

Introduction au réseau de l'Internet

Ouvrage de référence: *Computer networking: A Top-Down approach featuring the Internet* Par Jim Kurose and Keith Ross

Internet

- Qu'est-ce qu'internet ?
- Qu'est-ce qu'un protocole ?
- Les bords du réseau
- Les cœurs du réseau
- Accès au réseau
- Couches de protocoles, modèles de services
- Modèles de réseaux

1. Internet, une vue d'ensemble

En 2016, sans doute 2 à 8 millions d'appareils connectés

- Hôtes ou systèmes terminaux
- Exécutent des applications réseau

Des liens de communication

- Cuivre, fibre optique, radio, satellite
- Taux de transfert = bande passante

Des routeurs

- Transmettent des paquets (morceaux d'information)

Tout routeur est une passerelle = Gateway

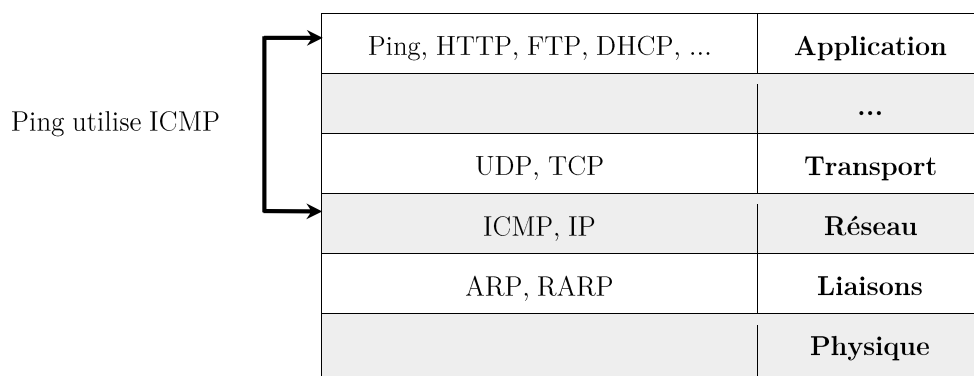
Il existe plusieurs protocoles qui contrôlent l'émission et la réception des messages. Par exemple : TCP, IP, HTTP, FTP, ICMP, DHCP

Il existe une IP unique par hôte connecté sur Internet du type :

192.168.1.0

Chaque nombre peut aller de 0 à 255 et constitue donc 256 valeurs différentes.

Au total, nous avons $(2^8)^4$ possibilités d'IP.



1.1. Les différentes classes de réseau

Ils se notent de A à E :

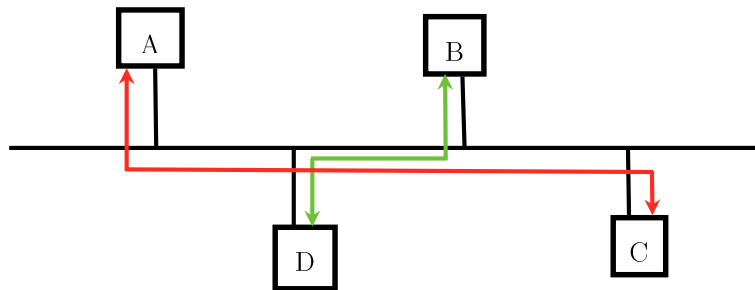
A
[0 => 127]

B, unicast
[]

C
[]

