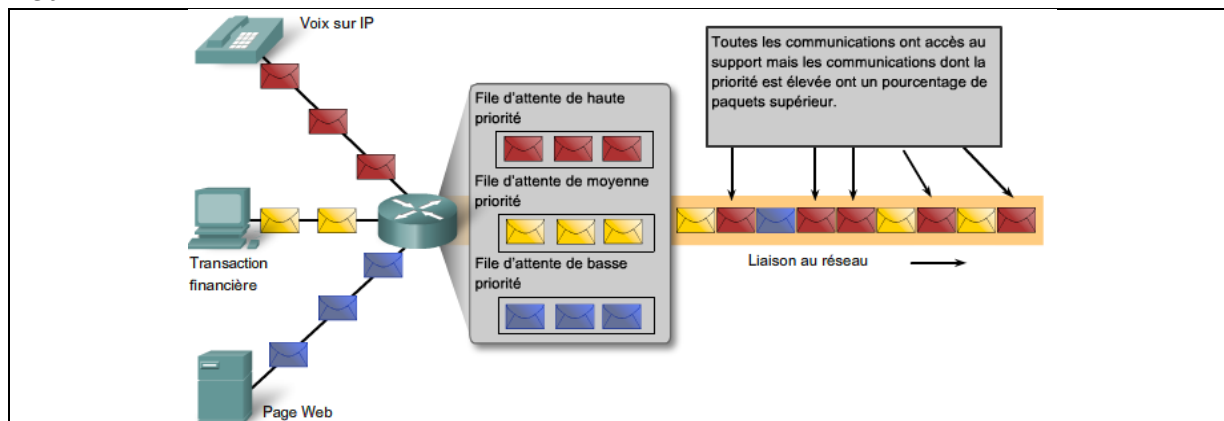
Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.



- **Qualité de service (QOS)**

Les transmissions audio et vidéo en direct exigent un niveau de qualité constant et un service ininterrompu qui n'était pas indispensable aux applications informatiques traditionnelles. La qualité de ces services est évaluée par rapport à la qualité que l'on obtiendrait en assistant en personne à la même présentation audio ou vidéo. Les réseaux audio et vidéo traditionnels sont conçus pour ne prendre en charge qu'un seul type de transmission. Ils peuvent donc offrir un niveau de qualité acceptable. Sur un réseau convergent, les services nécessitant un haut niveau de qualité de service seront prioritaires devant les autres.

Les périphériques intermédiaires qui assurent la qualité de service gèrent des files d'attente selon le niveau de priorité des messages. Ainsi, les messages d'un service de voix sur IP seront prioritaires devant ceux d'un service de transaction financière, eux-mêmes prioritaires devant ceux du service web.



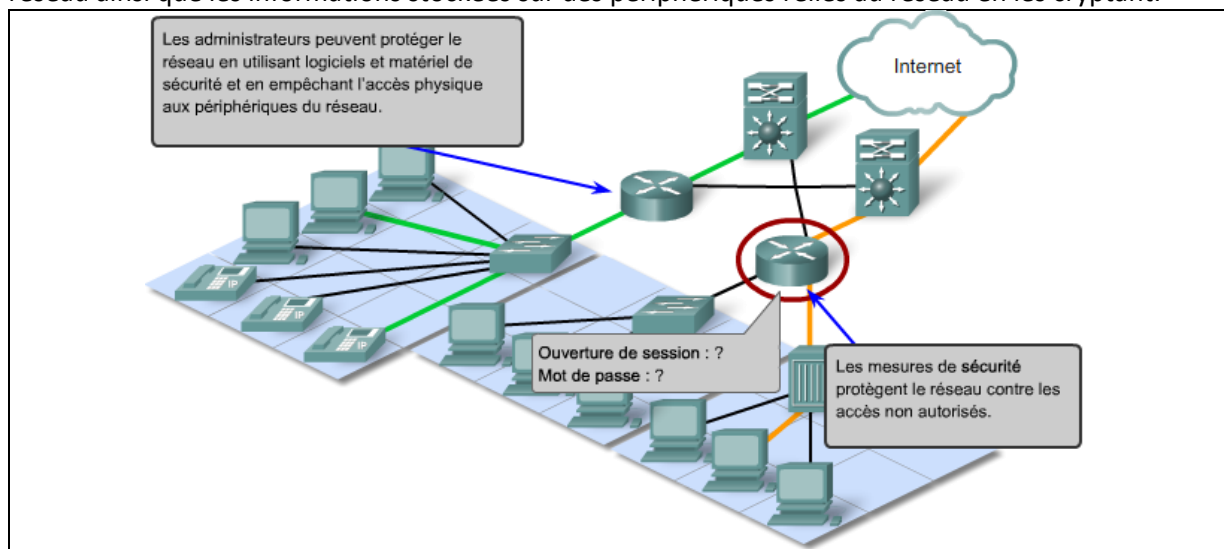
- **Sécurité**

L'infrastructure réseau, les services et les données contenues par un réseau relié à des ordinateurs sont des actifs personnels et professionnels essentiels. Toute compromission de l'intégrité de ces actifs pourrait avoir de graves conséquences professionnelles et financières.

En matière de sécurité des réseaux, deux points doivent être pris en considération pour éviter des conséquences graves : la sécurité de l'infrastructure réseau et la sécurité du contenu.

Sécuriser l'infrastructure réseau implique de sécuriser matériellement les périphériques qui assurent la connectivité du réseau et d'empêcher tout accès non autorisé au logiciel de gestion qu'ils hébergent.

Sécuriser le contenu consiste à protéger les informations contenues dans les paquets transmis sur le réseau ainsi que les informations stockées sur des périphériques reliés au réseau en les cryptant.



2 Connexion des périphériques

2.1 Les supports de transmission

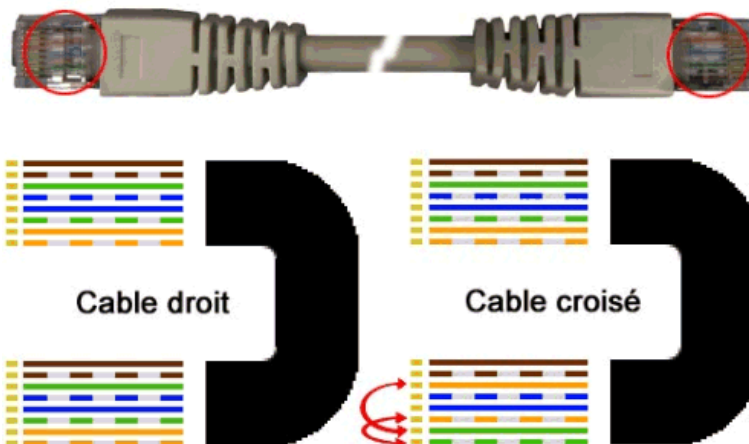
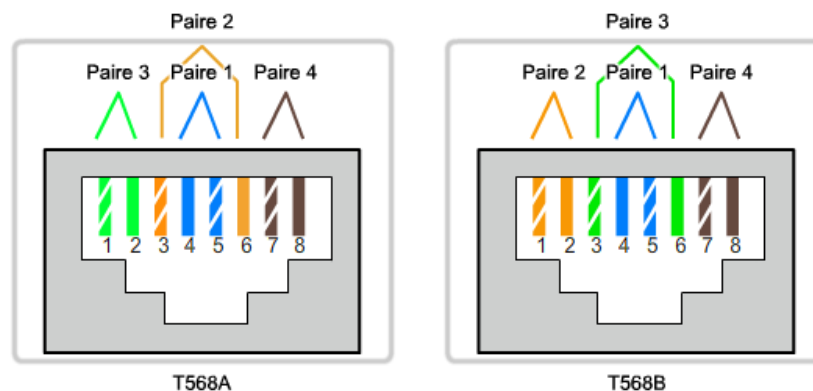
- **Le cuivre : câbles coaxiaux ou à paires torsadées**

Divers organismes de normalisation contribuent à la définition des propriétés physiques, électriques et mécaniques des supports disponibles pour différentes communications de données. Ces spécifications garantissent que les câbles et connecteurs fonctionnent comme prévu avec différentes mises en œuvre.

Par exemple, des normes pour les supports en cuivre sont définies pour :

- Le type de câblage en cuivre utilisé
- La bande passante de la communication
- Le type de connecteurs utilisés
- Le brochage et les codes couleur des connexions avec le support
- La distance maximale du support

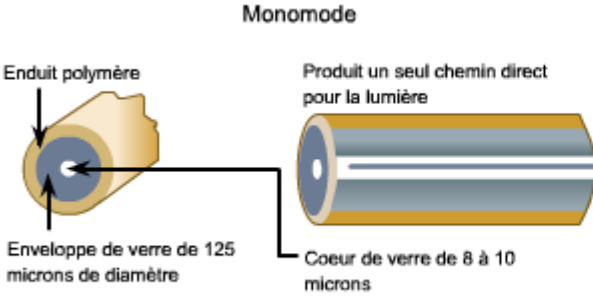
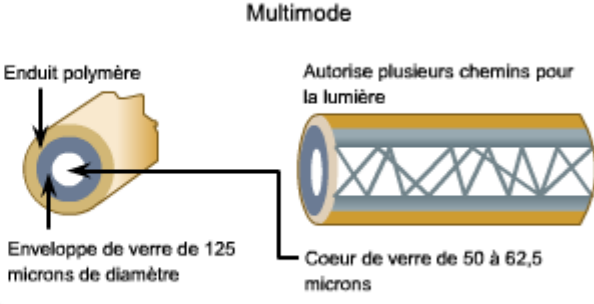
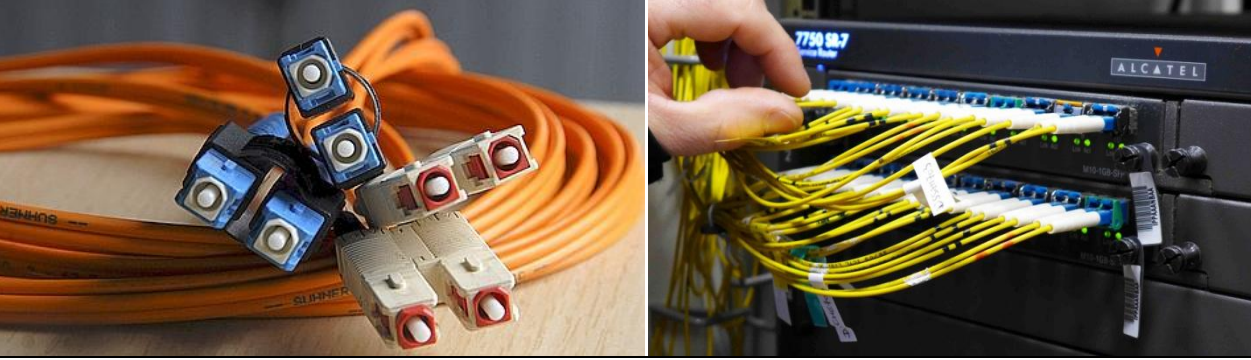
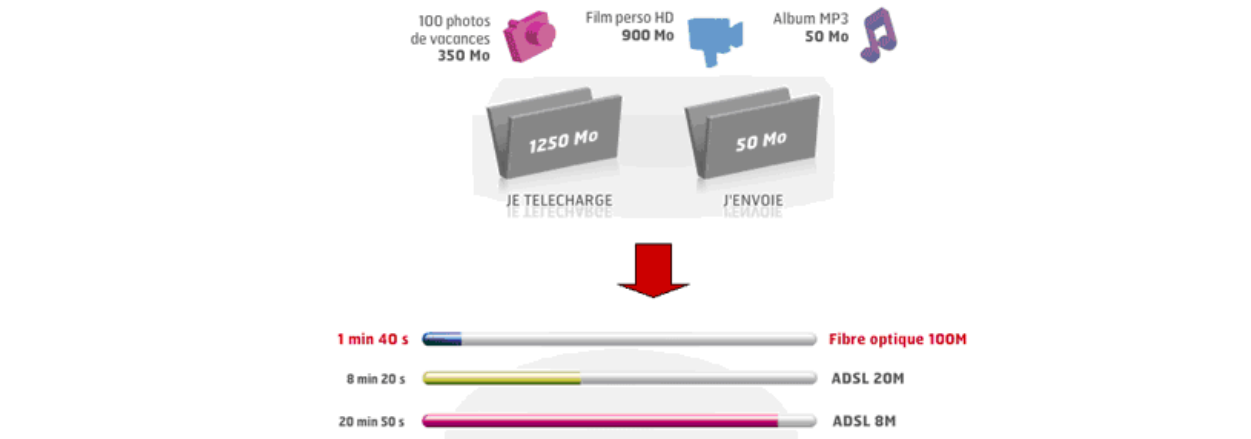
	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T
Supports	EIA/TIA catégorie 3, 4, 5 UTP, quatre paires	EIA/TIA catégorie 5 UTP, deux paires	Fibre multimode de 50/62.5 microns	STP	EIA/TIA catégorie 5 (ou supérieure) UTP, quatre paires
Longueur maximale des segments	100 m	100 m	2 km	25 m	100 m
Topologie	En étoile	En étoile	En étoile	En étoile	En étoile
Connecteur	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	



• **Le verre : fibre optique**

Le câblage en fibre optique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Les bits sont codés sur la fibre comme impulsions lumineuses. Le câblage en fibre optique prend en charge des débits de bande passante de données brutes très élevés.

Des lasers ou des diodes électroluminescentes (DEL) génèrent les impulsions lumineuses utilisées pour représenter les données transmises sous forme de bits sur le support. Des dispositifs à semi-conducteur électronique appelés photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.

Monomode	Multimode
 <p>Enduit polymère</p> <p>Enveloppe de verre de 125 microns de diamètre</p> <p>Produit un seul chemin direct pour la lumière</p> <p>Coeur de verre de 8 à 10 microns</p> <ul style="list-style-type: none"> • Coeur de petit diamètre • Moins de dispersion • Adapté aux applications longue distance (jusqu'à 100 km) • Utilise des lasers comme source lumineuse souvent dans des réseaux fédérateurs de campus pour une distance de plusieurs milliers de mètres 	 <p>Enduit polymère</p> <p>Enveloppe de verre de 125 microns de diamètre</p> <p>Autorise plusieurs chemins pour la lumière</p> <p>Coeur de verre de 50 à 62,5 microns</p> <ul style="list-style-type: none"> • Coeur d'un diamètre plus large que le câble monomode (50 microns ou plus) • Autorise une plus grande dispersion et, par conséquent, un affaiblissement du signal • Adapté aux applications longue distance, mais sur une distance plus courte que la fibre monomode (jusqu'à 2 km environ) • Utilise des DEL comme source lumineuse souvent dans des LAN ou des distances de quelques centaines de mètres au sein d'un réseau de campus
	
 <p>100 photos de vacances 350 Mo</p> <p>Film perso HD 900 Mo</p> <p>Album MP3 50 Mo</p> <p>1250 Mo JE TELECHARGE</p> <p>50 Mo J'ENVOIE</p> <p>1 min 40 s Fibre optique 100M</p> <p>8 min 20 s ADSL 20M</p> <p>20 min 50 s ADSL 8M</p>	

• **Ondes électromagnétiques : sans fil**

Les supports sans fil transportent des signaux électromagnétiques à des fréquences radio et micro-ondes qui représentent les chiffres binaires des communications de données. En tant que support réseau, la transmission sans fil n'est pas limitée aux conducteurs ou voies d'accès, comme les supports en cuivre et à fibre optique.

Les technologies de communication de données sans fil fonctionnent bien dans les environnements ouverts. Cependant, certains matériaux de construction utilisés dans les bâtiments et structures, ainsi que le terrain local, limitent la couverture effective. De plus, la transmission sans fil est sensible aux interférences et peut être perturbée par des appareils aussi courants que les téléphones fixes sans fil, certains types d'éclairages fluorescents, les fours à micro-ondes et d'autres communications sans fil.

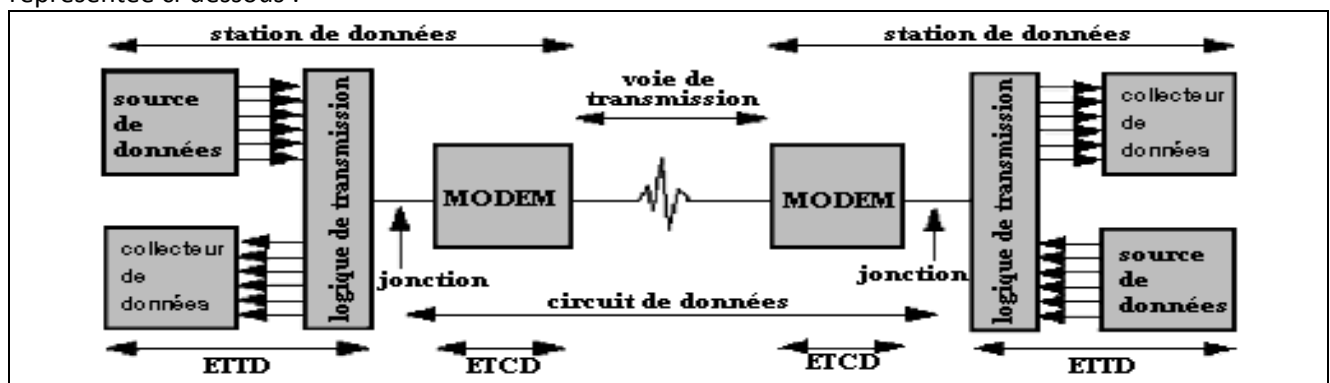
En outre, la couverture de communication sans fil n'exigeant aucun accès à un fil physique de support, des périphériques et utilisateurs non autorisés à accéder au réseau peuvent accéder à la transmission. La sécurité du réseau constitue par conséquent un composant essentiel de l'administration de réseau sans fil.

