JFA 1

# CM 3
# Communication et fonctionnement bas niveau

**Jean-François ANNE**
jean-francois.anne@unicaen.fr
http://www.jfanne.fr
IUT de CAEN – Campus 3

IUT GRAND OUEST NORMANDIE – INFO – R 2.04

2022 - 2023

JFA 2

## Sommaire



IUT GRAND OUEST NORMANDIE – INFO – R 2.04

JFA 3

# Définition d'un réseau

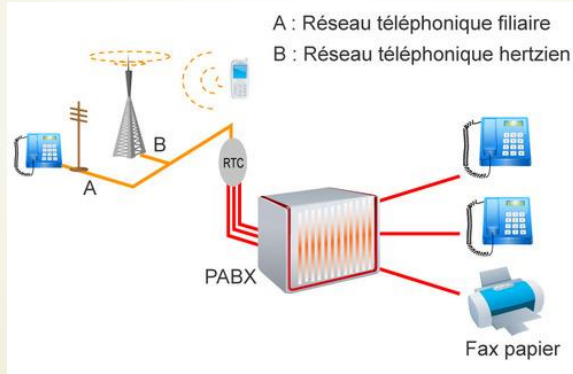
- C'est un ensemble d'équipements permettant à des individus ou à des groupes de partager des informations et des services d'un point à un autre.
- Exemples :
  - Réseau Téléphonique
  - Réseau Postal
  - Réseau Bancaire
  - Réseaux Informatiques

IUT GRAND OUEST NORMANDIE iNFO R 2.04

JFA 4

# Définition d'un réseau

- Exemples :
  - Réseau Téléphonique



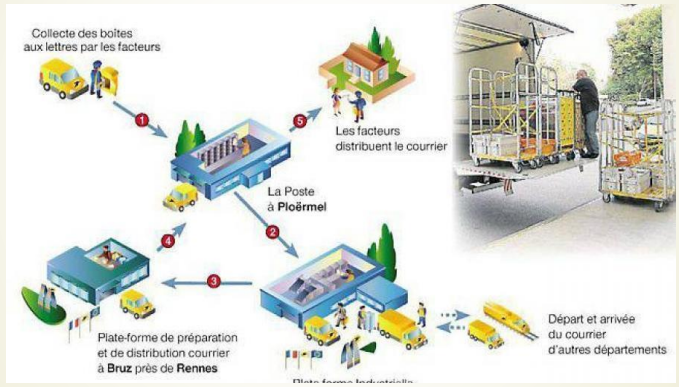

https://standard-telephonique.ooreka.fr/comprendre/installation

IUT GRAND OUEST NORMANDIE iNFO R 2.04

JFA 5

# Définition d'un réseau

- Exemples :
  - Réseau Postal

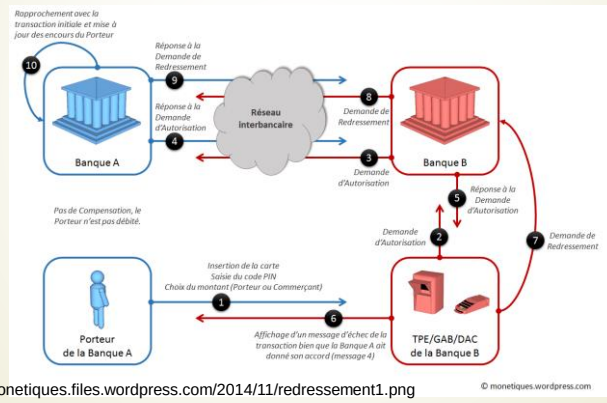



http://www.ouest-france.fr/sites/default/files/styles/image-900x500/public/2013/10/07/quel-parcours-pour-une-lettre-postee-ploermel-3f0.jpg?itok=_OtYQ2Pi

JFA 6

# Définition d'un réseau

- Exemples :
  - Réseaux Bancaires

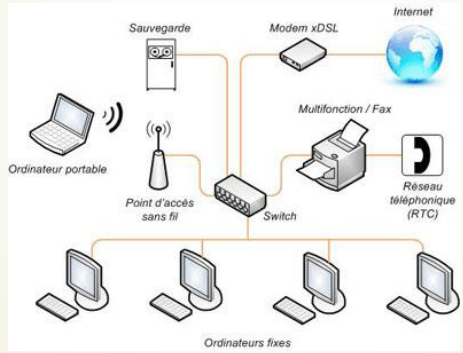



https://monetiques.files.wordpress.com/2014/11/redressement1.png

JFA 7

# Définition d'un réseau

- Exemples :
  - Réseaux Informatiques




http://www.abmsi.fr/wp-content/uploads/2010/01/Reseau-TPE-ECOLES.jpg

JFA 8

# Les réseaux de Données

Un réseau de données Informatique est un ensemble d'équipements reliés entre eux pour échanger de l'information :

- Les équipements terminaux qui sont consommateurs et émetteurs de données seront des Ordinateurs, Imprimantes, Faxes, ….,
- Les équipements d'interconnexion nécessaires aux échanges seront des points d'accès, modems, box, hubs, switches, routeurs/ passerelles, firewall, etc…
- Les équipements sont reliés par des supports physiques.
- Les données échangées seront des données numériques sous forme de mots binaires codés, qui seront transportées par des signaux Analogiques ou Numériques en suivant des règles précises dictées par des protocoles.