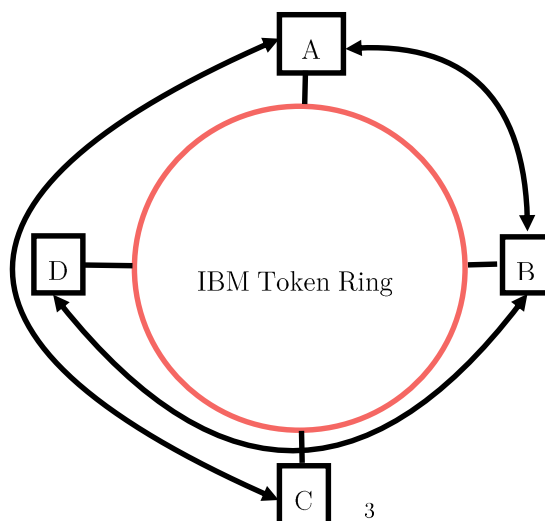
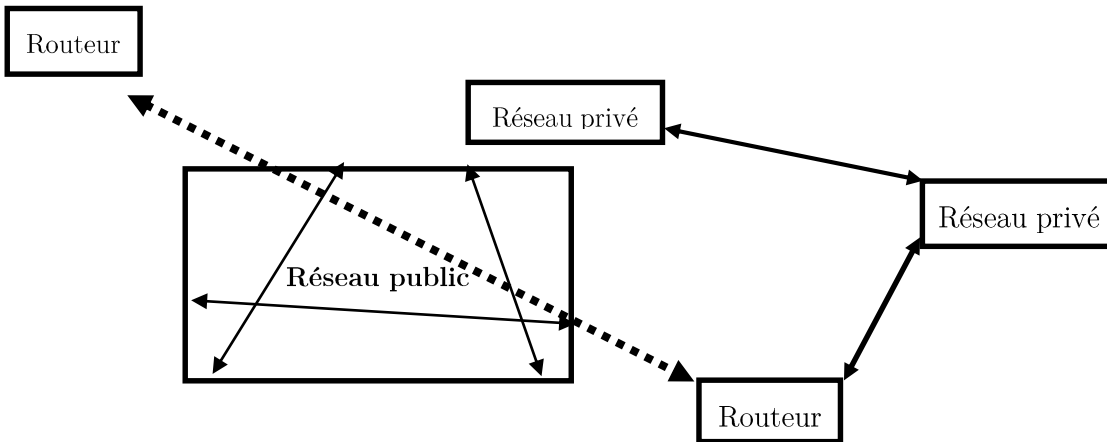
D, multicast
[]

E, expérimental
[]