Normes	Bluetooth 802.15	802.11 (a, b, g, n), HiperLAN 2	802, 11, MMDS, LMDS	GSM, GPRS, CDMA, 2.5- 3G
Vitesse	<1 Mbits/s	1 - 54+ Mbits/s	22 Mbits/s+	10 - 384 Kbits/s
Plage	Courte	Moyenne	Moyenne - Longue	Longue
Applications	Peer to peer entre périphériques	Réseaux d'entreprise	Accès fixe à la boucle locale	Assistants numériques personnels, téléphones mobiles, accès cellulaire

2.2 Transmission longue distance sur cuivre

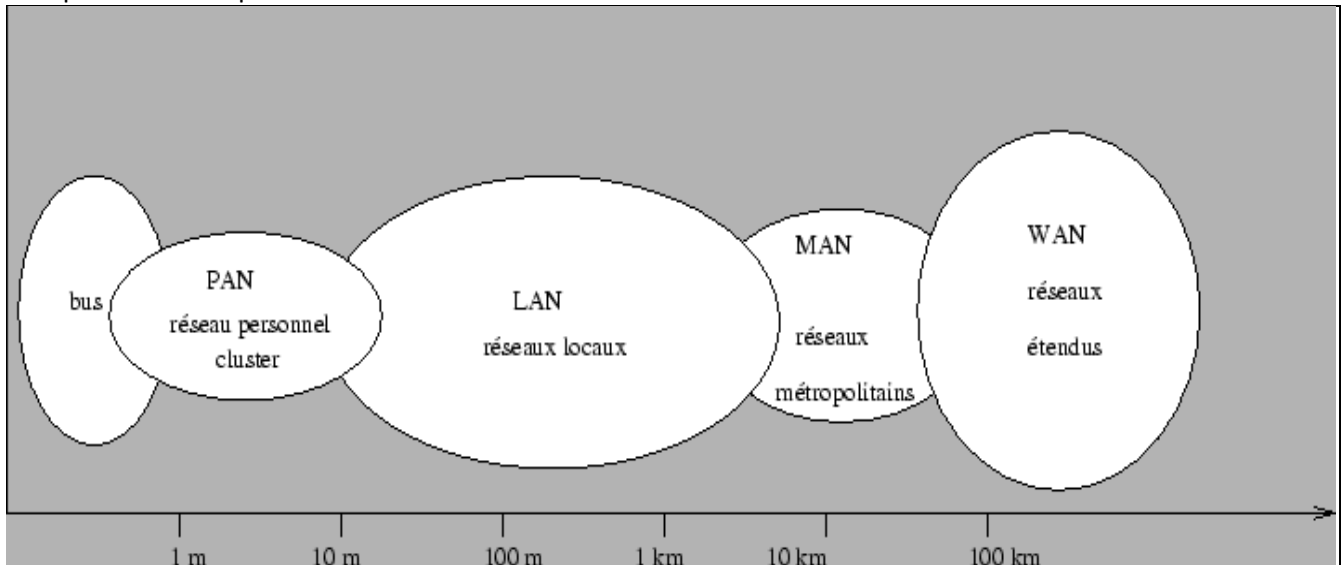
Un signal transmis en bande de base se dégrade rapidement à la distance. Ainsi les normes de câblage imposent une longueur maximale de 100 m pour une connexion directe sans amplification du signal.

Lorsque la longueur entre émetteur et récepteur devient trop importante, on utilise de manière quasi-générale la solution de la modulation. Une liaison télé-informatique classique (en modulation) est représentée ci-dessous :



2.3 Classification des réseaux de données

On peut faire une première classification des réseaux de données à l'aide de leur taille.



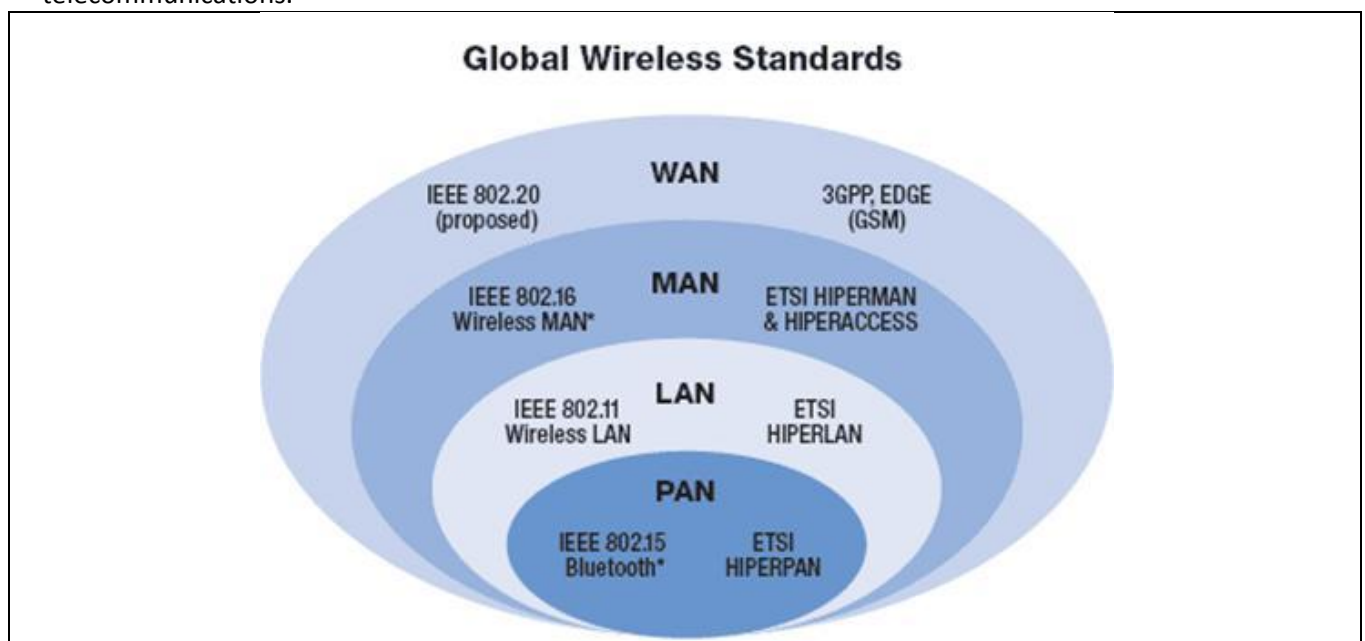
Les **bus** que l'on trouve dans un ordinateur pour relier ses différents composants (mémoires, périphériques d'entrée-sortie, processeurs, ...) peuvent être considérés comme des réseaux dédiés à des tâches très spécifiques. Certains réseaux industriels sont aussi appelés **bus de terrain** ou **réseau de terrain**.

Un **réseau personnel (Personal Area Network)** interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, un agenda électronique... Un cluster est un groupe d'unités centrales reliées entre elles de manière à agir comme un seul ordinateur soit pour pouvoir faire de la répartition de charges soit du calcul distribué.

Un **réseau local (Local Area Network)** peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.

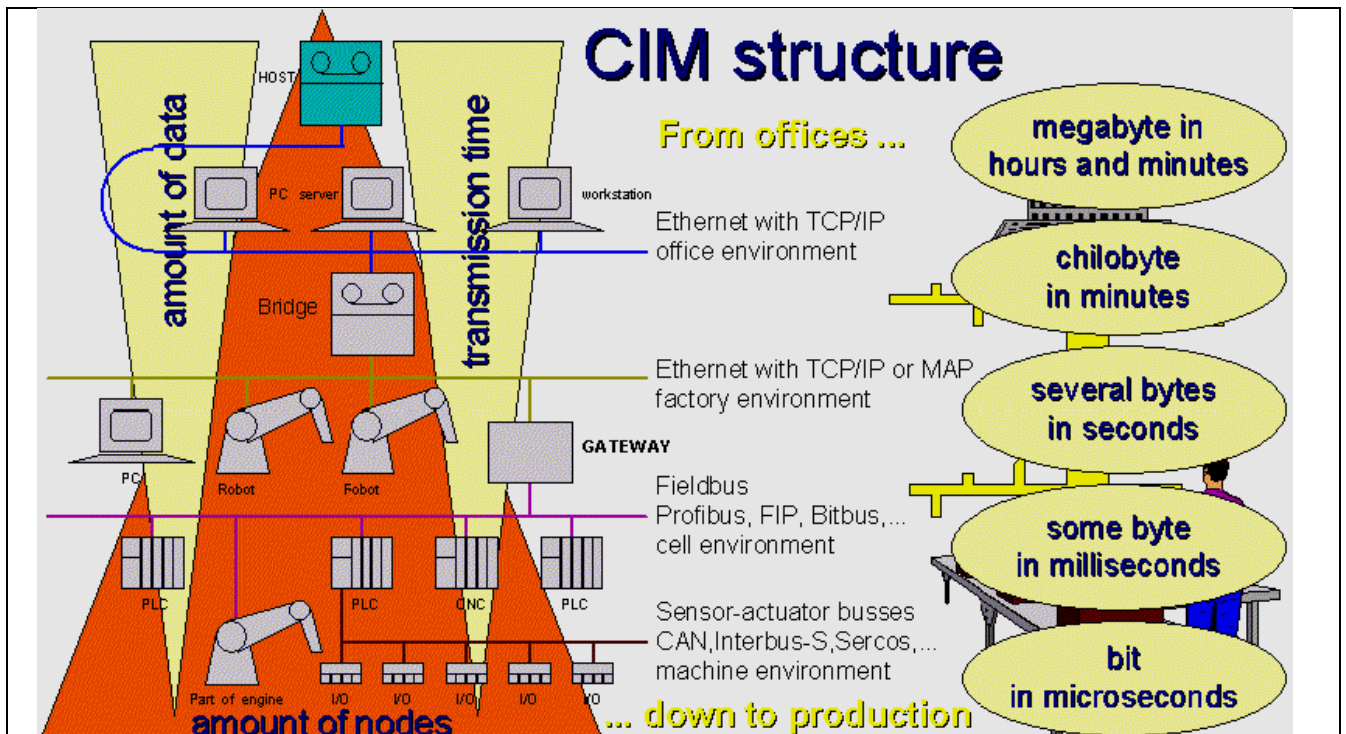
Un **réseau métropolitain (Metropolitan Area Network)** interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.

Un **réseau étendu (Wide Area Network)** permet de communiquer à l'échelle d'un pays, ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.



Un **réseau de terrain** permet à des systèmes électronique de communiquer entre eux sur des distances pouvant aller jusqu'à quelques **km** (électronique dans les véhicules, ateliers, usines, bâtiments, ouvrages d'arts...). Les éléments reliés au réseau sont des calculateurs, automates, capteurs, actionneurs,.... Il existe deux types de réseaux de terrain : les standards de fait (**Interbus-S, ASI, Lonworks**) et les standards internationaux (**WorldFip, Profibus, ...**). Tous les réseaux de terrain ont un ancêtre commun : la **boucle de courant 4-20mA**.

En milieu industriel, de nombreux type de réseaux de données sont mis en œuvre. On utilise le modèle de la pyramide CIM (Computer Integrated Manufacturing) pour déterminer la meilleure stratégie d'implantation en fonction du volume et du type de données à traiter, du nombre de nœuds à interconnecter et du besoin de rapidité de transmission.



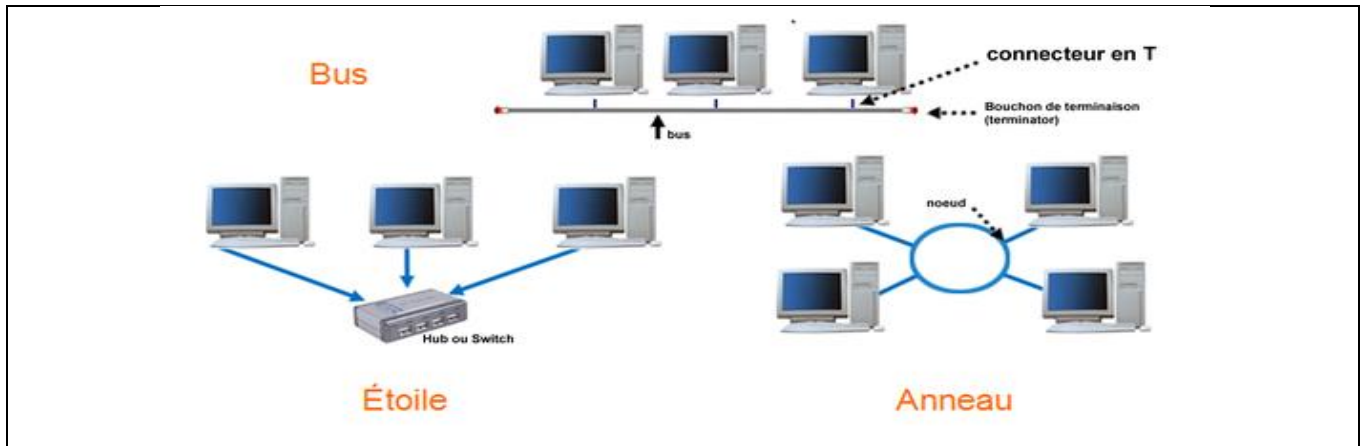
NIVEAUX		FONCTIONS	TYPES DE MESSAGES		TEMPS DE REACTION
USINE	4	gestion centrale	fichiers	4	heures/jours
ATELIER	3	gestion de production	tables, fichiers	3	secondes/minutes
CELLULE	2	contrôle-commande	variables, évènements	2	secondes
MACHINE	1	automatismes robots	octets	1	x100 ms
TERRAIN	0	capteurs, actionneurs	bits	0	milli-seconde

2.4 Topologie des réseaux

La manière dont sont interconnectées les machines est appelée « topologie ». On distingue la topologie physique (la configuration spatiale, visible, du réseau) de la « topologie logique ». La topologie logique représente la manière dont les données transitent dans les câbles.

Aujourd'hui, la topologie logique la plus courante est **Ethernet**.

Les principales topologies physiques sont les topologies en bus, en étoile et en anneau.



- **Topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

Cette topologie est obsolète dans les réseaux de données mais couramment utilisé dans les réseaux de terrain.

- **Topologie en étoile**

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé **switch (commutateur)**. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du commutateur sans pour autant paralyser le reste du réseau.

- **Topologie en anneau**

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre-eux va "avoir la parole" successivement.

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé **MAU, Multistation Access Unit**) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.

Sur les réseaux de données, c'est la topologie en étoile qui la plus répandue.

3 Fonctionnement d'un réseau

3.1 Le modèle de référence OSI

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés (**SNA** d'**IBM**, **DECnet** de **DEC**, **DSA** de **Bull**, **TCP/IP** du **DoD**,...) et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux «propriétaires» si une norme internationale n'était pas établie. Cette norme établie par l'**International Standard Organization (ISO)** est la norme **Open System Interconnection (OSI)**, interconnexion de systèmes ouverts).

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de constructeurs différents.

Le modèle de référence OSI est une représentation abstraite en couches servant de guide à la conception des protocoles réseau. Il divise le processus de réseau en sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques.

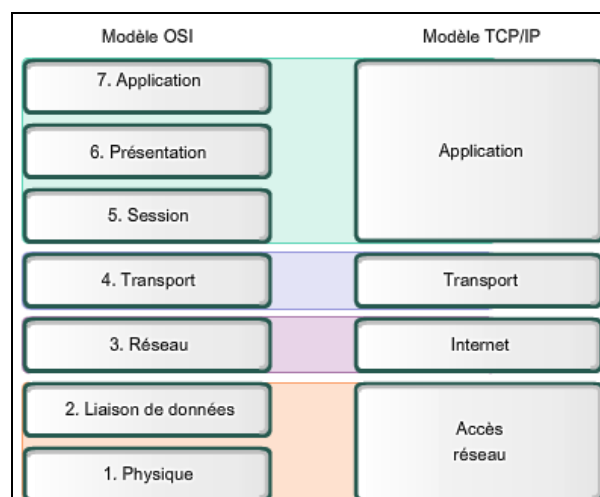
7- Application	La couche application permet d'obtenir une connectivité de bout en bout entre des individus dans le réseau humain à l'aide de réseau de données.
6- Présentation	La couche présentation fournit une représentation commune des données transférées entre des services de la couche application.
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 rassembler les données de communications individuelles entre périphériques finaux.
3- Routage	La couche réseau fournit des services pour échanger les parties de données individuelles sur le réseau entre des périphériques terminaux identifiés.
2- Liaison	Les protocoles de la couche liaison de données décrivent des méthodes d'échanges de trames de données entre des périphériques sur un support commun.
1- Physique	Les protocoles de la couche physique décrivent les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

Malheureusement, du fait de la rapidité avec laquelle Internet basé sur TCP/IP a été adopté, ainsi que de la vitesse avec laquelle il s'est développé, le développement et l'acceptation de la suite de protocoles OSI sont restés à la traîne. Même si peu de protocoles développés à l'aide des spécifications OSI font l'objet d'une utilisation répandue aujourd'hui, le modèle OSI à sept couches a apporté des contributions essentielles au développement d'autres protocoles et produits pour tous les types de nouveaux réseaux.

3.2 Comparaison des modèles OSI et TCP/IP

Les protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle de référence OSI. Dans le modèle OSI, la couche d'accès réseau et la couche application du modèle TCP/IP sont encore divisées pour décrire des fonctions discrètes qui doivent intervenir au niveau de ces couches.

Au niveau de la couche d'accès au réseau, la suite de protocoles TCP/IP ne spécifie pas quels protocoles utiliser lors de la transmission à travers un support physique ; elle décrit uniquement la remise depuis la couche Internet aux protocoles réseau physiques.



Les couches OSI 1 et 2 traitent des procédures nécessaires à l'accès aux supports et des moyens physiques pour envoyer des données à travers un réseau.

Les protocoles qui constituent la suite de protocoles TCP/IP peuvent être décrits selon les termes du modèle de référence OSI. Dans le modèle OSI, la couche d'accès réseau et la couche application du modèle TCP/IP sont encore divisées pour décrire des fonctions discrètes qui doivent intervenir au niveau de ces couches.

