

## Réseau

Bande passante : Quantité d'informations pouvant être transmis dans un intervalle de temps  
(Généralement Bits par seconde)

Débit : la mesure du transfert des bits par seconde sur un support donné.

### Le Cisco IOS :

Tous les équipements réseau ont des systèmes d'exploitation

CISCO a ce qu'on appelle IOS pour ses équipements (Internetwork Operating System)

L'IOS est stocké dans la mémoire Flash

L'accès aux périphériques CISCO se fait par :

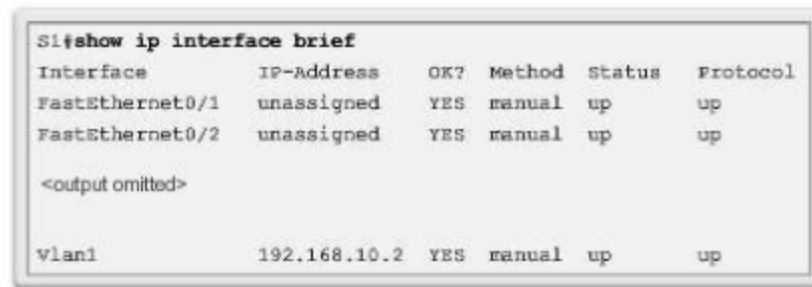
Console (nécessite un câble de console spécial) - Hors réseau

Telnet / SSH (Secure Shell) - Connexion à distance

port AUX - Hors réseau

Les modes de fonctionnement :

- Mode Utilisateur : Ping / Show / Enable ...
- Mode privilégié : Mode d'utilisateur + Debug commands / Reload / Configure
  - Commande enable/disable pour passer/quitter mode privilégié
  - Quelques commandes :
    - Show mac-address-table
    - Show arp
    - Show vlan
    - Show interfaces
    - Show version
    - Show running-config/startup-config
  - Configuration de nom de hôte :
    - Configure terminal
    - Hostname <nomHôte>
  - Activer un mot de passe pour passer à mode privilégié :
    - Enable password
  - Configuration d'une interface :
    - Configure terminal
    - Interface <nomInterface>
    - Ip address <adresseIP> <masqueSousReseau>
    - No shutdown



```

S1#show ip interface brief
Interface          IP-Address      OK? Method Status  Protocol
FastEthernet0/1    unassigned      YES manual  up      up
FastEthernet0/2    unassigned      YES manual  up      up
<output omitted>
vlan1              192.168.10.2    YES manual  up      up

```

- Mode Configuration globale :

### Modele TCP/Ip :

Application -> Transport -> internet -> acces réseau

Modèle OSI :

Application->Présentation -> Sessions (http/DHCP/DNS/Telnet/FTP)

Transport->TCP/UDP

Réseau -> IP

Liaison de données->Physique

Adresse Logique : IP

Adresse Physique : MAC

Adressage IP Dynamique : DHCP : Dynamic Host Configuration Protocol

La Couche appliation :

Les protocoles :

DNS (Domain Name Service) : Traduire une adresse web en IP

Telnet : Emulation de terminal

DHCP (Dynamic Host Control Protocol) : Attribuer les Adresses IP, masque de sous réseau et passerelle par défaut à une hote :

Client envoie DHCP Discover

Serveur DHCP répond par DHCP Offer

Client envoie DHCP Request

Serveur Envoie DHCP Ack

FTP : File Transfer Protocol

HTTP : HyperText Transfer Protocol (Navigation Web)

SMTP : Simple Mail Transfer Protocol (Envoi des Emails )

IMAP : Internet Message Access Protocol

POP : Post Office Protocol ( Réception des Emails)

Roles de chaque couche :

**Présentation :**

- Codage et conversion des données de la couche application
- Compression
- Chiffrement et déchiffrement

**Session :**

- Créer et gérer les communications entre source et destination

**Les deux modèles d'application :**

**PeerToPeer :**

- Chaque hôte joue à la fois le rôle de client et serveur en fonction de chaque requête
- Les deux périphériques sont égaux.

