Sommaire

1 Introduction et historique

TCP / IP est surtout connu comme le protocole de l'Internet.

Un protocole est un ensemble de règles, de procédures qui déterminent le processus de réalisation d'une action.

TCP / IP est un protocole de communication : Il décrit comment les messages sont transportés et adressés dans un réseau.

Rappel historique :

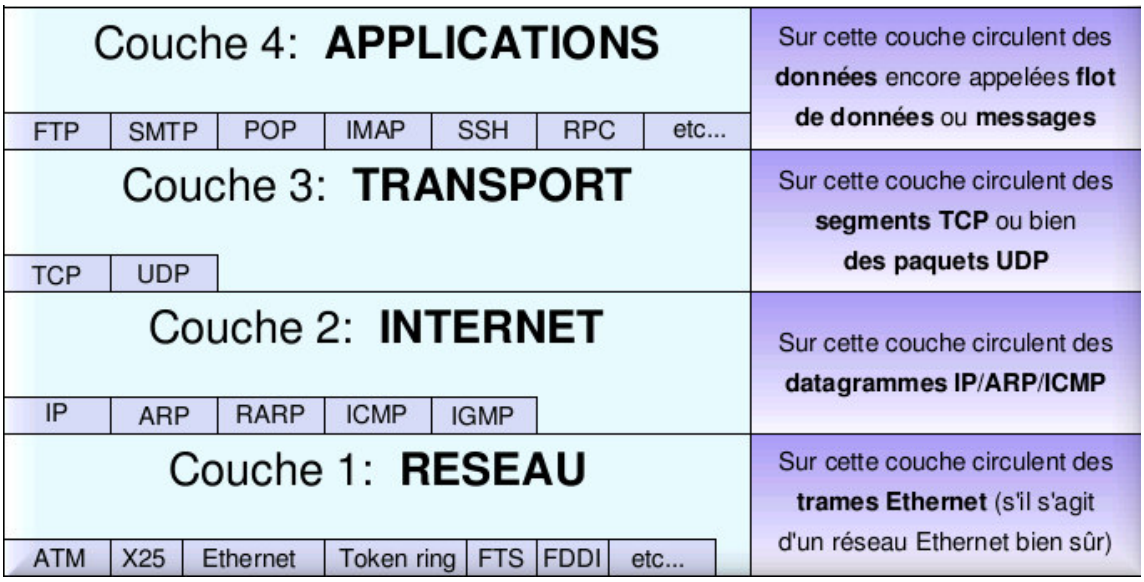
- TCP / IP est issu des travaux de l'Agence de Recherche pour les Projets Avancés du Ministère de la Défense des Etats-Unis l'ARPA
- Au départ, le réseau ARPANET, ancêtre de l'Internet dans les années 60 utilisait le protocole NCP (Network Control Protocol).
- TCP / IP fût développé dans les années 70 et a remplacé NCP sur ARPANET en 1983.
- TCP / IP a été développé et implanté au départ en environnement UNIX.

Il doit sa célébrité actuelle au développement du réseau Internet qui l'impose comme un standard de fait.

2 Les protocoles TCP/IP

Les protocoles TCP/IP se situent dans un modèle nommé "familles de protocoles TCP/IP". Chaque couche du modèle TCP/IP correspond à une ou plusieurs couches du modèle OSI.

Les protocoles sont définis à l'intérieur des quatre couches de TCP/IP :



Ces protocoles sont également définis à travers des documents appelés RFC (*Request For Comments* - Appels à commentaires) qui définissent des règles sur les protocoles, les réseaux… Ces RFC sont au nombre de plus de 3000 aujourd'hui.

Voir entre autre le site : http://www.en.ixus.net/modules.php?name=Rfc

Extrait de liste de RFC :

RFC 97 : First Cut at a Proposed Telnet Protocol
RFC 98 : Logger Protocol Proposal
RFC 99 : Network Meeting
RFC 100 : Categorization and guide to NWG/RFCs
RFC 101 : Notes on the Network Working Group meeting
RFC 102 : Output of the Host-Host Protocol glitch cleaning committee
RFC 103 : Implementation of Interrupt Keys
RFC 104 : Link 191
RFC 105 : Network Specifications for Remote Job Entry and Remote Job Output Retrieval at UCSB
RFC 106 : User/Server Site Protocol Network Host Questionnaire
RFC 107 : Output of the Host-Host Protocol Glitch Cleaning Committee
RFC 108 : Attendance list at the Urbana NWG meeting
RFC 109 : Level III Server Protocol for the Lincoln Laboratory NIC 360/67 Host
RFC 110 : Conventions for using an IBM 2741 terminal as a user console for access to network server hosts
RFC 111 : Pressure from the Chairman
RFC 112 : User/Server Site Protocol: Network host questionnaire responses
RFC 113 : Network activity report: UCSB Rand
RFC 114 : File Transfer Protocol
RFC 115 : Some Network Information Center policies on handling documents
RFC 116 : Structure of the May NWG Meeting
RFC 117 : Some comments on the official protocol
RFC 118 : Recommendations for facility documentation
RFC 119 : Network Fortran subprograms
RFC 120 : Network PL1 subprograms
RFC 121 : Network on-line operators
RFC 122 : Network specifications for UCSB's Simple-Minded File System
RFC 123 : Proffered Official ICP
RFC 124 : Typographical error in RFC 107