JFA 9

# Les réseaux de Données

IUT GRAND OUEST NORMANDIE iNFO R 2.04

Donc un réseau de données nécessite :

- Des supports de transmissions physiques (Fils de Cuivre, Fibre Optique, Air, …) ,
- Des protocoles de communications décrivant les règles de transmission :
  - Quel codage utiliser ?
  - À quelle vitesse communiquer ?
  - Organisation des données (bits, blocs, …)
  - Comment atteindre le destinataire,
  - ….

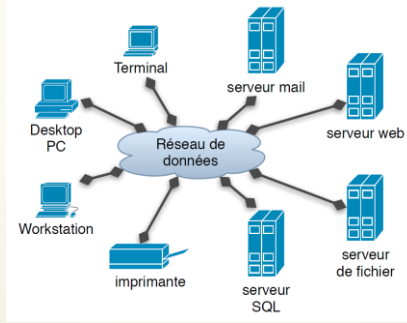
JFA 10

# L'objectif des réseaux de Données

IUT GRAND OUEST NORMANDIE iNFO R 2.04

Un réseau de données doit permettre :

- La transmission et la consultation des données,
- Le partage de ressources physiques,
- La sécurité des informations,



JFA 11

# Les principales applications des R. D.

R 2.04

Aujourd'hui, on utilise les réseaux de données informatiques pour :

- La consultation de pages Web,
- La messagerie électronique,
- La consultation de sites communautaires,
- Le commerce électronique,
- Le multimédia,
- L'interrogation de bases de données,
- Le transfert de fichiers,
- Le travail en groupe ou GroupWare

JFA 12

# Classification des réseaux de données

R 2.04

- **Les réseaux de données peuvent être classés par :**
  - **par leur architecture interne (filaire/non-filaire, équipements intermédiaires)**
  - **Par le type de commutations**
  - **par le type de transmission**
  - **Par le type de connexion**
  - **par leur étendue et leurs objectifs**
  - **par leur technique de transfert**
  - **par leur débit**
  - **par la qualité de service (fiabilité, délais, etc.)**

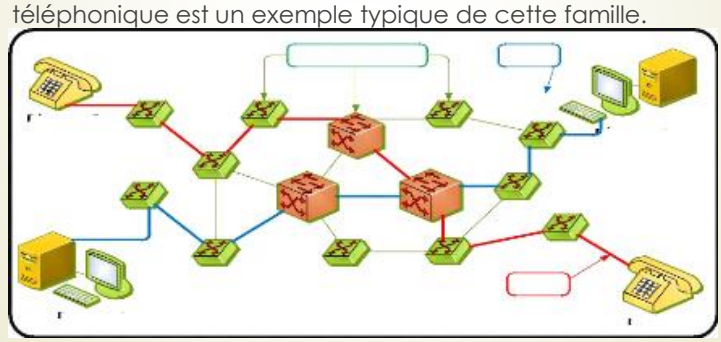
JFA 13

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE iNFO

R 2.04

- **Par le type de commutations**
  - **Commutation de circuits.** Technique qui permet l'allocation de voies de transmission pendant toute la durée d'une communication. Le circuit ainsi établit dispose de toutes les ressources disponibles sur les voies allouées. L'ancien réseau téléphonique est un exemple typique de cette famille.



https://www.memoireonline.com/09/13/7405/Conception-et-deploiement-de-la-technologie-MPLS-dans-un-reseau-metropolitain12.png

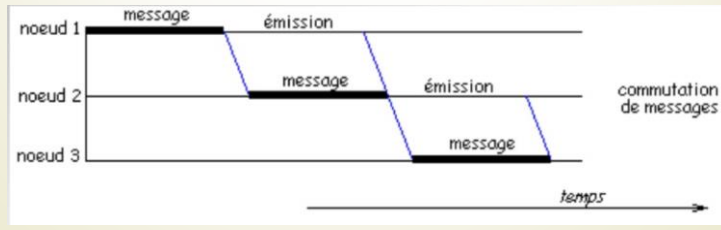
JFA 14

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE iNFO

R 2.04

- **Par le type de commutations**
  - **Commutation par messages.** Ici, il n'y a pas de réservation de ressources. Ainsi, les messages qui arrivent dans le nœud de commutation sont traités selon l'ordre d'arrivée. S'il y a trop de trafic, il y a attente dans la file. Donc le temps de traversée du réseau n'est pas constant et dépend des temps d'attente qui est fonction du trafic. L'avantage de cette technique est une meilleure utilisation des ressources puisqu'il n'y a pas de réservation. Ce mode de commutation est adaptée à un trafic sporadique et non continu n'ayant pas de contrainte de temps telles que les applications informatiques classiques (ex. transfert de fichiers). L'inconvénient est le temps d'attente.