Au niveau de la couche d'accès au réseau, la suite de protocoles TCP/IP ne spécifie pas quels protocoles utiliser lors de la transmission à travers un support physique ; elle décrit uniquement la remise depuis la couche Internet aux protocoles réseau physiques. Les couches OSI 1 et 2 traitent des procédures nécessaires à l'accès aux supports et des moyens physiques pour envoyer des données à travers un réseau.

Les principaux parallèles entre les deux modèles de réseau se situent aux couches 3 et 4 du modèle OSI. La couche 3 du modèle OSI, la couche réseau, est utilisée presque partout dans le monde pour traiter et documenter la plage des processus qui interviennent dans tous les réseaux de données afin d'adresser et d'acheminer des messages à travers un interréseau. Le protocole IP est le protocole de la suite TCP/IP qui contient la fonctionnalité décrite à la couche 3.

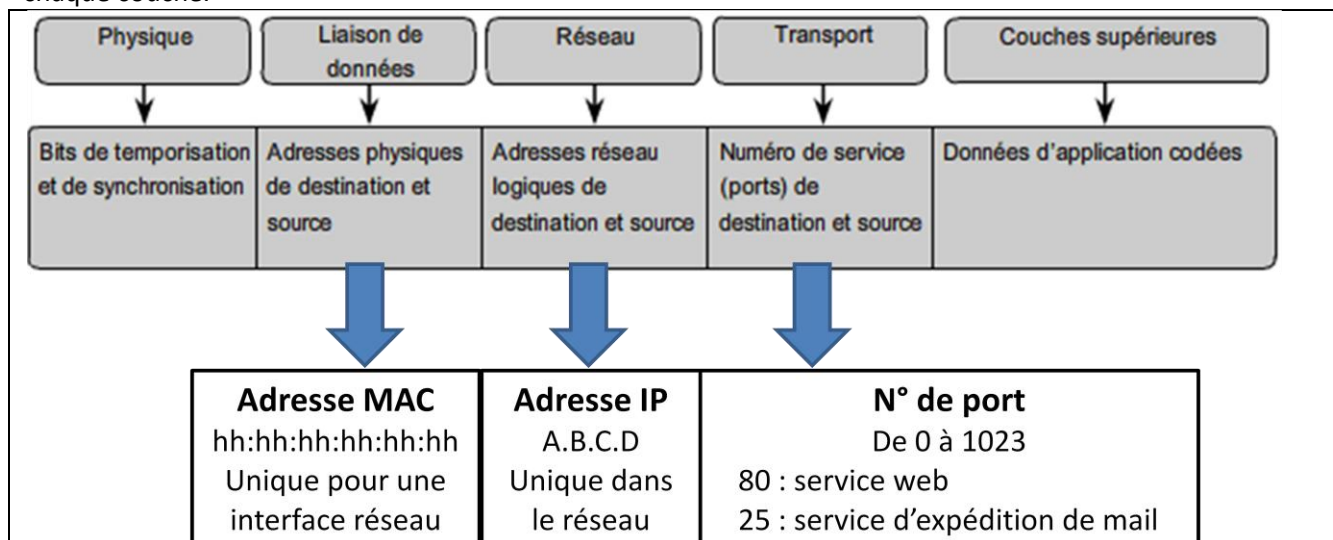
La couche 4, la couche transport du modèle OSI, sert souvent à décrire des services ou des fonctions générales qui gèrent des conversations individuelles entre des hôtes source et de destination. Ces fonctions incluent l'accusé de réception, la reprise sur erreur et le séquençement. À cette couche, les protocoles TCP/IP de contrôle de transmission et UDP fournissent les fonctionnalités nécessaires.

La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques à plusieurs applications d'utilisateur final. Les couches 5, 6 et 7 du modèle OSI sont utilisées en tant que références pour les développeurs et les éditeurs de logiciels d'application, afin de créer des produits qui doivent accéder aux réseaux pour des communications.

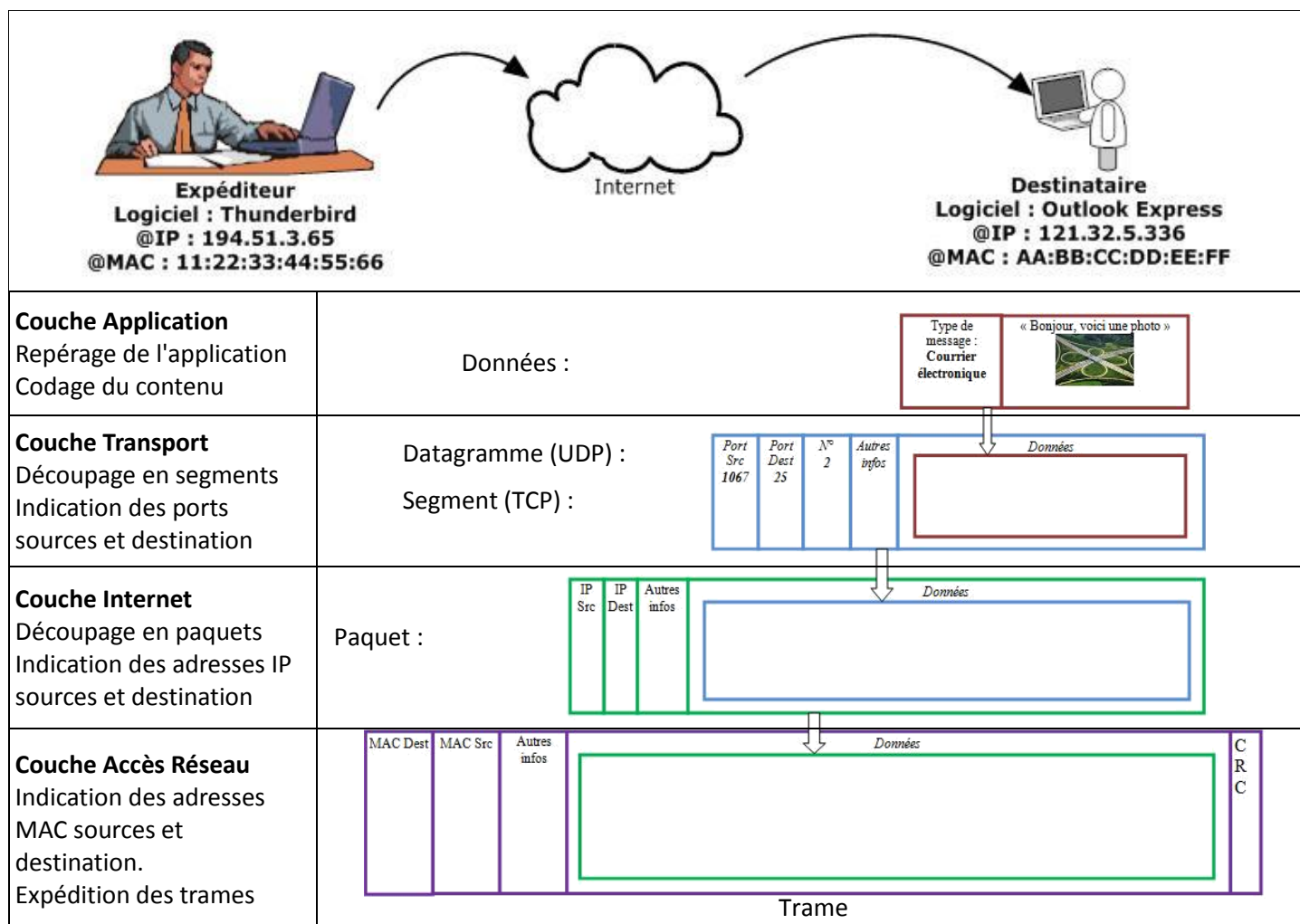
3.3 Principe de l'adressage et de l'encapsulation

Le modèle OSI décrit des processus de codage, de mise en forme, de segmentation et d'encapsulation de données pour la transmission sur le réseau. Un flux de données envoyé depuis une source vers une destination peut être divisé en parties et entrelacé avec des messages transmis depuis d'autres hôtes vers d'autres destinations. À n'importe quel moment, des milliards de ces parties d'informations se déplacent sur un réseau. Il est essentiel que chaque donnée contienne les informations d'identification suffisantes afin d'arriver à bonne destination.

Il existe plusieurs types d'adresses qui doivent être incluses pour livrer correctement les données depuis une application source exécutée sur un hôte à l'application de destination correcte exécutée sur un autre. En utilisant le modèle OSI comme guide, nous apercevons les différents identificateurs et adresses nécessaires à chaque couche.



Exemple : Un utilisateur veut envoyer un message (mail) conformément au schéma ci-dessous.



3.4 Adressage IPv4

3.4.1 Nécessité

Tous les périphériques appartenant à un même réseau doivent être identifiés de manière unique.

Bien que la majorité des adresses d'hôte IPv4 soient des adresses publiques utilisées dans les réseaux accessibles sur Internet, d'autres blocs d'adresses sont attribués à des réseaux qui ne nécessitent pas d'accès à Internet, ou uniquement un accès limité. Ces adresses sont appelées des adresses privées.

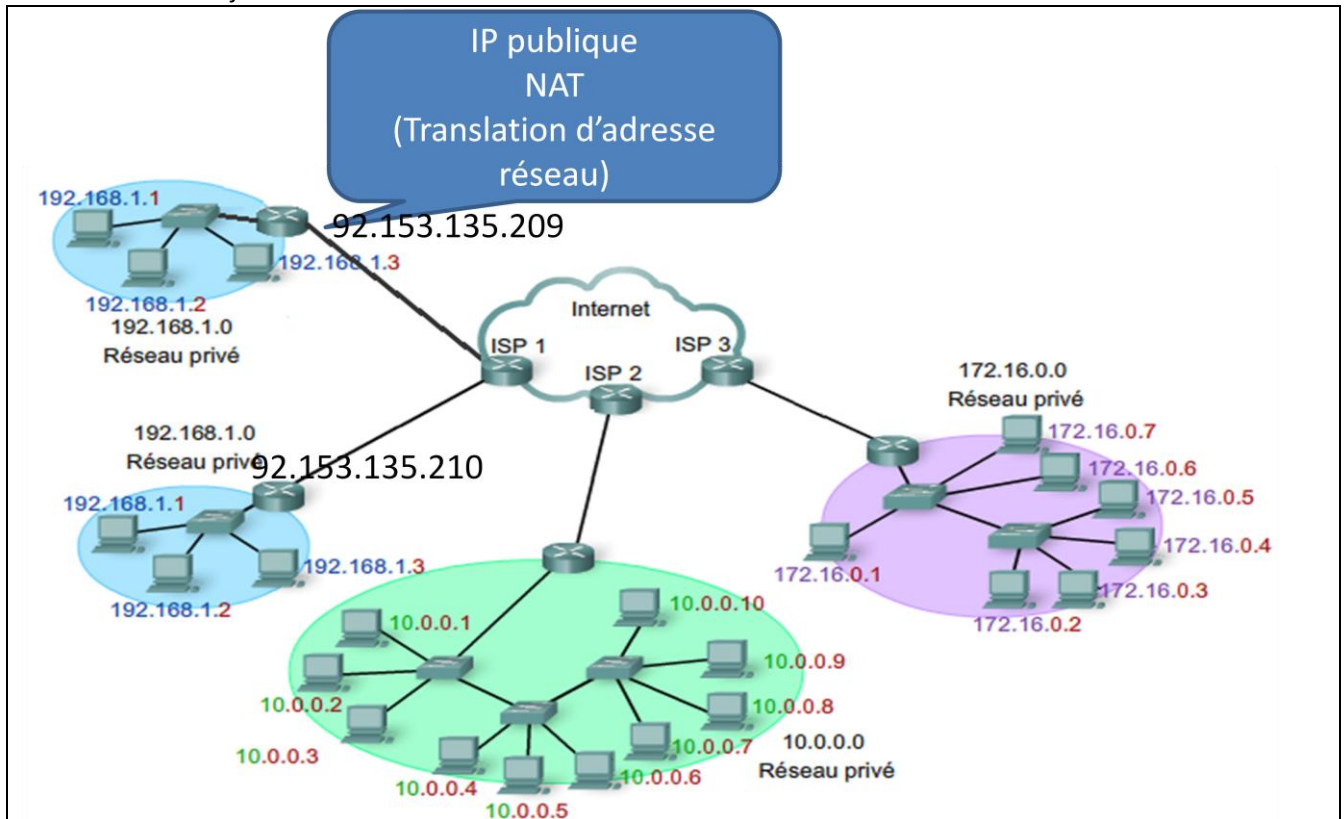
Les blocs d'adresses d'espace privé, comme illustrés, sont réservés aux réseaux privés. L'utilisation de ces adresses ne doit pas forcément être unique entre des réseaux externes. En règle générale, les hôtes qui ne nécessitent pas d'accès à Internet peuvent utiliser les adresses privées sans limitation. Toutefois, les réseaux internes doivent configurer des schémas d'adressage réseau pour garantir que les hôtes des réseaux privés utilisent des adresses IP qui sont uniques au sein de leur environnement de réseau.

Plusieurs hôtes de réseaux différents peuvent utiliser les mêmes adresses d'espace privé. Les paquets qui utilisent ces adresses comme source ou destination ne doivent pas être visibles sur Internet. Le routeur ou le périphérique pare-feu, en périphérie de ces réseaux privés, doivent bloquer ou traduire ces adresses. Même si ces paquets parvenaient sur Internet, les routeurs ne disposeraient pas de routes pour les acheminer vers le réseau privé en question.

Grâce à des services qui traduisent les adresses privées en adresses publiques, les hôtes d'un réseau privé peuvent accéder aux ressources présentes sur Internet. Appelés NAT (Network Address Translation), ces services peuvent être mis en œuvre sur un périphérique situé en périphérie du réseau privé.

Les services NAT permettent aux hôtes du réseau « d'emprunter » une adresse publique pour communiquer avec des réseaux externes. Bien que les services NAT soient associés à des limitations et à des problèmes de

performances, ils permettent aux clients de nombreuses applications d'accéder à des services sur Internet, sans difficulté majeure.



Dans la plupart des réseaux de données, l'immense majorité des hôtes sont des périphériques finaux, tels que des ordinateurs, des téléphones IP, des imprimantes et des assistants numériques personnels. Dans la mesure où ces hôtes représentent le plus grand nombre de périphériques au sein d'un réseau, le plus grand nombre d'adresses doit leur être attribué.

3.4.2 Attribution

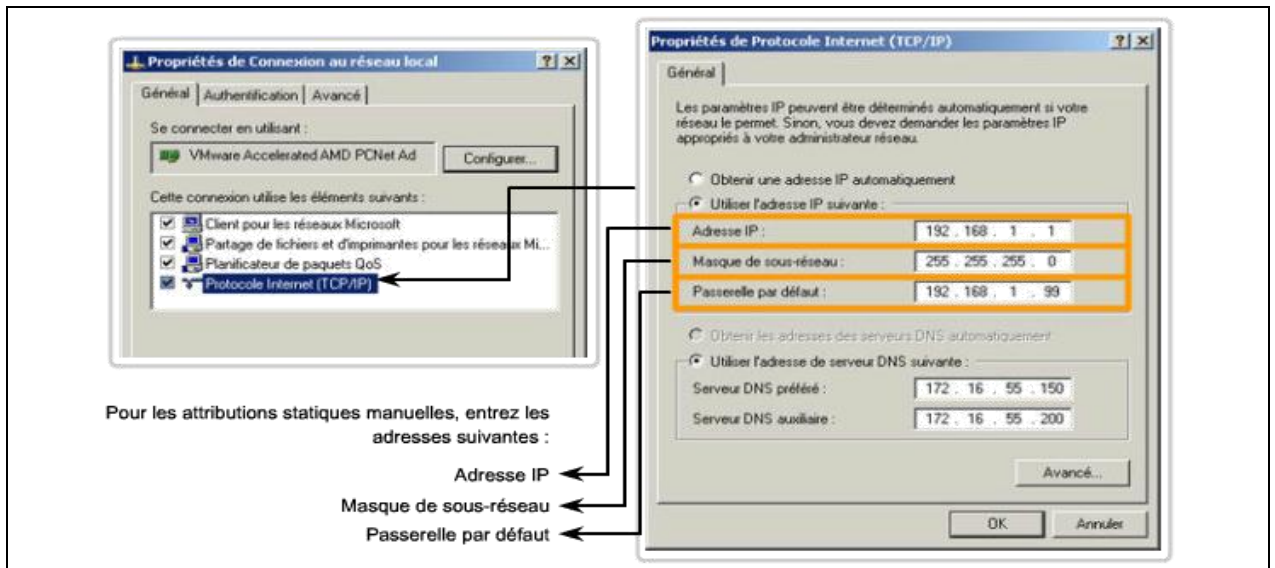
Les adresses IP peuvent être attribuées de manière statique ou de manière dynamique.

- **Attribution statique d'adresses**

Avec ce type d'attribution, l'administrateur réseau doit configurer manuellement les informations de réseau pour un hôte, comme indiqué dans la figure. Ces informations comportent, au minimum, l'adresse IP, le masque de sous-réseau et la passerelle par défaut.

Les adresses statiques présentent certains avantages sur les adresses dynamiques. Par exemple, elles conviennent pour les imprimantes, les serveurs et d'autres périphériques réseau, qui doivent être accessibles pour les clients d'un réseau. Si les hôtes ont l'habitude d'accéder à un serveur à une adresse IP particulière, cela peut poser des problèmes en cas de modification de cette adresse. De plus, l'attribution statique des informations d'adressage permet de mieux contrôler les ressources réseau. Toutefois, la configuration IP sur chaque hôte prend du temps.

Lorsque l'adressage IP statique est utilisé, il convient de tenir à jour une liste exacte des adresses IP attribuées à chaque périphérique. Ces adresses étant permanentes, en principe, elles ne seront pas réutilisées.