Quelqu'un veut envoyer un message,

Problème: collision



1.2. Internet, une vue orientée services

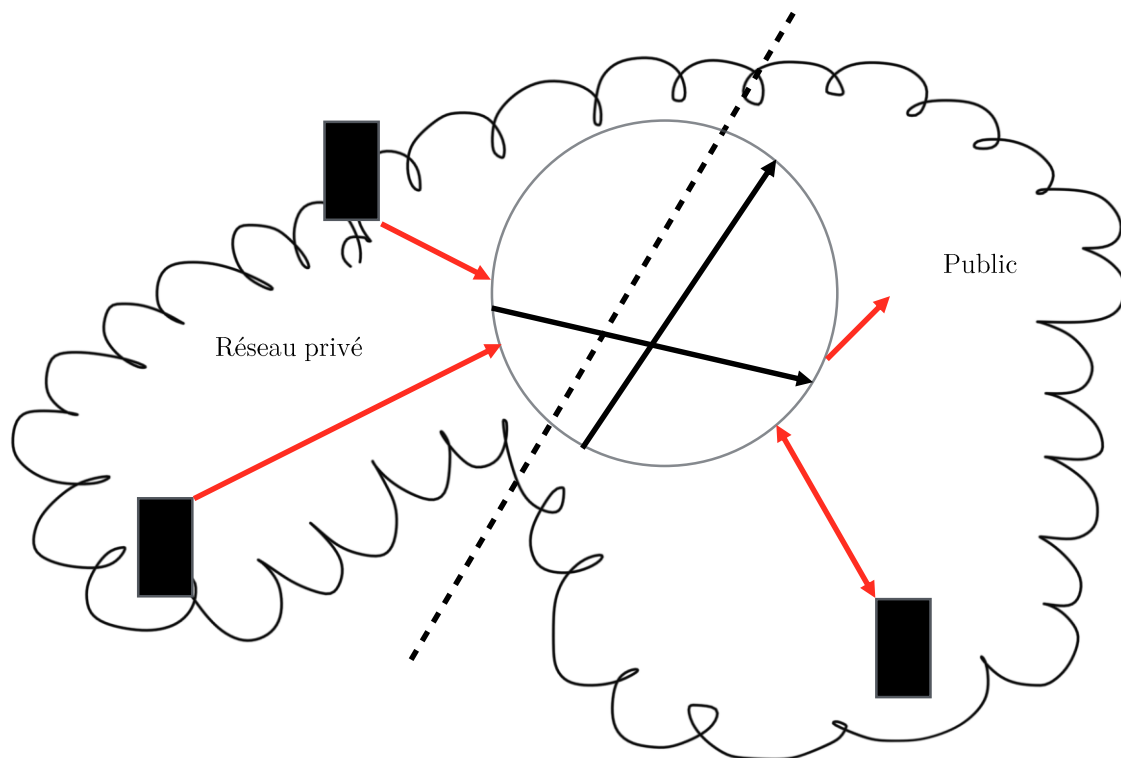
Infrastructures de communication

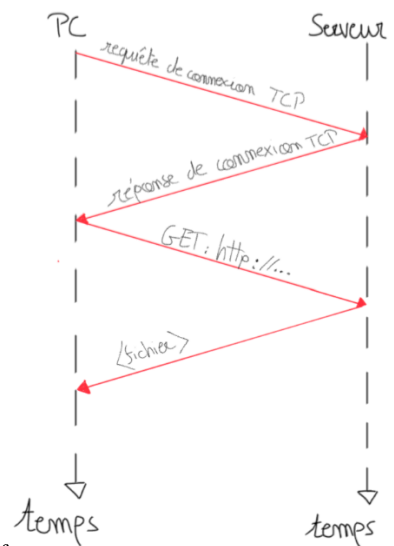
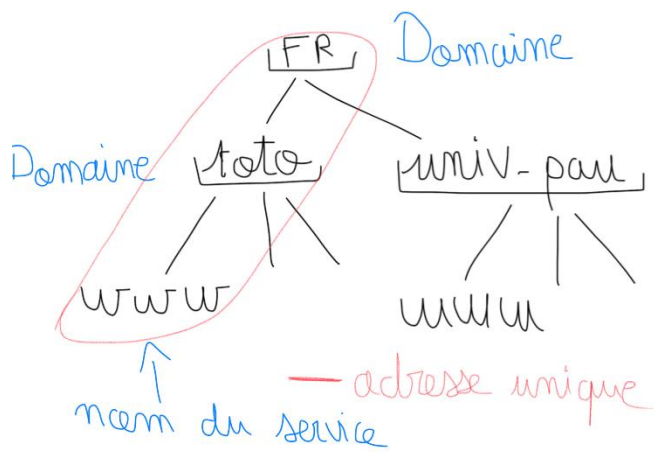
Différents services de communication sont offerts aux applications :

- Non connecté mais non fiable
- Connecté et fiable

2. Qu'est-ce qu'un protocole ?

Protocoles humains	Protocoles réseaux
Quelle heure est-il ?	Plutôt entre machines
J'ai une question	
Présentations	

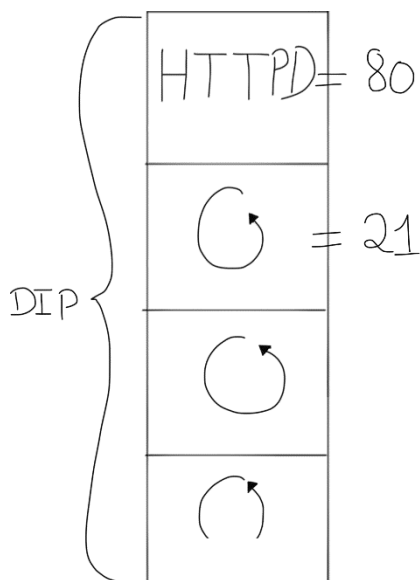




GET http://www.toto.fr/○ → si vide, direction vers index.html par défaut

Daemons = services qui fonctionnent en continu

httpd : daemon http



Un unique port par daemon

Par défaut : http://toto.fr:80/index.html

Un fichier texte html est sous la forme :

```

<HTML>
  <HEAD>
  </HEAD>
  <TITLE>
  </TITLE>
  <BODY>
    Texte
    Texte
  </BODY>
</HTML>

```

2.1. Les bords du réseau

- Systèmes terminaux (hôtes)
- Exécutent les « programmes applicatifs »
Ex : navigateur, email, chat, transfert de fichiers
- Modèle client-serveur :
 - Les hôtes clients émettent des requêtes et reçoivent des services des serveurs toujours actifs.
Ex : Navigateur, serveur web, client, service mail
- Modèle pair à pair :
 - Utilise peu (ou pas) de serveur dédiés
Ex : Gigatribe, BitTorrent, GUNet, Skype

2.1.1. Service orienté connexion

Objectif :

- Transfert de messages entre systèmes terminaux
- Poignée de main : établissement du dialogue
 - Le « Bonjour-Bonjour » du protocole humain
 - Fixe l'état des hôtes communicants
- TCP – Transmission Control Protocol : service orienté connexion d'internet
- Service TCP (RFC 793)
- Transfert de flux d'octets fiables et ordonnés
 - Si perte : accusés-réceptions et retransmissions
- Contrôle de flot
 - L'émetteur ne sature pas le récepteur
- Contrôle de congestion
 - Réseau congestionné : l'émetteur « ralentit son taux d'émission »
- Applications TCP :
 - HTTP (Web), FTP (Transfert de fichiers), Telnet (contrôle à distance), SMTP, DNS,...