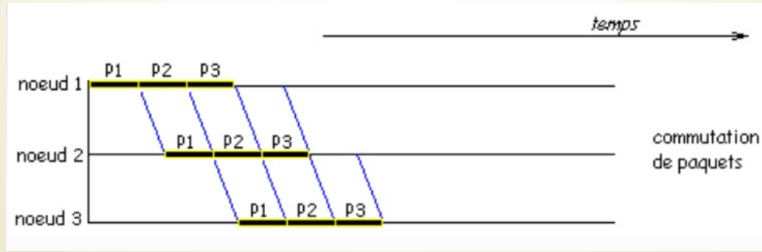


JFA 15

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE – INFO – R 2.04

- **Par le type de commutations**
  - **Commutation par paquets.** Technique qui permet des communications où les ressources sont affectées en fonction des besoins. L'information à transmettre est structurée en paquets de taille fixe, afin de rester en mémoire dans les commutateurs, ces derniers assurant leur acheminement de proche en proche. c'est le mode de transfert utilisé sur internet car il comporte les avantages suivants :
  - Résistance aux pannes, des nœuds intermédiaires
  - Utilisation rationnelle et efficace des lignes de transmission.




JFA 16

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE – INFO – R 2.04

- **Différence entre les types de commutations :**
  - **La différence majeure est que dans le cas de la commutation de circuits, l'allocation se fait par avance et statiquement, il y a réservation de la totalité de la bande passante disponible qu'elle soit ou non utilisée. Dans les deux autres cas, par contre, un circuit n'est utilisé qu'en cas de besoin et libéré aussitôt qu'il n'est plus nécessaire.**

JFA 17

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE iNFO

R 2.04

Deux critères permettent la classification des Réseaux, suivant le mode de transmission utilisé :

- Réseaux à diffusion :
  - Les réseaux à **diffusion** [*broadcast network*] ne possède qu'un seul canal de communication, lequel est partagé entre tous les équipements participant aux réseaux.
  - Une station émet sur le réseau un message à destination d'une autre en précisant l'adresse du destinataire (et sa propre adresse en tant qu'expéditeur). Chaque station du réseau voit passer le message et extrait l'adresse de destination, s'il s'agit de la sienne elle le traite et sinon l'ignore.
  - Dans ce type de réseau une station peut communiquer avec toutes les autres au moyen d'une adresse particulière dite de diffusion [adresse de *broadcast*], ou bien s'adresser à un sous-ensemble particulier par diffusion multipoint [adresse de *multicast*].

JFA 18

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE iNFO

R 2.04

- Point à Point :
  - Dans les réseaux point à point, un message pour aller de l'expéditeur au destinataire doit transiter par plusieurs stations intermédiaires. Il existe en général plus d'un chemin entre deux extrémités et c'est pourquoi les algorithmes de routage, dont l'objet est de choisir la meilleure route au sens d'un ou plusieurs critère(s) (on parle de métrique), y joue un rôle fondamental.

- En général, les réseaux de petites tailles, géographiquement parlant, utilise la diffusion, tandis que les grands utilisent le mode point à point. Dans ce type de réseau une station peut communiquer avec toutes les autres au moyen d'une adresse particulière dite de diffusion [*broadcasting*], ou bien s'adresser à un sous-ensemble particulier par diffusion multipoint [*multicasting*].

JFA 19

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

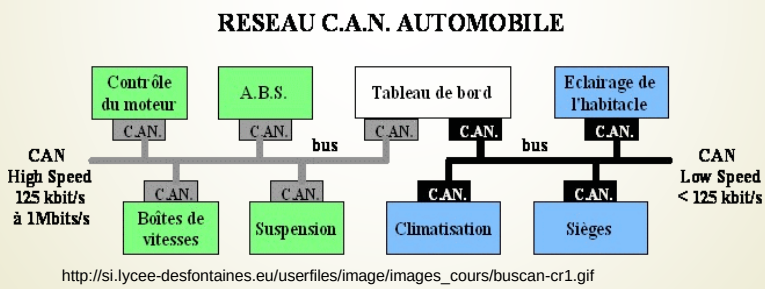
- En fonction de l'étendue géographique du réseau :
  - Les réseaux inter-circuits (Bus)
  - Les réseaux personnels (PAN)
  - Les réseaux locaux (LAN)
  - Les réseaux métropolitains (MAN)
  - Les réseaux étendus (WAN)

JFA 20

# Classification des réseaux de données

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- **Les réseaux inter-circuits (Bus)**
  - C'est un réseau de faible étendue (qq 10 cm)
  - Il permet de faire transiter des données d'un circuit électronique vers un autre circuit.
    - Ex: Bus CAN : Echange de données sur une voiture :