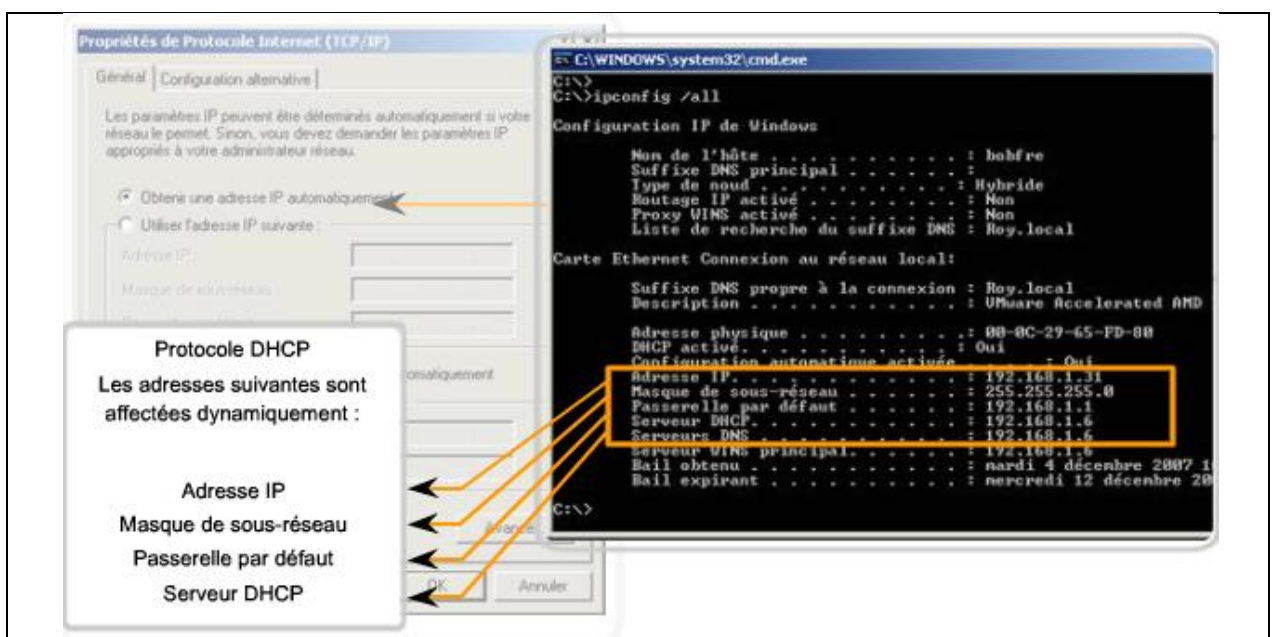
- **Attribution dynamique d'adresses**

En raison des difficultés associées à la gestion des adresses statiques, les périphériques des utilisateurs se voient attribuer leur adresse de manière dynamique, à l'aide du protocole DHCP (Dynamic Host Configuration Protocol), comme indiqué dans la figure.

Le protocole DHCP permet l'attribution automatique des informations d'adressage, telles que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et d'autres paramètres. La configuration du serveur DHCP nécessite qu'un bloc d'adresses appelé pool d'adresses soit défini de manière à être attribué aux clients DHCP d'un réseau. Les adresses attribuées à ce pool doivent être définies de manière à exclure toutes les adresses utilisées pour les autres types de périphérique.

Le protocole DHCP est généralement la méthode d'attribution d'adresses IP privilégiée pour les réseaux de grande taille, car le personnel de support du réseau est dégagé de cette tâche et le risque d'erreur de saisie est quasiment éliminé.

L'autre avantage de l'attribution dynamique réside dans le fait que les adresses ne sont pas permanentes pour les hôtes, elles sont uniquement « louées » pour une certaine durée. Si l'hôte est mis sous tension ou retiré du réseau, son adresse est renvoyée au pool et sera réutilisée. Cela est particulièrement intéressant pour les utilisateurs mobiles qui se connectent et se déconnectent d'un réseau.

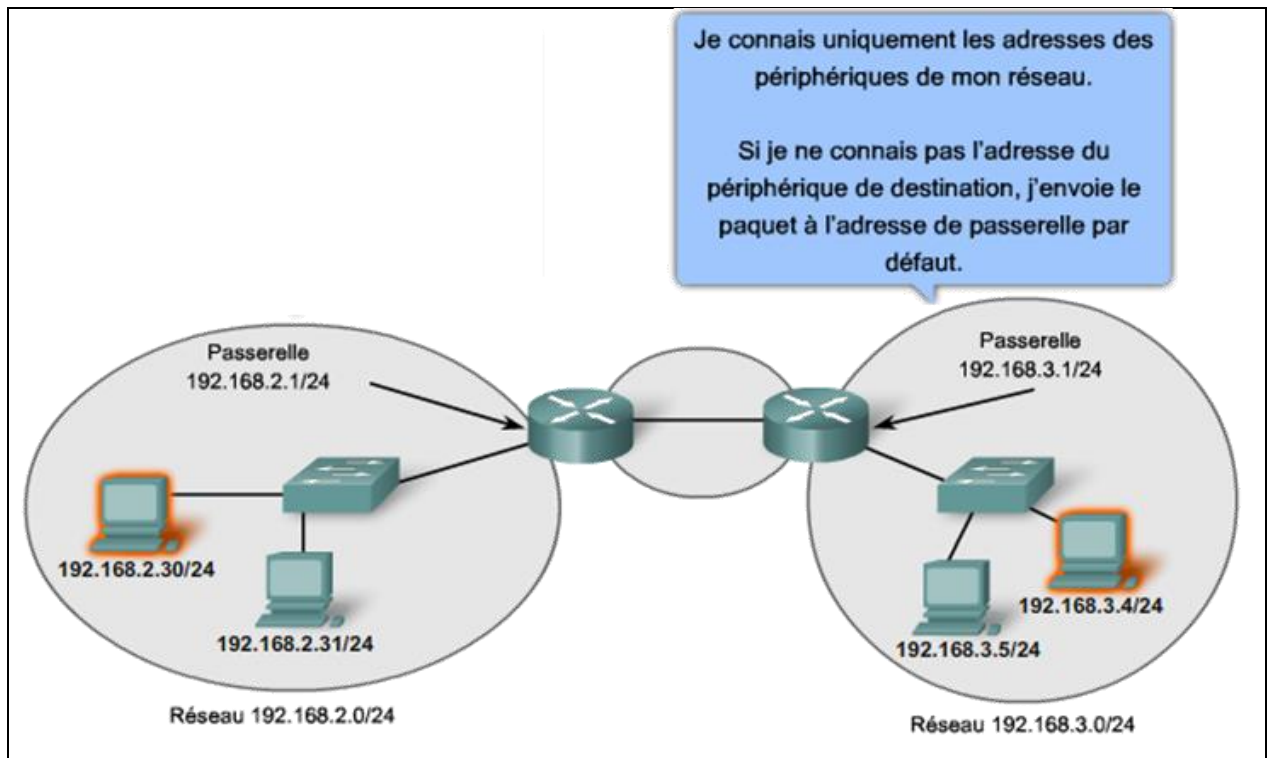


3.4.3 Passerelle par défaut

La passerelle, également appelée passerelle par défaut, est requise pour envoyer un paquet en dehors du réseau local.

Au sein d'un même réseau, les hôtes communiquent entre eux sans nécessiter de périphérique intermédiaire. Quand un hôte doit communiquer avec un autre réseau, un périphérique intermédiaire sert de passerelle avec l'autre réseau.

Cette passerelle est une interface de routeur connectée au réseau local. L'interface de la passerelle a une adresse IP appartenant au réseau auquel elle est connectée. Les hôtes sont configurés pour reconnaître cette adresse comme étant leur passerelle.



3.4.4 Constitution d'une adresse IPv4

Une adresse IPv4 est composée de 4 octets soit 32 bits. La notation couramment utilisée pour représenter ces adresses est notation « décimale pointée ».

Par exemple, l'adresse **10101100 00010000 00000100 00010100**

est exprimée en format décimal pointé de la manière suivante : **172.16.4.20**

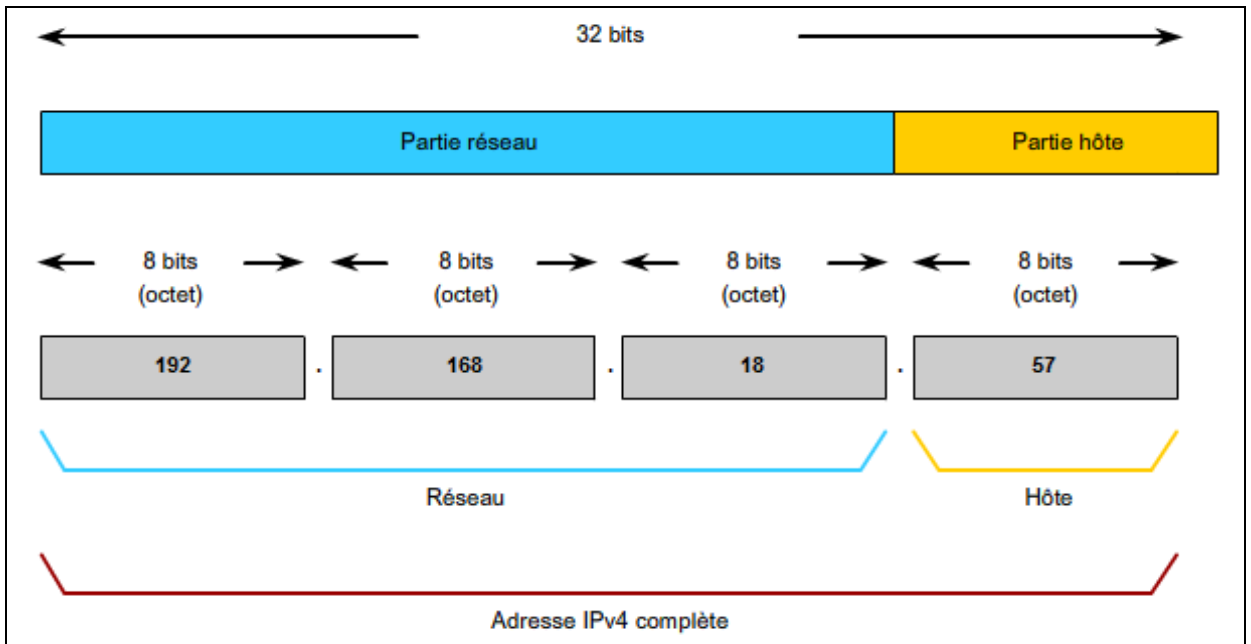
- **Parties réseau et hôte**

Pour chaque adresse IPv4, une partie des bits d'ordre haut représente l'adresse réseau. Au niveau de la couche 3, un réseau se définit par un groupe d'hôtes dont la partie adresse réseau de l'adresse contient la même configuration binaire.

Bien que l'ensemble des 32 bits définisse l'adresse IPv4 d'un hôte, un nombre variable de bits constitue la partie hôte de l'adresse. Le nombre de bits contenus dans la partie hôte détermine le nombre d'hôtes possible sur un réseau.

Par exemple, si un réseau particulier doit contenir au minimum 200 hôtes, il faut utiliser suffisamment de bits dans la partie hôte pour pouvoir représenter au moins 200 configurations binaires différentes.

Pour attribuer une adresse unique à 200 hôtes, il convient d'utiliser le dernier octet dans son intégralité. Avec 8 bits, nous pouvons obtenir un total de 256 configurations binaires différentes. Nous en déduisons que les bits des trois premiers octets représentent la partie réseau.

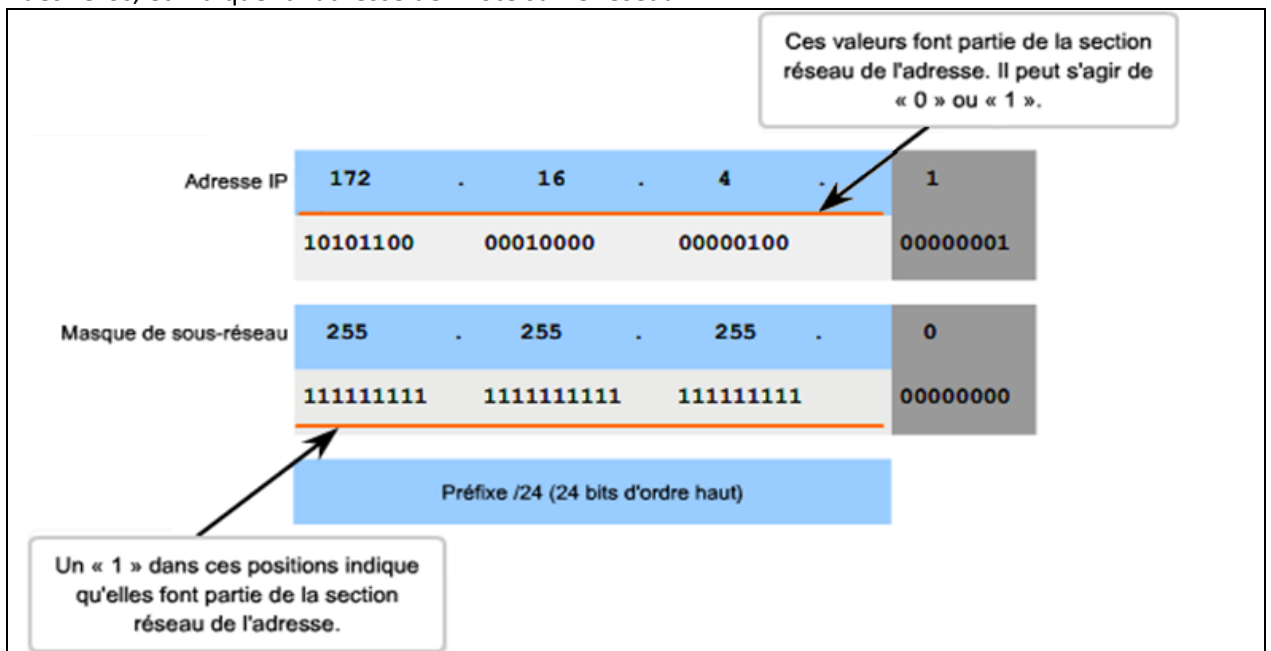


3.4.5 Masque de sous-réseau

Pour définir les parties réseau et hôte d’une adresse, les périphériques utilisent une configuration de 32 bits appelée « masque de sous-réseau ». Le masque de sous-réseau s’exprime dans le même format décimal pointé que celui de l’adresse IPv4. Le masque de sous-réseau est créé en plaçant le nombre binaire 1 dans chaque position de bit qui représente la partie réseau et en plaçant le nombre binaire 0 dans chaque position de bit qui représente la partie hôte.

Le masque de sous-réseau est aussi appelé « préfixe ». Ce dernier un nombre de 0 à 32 qui représente le nombre de bits à 1 dans le masque de sous-réseau. Il représente la même chose : la partie réseau d’une adresse.

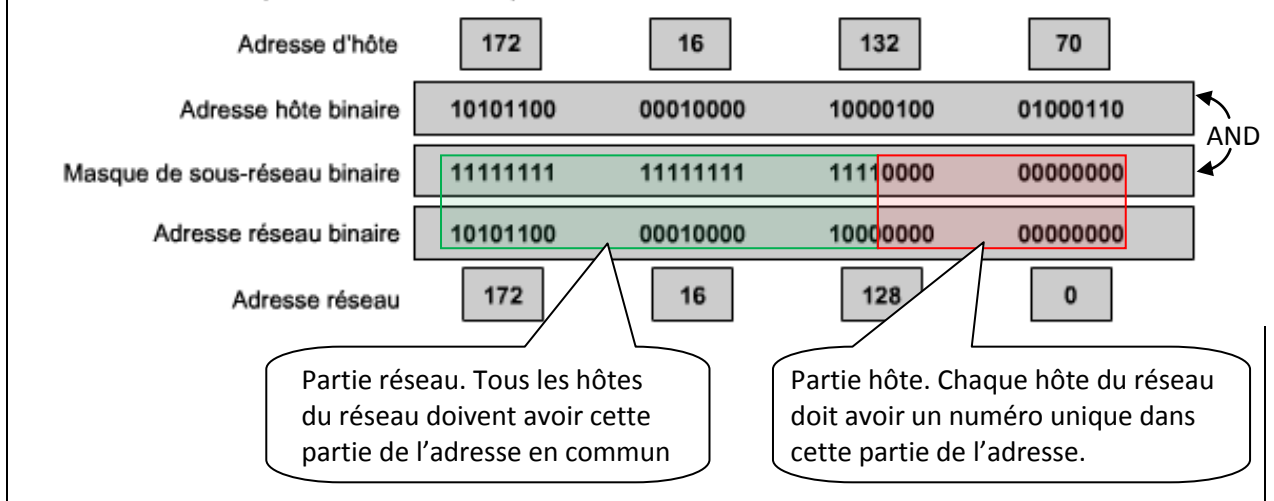
Par exemple, le préfixe /24, correspondant au masque de sous-réseau 255.255.255.0 (11111111.11111111.11111111.00000000). Les bits restants (à droite) du masque de sous-réseau sont des zéros, et indiquent l’adresse de l’hôte sur le réseau.



Exemple : Déterminer l’adresse de réseau de l’hôte 172.16.132.70/20

Pour déterminer l’adresse du réseau auquel appartient un hôte, on effectue le masquage de son adresse IP par son masque de sous-réseau. Le masquage est obtenu en effectuant une opération AND bit à bit entre les deux adresses :

Utilisation du masque de sous-réseau pour déterminer l'adresse réseau de l'hôte 172.16.132.70/20



Conclusion : L'hôte **172.16.132.70/20** fait partie du réseau **172.16.128.0/20**

Ce réseau a les caractéristiques suivantes :

Adresse de réseau	172 . 16 . 128 . 0
Adresse du premier hôte	172 . 16 . 128 . 1
...	...
Adresse du dernier hôte	172 . 16 . 143 . 254
Dernière adresse dans le réseau	172 . 16 . 143 . 255

Dernière adresse de réseau = adresse de diffusion

L'adresse de diffusion IPv4 est une adresse spécifique, attribuée à chaque réseau. Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour cela, un hôte peut envoyer un seul paquet adressé à l'adresse de diffusion du réseau.