Exemple : Torrenting/ Bittorrent

**Client/Serveur :**

- Les ressources sont stockées sur le serveur :
- Le client envoie une requête pour recevoir ses données (Descendant)

**Exemple : Navigation Web :**

Le navigateur commence par interpréter les trois parties de l'adresse URL :

1. http (protocole ou schéma)
2. www.cisco.com (nom du serveur)
3. index.html (nom du fichier demandé)

Le navigateur fait appel à un serveur de noms pour convertir www.cisco.com en adresse numérique

Selon les règles du protocole HTTP, envoie une requête GET au serveur et demande le fichier index.html

Le serveur envoie le code HTML de cette page Web

Le navigateur déchiffre le code HTML et met la page en forme

**REMARQUE :** La transmission des données vers la bonne application en cas d'exécution instantanée se fait par le numéro de port.

**La Couche Transport :**

**Rôle :**

- Etablissement de la session de communication temporaire
- liaison entre la couche application et les couches inférieures.

**Responsabilités :**

- Suivi des conversations
- Segmentation : Diviser les données en petits segments pour faciliter leur transmission
- Un en-tête est ajouté à chaque segment pour faciliter leur identification
- Identification des applications : Selon les numéros de port

Fiabilité :

Deux protocoles de la couches Transport selon les besoins de l'application :

TCP : Transmission Control Protocol (HTTP - telnet - ftp - SMTP)

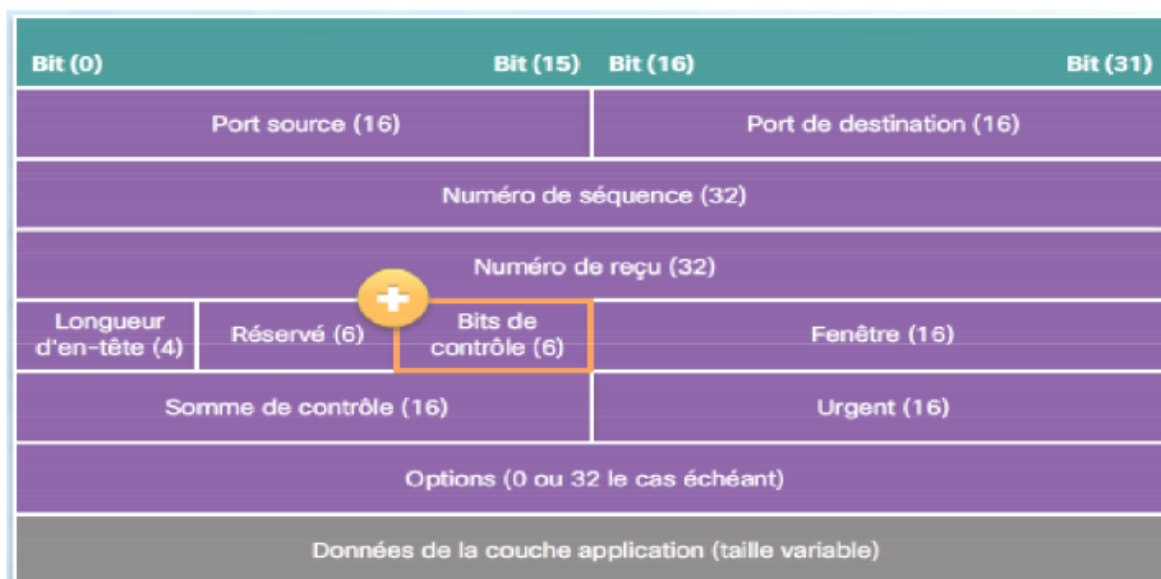
- Assure un acheminement fiable.
- Utilise les accusés de réception et d'autres mécanismes pour garantir la transmission
- Sollicite davantage le réseau

UDP : User Datagram Protocol => Acheminement au mieux (DNS - Voip - DHCP- IPTV)

- Fournit juste les fonctionnalités de base pour la transmission sans aucune garantie
- Moins de surcharge sur le réseau.