http://si.lycee-desfontaines.eu/userfiles/image/images_cours/buscan-cr1.gif

JFA 21

# Classification des réseaux de données

- I2C : Télévision

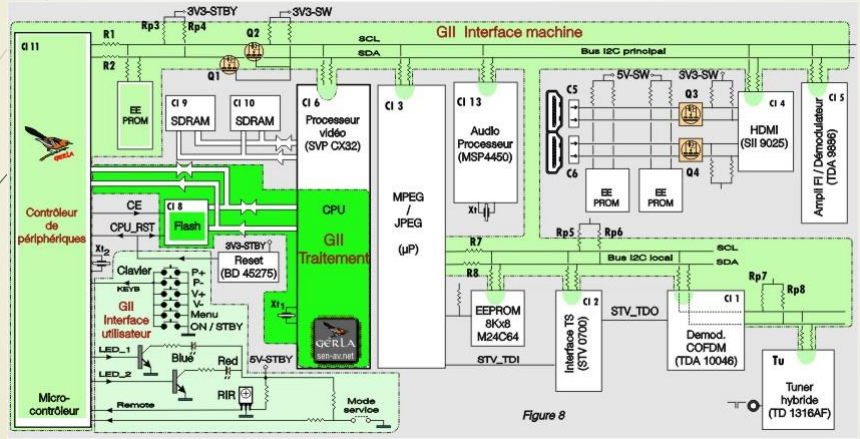


*Figure 8*

JFA 22

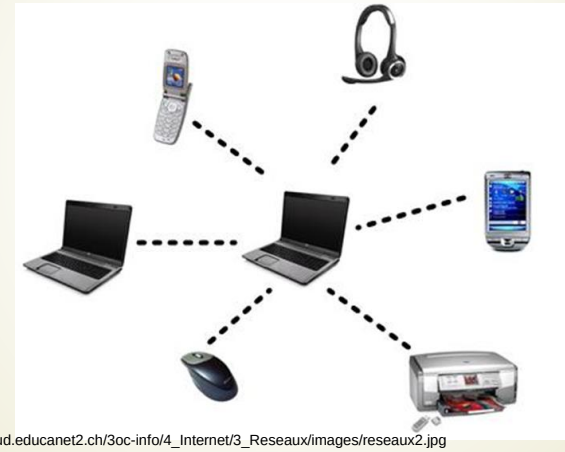
# Classification des réseaux de données

- **Les réseaux personnels PAN (Personal Area Network)**
  - Également appelé *réseau domestique*, un réseau personnel désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour d'un utilisateur. Ce type de réseau sert généralement à relier des périphériques tels qu'imprimante, téléphone portable, appareils domestiques à un ordinateur personnel. La liaison avec ces périphériques peuvent être câblées ou sans fil (par WIFI, Bluetooth par exemple).

JFA 23

# Classification des réseaux de données

- Les réseaux personnels PAN (Personal Area Network)



http://csud.educanet2.ch/3oc-info/4_Internet/3_Reseaux/images/reseaux2.jpg

JFA 24

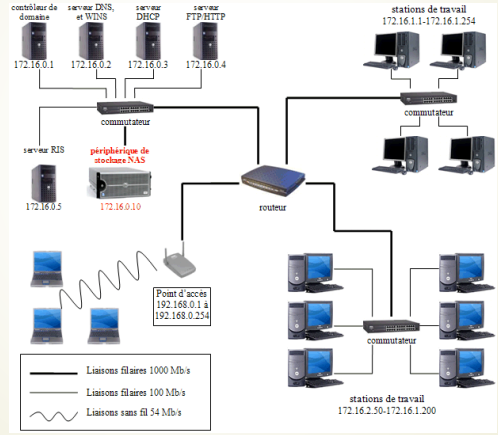
# Classification des réseaux de données

- **Les réseaux locaux (LAN) (Local Area Network)**
  - De taille supérieure, s'étendant sur quelques dizaines à centaines de mètres, un réseau local relie entre eux des ordinateurs appartenant à une même organisation et situés dans une même salle, un même bâtiment ou un même terrain. Un tel réseau peut reposer sur différentes technologies (câblés ou wifi), la plus répandue étant Ethernet. Du fait de la faible dimension de ce type de réseau, les délais de transmission sont courts avec peu d'erreurs, ce qui a l'avantage d'en simplifier l'administration. Couramment utilisé pour le partage de ressources communes, comme des périphériques, des données ou des applications, un réseau local bénéficie d'une vitesse de transfert de données s'échelonnant entre 10 Mb/s et 1 Gb/s. La taille d'un tel réseau peut atteindre jusqu'à 100 voire 1000 utilisateurs.

JFA 25

# Classification des réseaux de données

- Les réseaux locaux (LAN) (Local Area Network)




JFA 26

# Classification des réseaux de données

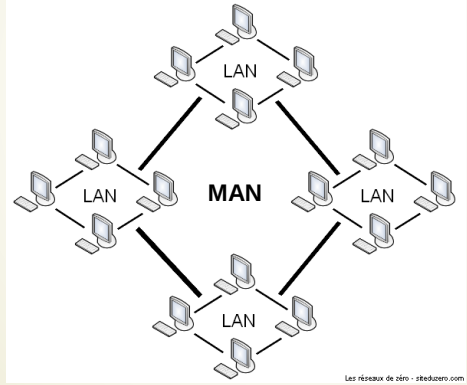
- **Les réseaux métropolitains (MAN) (Metropolitan Area Network)**
  - Un réseau métropolitain, également nommé réseau fédérateur, assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN avec des débits plus importants. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments, distants de quelques dizaines de kilomètres. Ainsi, un MAN permet à deux nœuds distants de communiquer comme s'il faisait partie d'un même réseau local. Un MAN est formé de commutateurs et de routeurs interconnectés par des liens à haut débit généralement en fibre optique.