L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau. Il s'agit de l'adresse dans laquelle les bits de la partie hôte sont tous des « 1 ».

Réseau			Hôte
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001

3.4.6 Les anciennes classes réseau

À l'origine, la spécification RFC1700 regroupait les plages d'adresses en classes appelées classe A, B et C. Elle a également établi des adresses de classe D (multidiffusion) et de classe E (expérimentales).

Remarque : Un hôte peut établir une connexion de type :

- Monodiffusion (unicast) : « Je parle directement à quelqu'un ».
- Diffusion (broadcast) : « Je parle à tout le monde ».
- Multidiffusion (multicast) : « Je parle à un groupe restreint ».

Les classes d'adresse monodiffusion A, B et C définissaient des réseaux d'une certaine taille, ainsi que des blocs d'adresses particuliers pour ces réseaux. Une entreprise ou une administration se voyait attribuer un bloc d'adresses entier de classe A, B ou C. L'utilisation de l'espace d'adressage s'appelait adressage par classe.

- **Blocs d'adresses A**

Un bloc d'adresses de classe A a été créé pour prendre en charge les réseaux de très grande taille, comportant plus de 16 millions d'adresses d'hôte. Les adresses IPv4 de classe A utilisaient un préfixe /8 invariable, le premier octet indiquant l'adresse réseau. Les trois octets restants correspondaient aux adresses d'hôte.

Afin de réserver un espace d'adresses aux classes d'adresse restantes, le bit de poids fort de l'octet de valeur supérieure devait être un zéro dans toutes les adresses de classe A. De ce fait, seuls 128 réseaux de classe A, de 0.0.0.0 /8 à 127.0.0.0 /8, étaient possibles, avant de se servir des blocs d'adresses réservées. Bien que les adresses de classe A réservaient la moitié de l'espace d'adressage, elles ne pouvaient être attribuées qu'à 120 entreprises ou administrations, en raison de leur limite de 128 réseaux.

- **Blocs d'adresses B**

L'espace d'adressage de classe B a été créé pour répondre aux besoins des réseaux de taille moyenne ou de grande taille, comportant plus de 65 000 hôtes. Les adresses IP de classe B utilisaient les deux premiers octets pour indiquer l'adresse réseau. Les deux octets suivants correspondaient aux adresses d'hôte. Comme avec la classe A, l'espace d'adressage pour les classes d'adresses restantes devait être réservé.

Pour les adresses de classe B, les deux bits de poids fort du premier octet étaient 10. Cela limitait le bloc d'adresses de la classe B à 128.0.0.0 /16-191.255.0.0 /16. Les classes B étaient attribuées plus efficacement que les adresses de classe A, car elles répartissaient 25 % de l'espace d'adressage IPv4 total entre environ 16 000 réseaux.

- **Blocs d'adresses C**

L'espace d'adressage de la classe C était le plus disponible des anciennes classes d'adresses. Cet espace d'adressage était réservé aux réseaux de petite taille, comportant 254 hôtes au maximum.

Les blocs d'adresses de classe C utilisaient le préfixe /24. Ainsi, un réseau de classe C ne pouvait utiliser que le dernier octet pour les adresses d'hôte, les trois premiers octets correspondant à l'adresse réseau.

Les blocs d'adresses de classe C réservaient l'espace d'adressage à la classe D (multidiffusion) et à la classe E (expérimentales) à l'aide d'une valeur fixe de 110 pour les trois bits les plus significatifs du premier octet. Cela limitait le bloc d'adresses de classe C à 192.0.0.0 /16 - 23.255.255.255 /16. Bien qu'il occupait seulement 12,5 % de l'espace d'adressage IPv4 total, il pouvait attribuer des adresses à 2 millions de réseaux.

- **Limites de l’adressage par classe**

Les besoins de certaines entreprises ou organisations n’étaient pas toujours couverts par ces trois classes. L’attribution par classe des adresses IP gaspillait souvent de nombreuses adresses, ce qui épuisait la disponibilité des adresses IPv4. Par exemple, une entreprise avec un réseau de 260 hôtes devait se voir attribuer une adresse de classe B avec plus de 65 000 adresses.

Bien que ce système par classe ait été abandonné à la fin des années 90, il n’a pas entièrement disparu dans certains des réseaux modernes. Par exemple, lorsque vous attribuez une adresse IPv4 à un ordinateur, le système d’exploitation examine l’adresse en question pour déterminer si elle appartient à la classe A, B ou C. Le système d’exploitation devine ensuite le préfixe utilisé par cette classe et attribue le masque de sous-réseau correspondant.

Quelques protocoles de routage font également ce type de supposition de masque. Lorsque ces protocoles de routage reçoivent une route annoncée, ils peuvent prévoir la longueur de préfixe en fonction de la classe de l’adresse.

Classe d’adresses	Plage du premier octet (décimal)	Bits du premier octet (les bits verts ne changent pas)	Parties réseau (N) et hôte (H) de l’adresse	Masque de sous-réseau par défaut (décimal et binaire)	Nombre de réseaux et d’hôtes possibles par réseau
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 réseaux (2 ⁷) 16 777 214 hôtes par réseau (2 ²⁴⁻²)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16 384 réseaux (2 ¹⁴) 65 534 hôtes par réseau (2 ¹⁶⁻²)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2 097 150 réseaux (2 ²¹) 254 hôtes par réseau (2 ⁸⁻²)
D	224-239	11100000-11101111	S.O. (multidiffusion)		
E	240-255	11110000-11111111	S.O. (expérimental)		

3.4.7 Plages d’adresse IPv4 exclues de l’adressage des hôtes

Pour diverses raisons, certaines adresses ne peuvent pas être attribuées à des hôtes. D’autres le peuvent, mais avec des restrictions concernant la façon dont les hôtes interagissent avec le réseau.

- **Adresses réseau et de diffusion**

La première et la dernière adresse ne peuvent pas être attribuées à des hôtes. Il s’agit respectivement de l’adresse réseau et de l’adresse de diffusion.

- **Route par défaut**

La route IPv4 par défaut est représentée de la manière suivante : 0.0.0.0.

La route par défaut est utilisée comme route « dernier recours » lorsqu’aucune route plus spécifique n’est disponible. L’utilisation de cette adresse réserve également toutes les adresses de la plage 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

- **Bouclage**

L’adresse de bouclage IPv4 127.0.0.1 est une autre adresse réservée. Il s’agit d’une adresse spéciale que les hôtes utilisent pour diriger le trafic vers eux-mêmes. L’adresse de bouclage crée un moyen rapide, pour les applications et les services TCP/IP actifs sur le même périphérique, de communiquer entre eux. En utilisant l’adresse de bouclage à la place de l’adresse d’hôte IPv4 attribuée, deux services actifs sur le même hôte peuvent contourner les couches les plus basses de la pile TCP/IP. Vous pouvez également envoyer une requête ping à l’adresse de bouclage afin de tester la configuration TCP/IP de l’hôte local.

Bien que seule l’adresse 127.0.0.1 soit utilisée, les adresses de la plage 127.0.0.0-127.255.255.255 sont réservées. Toutes les adresses de cette plage sont envoyées en boucle sur l’hôte local. Aucune des adresses de cette plage ne devrait jamais apparaître sur un réseau quel qu’il soit.

- **Adresses locales-liens**

Les adresses IPv4 du bloc d'adresses 169.254.0.0 à 169.254.255.255 (169.254.0.0 /16) sont conçues pour être des adresses locales-liens. Elles peuvent être automatiquement attribuées à l'hôte local par le système d'exploitation, dans les environnements où aucune configuration IP n'est disponible. Celles-ci peuvent être utilisées dans un réseau Peer to peer de petite taille ou pour un hôte qui ne peut pas obtenir d'adresse automatiquement auprès d'un serveur DHCP.

- **Les adresses de multidiffusion**

Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 - 224.0.0.255 sont des adresses de liaison locales réservées. Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local.

- **Les adresses expérimentales**

La plage d'adresses expérimentales IPv4 s'étend de 240.0.0.0 à 255.255.255.254. Actuellement, ces adresses sont répertoriées comme étant réservées pour une utilisation future (RFC 3330). Cela laisse à penser qu'elles pourraient être converties en adresses utilisables. Pour l'instant, leur utilisation dans des réseaux IPv4 n'est pas permise. Toutefois, ces adresses pourraient s'appliquer à la recherche.

- **Les adresses publiques**

Les adresses publiques sont routables sur internet et ne peuvent par conséquent pas être utilisées sur un réseau privé. Ces adresses étaient à l'origine réparties sur les trois classes de monodiffusion (A, B et C).

Enfin, Les seules adresses utilisables dans un réseau privé sont les suivantes :

- 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)

3.5 Exercices : Adressage IP

3.5.1 Définition de l'adresse réseau

Adresse d'hôte	10	91	172	38
Masque de sous-réseau	255	255	192	0
Adresse d'hôte en binaire	00001010	01011011	10101100	00100110
Masque de sous-réseau en binaire	11111111	11111111	11000000	00000000
Adresse réseau en binaire				
Adresse réseau en décimale				

S'exercer : CCNA1 Notion de base sur les réseaux – exercices chapitre 6.5.4

3.5.2 Calcul du nombre d'hôtes disponible

Adresse réseau	10	0	0	0
Masque de sous-réseau	255	255	252	0
Adresse réseau en binaire	00001010	00000000	00000000	00000000
Masque de sous-réseau en binaire	11111111	11111111	11111100	00000000
Nombre d'hôtes	<input type="text"/>			

S'exercer : CCNA1 Notion de base sur les réseaux – exercices chapitre 6.5.5

3.5.3 Calcul des adresses réseau, d'hôte et de diffusion

Adresse/préfixe donnés **175.5.152.64 /24**
de

Pour chaque ligne, entrez les valeurs du type d'adresse.

Type d'adresse	Entrez le DERNIER octet en binaire	Entrez le DERNIER octet en notation décimale	Entrez l'adresse complète en notation décimale
Réseau	<input type="text"/>	<input type="text"/>	<input type="text"/>
Diffusion	<input type="text"/>	<input type="text"/>	<input type="text"/>
Première adresse d'hôte utilisable	<input type="text"/>	<input type="text"/>	<input type="text"/>
Dernière adresse d'hôte utilisable	<input type="text"/>	<input type="text"/>	<input type="text"/>

S'exercer : CCNA1 Notion de base sur les réseaux – exercices chapitre 6.2.2

3.5.4 Calcul de la plage d'adresse utilisable pour les hôtes et de l'adresse de diffusion

Adresse réseau en décimale	10	57	128	0
Masque de sous-réseau en décimale	255	255	224	0
Adresse réseau en binaire	00001010	00111001	10000000	00000000
Masque de sous-réseau en binaire	11111111	11111111	11100000	00000000
Première adresse IP d'hôte utilisable en décimale				
Dernière adresse IP d'hôte utilisable en décimale				
Adresse de diffusion en décimale				
Prochaine adresse réseau en décimale				

S'exercer : CCNA1 Notion de base sur les réseaux – exercices chapitre 6.5.6

3.6 Principe du routage

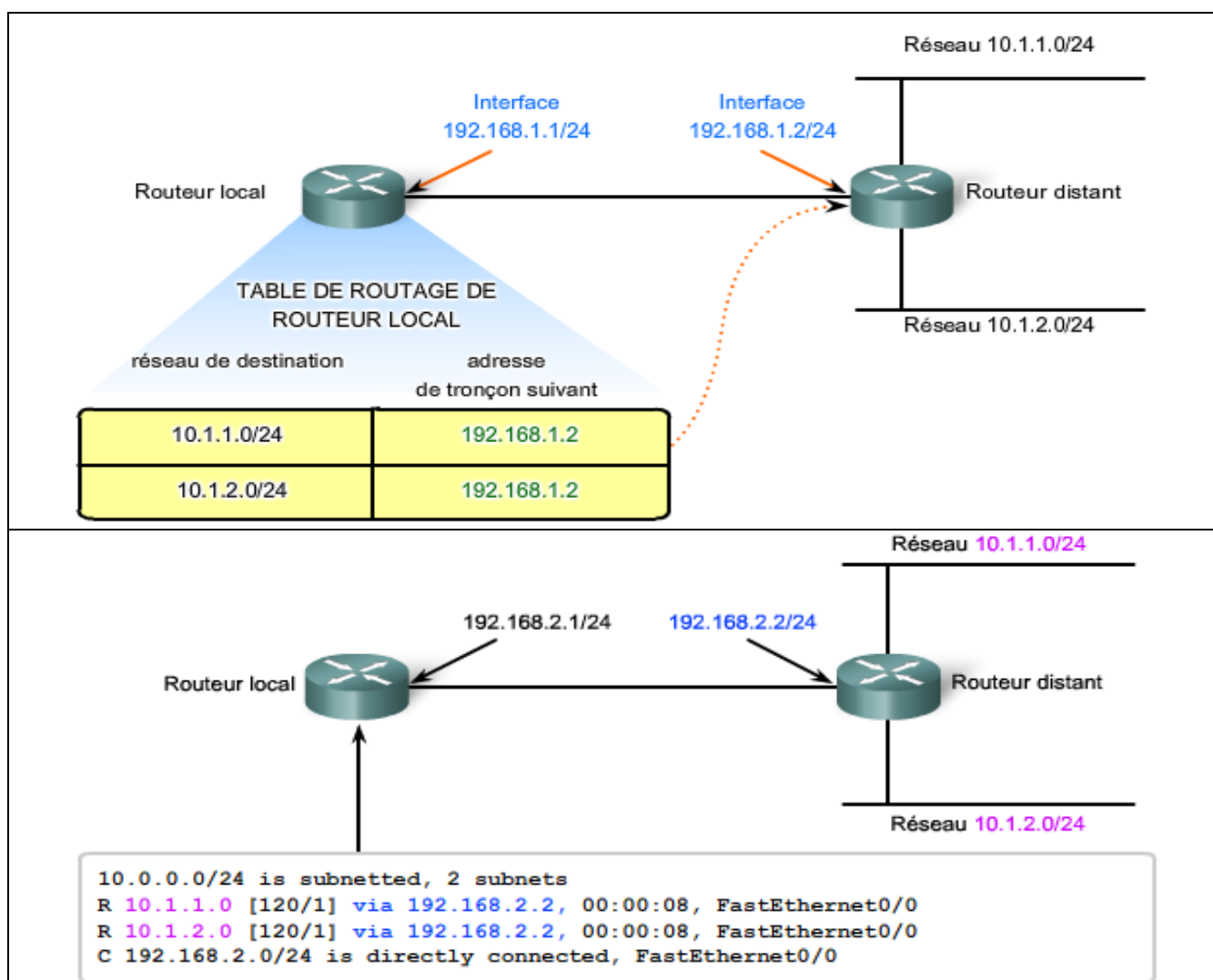
Si l'hôte de destination se trouve sur le même réseau que l'hôte source, le paquet est acheminé entre les deux hôtes sur le support local sans nécessiter de routeur.

Cependant, si l'hôte de destination et l'hôte source ne se trouvent pas sur le même réseau, le réseau local achemine le paquet de la source vers son routeur de passerelle. Le routeur examine la partie réseau de l'adresse de destination du paquet et achemine le paquet à l'interface appropriée. Si le réseau de destination est connecté directement à ce routeur, le paquet est transféré directement vers cet hôte. Si le réseau de destination n'est pas connecté directement, le paquet est acheminé vers un second routeur qui constitue le routeur de tronçon suivant.

Le transfert du paquet devient alors la responsabilité de ce second routeur. De nombreux routeurs ou sauts tout au long du chemin peuvent traiter le paquet avant qu'il n'atteigne sa destination.

Aucun paquet ne peut être acheminé sans route. Que le paquet provienne d'un hôte ou qu'il soit acheminé par un routeur intermédiaire, le routeur a besoin d'une route pour savoir où l'acheminer. S'il n'existe aucune route vers un réseau de destination, le paquet ne peut pas être transféré. Les routeurs utilisent des tables de routage qui contiennent les routes qu'ils connaissent. Ces tables peuvent être construites manuellement (routage statique) ou automatiquement (routage dynamique). Dans ce cas, les routeurs s'appuient sur des protocoles spécifiques comme le protocole RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), ...

Le réseau de destination peut être éloigné de la passerelle par un certain nombre de routeurs ou de sauts. La route vers ce réseau n'indique que le routeur de tronçon suivant vers lequel le paquet doit être transféré, et non le routeur final. Le processus de routage utilise une route de la table de routage pour mapper l'adresse du réseau de destination au tronçon suivant, puis transfère le paquet à cette adresse de tronçon suivant.