Les entetes :

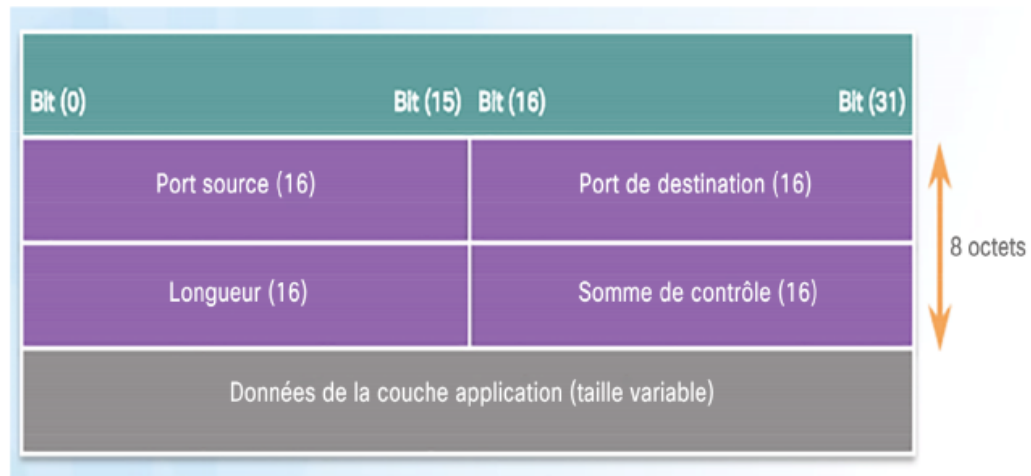
## Entête TCP



**URG** - Champ de pointeur urgent significatif  
**ACK** - Champ d'accusé de réception significatif  
**PSH** - Fonction Push  
**RST** - Réinitialiser la connexion  
**SYN** - Synchroniser les numéros de séquence  
**FIN** - Absence de données en provenance de l'expéditeur

# Entête UDP

- Le protocole UDP est un protocole sans état : aucun suivi
- Fiabilité prise en charge par l'application



La séparation des communication multiples se fait grace aux numéros de port :

Port Source : Port de l'application d'origine généré par l'expéditeur

Port Destination : Indique à la destination quel service est demandé; Exemple : les services web du port 80 sont demandés

Les ports reconnus :

- FTP - 20(Données)/21(Contrôle) - TCP
- SSH - 22 - TCP
- SMTP - 25 - TCP
- DNS - 53 - UDP/TCP
- DHCP - 67(Serveur)/68(Client) - UDP
- HTTP - 80 - TCP
- POP - 110 - TCP
- HTTPS - 443 - TCP

## Communication TCP :

3 étapes :

1. Vérification que la destination est bien présente sur le réseau
2. S'assurer que le périphérique de destination a un service actif et qu'il accepte les requêtes sur le numéro de port de destination que le client qui démarre la session a l'intention d'utiliser

3. Informer le périphérique de destination que le client source souhaite établir une session de communication sur ce numéro de port.

**Etablissement d'une session TCP :**

1. Le client envoie un SYN
2. Le serveur répond par SYN et ACK
3. Le Client répond par ACK

**Fermeture d'une session TCP :**

1. Le Client envoie FIN.
2. Le serveur répond par un ACK
3. Le serveur envoie un FIN
4. Le client répond par un ACK

**REGLES IMPORTANTS :**

**Num Seq = dernier Ack reçu**

**Num Ack = dernier num Seq reçu + données ( données = 1 en cas de SYN ou FIN)**

**La couche réseau :**

Le principal protocole est l'IP, il permet de :

La transmission des données en mode sans connexion

L'adressage et le routage des paquets entre stations par l'intermédiaire de routeurs

La fragmentation des données

Le protocole IP suit le principe d'acheminement au mieux:

Les champs de l'entete IP :

Version : indique la version du protocole IP (4 pour IPv4)

Longueur de l'en-tête : indique le nombre de mots de 32 bits constituant l'en-tête (5 pour une en-tête de 20 octets)

Type de Service (TOS) : désigne la qualité de service utilisable par le routeur (Indicateur de fiabilité, de priorité, de délai et de débit)

Longueur totale : longueur du paquet incluant l'en-tête et les données exprimée en octets (Permettant de spécifier une taille maximale de 65 535 octets)