2.1 Un peu de vocabulaire

Pour désigner les informations transmises, selon le niveau concerné, on parle :

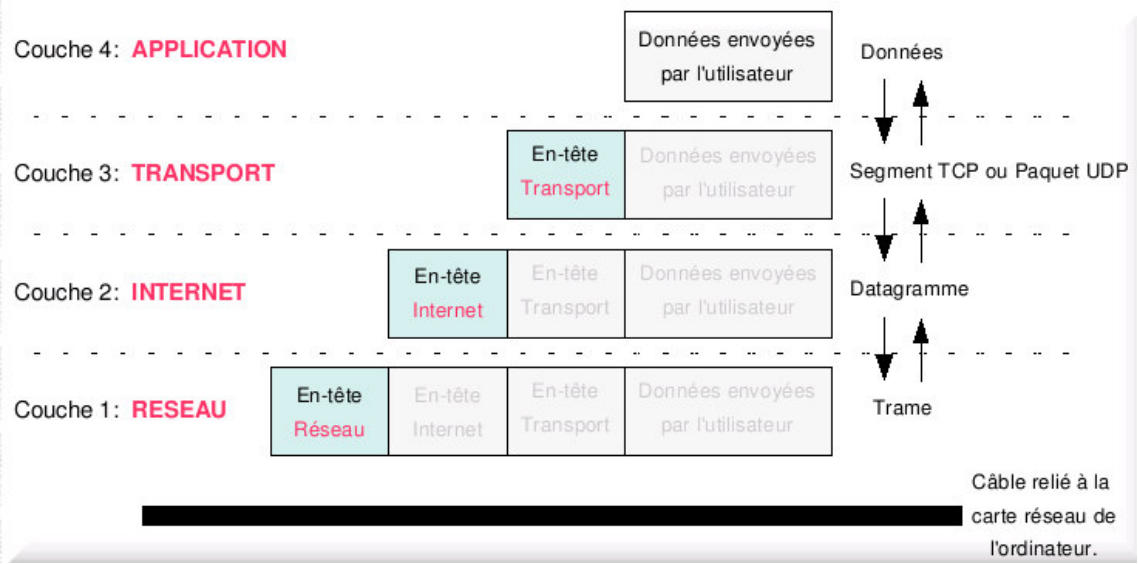
- De message (ou de flux) voire de données entre applications
- De paquet (ou segment) au niveau TCP
- De datagramme au niveau IP
- De trames au niveau de l'interface réseau (Ethernet ou Token-Ring).

2.2 L'encapsulation des protocoles

Chaque fois qu'une quantité d'information passe d'une couche à une autre, le protocole qui réceptionne cette quantité d'information y ajoute (ou enlève) un en-tête qui lui est spécifique.

C'est le fait d'ajouter ou d'enlever cet en-tête qu'on appelle encapsulation ou désencapsulation.

Mécanisme d'encapsulation - désencapsulation



2.3 Le protocole IP

Le protocole IP (*Internet Protocol*) permet la remise des paquets pour tous les autres protocoles de la suite.

- Il fournit un système de remise de données optimisé sans connexion.
- Il n'existe aucune garantie quant à la remise des paquets IP à leur destinataire ou à l'ordre dans lequel ils ont été envoyés.
- La fonctionnalité de contrôle du protocole (checksum) ne confirme que l'intégrité de l'en-tête IP, mais pas celles des données associées.
- Seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP ainsi que de leur ordre de réception.

2.4 Le protocole TCP

Le protocole TCP (*Transmission Control Protocol*) fournit un service sécurisé de remise des paquets, orienté connexion, encapsulé dans le protocole IP.

TCP :

- Garantit l'ordre de remise des paquets
- Vérifie l'intégrité de l'en-tête des paquets et des données qu'ils contiennent.
- Si un paquet TCP est endommagé ou perdu au cours de la transmission, TCP retransmet ce paquet.

Cette fiabilité fait de TCP un protocole bien adapté pour la transmission de données

2.5 Le protocole UDP

Le protocole UDP (*User Datagram Protocol*) est un autre protocole de transmission de données qui offre un service de datagrammes sans connexion et qui ne garantit ni la remise ni l'ordre des paquets délivrés.

- Les caractères de contrôle des données (checksum) sont facultatifs dans le protocole UDP.
- Ceci permet d'échanger des données sur des réseaux à fiabilité élevée sans utiliser de ressources réseau ou du temps de traitement.
- Le protocole UDP prend également en charge l'envoi de données d'un expéditeur vers plusieurs destinataires.

2.6 Le protocole ICMP

Le protocole ICMP (*Internet Control Message Protocol*), est un protocole de maintenance. Il permet à deux systèmes d'un réseau IP de partager des informations d'état et d'erreur.

La commande Ping utilise les paquets ICMP de demande d'écho et de réponse en écho afin de déterminer si un système IP donné d'un réseau fonctionne.