2.1.2. Service non connecté

Objectif :

- Transfert de données entre systèmes terminaux
- Aucun échange

UDP – User Datagram Protocol (RFC 768)

- Non connecté
- Transfert non-viable
- Pas de contrôle de flot
- Pas de contrôle de congestion
- Applications UDP :
 - Flux multimédia, visio-conférence, DNS, VoIP

2.2. Le cœur du réseau

Question FONDAMENTALE : Comment sont transférés les messages sur le réseau ?

Deux types de méthodes de transfert :

- Commutation par circuit : un circuit par échange
- Commutation par paquet : messages envoyés en morceaux sur le réseau

2.2.1. Circuit :

- Ressources réservées de bout en bout pour un appel
- Pas de partage (ressources dédiées)
- Performances garanties
- Etablissement de l'appel nécessaire
- Ressources réseau (ex : bande passante) découpées en tranches :
 - Tranches allouées aux échanges
 - Ressource inactive si non utilisée par moment lors de l'échange actif (pas de partage)
- Deux manières de découper :
 - En fréquence : découpage en bandes (FDM)
 - En temps : intervalles cycliques (TDM)
- Multiplexage : envoi sur un même canal de plusieurs messages

Exercice :

Combien de temps faut-il pour envoyer un fichier de 640 000 bits de l'hôte A vers un hôte B sur un réseau à commutation de circuit ?

- Tous les liens ont une bande passante de 1,536 Mbps
- Chaque lien utilise TDM avec 24 slots/seconde
- Il faut 500 ms pour établir le circuit de bout en bout

$$\frac{\text{Bande-passante}}{\text{nbr-de-slots}} = \frac{1536000}{24} = 64000 = 64\text{kbps} \quad \text{temps} = \frac{640000}{64000} = 10\text{s} + \text{temps-du-circuit}$$

Temps : 10 + 0,5 s = 10,5 secondes

Avec fréquence : 24 canaux / fréquence :

Même temps.

2.2.2. Paquets

Division du flux de données (messages) en paquets

- Partage des ressources pour les paquets des utilisateurs A et B
- Totalité de la bande passante pour chaque paquet
- Utilisation des ressources uniquement quand nécessaire

Dispute des ressources

- Demandes cumulées > quantité de ressources disponibles
- Congestion : file d'attente des paquets pour utilisation d'un lien
- Stocker et acheminer

Pas de motifs fixes dans la séquence de paquets issus de A et de B

- Partage à la demande ← multiplexage statique

Commutation du paquet ou de circuit.

Plus d'utilisateurs avec la commutation de paquets.

- Lien à 1Mbps
- Utilisateur :
 - Emet 100 Kbps si actif
 - Actif 10% du temps
- Commutation de circuits :
- 10 utilisateurs concurrents

- Commutation de paquets. Avec 35 utilisateurs, la probabilité d'avoir plus de 10 actifs est inférieure à 0.004

$$P(A > 10) = 1 - \left(\sum_{i=0}^{10} 0,1^i \times 9^{(35-i)} \times c_{35}^i \right)$$

2.2.3. Réseaux à commutation de paquets : routage

Objectifs :

Transmettre des paquets de la source à la destination au travers des routeurs

Rôle du routage :

- Déterminer le(s) chemin(s) que vont prendre les paquets entre une source et une destination en essayant de trouver de bons chemins
- Routeur source : 1^{er} routeur accessible à la machine source
- Routeur destination : 1^{er} routeur accessible à la machine destination
- La problématique du routage se réduit à un chemin entre les routeurs sources et destinations
- La notion de bon chemin se traduit par la minimisation d'un coût
- Celui-ci dépend de la politique choisie : temps d'acheminement, ressources utilisées, ...