JFA 27

# Classification des réseaux de données

R 2.04

- Les réseaux métropolitains (MAN) (Metropolitan Area Network)




http://csud.educanet2.ch/3oc-info/4_Internet/3_Reseaux/images/reseaux5.png

JFA 28

# Classification des réseaux de données

R 2.04

- **Les réseaux étendus (WAN) (Wide Area Network)**
  - Constitués d'interconnexions de LAN, voire de MAN, les réseaux étendues sont capables de transmettre des informations sur des milliers de kilomètres à travers le monde entier par le biais de routeurs et de liaisons nationales ou internationales à très haut débit, appelées épines dorsales (backbone en anglais). Puisque la majeure partie du trafic d'un WAN se situe dans les LAN qui le constituent, les routeurs sont investis d'une mission importante: contrôler le trafic. Ils doivent être paramétrés avec des informations appelées ***routes*** qui leur indiquent comment acheminer des données entre les réseaux. En outre, l'épine dorsale est un ensemble de lignes téléphoniques très rapides utilisées par les opérateurs de télécommunications pour transmettre de gros volumes de trafic.

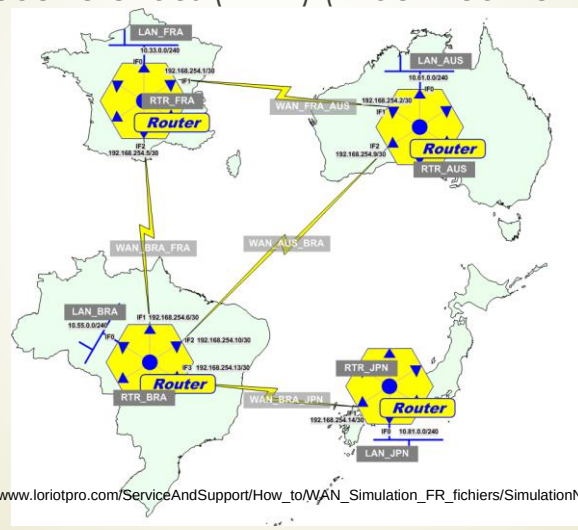
  - Internet est le plus grand WAN !

JFA 29

# Classification des réseaux de données

R 2.04

- Les réseaux étendus (WAN) (Wide Area Network)



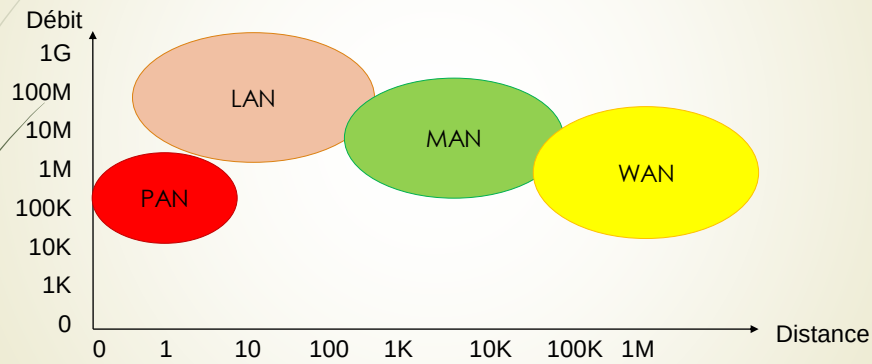

https://www.loriotpro.com/ServiceAndSupport/How_to/WAN_Simulation_FR_fichiers/SimulationNetwork.png

JFA 30

# Classification des réseaux de données

R 2.04

- **En fonction de l'étendue géographique du réseau :**



JFA 31

## Adressage IP V4

IUT GRAND OUEST NORMANDIE – INFO – R 2.04

- Le modèle TCP/IP utilise un système particulier d'adressage qui porte le nom de la couche réseau de ce modèle : l'adressage IPv4. La suite présente le fonctionnement de cet adressage dans la version IPv4.
- De façon très académique, on débute avec le format des adresses IPv4. On définit ensuite les classes d'adresses IPv4 qui correspondent au tout premier mode de découpage de l'espace d'adressage. Comme ce mode de découpage ne convenait pas du tout au développement de l'Internet, on passe en revue la chronologie des améliorations apportées depuis 1980 : les sous-réseaux ou subnetting, la traduction d'adresses ou Native Address Translation (NAT) et enfin le routage inter-domaine sans classe.

JFA 32

## Adressage IP V4

IUT GRAND OUEST NORMANDIE – INFO – R 2.04

Le protocole IPv4 sert à véhiculer trois types de trafic distincts :

- Unicast : Le trafic unicast désigne une communication entre un **hôte source unique** et un **hôte destination unique** lui aussi.
- Multicast : Le trafic multicast désigne une communication entre **un hôte source unique** et un **groupe d'hôtes** qui ont choisi de recevoir le flux émis par la source.
- Broadcast : Le trafic broadcast désigne un flux émis **par un hôte** à destination de **tous les autres hôtes** appartenant au même domaine de diffusion. Ce type de trafic ne peut exister que sur les réseaux dits de diffusion comme Ethernet. Par exemple, le protocole ARP.