2.7 Les autres protocoles

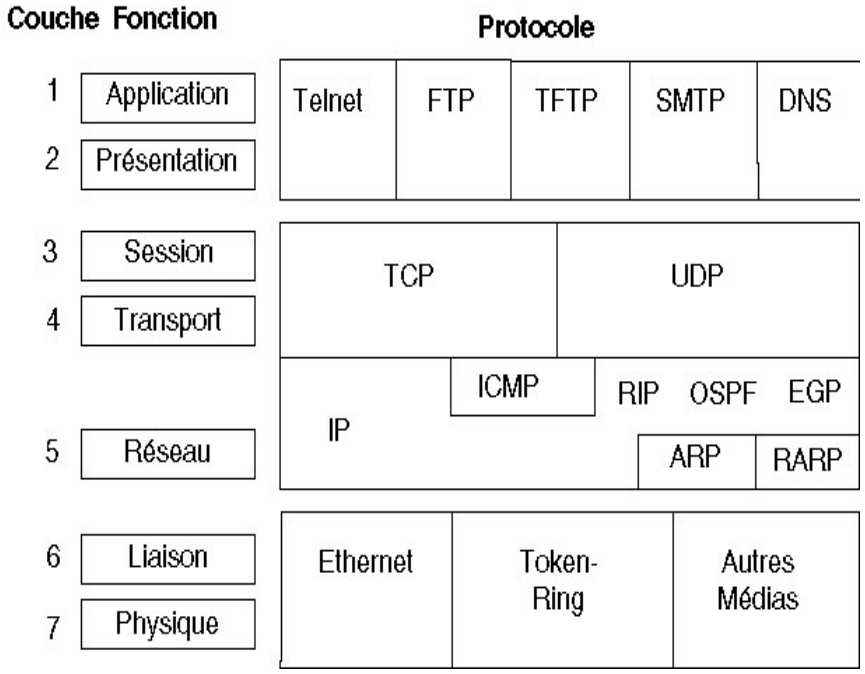
Il existe bien d'autres protocoles TCP/IP qui ont tous une fonction bien particulière. Ils seront vus plus en détail ultérieurement.

Ils sont cités et positionnés dans le schéma ci-après.

2.8 Les protocoles TCP/IP dans le modèle OSI

2.8.1 Positionnement

Modèle de référence OSI ***Ensemble de protocoles TCP/IP***



2.8.2 Fonctionnement général

A titre d'exemple, une application assurant le transfert de fichiers à l'aide de TCP effectue les opérations suivantes pour envoyer les données :

1. La couche de l'application envoie un flux de données vers la couche de transport de l'ordinateur source.
2. La couche de transport découpe le flux en segments TCP, ajoute à chaque segment un en-tête comportant un numéro de séquence et envoie les segments vers la couche Internet (IP). Le système calcule une somme de contrôle.
3. La couche IP crée un paquet comportant un échantillon des données, dont le segment TCP. Elle ajoute un en-tête de paquet contenant les adresses IP source et destination. La couche IP détermine également l'adresse physique de l'ordinateur destinataire ou celle de l'ordinateur intermédiaire en direction de celui-ci. Elle transmet le paquet et l'adresse physique à la couche de liaison. Le système calcule une autre somme de contrôle.
4. La couche de liaison transmet le paquet IP dans la partie Donnée d'une trame de liaison envoyée vers l'ordinateur destinataire. Si le destinataire accessible est un ordinateur intermédiaire (une passerelle), l'étape 3 se reproduit avec l'ordinateur suivant jusqu'à ce que la destination finale soit atteinte.
5. La couche de liaison de l'ordinateur destinataire final rejette l'en-tête de liaison et transmet le paquet IP à la couche IP.

6. La couche IP vérifie l'en-tête du paquet IP. Si la somme de contrôle ne correspond pas à celle calculée par la couche IP, celle-ci rejette le paquet.
7. Dans le cas contraire, la couche IP retire l'en-tête IP et passe le segment TCP à la couche TCP. Celle-ci contrôle le numéro de séquence et détermine si ce segment correspond au segment attendu dans la reconstitution.
8. La couche TCP calcule le checksum de contrôle pour l'en-tête TCP et les données.
    - Si cette valeur ne correspond pas à celle transmise dans l'en-tête, la couche TCP abandonne le segment.
    - Si la valeur de la somme de contrôle est correcte et que le segment se présente dans le bon ordre, la couche TCP envoie un accusé de réception à l'ordinateur source.
9. La couche TCP retire l'en-tête TCP et transmet les octets du segment reçu à l'application.
10. Pour finir, l'application du poste destinataire reçoit les données, exactement comme s'il existait une connexion directe avec l'application de l'ordinateur source.

3 Adressage

L'adressage désigne la façon d'identifier, à l'aide d'une adresse unique, un équipement sur un réseau.

3.1 Adresses physiques (MAC)

Au niveau de la couche de liaison, les nœuds (machines disposant d'une adresse) utilisent une adresse dite « physique » pour communiquer. Le format de ces adresses physiques diffère selon les réseaux, et elles sont assignées de différentes manières.