3.7 Principe du nommage – Service DNS (Domaine Name System)

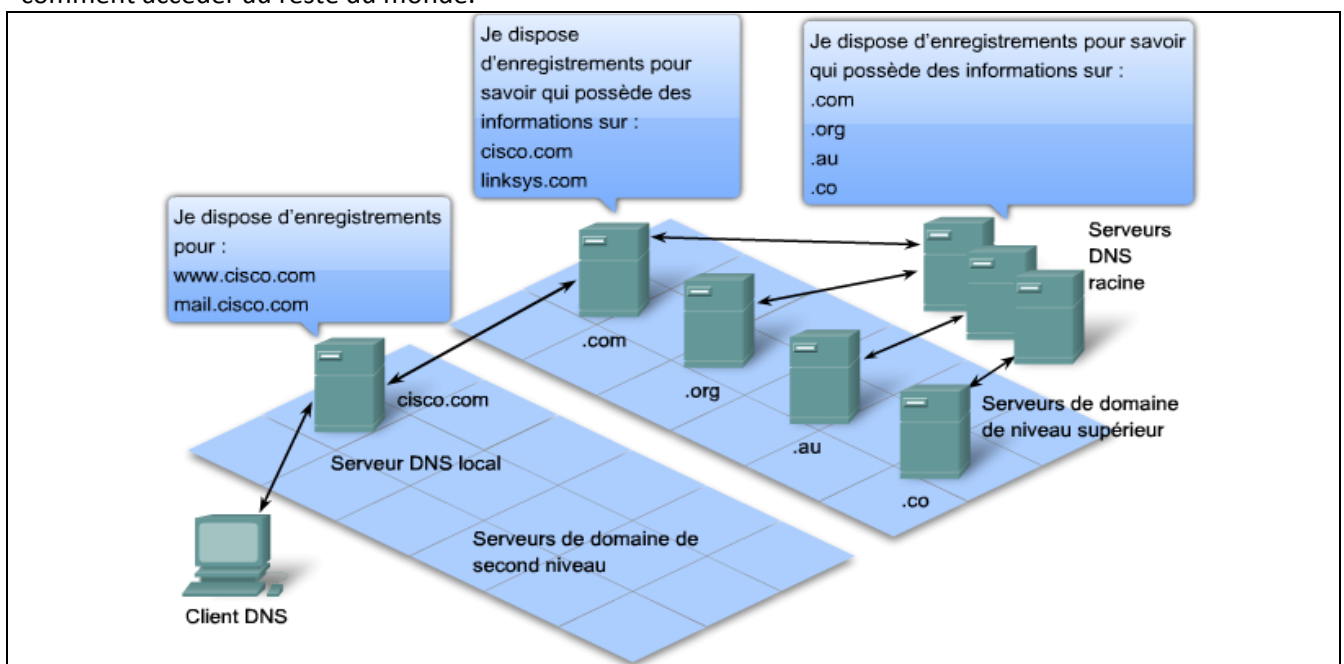
Sur les réseaux de données, les périphériques sont étiquetés par des adresses IP numériques, ce qui leur permet de participer à l'envoi et à la réception de messages via le réseau. Cependant, la plupart des utilisateurs mémorisent très difficilement ces adresses numériques. Pour cette raison, des noms de domaine ont été créés pour convertir les adresses numériques en noms simples et explicites.

Sur Internet, ces noms de domaine (par exemple, `www.cisco.com`) sont beaucoup plus faciles à mémoriser que leurs équivalents numériques (par exemple, `198.133.219.25`, l'adresse numérique du serveur de Cisco). De plus, si Cisco décide de changer d'adresse numérique, ce changement est transparent pour l'utilisateur car le nom de domaine demeure `www.cisco.com`. La nouvelle adresse est simplement liée au nom de domaine existant et la connectivité est maintenue. Lorsque les réseaux étaient de petite taille, il était simple de maintenir le mappage entre les noms de domaine et les adresses qu'ils représentaient. Cependant, les réseaux étant aujourd'hui de plus grande taille et le nombre de périphériques plus élevé, ce système manuel ne fonctionne plus.

Le protocole DNS (Domain Name System) a été créé afin de permettre la résolution des adresses pour ces réseaux. Il utilise un ensemble distribué de serveurs qui assurent un service automatisé pour associer les noms des ressources à l'adresse réseau numérique requise.



Il est impossible de stocker les données DNS du monde entier sur une seule machine. C'est pour cela qu'on été mis en place les déléguations : Chaque serveur ne connaît que la zone qui lui a été déléguée mais sait comment accéder au reste du monde.



3.8 Chemin suivi par l'information

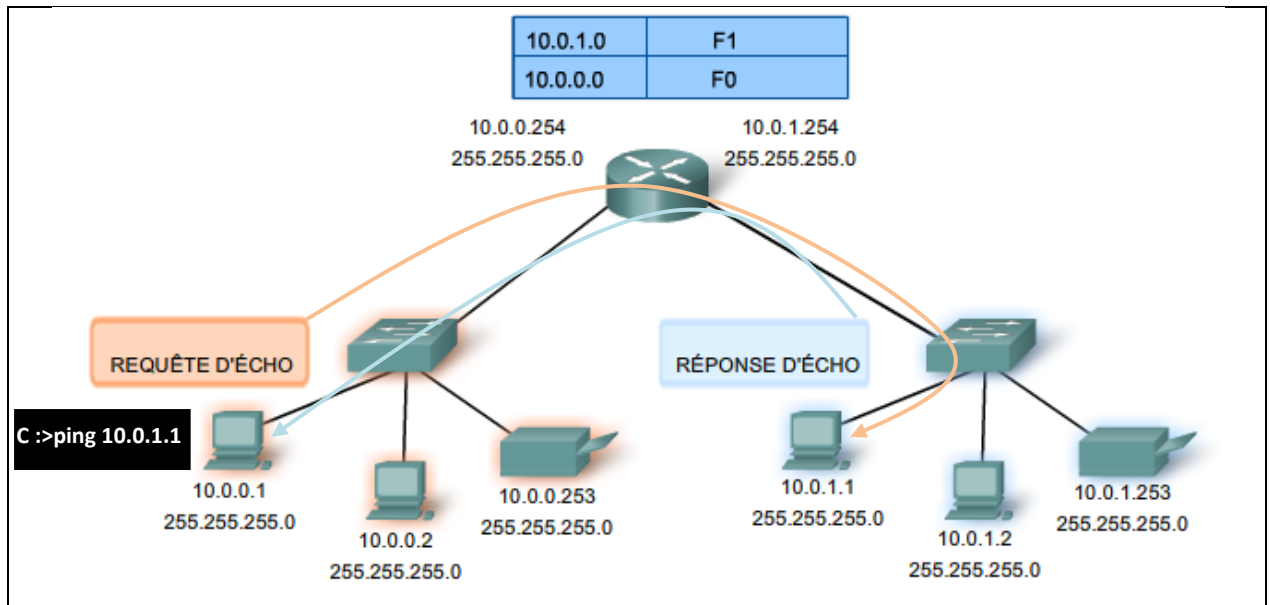
3.8.1 La commande ping

La commande ping est un utilitaire qui permet de tester une connectivité IP entre des hôtes. Elle envoie des demandes de réponse à une adresse hôte spécifiée. Elle utilise un protocole de couche 3 qui fait partie de la suite de protocoles TCP/IP appelée ICMP (Internet Control Message Protocol). Elle utilise un datagramme ICMP Echo Request.

Si l'hôte, à l'adresse spécifiée, reçoit une demande Echo, il répond par un datagramme ICMP Echo Reply. Pour chaque paquet envoyé, la commande ping mesure la durée de réception de la réponse.

Au fur et à mesure de la réception des réponses, la commande ping affiche l'intervalle de temps écoulé entre le moment où la requête ping a été envoyée et le moment de réception de la réponse. Cela permet de mesurer les performances du réseau. La commande ping a une valeur de délai d'attente pour la réponse. Si la réponse n'est pas reçue dans le délai imparti, la commande ping abandonne l'opération et affiche un message indiquant que la réponse n'a pas été reçue.

Une fois toutes les requêtes envoyées, l'utilitaire ping présente la sortie des résultats avec un récapitulatif des réponses. Cette sortie indique le taux de réussite et le délai moyen aller-retour, jusqu'à la destination.



3.8.2 La commande traceroute (tracert)

La commande traceroute (tracert) est un utilitaire qui permet d'identifier le chemin entre des hôtes. L'analyse du chemin génère une liste de sauts qui ont été traversés sur le trajet.

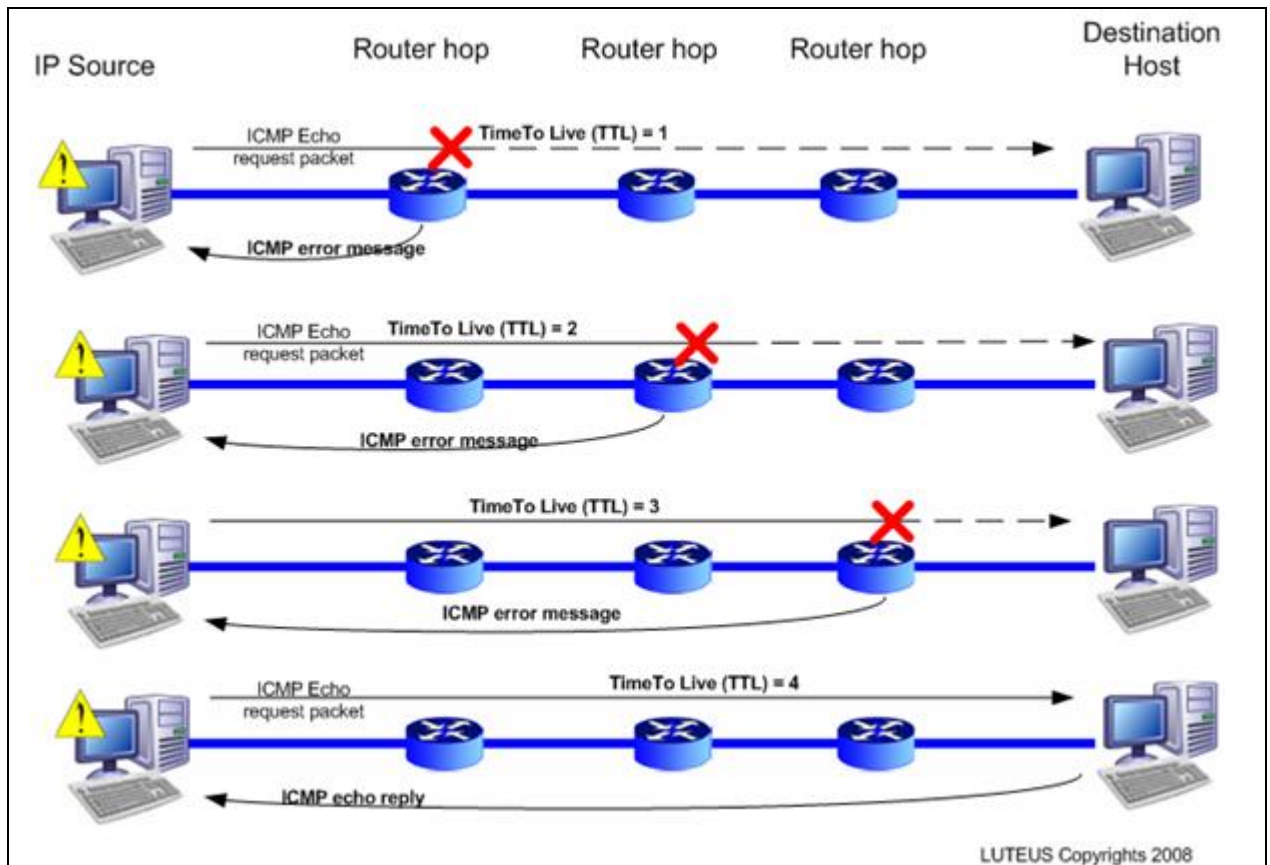
Cette liste peut fournir d'importantes informations pour la vérification et le dépannage. Si les données parviennent à destination, l'analyse du chemin répertorie tous les routeurs rencontrés sur le chemin.

Si les données n'atteignent pas un des sauts sur leur parcours, l'adresse du dernier routeur qui a répondu à l'analyse est renvoyée. Elle indique, soit l'endroit où le problème est survenu, soit l'endroit où des restrictions de sécurité s'appliquent.

La commande traceroute utilise une fonction de durée de vie dans l'en-tête de la couche 3 et le message ICMP Time Exceeded (Dépassement du délai). Le champ TTL permet de limiter le nombre de sauts qu'un paquet peut rencontrer. Lorsqu'un paquet traverse un routeur, le champ TTL est décrémenté de 1. Lorsque la durée de vie atteint zéro, le routeur ne transmet pas le paquet, et ce dernier est abandonné.

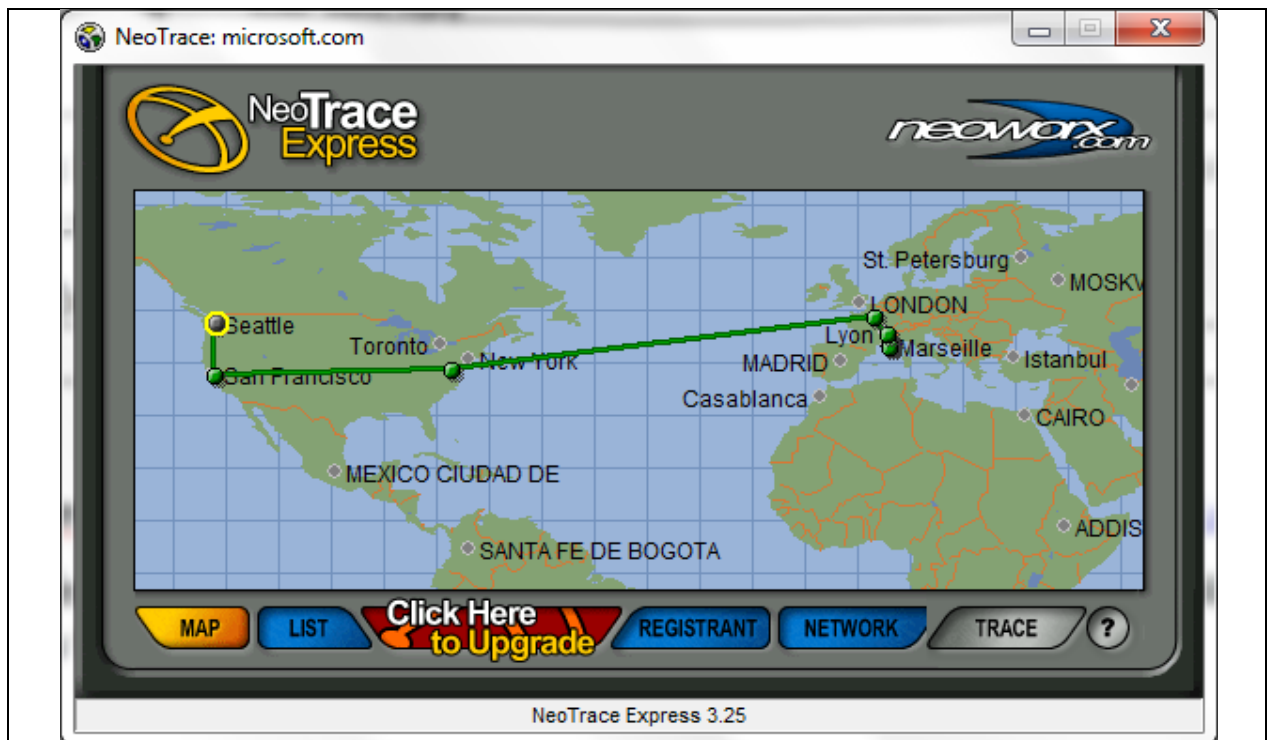
Outre abandonner le paquet, le routeur envoie en principe un message ICMP Time Exceeded (Délai dépassé) adressé à l'hôte source. Ce message contient l'adresse IP du routeur qui a répondu.

Le délai de TTL par défaut est fixé à 30.



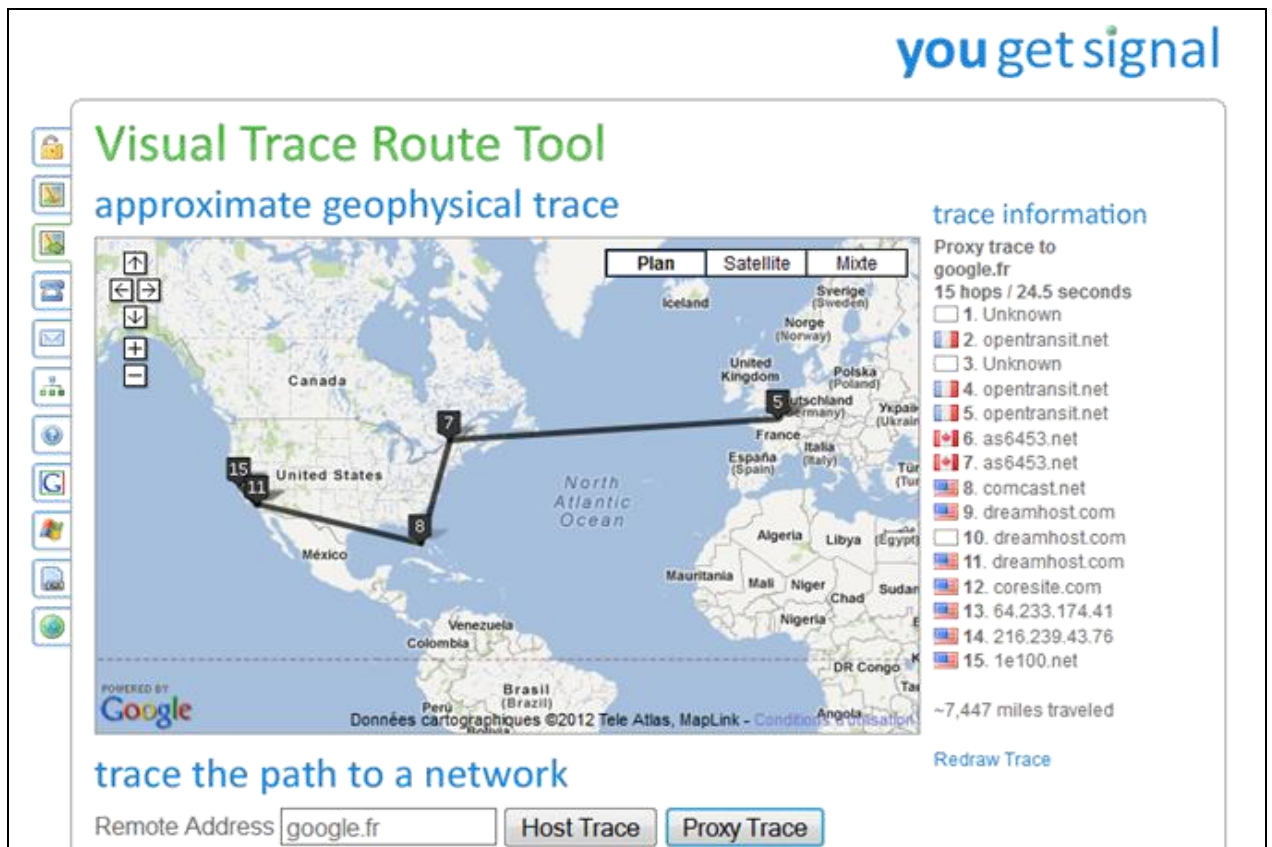
Il existe des logiciels qui fournissent une représentation graphique du chemin parcouru par l'information sur une carte du monde :

Neotrace (Express version gratuite, Pro évaluation pendant 30 jours)



Visual Traceroute : outil en ligne accessible à l'adresse <http://www.yougetsignal.com/tools/visual-traceroute/>

Cet outil très simple à utiliser présente toutefois l'inconvénient de passer obligatoirement par les serveurs du fournisseur du service.