JFA 33

## Adressage IP V4

- Les adresses IP V4 (Version 4) :
  - Distribuées par IANA (***Internet Assigned Numbers Authority)***
  - Les adresses sont codées sur 32 bits.
  - Elles sont représentées sous forme de 4 nombres décimaux allant de 0 à 255 séparés par des points,
  - On peut avoir 4 294 967 296 hôtes maximum,
  - Certaines adresses sont réservées à des usages particuliers,
  - Adresses privées ou publiques,
  - Aucune d'adresse publique disponible depuis février 2011.

Exemple : 176.26.142.26

JFA 34

## Les classes d'adresses IP

- Toutes les adresses IP sont réparties en différentes classes.
- À chaque classe correspond un nombre déterminé de bits pour le réseau et pour la machine.

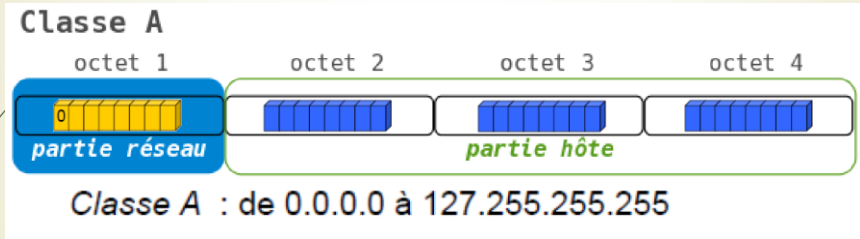

- La **masque réseau** sert à **départager** la partie réseau et la partie Hôte
- Notation CIDR : consiste à faire suivre l'adresse de /X, avec X = le nombre de bits à 1 du masque de sous-réseau (entre 0 et 32). Ex ici : 176.26.142.26/16
- Ce sont principalement les classes A à C qui sont couramment utilisées. Les classes D et E sont réservées à des usages particuliers.

JFA 35

## La Classe A

R 2.04

- Dans la classe A, le premier bit est à 0,
- Le masque réseau vaut 255.0.0.0



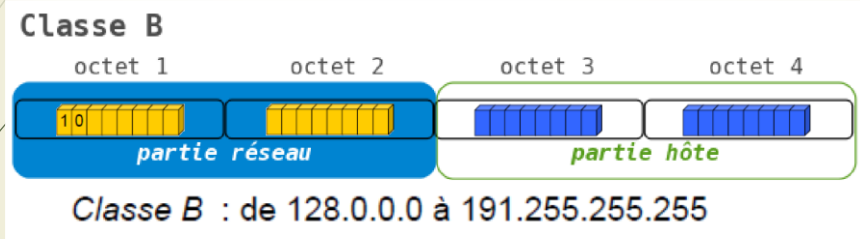

- Les adresses de classe A permettent donc de créer des réseaux (127) avec beaucoup de machines (16777216), Nous retrouverons ces adresses principalement sur des backbones.

JFA 36

## La Classe B

R 2.04

- Dans la classe B, les deux premiers bits sont à 10,
- Le masque vaut 255.255.0.0



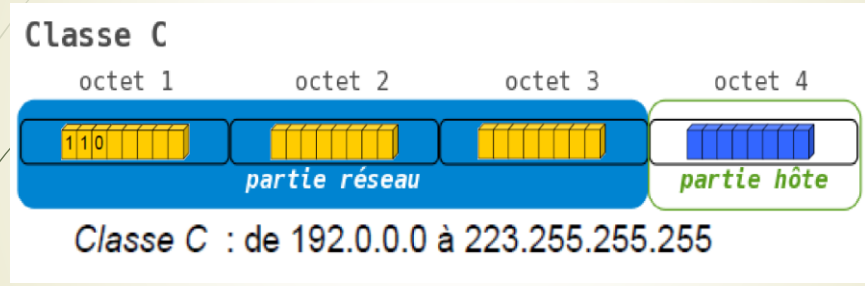

- Les adresses de classe B permettent donc d'équilibrer le nombre de réseaux (16384) et de machines (65534)

JFA 37

## La Classe C

R 2.04

- Dans la classe C, les trois premiers bits sont à 110,
- Le masque vaut 255.255.255.0



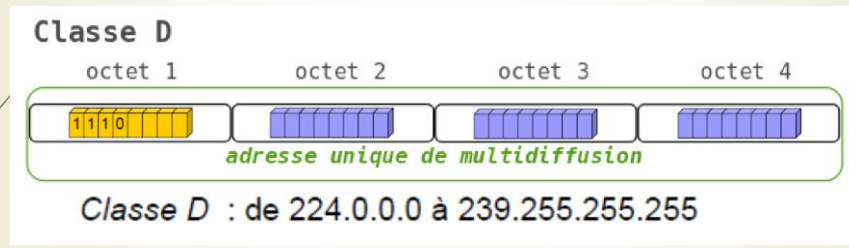

- Les adresses de classe C permettent donc de créer beaucoup de réseaux (2097152) avec peu de machines(254). Nous retrouverons ces adresses chez les particuliers ou sur les réseaux locaux (LANs).