- Une adresse physique pour un réseau Ethernet, est une valeur numérique à six octets (par exemple : 10-20-21-60-70-80) définie par le constructeur de la carte.
- Cette adresse est unique et ne peut être modifiée.
- Ces adresses physiques sont également appelées « adresses MAC » (*Media Access Control*).

3.2 Adresse logique IP

L'adresse IP d'un nœud est une adresse « logique » définie indépendamment de toute topologie d'ordinateur ou de réseau. Son format reste identique quel que soit le support utilisé (câble, fibre…).

Pour être en mesure d'échanger des paquets entre différents ordinateurs, TCP/IP nécessite l'utilisation de trois valeurs :

- **Une adresse IP** qui identifie de manière unique chaque hôte sur le réseau,
- **Un masque de sous-réseau** qui permet de distinguer le type de réseau ou de segmenter celui-ci en plusieurs sous-réseaux.
- **Une passerelle (routeur) par défaut** qui est l'adresse IP où sont envoyés les paquets destinés aux autres réseaux ou sous-réseaux.

3.3 Assignation d'adresses IP à des adresses physiques

Pour envoyer les paquets vers les autres nœuds du réseau, les nœuds qui utilisent les protocoles TCP/IP traduisent les adresses IP de destination en adresses physiques MAC.

L'application émettrice indique son adresse IP dans le paquet émis, l'application réceptrice peut utiliser cette adresse IP pour répondre.

3.3.1 Le protocole ARP

Sur les réseaux à diffusion, tels qu'Ethernet, Token-Ring, l'envoi d'un paquet entre un émetteur et un destinataire se fait grâce aux adresses MAC.

le protocole ARP (*Address Resolution Protocol*) à la charge de retrouver l'adresse Mac à partir de l'adresse IP.
Pour trouver l'adresse physique,

- Il vérifie dans son cache si l'adresse IP destinataire existe
- Sinon, Il diffuse un paquet ARP qui contient l'adresse IP destinataire.
  - Le nœud qui contient l'adresse IP destinataire renvoie son adresse physique
  - Il met à jour son cache en ajoutant une entrée correspondante (adresse IP / adresse MAC)
- Il utilise l'adresse MAC pour diffuser la trame

Le cache contenant la table d'assignation s'appelle cache de résolution d'adresse.

3.3.2 Le protocole RARP

Le protocole RARP (Reverse Adress Resolution Protocol) assure la fonction inverse d'ARP, à savoir retrouver un e adresse IP à partir de l'adresse MAC.

4 L'adressage IP

4.1 Présentation

Une adresse IP est représentée par 4 octets. Contrairement à une adresse MAC, elles sont configurables par l'utilisateur.

- Chaque nœud du réseau (les switchs ou les hubs ne sont pas considérés comme des nœuds) est identifié par une adresse IP.
- Cette adresse doit être unique sur un même réseau.
- Si un ordinateur est équipé de plusieurs cartes réseau, chacune d'entre elles dispose de sa propre adresse IP.

4.2 Le format des adresses IPV4

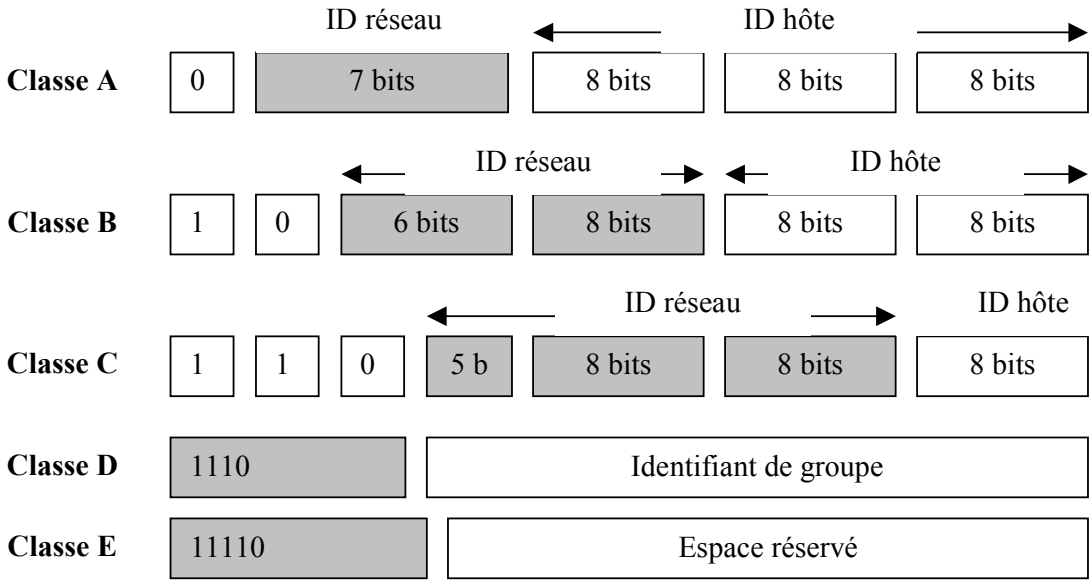
Les adresses IP sont des nombres de 32 bits qui contiennent 2 champs :

- Un identifiant de réseau (TCP/IP se réfère à chaque réseau local comme à un sous-réseau) : adresse logique du sous-réseau auquel l'équipement appartient.
- Un identifiant d'hôte (un ordinateur ou un périphérique sur un réseau TCP/IP est appelé hôte) : adresse logique de l'équipement sur le sous-réseau (identifiant de manière unique chaque hôte sur le sous-réseau).
- La concaténation des deux champs constitue une adresse IP unique (ex : 192.168.0.1).