3.9 Notions de base sur la création de sous-réseaux

La création de sous-réseaux permet de créer plusieurs réseaux logiques à partir d'un seul bloc d'adresses. Puisque nous utilisons un routeur pour interconnecter ces réseaux, chaque interface du routeur doit disposer d'un ID réseau unique. Tous les nœuds de cette liaison se trouvent sur le même réseau.

Nous créons les sous-réseaux au moyen d'un ou de plusieurs bits d'hôte en tant que bits réseau. Pour cela, il convient de développer le masque pour emprunter quelques bits de la partie hôte de l'adresse et créer d'autres bits réseau. Plus les bits d'hôte utilisés sont nombreux, plus le nombre de sous-réseaux qui peuvent être définis est important. Pour chaque bit emprunté, il faut doubler le nombre de sous-réseaux disponibles. Par exemple, en empruntant 1 bit, on peut définir 2 sous-réseaux. En empruntant 2 bits, on peut définir 4 sous-réseaux. Toutefois, pour chaque bit emprunté, le nombre d'adresses disponible par sous-réseau décroît.

Emprunt de bits pour sous-réseaux

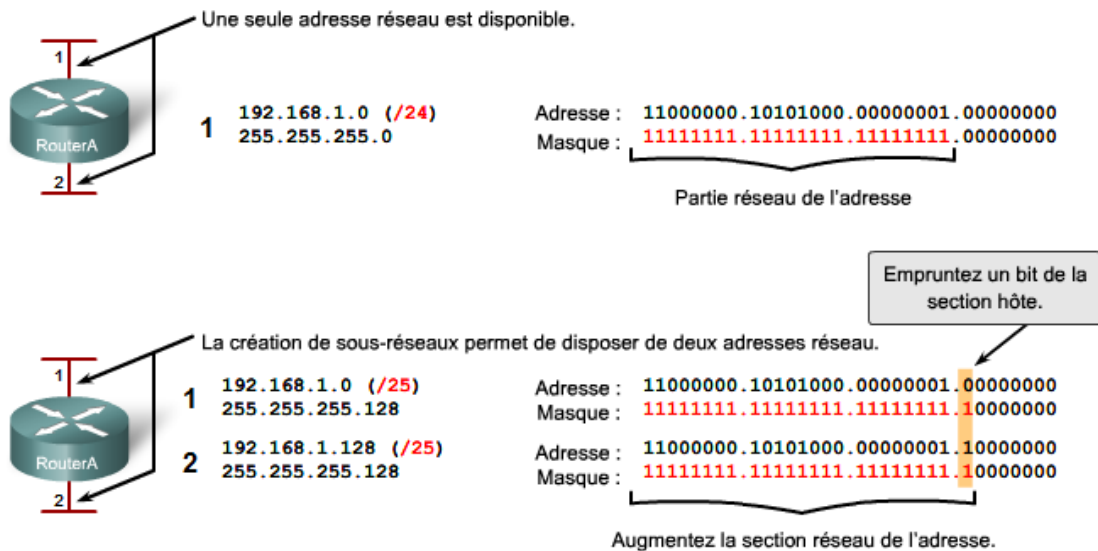


Schéma d'adressage : exemple de 2 réseaux

Sous-réseau	Adresse réseau	Plage d'hôtes	Adresse de diffusion
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

3.9.1 Nombre de sous-réseaux

Utilisez la formule suivante pour calculer le nombre de sous-réseaux :

$$2^n \text{ où } n = \text{le nombre de bits empruntés}$$

Dans notre exemple, nous obtenons :

$$2^1 = 2 \text{ sous-réseaux}$$

3.9.2 Le nombre d'hôtes

Pour calculer le nombre d'hôtes par réseau, il faut utiliser la formule :

$$2^n - 2 \text{ où } n = \text{le nombre de bits laissés pour les hôtes.}$$

Après application de cette formule, ($2^7 - 2 = 126$), on déduit que chacun de ces sous-réseaux peut avoir 126 hôtes.

Pour chaque sous-réseau, examinons le dernier octet dans sa forme binaire. Les valeurs de cet octet pour les deux réseaux sont les suivantes :

- Sous-réseau 1 : 00000000 = 0
- Sous-réseau 2 : 10000000 = 128

3.9.3 Exercice

On attribue le réseau 132.45.0.0/16. Il faut redécouper ce réseau en 8 sous-réseaux.

- Combien de bits supplémentaires sont nécessaires pour définir huit sous-réseaux ?

- Combien d'hôtes pourront être adressés dans chaque sous-réseau ?

- Quel est le masque réseau qui permet la création de huit sous-réseaux ?

- Quelle est l'adresse réseau de chacun des huit sous-réseaux, la plage des adresses utilisables ainsi que leurs adresses de broadcast ?

N° Sous-réseau	Adresse sous-réseau	Adresse premier hôte	Adresse dernier hôte	Adresse de broadcast
0				
1				
2				
3				
4				
5				
6				
7				

3.9.4 Découpage des réseaux à des tailles appropriées

Théoriquement, tous les réseaux d'un inter-réseau d'une grande entreprise ou d'une administration permettent d'accueillir un nombre défini d'hôtes.

Certains réseaux, comme les liaisons WAN de point à point, nécessitent seulement deux hôtes, au maximum. D'autres, comme un réseau local d'utilisateurs dans des bureaux ou un service de grande taille, doivent accueillir des centaines d'hôtes. Les administrateurs réseau doivent développer un schéma d'adressage inter-réseau de façon à pouvoir accueillir le nombre maximal d'hôtes pour chaque réseau. Le nombre d'hôtes dans chaque division du réseau doit prévoir un nombre plus important d'hôtes.

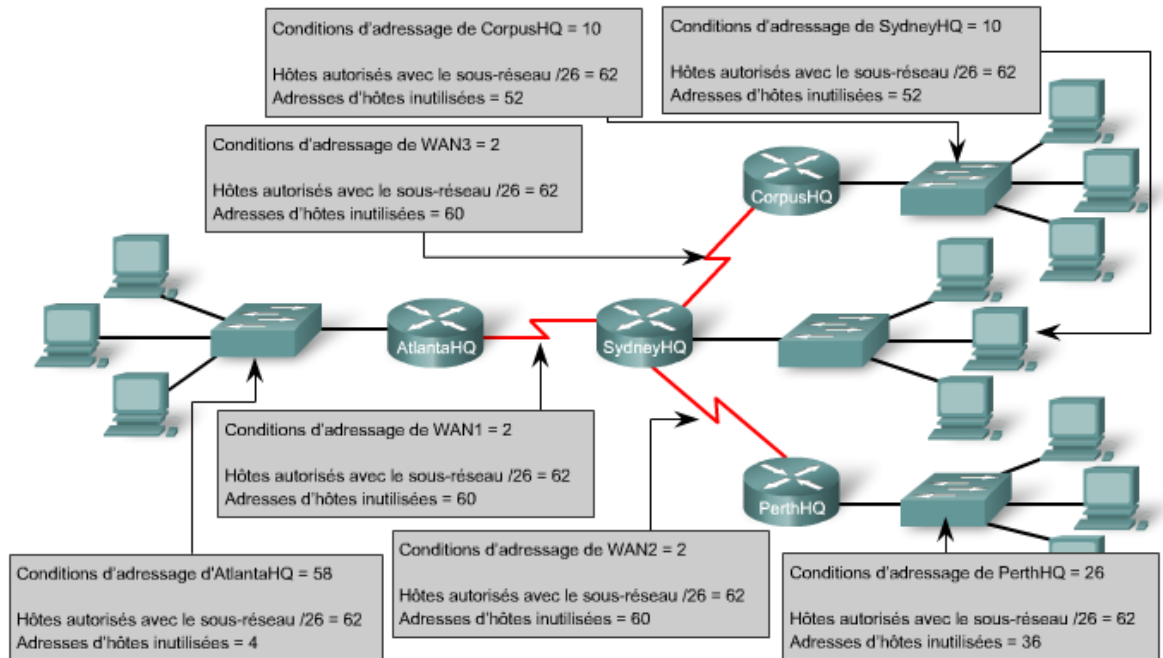
Il est nécessaire de connaître d'abord le nombre total d'hôtes requis par l'inter-réseau entier de l'entreprise. Nous devons utiliser un bloc d'adresses suffisamment grand pour pouvoir accueillir l'ensemble des périphériques appartenant à tous les réseaux d'entreprise. Il s'agit, entre autres, des périphériques d'utilisateurs, des serveurs, des périphériques intermédiaires et des interfaces de routeur.

Le découpage en sous-réseaux de tailles appropriées permet d'économiser les adresses IP :

Nous créons des sous-réseaux en fonction du nombre d'hôtes, y compris des interfaces de routeur et des connexions WAN dont nous avons besoin. Soit le scénario suivant :

- AtlantaHQ - 58 adresses d'hôte
- PerthHQ - 26 adresses d'hôte
- SydneyHQ - 10 adresses d'hôte
- CorpusHQ - 10 adresses d'hôte
- Liaisons WAN - 2 adresses d'hôte (chacune)

Avec de tels besoins, il est évident que l'utilisation d'un schéma de création de sous-réseaux standard serait inefficace. Dans cet inter-réseau, la création de sous-réseaux standards nécessite que chaque sous-réseau ait des blocs fixes de 62 hôtes, ce qui implique que de nombreuses adresses potentielles seront gaspillées. Ce gaspillage est particulièrement évident dans la figure ci-dessous, où nous voyons que le réseau LAN PerthHQ prend en charge 26 utilisateurs, alors que les routeurs des réseaux LAN SydneyHQ et CorpusHQ ne prennent en charge que 10 utilisateurs chacun.



De ce fait, avec le bloc d'adresses 192.168.15.0 /24, nous créons un schéma d'adressage à la fois pour répondre aux besoins et ne pas gaspiller d'adresses potentielles.



Adresses nécessitant un nom	Adresse de sous-réseau	Plage d'adresses	Adresse de diffusion	Réseau / préfixe
AtlantaHQ - 58				
PerthHQ - 26				
SydneyHQ - 10				
CorpusHQ - 10				
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

3.10 TP Création d'un réseau étendu

3.10.1 Objectif du TP

Il s'agit de créer un réseau local, ce qui suppose de connecter des périphériques réseau et de configurer les ordinateurs hôtes pour une connectivité réseau de base.

3.10.2 Qu'allez-vous apprendre ?

Vous apprendrez à :

- Concevoir une topologie logique.
- Conception d'une topologie physique.
- Configurer la topologie logique.
- Vérifier la connectivité du réseau.

3.10.3 A quoi cela va t-il vous servir ?

Concevoir une infrastructure réseau local basée sur les mécanismes de routage.

3.10.4 De quelles connaissances avez-vous besoin ?

Vous devez avoir compris et appris le cours et les travaux dirigés sur la numération et la représentation des caractères, ainsi que le cours sur les transmissions numériques.

3.10.5 Quel est le matériel dont vous avez besoin ?

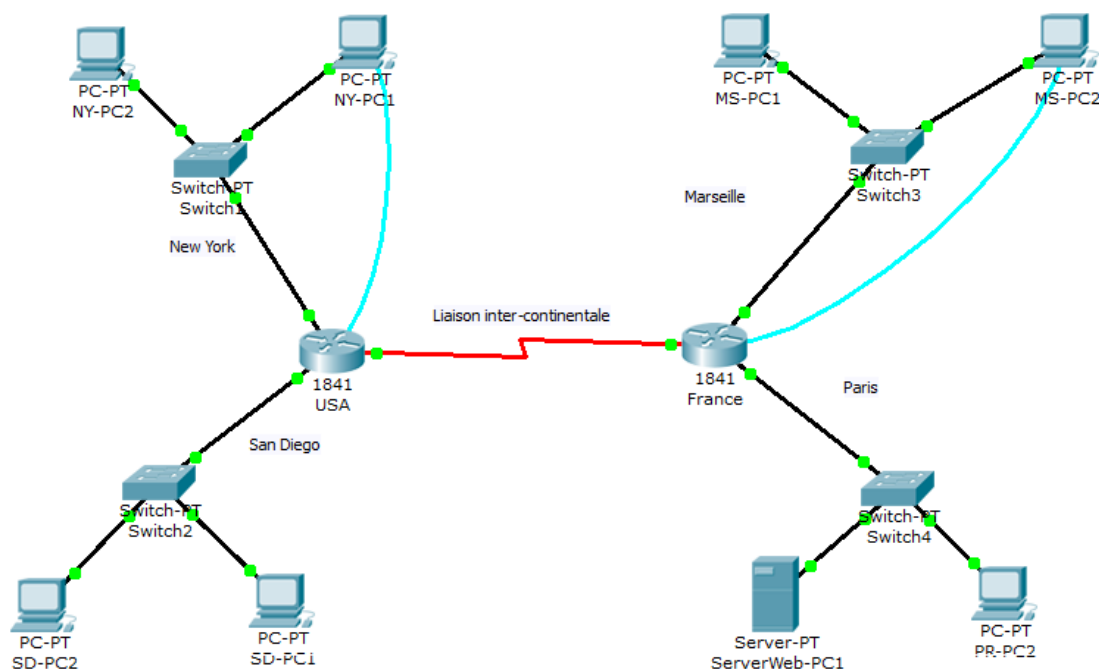
- ⇒ 8 ordinateurs.
- ⇒ 2 routeurs Cisco
- ⇒ switches
- ⇒ Câbles réseaux
- ⇒ 1 câble Serial
- ⇒ 2 câbles Console

Ou

- ⇒ Le logiciel Packet Tracer

3.10.6 Fichiers de TP

- ReseauEtendu.pdf
- ReseauEtendu.pka



4 Architecture client/serveur

4.1 Définition

Les informations qu'un utilisateur souhaite consulter ne sont pas toujours stockées sur son propre périphérique. Il est fréquent que celles-ci soient situées sur un autre périphérique connecté au réseau. Le modèle constitué du demandeur et du fournisseur de données au travers du réseau s'appelle modèle client/serveur.

Dans ce modèle d'architecture, le périphérique qui :

- demande les informations est nommé client
- répond à la requête est nommé serveur.

Les processus client et serveur sont considérés comme faisant partie de la couche application.

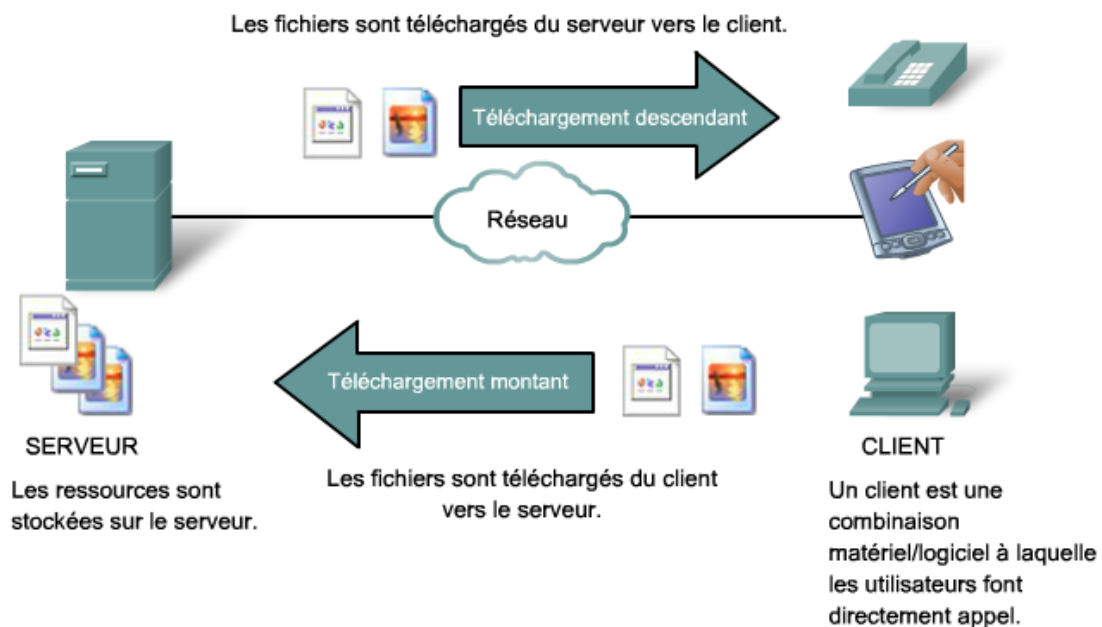
Le client commence l'échange en demandant des données au serveur, qui répond en envoyant un ou plusieurs flux de données au client. Les protocoles de couche application décrivent le format des requêtes et des réponses entre clients et serveurs. Outre le transfert de données effectif, cet échange peut également nécessiter des informations de contrôle, telles que l'authentification de l'utilisateur et l'identification d'un fichier de données à transférer.

Bien que les données soient généralement décrites comme étant transmises du serveur au client, certaines données sont toujours transmises du client au serveur. Le flux de données peut être égal dans les deux sens ou même plus important dans le sens client vers serveur.

Par exemple, un client peut transférer un fichier vers le serveur à des fins de stockage.

Le transfert de données :

- d'un client vers un serveur est désigné par le terme **téléchargement montant (upload)**,
- d'un serveur vers un client est désigné par le terme **téléchargement descendant (download)**.