Identificateur : identifie le paquet pour la fragmentation (Tous les fragments d'un même paquet identifiés par le même numéro)

**Drapeaux : gère la fragmentation:**

**"DF " (don't fragment): demande au routeur de ne pas fragmenter le paquet**

**"MF" (more fragment) : est positionné à 1 dans tous les fragments sauf le dernier**

**Position du fragment (offset):** position du fragment dans paquet La valeur du premier fragment est 0 Les fragments suivant sont exprimés en multiples de 8 octets

Durée de vie (Time To Live - TTL) : évite la circulation infinie des paquets sur le réseau  
Un paquet dont la durée de vie passe à 0 est détruit

Protocol: protocole de la couche supérieure (encapsulation)  
1 pour ICMP, 2 pour IGMP, 6 pour TCP, 17 pour UDP,...

Total de contrôle (checksum): vérifier validité de l'entête  
Adresse IP source : 172.24.91.201  
Adresse IP destination : Représentée en décimal pointé : 172.24.91.202

**En cas ou deux réseaux connectés à un meme routeur ont des longueurs de trame maximales différents (MTU max transfer unit) , la technique de fragmentation/réassemblage est activé...**

**Les champs les plus significatifs pour la fragmentation (Protocle IP)**

- **identification 16bits**
- **1 bit réservé**
- **Dont Fragment DF 1 bit**
- **More Fragment MF 1 bit**
- **Offset 13 bits**

**Protocole ARP** : Address Resolution Protocol

Il réalise la correspondance entre l'adresse physique MAC et logique IP

Si l'IP destination n'est pas sur le meme réseau, l'adresse MAC sera celle de la passerelle par défaut du réseau actuel

Pour lister la table ARP :

- Show ip arp (Cisco IOS)
- Arp -a (windows)

**Protocole ICMP** : il controle le traffic IP

**Routing IP** : Connaitre l'adresse MAC de destination à partir de son adresse IP

Chaque routeur doit connaitre l'adresse du routeur suivant

Deux types de routage :

- Routage statique :
  - Table de routage établie au départ des entrées peuvent être Rajoutées manuellement avec la commande « ip route »
- Routage dynamique :

- Table de routage mise à jour périodiquement à l'aide de protocoles spécifiques (RIP - Routing Information Protocol / OSPF - Open Shortest Path First)

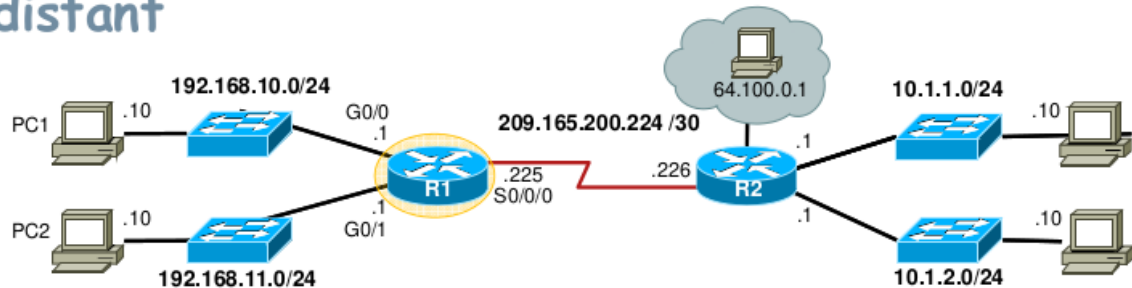
Une adresse réseau (IP) a une portée de bout en bout

Une adresse physique (MAC) a une portée locale dans son réseau ou sous-réseau

Table de routage :

- "netstat -a" windows
- "Show ip route" IOS :
  - Il existe des codes : (La façon dont le réseau a été appris par le routeur)
    - C : Connected
    - S : Static
    - L : Local
    - M : Mobile
    - R : RIP
    - OSPF : OSPF
- Exple :