Attention, la représentation décimale est utilisée en raison de sa facilité de visualisation et mémorisation. Néanmoins, la codification s'appuie sur une notation binaire.

Il a été défini 3 classes d'adresses en fonction de la taille des réseaux :

- Des grands réseaux→ Classe A (IBM, Xerox, DEC, Hewlett-Packard, ...)
- Des réseaux moyens → Classe B (Microsoft par exemple)
- Des petits réseaux → Classe C



Exercice :

pour chacune des classes A, B et C

- calculer la plus petite et la plus grande valeur décimale du premier octet
- calculer le nombre de réseaux théoriquement adressables
- calculer le nombre d'hôtes théoriquement adressables par réseaux
- calculer le nombre total d'hôtes adressables

Classe	+ petite valeur 1er octet	+ grande valeur 1er octet	Nombre réseaux	Nombre hôtes par réseau	Nombre hôtes Total
A					
B					
C					

Classe A : (valeur du premier octet comprise entre 0 et 127)

- Le premier bit est forcé à 0.
- Avec les 7 bits restant, nous pouvons définir 126 adresses réseaux (l'adresse 127 étant réservée). Chacune de ces adresses pouvant supporter plus de 16 millions de machines (2^{24}), nous obtenons plus de 2 milliards ($126*2^{24}$) d'adresses théoriques.

Classe B : (valeur du premier octet comprise entre 128 et 191)

- Les 2 premiers bits sont forcés à 10.
- Avec les 14 bits restant, nous pouvons définir plus de 16384 réseaux de plus de 65535 machines chacune, soit plus de 975 millions d'adresses théoriques.

Classe C : (valeur du premier octet comprise entre 192 et 223)

- Dans cette classe, les 3 premiers bits sont forcés à 110.
- On peut définir avec les 21 bits qui restent 2097152 réseaux (2^{21}) comprenant chacun 256 machines soit près de 540 millions de machines connectées.

Classe D : La classe D est réservée au multicast. C'est un moyen pour envoyer des données d'un serveur vers de multiples clients en une seule opération.

Classe E : La classe E est réservée pour un usage ultérieur.

Malgré ces possibilités d'adressage, la capacité initialement prévue est insuffisante et sera mise à défaut d'ici quelques années. L'IPNG (*Internet Protocol Next Generation*) devrait permettre de résoudre ces difficultés en utilisant un adressage sur 128 bits contre 32 actuellement : IP v6. Les adresses IP V4 resteront compatibles avec la nouvelle numérotation.

4.3 Les adresses IP réservées

Un certain nombre d'adresses sont réservées pour des utilisations particulières: Elles n'ont pas d'existence physique et ne doivent en aucun cas être utilisées en temps qu'adresse de machine.

4.3.1 Adresse de réseau

On désigne l'adresse de réseau en spécifiant tous les bits de l'hôte à 0.

Ex : 192.168.1.0 désigne le réseau 192.168.1 pour un réseau de classe C

4.3.2 Adresse de diffusion(broadcast)

On désigne adresse de diffusion lorsque tous les bits de l'hôte sont à 1

Ex : 192.168.1.255 est diffusée à tous les éléments du réseau. Une diffusion sert à mettre en place des tables de routage dans les switchs (qui est où).

4.3.3 Adresse de bouclage

Lorsque l'adresse IP commence par 127 (127.0.0.1), cette adresse est appelée adresse de bouclage (Loopback). Cette adresse permet
Soit des communications inter processus sur la même machine
Soit de vérifier que les éléments (carte réseau, protocoles TCP/IP) sont correctement installés.

Ce type de communication ne sort jamais de la machine.

```
C:\Documents and Settings\philippe>tracert 127.0.0.1

Détermination de l'itinéraire vers localhost [127.0.0.1]
avec un maximum de 30 sauts :

  1    <1 ms    <1 ms    <1 ms  localhost [127.0.0.1]

Itinéraire déterminé.
```

4.3.4 Adresse IP à 0

Lorsque tous les bits de l'adresse IP sont à 0 (0.0.0.0), cette demande est dirigée vers le serveur DHCP qui répond en envoyant une adresse valide.

4.3.5 Résumé des adresses IP particulières

Tout à 0		"Cet ordinateur" (1)
Tout à 0	id-ord	Cet ordinateur (id-ord) sur ce réseau (1)
Tout à 1		Diffusion limitée au réseau d'attachement (2)
Id-réseau	Tout à 1	Diffusion dirigée vers ce réseau (2)
127	Nombre quelconque (souvent 1)	Adresse de rebouclage (3)

(1) : Autorisé uniquement au démarrage du système. N'est pas une adresse valide
(2) : N'est pas une adresse valide
(3) : Ne doit jamais apparaître sur le réseau

4.3.6 Adresses Statiques ou dynamiques

Quand une configuration IP est réalisée sur chaque machine en spécifiant de façon fixe son adresse, on parle de **configuration statique.**

Si l'affectation est laissée à la charge d'un serveur sur le réseau, on parle d'affectation dynamique. Le serveur chargé d'attribuer les adresses IP fait appel au protocole DHCP (Dynamic Host Configuration Protocol).