3. Couche application

3.1. Quelques applications

- Courrier électronique
- Web
- Messagerie instantanée
- Connexion à distance
- Calcul massivement parallèles
- Partage de fichiers pair à pair
- Jeux en réseau
- Vidéo diffusion
- Téléphonie sur le web
- Vidéo confère en temps réel

3.2. Architecture client-serveur

- Serveur :
- Hôte toujours actif
- Adresse IP permanente

Fermes de serveurs → passage à l'échelle

- Clients :
 - Communiquent avec le serveur
 - Connexion intermittente
 - Adresse IP dynamique
 - Ne communiquent pas entre eux

3.3. Vraie architecture pair à pair

- Serveur pas toujours actif
- Systèmes terminaux communiquent directement entre eux
- Pairs connectés de façon intermittente
- Changement d'adresse IP
- Ex : Gnutella

3.4. Hybrides entre client-serveur et pair à pair

3.4.1. Principe

- Un serveur central sert d'annuaire pour enregistrer/trouver les pairs
- Un pair recherche dans l'annuaire un ou plusieurs pairs correspondant à sa demande
- Ensuite, le pair demandeur se met en relation directe avec ces pairs
- Gestion plus facile !

3.4.2. Napster

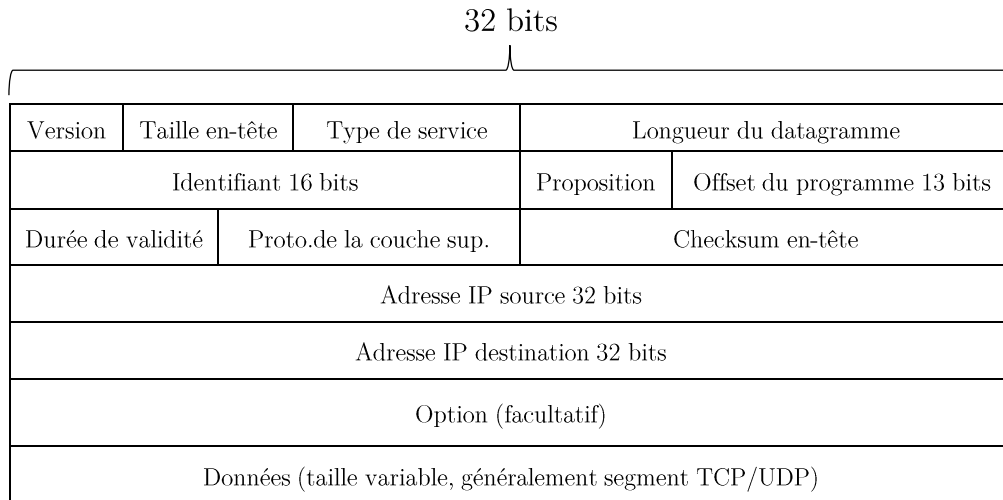
- Partage de fichiers pair à pair
- Recherche centralisée :
 - Enregistrement du contenu des pairs sur le serveur central
 - Requêtes sur le même serveur central pour trouver un fichier

3.4.3. Messagerie instantanée

- Deux utilisateurs qui chattent -> pair à pair
- Détection de présence centralisée :
 - Enregistrement de l'adresse IP sur le serveur central à la connexion
 - Serveur central contacte pour trouver les adresses IP des contacts

4. IP : Internet Protocol

4.1. Forme de datagramme IP

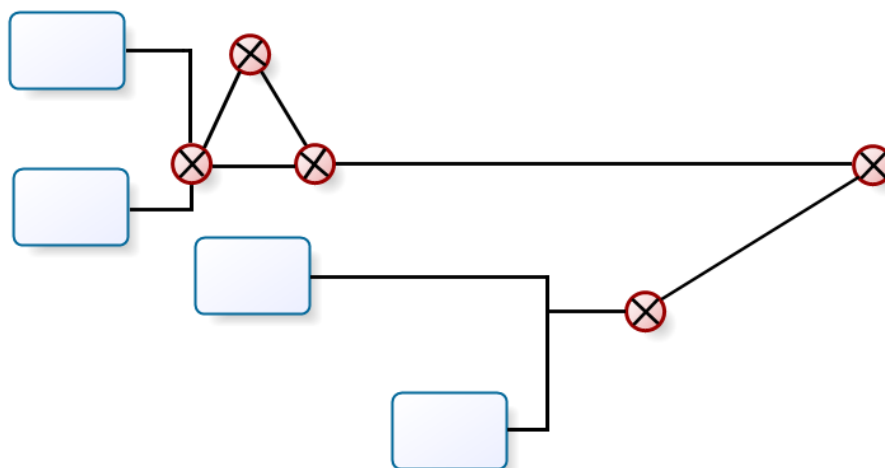


- * Version : numéro de version du protocole IP
 - * Taille en-tête :
 - * Type de service : type de données
 - *
 - * Durée de validité : nombre max de sauts restants (décrémenté à chaque routeur)
 - * Protocole de la couche supérieure : à qui livrer la charge utile
 - * Checksum : façon algorithmique de vérifier le checksum
 - * Etiquette temporelle
 - * Route prise
 - * Liste des routeurs à visiter
 - * ...
- } Options

Quel surcoût avec TCP ?