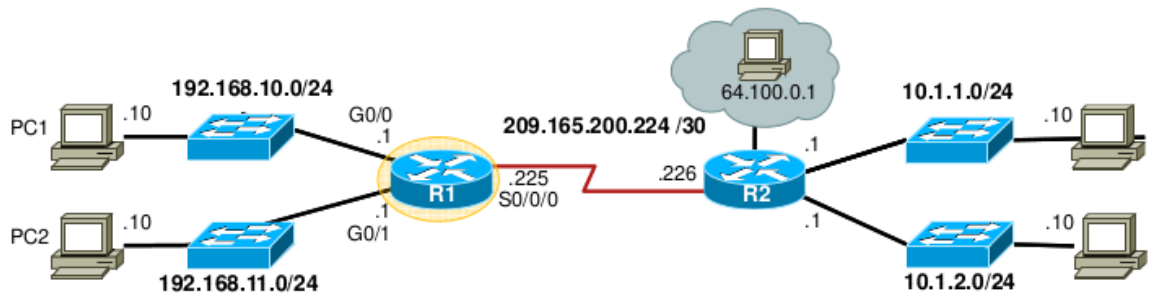
## Entrées d'une table de routage d'un réseau distant



<b>D</b>	10.1.1.0/24	[90/2170112]	via	209.165.200.226,	00:00:05,	Serial10/0/0
----------	-------------	--------------	-----	------------------	-----------	--------------

<b>A</b>	Indique la façon dont le réseau a été « appris » par le routeur.
<b>B</b>	Identifie le réseau de destination.
<b>C</b>	Identifie la distance administrative (fiabilité) de la route source.
<b>D</b>	Identifie la métrique pour atteindre le réseau distant.
<b>E</b>	Identifie l'adresse IP du saut suivant pour atteindre le réseau distant.
<b>F</b>	Identifie le temps écoulé depuis que le réseau a été découvert.
<b>G</b>	Identifie l'interface de sortie du routeur utilisée pour atteindre le réseau de destination.





A	B	C
C L	192.168.10.0/24 is directly connected, 192.168.10.1/32 is directly connected,	GigabitEthernet0/0 GigabitEthernet0/0

•

Étapes de configuration d'un routeur :

- Enable
- Configure terminal
- hostname <chooseHostname>
- Line console 0
- [config-line]Password <cisco>
- Login
- Exit
- Line vty 0 4
- Password <cisco>
- login
- Exit
- Copy running-config startup-config

Configuration des interfaces LAN :

- Enable
- Configure terminal
- Interface <nomInterface> 0/0 [Exple : interface gigabitethernet 0/0]
- [config-if] Ip address <AdresseSouhaité> <MasqueSousRéseau>
- No shutdown
- Exit

```

R1# show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       192.168.10.1    YES manual up          up
GigabitEthernet0/1       192.168.11.1    YES manual up          up
Serial0/0/0              209.165.200.225 YES manual up          up
Serial0/0/1              unassigned      YES NVRAM  administratively down down
Vlan1                    unassigned      YES NVRAM  administratively down down
R1#
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209 165 200 226, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
R1#

```

#### Limitations de IPv4:

- Manque d'adresses IP
- Croissance de la table de routage internet
- Absence de connectivité bout en bout

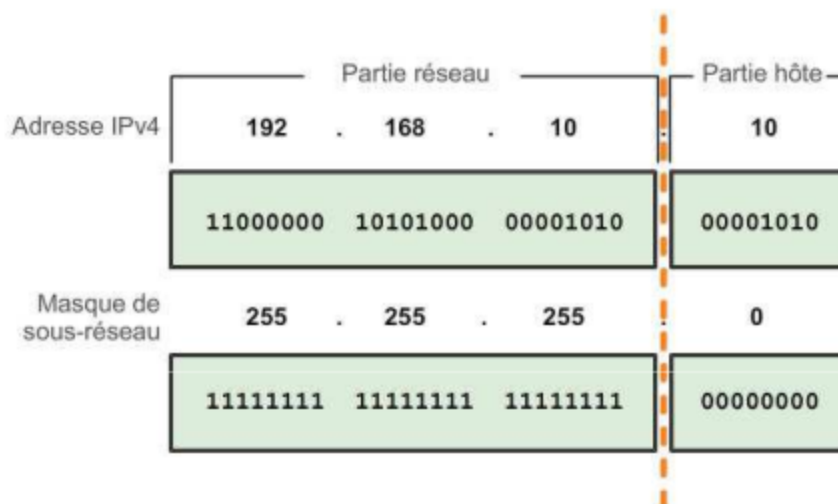
#### IPv6 :

- Amélioration du traitement des packets
- Elimination du besoin des NATs
- Sécurité intégré

#### Adressage IPv4 :

Les adresse IPv4 sont exprimés en 32 bits en total 4 \* 1 octet séparés par des points.