Attention : 2 machines sur le réseau ne peuvent pas avoir la même adresse. Cela représente un conflit.

4.4 Le protocole DHCP

Le protocole DHCP (*Dynamic Host Configuration Protocol*) permet une configuration dynamique des adresses IP et des informations associées. Ceci signifie que chaque hôte du réseau est capable de solliciter de lui-même une configuration IP auprès d'un serveur spécialisé appelé serveur DHCP. Le serveur DHCP lui attribuera une adresse IP, l'adresse d'une passerelle par défaut ainsi que d'autres paramètres réseaux.

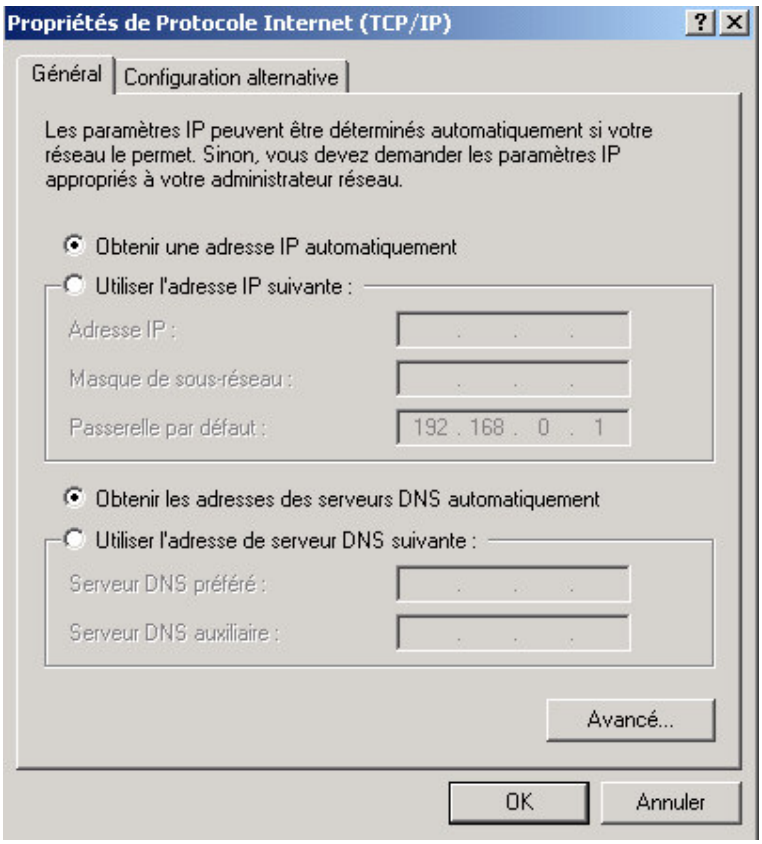
L'administrateur de réseau contrôle le mode d'attribution des adresses IP en spécifiant une durée de bail qui indique combien de temps l'hôte peut utiliser une configuration IP attribuée, avant de devoir solliciter le renouvellement du bail auprès du serveur DHCP.

Le protocole DHCP

- Facilite la gestion du réseau
- Empêche les conflits d'adresse
- Contrôle l'affectation des adresses IP de manière centralisée

Un serveur DHCP peut être une machine équipée d'un OS serveur (NT4, 2000, 2003 Serveur, Linux …) ou un routeur équipé de cette fonction.

Configuration de l'adressage IP sous Windows XP Pro



4.5 Les adresses privées

L'INTERNIC qui est l'organisme qui gère les affectations des adresses IP a réservé quelques adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet, sans risquer de créer des conflits d'adresses IP sur le réseau. Il s'agit des adresses suivantes:

- 10.0.0.1 à 10.255.255.254
- 172.16.0.1 à 172.31.255.254
- 192.168.0.1 à 192.168.255.254

Ces adresses ne sont pas affectées sur Internet.

5 Les masques de sous réseau

5.1 Présentation

En utilisant des adresses de classe A, B ou C, le nombre d'ordinateurs est souvent supérieur au besoin. Il peut être utile pour des besoins de gestion ou de confidentialité de segmenter le réseau en plusieurs sous-réseaux. La technique utilisée se base sur le masque de sous réseaux. Cette segmentation permet d'utiliser une partie des bits d'adresse hôte pour identifier les sous-réseaux.

Les masques de sous-réseau ont le même format que les adresse IP, soit quatre octets en décimal séparés par des points. Le principe de fonctionnement est le suivant :

- Les bits du masque de sous réseau correspondant dans l'adresse IP au réseau ainsi qu'au sous réseau sont à 1
- Les bits correspondant à l'ordinateur sont à 0

Masque de sous réseau par défaut sans segmentation :

- Classe A 255.0.0.0
- Classe B 255.255.0.0
- Classe C 255.255.255.0

Dans ce cas, les bits à 1 correspondent aux bits de l'adresse IP définissant le réseau.