- * 20 octets de TCP
 - * 20 octets d'IP
- ⇒ 40 octets + surcoût de la couche application

4.2. Fragmentation et réassemblage IP



Les liens réseau ont une MTU (Maximal Transfert Unit)

- Plus grande trame autorisée au niveau des liaisons
- Différents types de liens

Les grands datagrammes IP sont fragmentés sur le réseau

- Un datagramme devient plusieurs datagrammes
- Ils sont réassemblés uniquement arrivés à destination
- Les bits de l'en-tête IP sont utiles pour identifier et relier les fragments reliés

4.3. Adresse IPV4 : Principes

Adresse IPV4 : identifiants 32 bits de l'interface d'un hôte et d'un routeur

Interface : connexion entre un hôte ou un routeur et un lien physique :

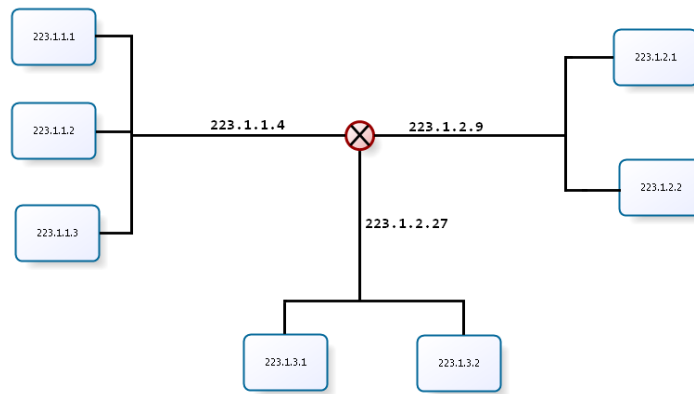
- Un routeur à plusieurs interfaces
- Un hôte a généralement une interface
- L'adresse IP est associée à chaque interface

Base 10 :

223.1.1.1 = 4 octets, avec 8 bits par octet. Donc il y a un total de 32 bits, ce qui donne un nombre 2^{32} combinaisons différentes possibles.

Base 2 :

223.1.1.1 = 223	1	1	00000001	
223.1.1.1 = 223	00000001	00000001	00000001	00000001
223.1.1.1 = 11011111	00000001	00000001	00000001	



ARP (Protocol Couche Liaison) : IP => @Mac

RARP : @Mac => IP

Utilisation d'un masque de connexion :
255.255.255.0

4.4. Adresse IPV4 en Classe

4.4.1. Adresse générales

Classe	Bits au départ	Début	Fin	Notation CIDR	Masque de réseau
A	0	0.0.0.0	127.255.255.255	/8	255.0.0.0
B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
D (Multicast)	1110	224.0.0.0	239.255.255.255		Non définit
E (Réservée)	1111	240.0.0.0	255.255.255.255		Non définit

4.4.2. Adresses privées :

De manière globale :

Classe	Début	Fin
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.1.0	192.168.255.255

De manière plus précise :

Adresse	Masque	Description	Référence
0.0.0.0	\8	Adresse réseau par défaut	RFC 1700
10.0.0.0	\8	Adresses privées	RFC 1918
127.0.0.0	\8	Adresse de bouclage (localhost)	RFC 1122
169.254.0.0	\16	Adresses locales auto-configurées	RFC 3927
172.16.0.0	\12	Adresses privées	RFC 1918
192.0.0.0	\24	Réservées par l'IETF	RFC 5736
192.0.2.0	\24	Réseau de TEST-NET-1	RFC 5737
192.88.99.0	\24	6to4 anycast	RFC 3068
192.168.0.0	\16	Adresses privées	RFC 1918
192.18.0.0	\15	Tests de performance	RFC 2544
192.51.100.0	\24	Réseau de TEST-NET-2	RFC 5737
203.0.113.0	\24	Réseau de TEST-NET-3	RFC 5737
224.0.0.0	\4	Multicast	RFC 3171
240.0.0.0	\4	Réservé à un usage non précisé	RFC 112
255.255.255.255	\32	Broadcast limité	RFC 919