Partie réseau et partie hôte:



Pour déterminer l'adresse réseau, on fait Adresse IPv4 AND Masque de sous réseau

## Masques de sous-réseau valides

Valeur du masque de sous-réseau	Valeur du bit							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Longueur du préfixe :

Comparaison du masque de sous-réseau et de la longueur de préfixe		
Masque de sous-réseau	Adresse 32 bits	Longueur de préfixe
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Décimale à point		Bits significatifs affichés en binaire
Adresse réseau	10.1.1.0/24	10.1.1.00000000
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.254	10.1.1.11111110
Adresse de diffusion	10.1.1.255	10.1.1.11111111
Nombre d'hôtes: $2^8 - 2 = 254$ hôtes		

Les différents types d'adresses d'un réseau exple : 192.168.10.0/24

- Adresse réseau : 192.168.10.0 (Partie Hôte complètement à 0)
- Adresses Haute:
  - Première Adresse 192.168.10.1
  - Dernière Adresse 192.168.10.254
- Adresse de diffusion 192.168.10.255 (Partie hôte complètement à 1)

Communication:

- Monodiffusion :
  - Utiliser l'adresse de l'équipement destinataire en tant qu'adresse de destination
- Diffusion (un à tous)
  - La partie hôte du réseau est remplie par des 1
- Multidiffusion :
  - 224.0.0.0 à 239.255.255.255

Les classes d'adresses IP					
Classe de l'adresse	Plage du premier octet (décimal)	Bits du premier octet (les bits en vert 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	128réseaux ( $2^7$ ) 16777214hôtes par réseau ( $2^{24}-2$ )
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16384réseaux ( $2^{14}$ ) 65534hôtes par réseau ( $2^{16}-2$ )
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2097150réseaux ( $2^{21}$ ) 254hôtes par réseau ( $2^8-2$ )
D	224-239	11100000-11101111	ND (multidiffusion)		
E	240-255	11110000-11111111	ND (expérimental)		

- **Adresses de bouclage** (127.0.0.0 /8 ou 127.0.0.1)
  - Utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle
- **Adresses link-local** (169.254.0.0 /16 ou 169.254.0.1)
  - Communément appelées adresses APIPA (Automatic Private IP Addressing)
  - Utilisées par le client Windows pour se configurer automatiquement si aucun serveur DHCP n'est disponible.
- **Adresses TEST-NET** (192.0.2.0 /24 ou 192.0.2.0 à 192.0.2.255)
  - Utilisées pour l'enseignement et l'apprentissage.

## NAT : Network Address Translation

Les adresses privés :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

**Implémentation:** le routeur NAT doit:

- *Datagrammes sortant: remplacer* (@ IP source, # port) de chaque datagramme sortant par (@ NAT IP, nouveau # port)  
... Les clients/serveurs à distance vont répondre avec (@ NAT IP, nouveau # port) comme adresse de destination.
- *mémoriser (dans la table de traduction NAT)* chaque paire de traduction (@ IP source, # port) à (@ NAT IP, nouveau # port)
- *Datagrammes entrant: remplacer* (@ NAT IP, nouveau # port) dans les champs de destination de chaque datagramme entrant avec la correspondance (@ IP source, # port) stockée dans la table NAT

## Adressage IPv6 :

Passage de l'ipv4 à l'ipv6 :

- Double pile
- Tunnelisation
- Traduction

Une adresse ipv6 est composée de 128 bits (8 \* 16 bits)

Longueur de préfixe standard est 64 bits

Ségmentation des réseau ipv6 :