Ex :

Adresse : 192.168.10.20
Masque : 255.255.255.0

Pour obtenir l'adresse de réseau, on effectue un et entre l'adresse et le masque

- → Adresse de réseau = 192.168.10.0
- → Adresse de machine = 20

Comme l'adresse réseau résultant du masque correspond à l'adresse de réseau, on en déduit que le réseau n'est pas segmenté.

5.2 La notion de passerelle

Toutes les machines d'un même réseau et communiquant entre elles disposent de la même adresse de réseau. Quand une machine définit comme adresse de destination une machine n'appartenant pas au réseau, cette adresse est soumise à la passerelle qui est chargée de

- Rechercher l'hôte de destination
- Router le paquet vers cet hôte de destination.

Une passerelle est une machine (serveur équipée de 2 cartes réseaux ou routeur) assurant les fonctions de routage vers les autres réseaux.

Pour déterminer si le paquet appartient au réseau, la machine émettrice applique son masque de sous réseau à l'adresse IP de destination.

- Si le réseau de l'adresse IP de destination est identique à celui de la machine, le paquet concerne le réseau local (réseau et sous réseau).

- Si le réseau de l'adresse IP de destination est différent de celui de la machine, le paquet sera envoyé vers la passerelle.

5.3 La segmentation

Le but de la segmentation est multiple

- Etendre un réseau vers un autre bâtiment ou un autre site à travers un routeur (les 2 sous réseaux ne peuvent avoir la même adresse).
- Séparer des groupes de machines dans un même réseau physique (chaque groupe de machine ayant son propre sous réseau, ils ne peuvent se voir directement).
- Conserver une même adresse de réseau de base (classe B ou C) et travailler sur les sous réseaux afin d'optimiser le nombre de machines dans le cas de grands réseaux privés.

Exemple de segmentation :

On considère un réseau de classe C : 192.168.1.0

- Le masque de sous-réseau est 255.255.255.0
- Ce réseau permet d'identifier 254 machines.

On souhaite créer 4 sous -réseaux dans ce réseau.

- Ces sous-réseaux seront pris dans le 4 éme octet désignant les machines
- Le nouveau masque de sous réseau sera 255.255.255.192 (dernier octet : 1100 0000)
- Les nouveaux sous réseaux créés seront :
  - 192.168.1.0 (dernier octet : 0000 0000 → 00H)
  - 192.168.1.64 (dernier octet : 0100 0000 → 40H)
  - 192.168.1.128 (dernier octet : 1000 0000 → 80H)
  - 192.168.1.192 (dernier octet : 1100 0000 → C0H)
- Les adresses machines seront codées sur les 6 bits de poids faible du dernier octet, ce qui donne de 000001 (01H)→ 111110 (3EH) donc de 1 →62 (Les adresses tout à 0 ou 1 sont réservées)
- On pourra donc adresser 62 machines par sous réseaux, les adresses IP allant de :
  - 192.168.1.1 → 192.168.1.62
  - 192.168.1.65 → 192.168.1.126
  - 192.168.1.129 → 192.168.1.190
  - 192.168.1.193 → 192.168.1.254

- En utilisant 2 bits, on crée 4 sous réseaux (2^2) de 61 machines (2^6 -2)
- En utilisant 3 bits, on crée 8 sous réseaux (2^3) de 30 machines (2^5 -2)
- …

Remarques :

- Un numéro de sous réseau ne peut être composé de bits tous positionnés à zéro ou tous positionnés à un (ces configurations sont réservées). Autrement dit, les valeurs minimum (zéro) et maximum ne peuvent être utilisées pour identifier un sous réseau.
- Pour créer des sous réseaux, on peut utiliser n'importe quel bit de ou des octets (classe B) de codage des nos de machine. Néanmoins, il est plus facile d'utiliser les bits de poids fort.

6 Exercices

6.1 Exercice

En reprenant le découpage en classe et le nombre de réseaux, calculer le nombre de réseaux affectables disponibles sur Internet en tenant compte :

- Des adresses réservées
- Des adresses privées

6.2 Exercice (base Exonet 25)

6.2.1 Contexte de travail

Vous souhaitez installer sur une station Windows le service d'accès réseau à distance pour vous connecter à votre prestataire de services Internet. Lors du paramétrage de ce service, vous déclarez que l'adresse IP du serveur distant est 134.157.130.45.

6.2.2 Travail à Réaliser

1. A quelle classe d'adresses IP appartient l'adresse du serveur distant ?
2. Le masque de sous-réseau utilisé est 255.255.255.128. Combien de sous-réseaux peuvent-être définis ?
3. Lors d'une connexion, la station se voit allouer l'adresse 134.157.130.19. Précisez à quel sous-réseau est associée la station.