Adresse IPV4

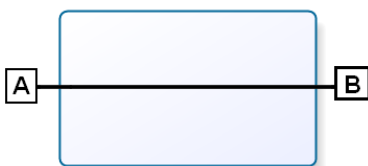
Partie sous-réseau (bits de poids fort)

Partie hôte (bits de poids faible)

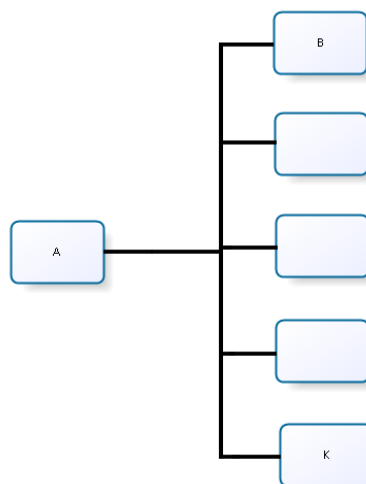
Qu'est-ce qu'un sous réseau ?

- Interfaces de périphériques ayant le même sous-réseau logique dans leur adresse IP
- Peuvent s'atteindre directement sans passer par une passerelle (Gateway)

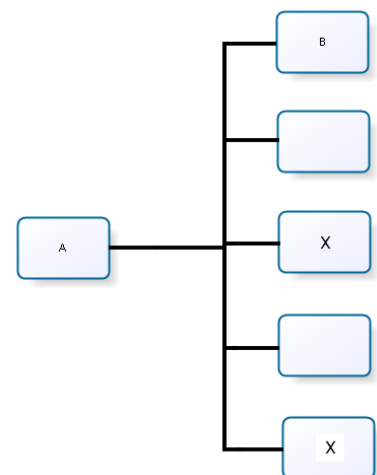
Unicast :



Broadcast :

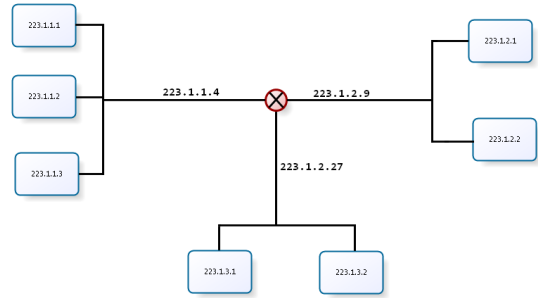


Multicast :



223.1.1.1		223.1.1.3
Application	Message	Application
Transport		Transport
Réseau	IP Logique	Réseau
Liaison	ARP	Liaison
Physique	@MAC	Physique

Envoi du message sous forme électrique



- @IP : 223.1.1.1
- @Réseau : 223.1.1.0
- @Masque : 255.255.255.0
- @Broadcast : 223.1.1.255
- @Gateway : 223.1.1.4

223.1.1.1 effectue un broadcast en demandant whois/whoas 223.1.1.3

Par contre pour envoyer un message de 223.1.1.1 à 223.1.3.1, un broadcast car 'x'223.1.x.1 est différent d'une adresse à l'autre. Il faut donc passer par le Gateway.

4.4.3. Masque

A	[0.0.0.0 – 127.0.0.0]	} Réseau strict
B	[128.0.0.0 – 191.255.0.0]	
C	[192.0.0.0 – 223.255.255.0]	

- Le masque de la classe A se trouve sur le premier octet (ex : 127) et se note aussi /8 pour les huit premiers bits
- Le masque de la classe B se trouve sur les deux premiers octets (ex : 191.255) et se note aussi /16
- Le masque de la classe C se trouve sur les trois premiers octets (ex : 223.255.255) et se note aussi /24

Aujourd'hui, à cause d'une importante perte d'adresses, les classes peuvent prendre n'importe quel masque /x

Ex : classe A avec un masque \20

Masque se code sur les 16 premiers octets de façon normale : 11111111.11111111...

Les quatre octets manquants se codent de la manière suivante : 11111111.11111111.11110000.00000000

Le nombre binaire 11110000 donne le nombre 240 en décimal.

Au final, le masque \20 de la classe A se note : 255.255.240.0