JFA 38

## La Classe D

R 2.04

- Dans la classe D, les quatre premiers bits sont à 1110,
- C'est une classe d'adresse de Multidiffusion,



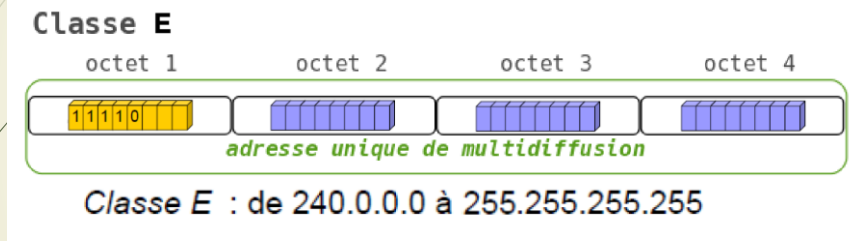

- Les adresses de classe D sont réservées pour les communications multicast ou broadcast.

JFA 39

## La Classe E

R 2.04

- Dans la classe E, les cinq premiers bits sont à 11110,
- C'est une classe d'adresse réservée,




- Les adresses de classe E sont réservées à des usages particuliers (indéterminé). Elles étaient réservées pour une utilisation future, mais c'est trop tard pour les utiliser maintenant car les hôtes anciens ne les accepteraient pas.

JFA 40

## Les adresses spéciales

R 2.04

- L'adresse IP 0.0.0.0 (la plus basse), est utilisée par les hôtes au démarrage, elle signifie : Ce réseau ou cet hôte, ou réseau par défaut dans les tables de routage,
- Les adresses IP contenant des 0 comme numéro de réseau se rattachent au réseau en cours, elles permettent à des machines de se rapporter à leur réseau sans en connaître le numéro.
- L'adresse IP 255.255.255.255 qui est la plus haute désigne tous les hôtes sur ce réseau.
- L'adresse IP avec tous les bits de l'hôte à 1 est une adresse de broadcast, elle permet de joindre toutes les machines du réseau auquel appartient cet hôte.
  - Ex : 192.168.255.255

JFA 41

## Les adresses Privées

R 2.04

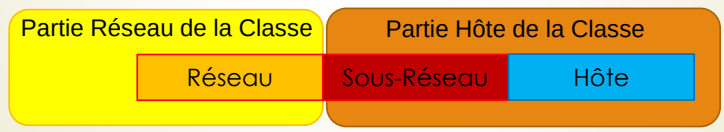
- Plusieurs adresses sont réservées et dites privées.
- Elles sont utilisables en interne, et ne sont pas routables : elles ne sortiront pas de votre réseau.
- Elles sont prévues pour être utilisées avec un NAT (Network Address Translation) ou avec un DHCP pour un accès internet.
  - 10.0.0.0 /8 : de 10.0.0.0 à 10.255.255.255
    - => 1 réseau de classe A,
  - 172.16.0.0 /12 de 172.16.0.0 à 172.31.255.255
    - => 16 réseaux de classe B,
  - 192.168.0.0 /16 de 192.168.0.0 à 192.168.255.255
    - => 256 réseaux de classe C.

JFA 42

## Les sous réseaux (Subnetting)

R 2.04

- L'adresse IP possède une partie réseau de 8, 16 ou 24 bits suivant la classe d'adresse et une partie hôte. Ces masques par défaut ne permettent pas forcément de coller aux besoins. C'est pourquoi, il peut être intéressant de subdiviser les réseaux par défaut au moyen d'un masque de sous-réseau.
- Un masque de sous-réseau est un nombre de la même taille que l'adresse. Les premiers bits sont à 1 et désignent la partie réseau. Les derniers bits sont à 0 et désignent la partie hôte. Mais la partie réseau est plus grande que la classe à laquelle il appartient !




- Ex : 255.255.255.0, pour un réseau de classe B, cela permet d'avoir 256 sous-réseaux de 254 machines.

JFA 43

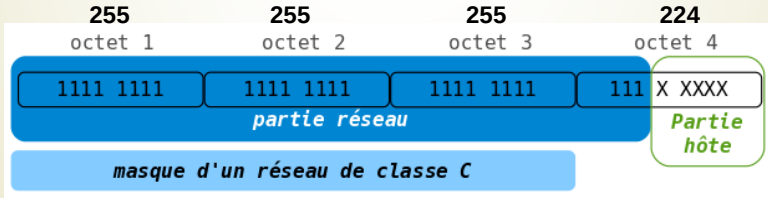
# Les sous réseaux (Subnetting)

R 2.04

- Pour illustrer le fonctionnement du découpage en sous-réseaux :

  Exemple de classe C : 192.168.1.0

  masque réseau : 255.255.255.0 (/24)
- Le nombre d'hôtes maximum de ce réseau est donc de 254.
- On réserve 3 bits supplémentaires du 4ème octet en complétant le masque réseau. De cette façon on augmente la partie réseau de l'adresse IPv4 et on diminue la partie hôte.
- Masque de sous réseau :