6.3 Exercice : (base Exonet 61)

6.3.1 Contexte de travail

Un établissement scolaire utilise un serveur mandataire (Proxy) nommé KIKA-AKC dans le DNS, pour contrôler les accès à Internet.
Ce Proxy permet entre autre d'autoriser ou pas l'accès à Internet en fonction de l'adresse IP du réseau auquel appartient la machine.
L'administrateur du réseau a organisé son plan d'adressage en fonction des salles.
Chaque salle dispose d'une plage d'adresses spécifique qui va permettre au niveau du Proxy d'interdire ou d'autoriser l'accès à Internet à tous les postes de la salle.

- L'annexe 1 donne le plan d'adressage utilisé.
- L'annexe 2 donne les règles d'accès à Internet pour la journée du 28 janvier 2002

6.3.2 Travail à Réaliser

1. Déterminer quelles sont les salles qui n'ont pas accès à Internet le 28 janvier.
2. Expliquer pourquoi le Proxy peut appliquer des masques différents alors que les postes sont tous configurés avec le même masque et la même adresse réseau.
3. Donner la ou les règles à appliquer pour interdire l'accès à la salle 204 et 208.
4. Donner la règle à appliquer pour interdire l'accès à la salle 201 et 202.
5. Expliquer les autres fonctions d'un Proxy.

6.3.3 Annexes 1 :Plan d'adressage

Adresse IP du réseau de l'établissement :
10.100.40.0
Masque du réseau :
255.255.255.0
Plage d'adresses par salle :

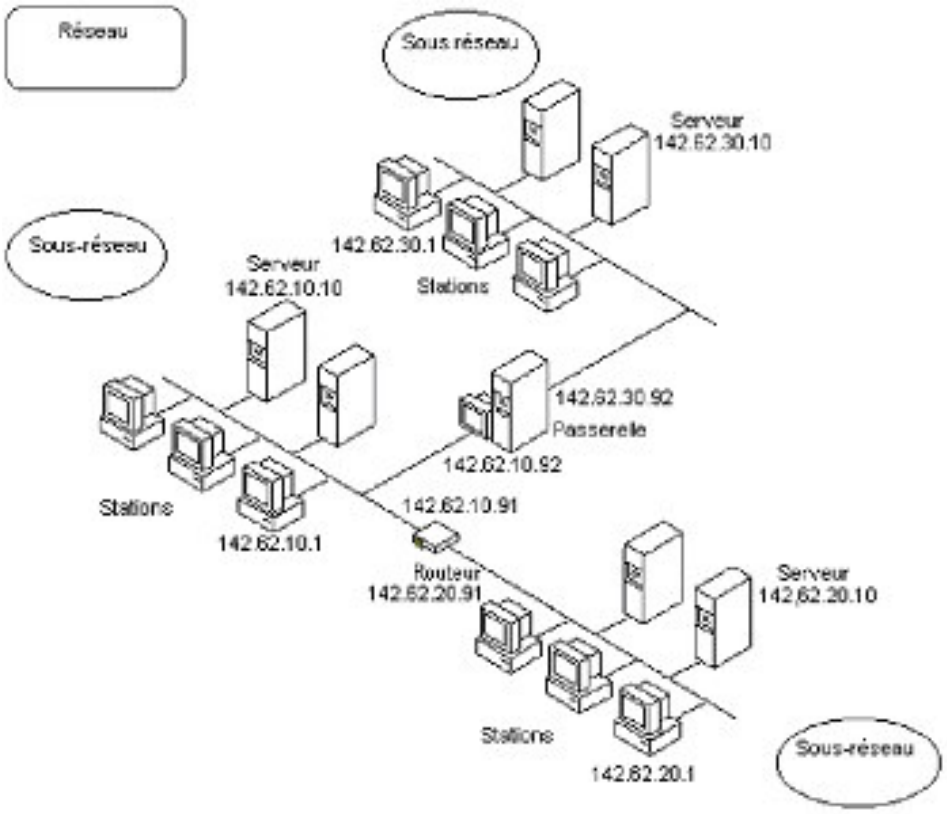
Salle 201 : 10.100.40.1 à 10.100.40.15	**Salle 206 :** 10.100.40.129 à 10.100.40.142
Salle 202 : 10.100.40.17 à 10.100.40.31	**Salle 207 :** 10.100.40.145 à 10.100.40.158
Salle 203 : 10.100.40.33 à 10.100.40.62	**Salle 208 :** 10.100.40.161 à 10.100.40.174
Salle 204 : 10.100.40.65 à 10.100.40.70	**Salle 209 :** 10.100.40.177 à 10.100.40.190
Salle 205 : 10.100.40.96 à 10.100.126	**Salle 210** : 10.100.40.73 à 10.100.40.78

6.3.4 Annexe 2 : Règles du 28 Janvier 2002

Accès autorisé à tous sauf aux réseaux ci-dessous :
10.100.40.32 masque 255.255.255.224
10.100.40.128 masque 255.255.255.192

6.4 Exercice : (base exonet 21)

6.4.1 Contexte de travail



6.4.2 Travail à Réaliser

1. Pourquoi la passerelle placée au milieu du schéma possède-t-elle deux adresses IP ?
2. Proposez une adresse réseau et un masque pour chaque sous-réseau