4.2 Serveurs

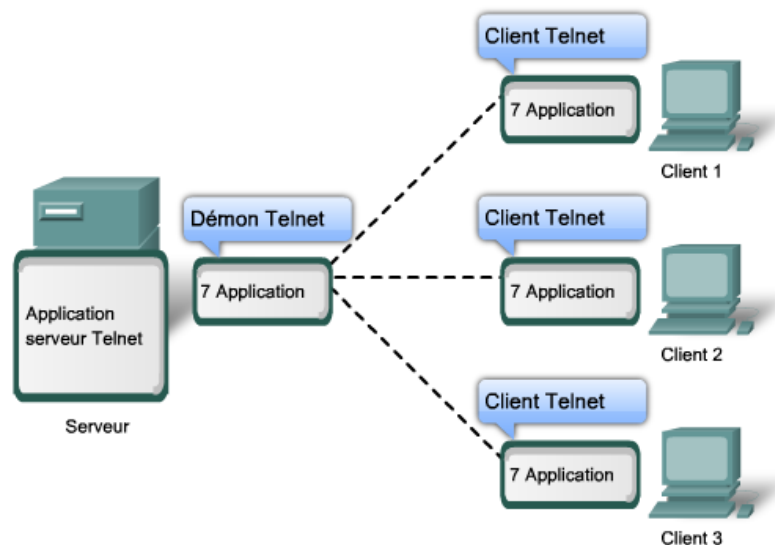
Un serveur est généralement un ordinateur qui contient des informations à partager avec de nombreux systèmes clients. Par exemple, les pages Web, les documents, les bases de données, les images, les fichiers vidéo et les fichiers audio peuvent tous être stockés sur un serveur et transmis à des clients demandeurs.

Différents types d'applications serveur peuvent avoir différents besoins en matière d'accès du client. Certains serveurs peuvent nécessiter l'authentification des informations du compte utilisateur pour vérifier que l'utilisateur est autorisé à accéder aux données requises ou à effectuer une opération spécifique.

Dans un réseau client/serveur, le serveur exécute un service, ou processus, parfois nommé démon de serveur. Comme la plupart des services, les démons s'exécutent généralement en tâche de fond et ne sont pas sous le contrôle direct de l'utilisateur final. Les démons sont décrits comme « étant à l'écoute » d'une requête de la part d'un client car ils sont programmés pour répondre chaque fois que le serveur reçoit une requête pour le service fourni par le démon. Lorsqu'un démon « entend » une requête d'un client, il échange les messages appropriés avec le client, comme requis par son protocole, puis envoie les données requises au client dans le format approprié.

Les serveurs comportent généralement plusieurs clients demandant des informations en même temps. Par exemple, un serveur Telnet peut comporter de nombreux clients demandant à se connecter à ce serveur. Ces requêtes de client individuelles doivent être traitées simultanément et séparément pour que le réseau fonctionne correctement. Les processus et les services de la couche application sont assistés par les fonctions des couches inférieures pour gérer correctement les conversations multiples.

Les processus serveur peuvent prendre en charge plusieurs clients.



4.3 Principaux services et protocoles associés

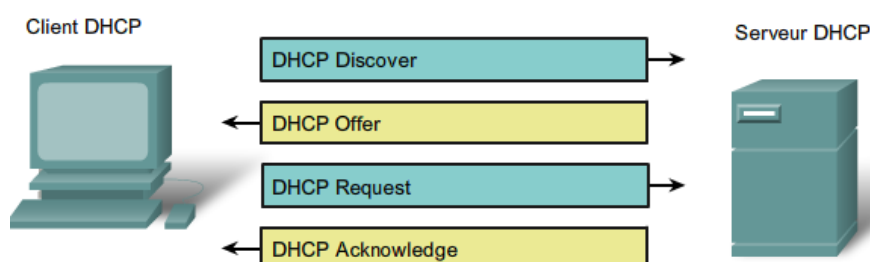
4.3.1 Service de configuration TCP/IP automatique : protocole DHCP

Le service fourni par le protocole DHCP (Dynamic Host Configuration Protocol) permet aux périphériques d'un réseau d'obtenir d'un serveur DHCP des adresses IP et d'autres informations. Ce service automatise l'affectation des adresses IP, des masques de sous-réseau, d'une adresse IP de passerelle et d'autres paramètres de configuration de la couche réseau.

Il permet à un hôte d'obtenir une adresse IP dynamiquement lorsqu'il se connecte au réseau. Le serveur DHCP est contacté et une adresse est demandée. Le serveur DHCP choisit une adresse dans une plage d'adresses configurée (nommée pool) et affecte cette adresse à l'hôte pour une durée définie.

Sur les réseaux locaux plus importants ou sur les réseaux dont les utilisateurs changent fréquemment, le protocole DHCP est préférable.

Les adresses attribuées via le protocole DHCP ne sont pas affectées aux hôtes définitivement mais uniquement pour une durée spécifique (bail). Si l'hôte est mis hors tension ou retiré du réseau, l'adresse est retournée au pool pour être réutilisée.

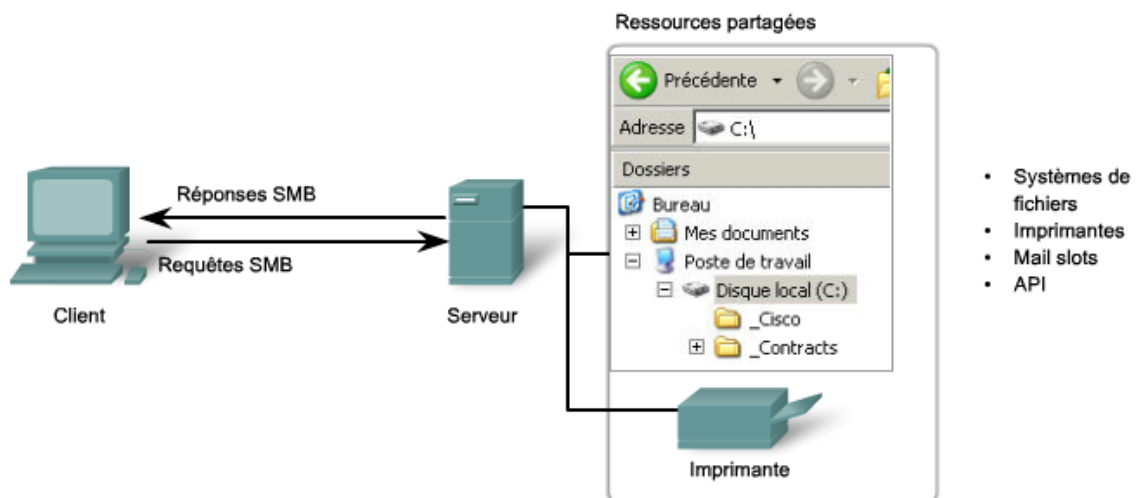


4.3.2 Service de partage de fichiers : protocole SMB

Le protocole SMB (Server Message Block) est un protocole de partage de fichiers client/serveur. Il fut développé par IBM à la fin des années 80 pour décrire la structure des ressources réseau partagées telles que les répertoires, les fichiers, les imprimantes et les ports série. Il s'agit d'un protocole de requête-réponse. Contrairement au partage de fichiers pris en charge par le protocole FTP, les clients établissent une connexion à long terme aux serveurs. Une fois la connexion établie, l'utilisateur du client peut accéder aux ressources résidant sur le serveur comme si elles étaient situées localement sur l'hôte client.

Le protocole SMB est à la base du système de partage de fichiers des réseaux Microsoft.

Les systèmes d'exploitation LINUX et UNIX fournissent également une méthode de partage des ressources avec les réseaux Microsoft à l'aide d'une version de SMB nommée SAMBA. Les systèmes d'exploitation Apple Macintosh prennent en charge eux aussi le partage des ressources via le protocole SMB.



SMB est un protocole client-serveur et requête-réponse. Les serveurs peuvent mettre leurs ressources à la disposition des clients sur le réseau.

4.3.3 Service web : protocole http

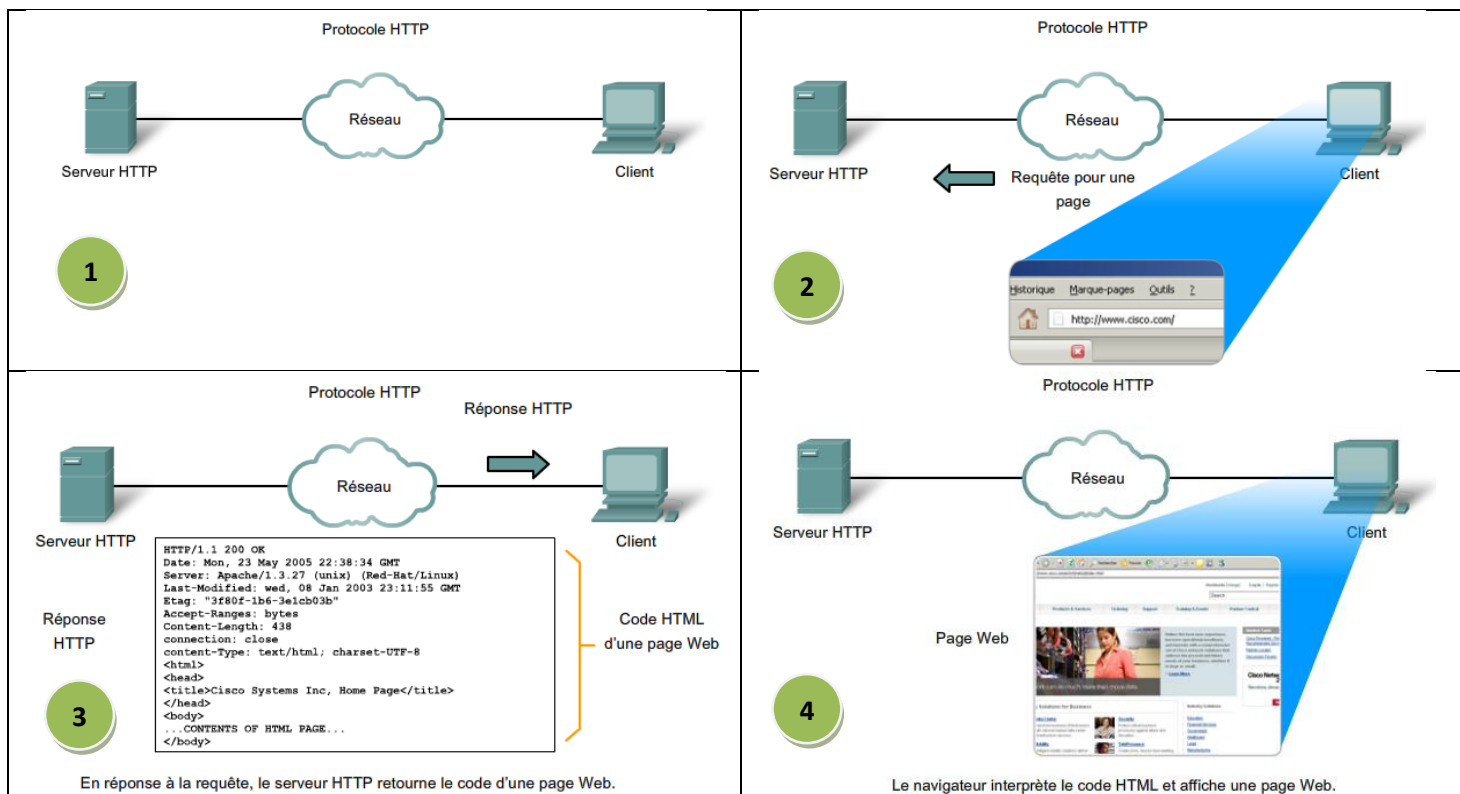
Le protocole HTTP est utilisé à travers le Web pour le transfert des données et constitue l'un des protocoles d'application les plus utilisés.

C'est un protocole de requête/réponse. Lorsqu'un client (généralement un navigateur Web) envoie une requête à un serveur, le protocole HTTP définit les types de messages que le client utilise pour demander la page Web, ainsi que les types de messages que le serveur utilise pour répondre. Les trois types de messages courants sont GET, POST et PUT.

- GET est une requête cliente pour obtenir des données. Un navigateur Web envoie le message GET pour demander des pages à un serveur Web.
- POST sert à envoyer des messages qui téléchargent des données vers le serveur Web. Par exemple, lorsque l'utilisateur entre des données dans un formulaire incorporé à une page Web, la requête POST comprend les données dans le message envoyé au serveur.
- PUT télécharge des ressources ou du contenu vers le serveur Web.

Bien qu'il soit remarquablement flexible, le protocole HTTP n'est pas un protocole sécurisé. Les messages POST téléchargent des informations vers le serveur dans un format de texte clair pouvant être intercepté et lu. De même, les réponses du serveur (généralement, des pages HTML) ne sont pas chiffrées.

Pour une communication sécurisée via Internet, le protocole HTTPS (HTTP Secure) est utilisé lors de l'accès aux informations du serveur Web ou de leur publication. Le protocole HTTPS peut procéder à l'authentification et au chiffrement pour sécuriser les données pendant qu'elles circulent entre le client et le serveur. Le protocole HTTPS spécifie des règles supplémentaires de transmission de données entre la couche application et la couche transport.



Le serveur HTTP le plus utilisé est Apache HTTP Server qui sert environ 55 % des sites web en janvier 2013. (Source : http://fr.wikipedia.org/wiki/Serveur_HTTP)

4.3.4 Service de transfert de fichier : protocole FTP

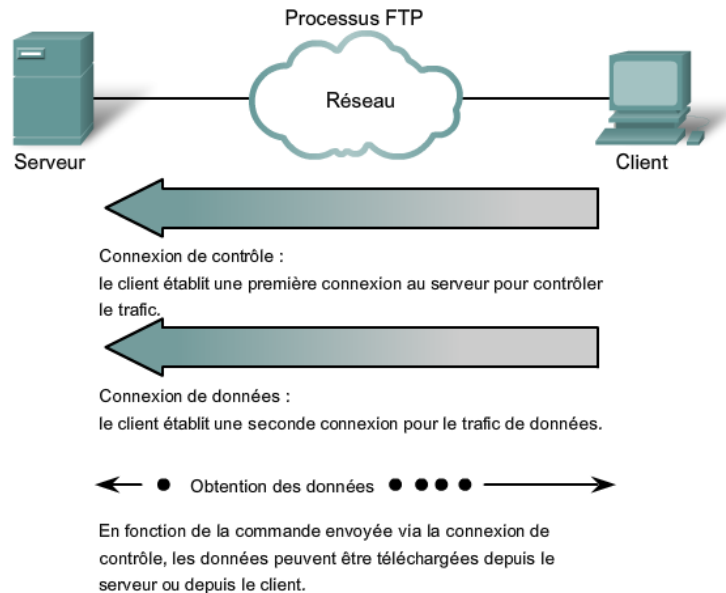
Le protocole FTP (File Transfer Protocol) a été développé pour permettre le transfert de fichiers entre un client et un serveur. Un client FTP est une application s'exécutant sur un ordinateur et utilisée pour extraire des fichiers d'un serveur exécutant le démon FTP.

Pour transférer les fichiers correctement, le protocole FTP nécessite que deux connexions soient établies entre le client et le serveur : une connexion pour les commandes et les réponses et une autre pour le transfert même des fichiers.

Le client établit la première connexion au serveur sur le port TCP 21. Cette connexion est utilisée pour le trafic de contrôle et se compose de commandes clientes et de réponses serveur.

Le client établit la seconde connexion au serveur via le port TCP 20. Cette connexion est destinée au transfert même des fichiers et est établie à chaque transfert de fichiers.

Le transfert de fichiers peut s'effectuer dans l'une des deux directions. Le client peut télécharger un fichier à partir du serveur ou en direction du serveur.



4.4 TP Services réseaux

4.4.1 Objectif du TP

Configurer les services réseaux sur un serveur afin de répondre aux besoins des postes clients (paramètres IP, partage de fichiers, pages web)..

4.4.2 Qu'allez-vous apprendre ?

Vous apprendrez à :

- Installer et configurer un serveur Linux Suse.
- Installer et configurer le service DHCP.
- Installer et configurer le service SAMBA.
- Installer et configurer le service APACHE.
- Installer et configurer le service FTP.

4.4.3 A quoi cela va t-il vous servir ?

Concevoir une infrastructure réseau client/serveur.

4.4.4 De quelles connaissances avez-vous besoin ?

Vous devez savoir mettre en réseau deux ordinateurs et leur assigner une adresse IP fixe.

4.4.5 Quel est le matériel dont vous avez besoin ?

- ⇒ 2 ordinateurs.
- ⇒ 1 switch (éventuellement)
- ⇒ Câbles réseaux
- ⇒ DVD Linux Suse

4.4.6 Fichiers de TP

- Activite_Configuration de services reseaux.pdf
- Fiches_Configuration de services reseaux.pdf
- Procedure virtualisation du serveur.docx



5 Références

- Cours de l'Académie Cisco : CCNA Exploration – Notions de base sur les réseaux
- Cours de réseaux Master 1 d'informatique - Pascal Nicolas - Université d'Angers
<http://www.scribd.com/doc/2969777/Cours-de-reseaux-Maitrise-dinformatique-Universite-dAngers>
- Did You Know 3.0 –
<http://www.youtube.com/watch?v=Gv8pmlr3a7k&feature=fvwrel>
- L'influence croissante d'internet dans notre vie quotidienne
<http://www.fsa.ulaval.ca/personnel/vernag/eh/f/cons/internet.htm>
- Centre pour l'Education et la Sensibilisation à la Coopération Internationale (dossier 11 : Internet, poste et télécommunications)
http://www.genevedecouverte.ch/fr/internet_et_communication.html
- Inetdoc.net Interconnexion réseau et logiciel libre
<http://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.exercises.html>
- Réseaux locaux industriels et réseaux embarqués – Karen Godary
http://www.polytech.univ-montp2.fr/~karen.godary/Info_Indus/