JFA 44

# Les sous réseaux (Subnetting)

R 2.04

- Pour illustrer le fonctionnement du découpage en sous-réseaux :

| Adresse réseau | 192.168.1.0 | | | |
|---|---|---|---|---|
| Masque de réseau | 255.255.255.0 | | | |
| Masque de sous réseau | 255.255.255.224 | | | |
| Nom et Adresse du sous réseau | | Début Plage Adresse | Fin Plage Adresse | Adresse de diffusion (Broadcast) |
| Sous-réseau 0 | 192.168.1.0 | 192.168.1.1 | 192.168.1.30 | 192.168.1.31 |
| Sous-réseau 1 | 192.168.1.32 | 192.168.1.33 | 192.168.1.62 | 192.168.1.63 |
| Sous-réseau 2 | 192.168.1.64 | 192.168.1.65 | 192.168.1.94 | 192.168.1.95 |
| Sous-réseau 3 | 192.168.1.96 | 192.168.1.97 | 192.168.1.126 | 192.168.1.127 |
| Sous-réseau 4 | 192.168.1.128 | 192.168.1.129 | 192.168.1-158 | 192.168.1-159 |
| Sous-réseau 5 | 192.168.1.160 | 192.168.1.161 | 192.168.1.190 | 192.168.1.191 |
| Sous-réseau 6 | 192.168.1.192 | 192.168.1.193 | 192.168.1.222 | 192.168.1.223 |
| Sous-réseau 7 | 192.168.1.224 | 192.168.1.225 | 192.168.1.254 | 192.168.1.255 |

JFA 45

# Les sous réseaux (Exemple)

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- Adresse IP : 192.168.1.96
- masque de réseau : 255.255.255.192
  - Quelle est la classe de l'adresse IP ?
  - Le masque correspond-t-il à la classe trouvée ?
  - Si non, combien a-t-on de sous réseaux ?
  - Combien a-t-on de bits restants pour la partie hôte ?
  - Combien peut-on avoir de machines dans chacun des sous réseaux ?
  - Pour l'adresse IP ci-dessus, dans quel sous réseau sommes nous ?
  - Pour l'adresse IP ci-dessus, quel est le numéro de machine ?

JFA 46

# Les sous réseaux (Exemple)

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- Adresse IP : 192.168.1.96
- masque de réseau : 255.255.255.192
- ***Quelle est la classe de l'adresse IP ?***

  Il faut convertir le premier chiffre de l'adresse IP pour connaître la classe d'adresse IP :

  $192_{10} = 11000000_2$
  - ***Le binaire commençant par 110, on est en classe C***
  - ***Le masque par défaut de la classe C est 255.255.255.0***
- ***Le masque correspond-t-il à la classe trouvée ?***
  - Non, Le masque fourni n'est pas le même donc on a des sous réseaux !
- ***Si non, combien a-t-on de sous réseaux ?***
  - Le masque de la classe est : 255.255.255.0
  - Le masque fourni est : 255.255.255.192
  - En binaire : 11111111.11111111.11111111.11000000
  - ***On a donc 2 bits supplémentaires pour faire des sous réseaux, soit 4 sous réseaux !***

JFA 47

# Les sous réseaux (Exemple)

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- Adresse IP : 192.168.1.96
- masque de réseau : 255.255.255.192
- ***Combien a-t-on de bits restants pour la partie hôte ?***
  - Comme on prend 2 bits pour les sous réseaux sur les 8 bits de disponibles pour la classe, ***il reste donc 6 bits pour les machines***
- ***Combien peut-on avoir de machines dans chacun des sous réseaux ?***
  - Avec 6 bits pour coder les machines, on a $2^6-2$ = **62 machines**, car on ne doit pas utiliser les adresses :
    - $0_{10} = 000000_2$
    - $63_{10} = 111111_2$
    - Car ces adresses sont réservées !
- ***Pour l'adresse IP ci-dessus, dans quel sous réseau sommes nous ?***
  - $96_{10} = 01100000_2$
    - On a les 2 bits de gauche qui représente le sous réseau soit $01_2 = 1_{10}$
    - ***On est donc dans le sous réseau 1.***
- ***Pour l'adresse IP ci-dessus, quel est le numéro de machine ?***
  - $96_{10} = 01100000_2$
    - On a les 6 bits de droite pour le numéro de machine soit $100000_2 = 32_{10}$
    - ***On est donc sur la machine 32.***

JFA 48

# Les sous réseaux (Exemple)

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- Adresse IP : 192.168.1.96
- masque de réseau : 255.255.255.192
  - Quelle est la classe de l'adresse IP ?
  - Le masque correspond-t-il à la classe trouvée ?.
  - Si non, combien a-t-on de sous réseaux ?
  - Combien a-t-on de bits restants pour la partie hôte ?
  - Combien peut-on avoir de machines dans chacun des sous réseaux ?
  - Pour l'adresse IP ci-dessus, dans quel sous réseau sommes nous ?
  - Pour l'adresse IP ci-dessus, quel est le numéro de machine ?

| Partie Réseau de la Classe 192.168.1 | Partie Hôte de la Classe 96 | |
|---|---|---|
| 11000000.10101000.00000001. | 01 | 100000 |

JFA 49

# Les sous réseaux (Exemple)

R 2.04

- Adresse IP : 192.168.1.96
- masque de réseau : 255.255.255.192
  - L'adresse IP commençant en binaire par 11000000 (192), on est donc en classe C, avec un masque par défaut de 255.255.255.0,
  - Le masque fournit étant différent, on a donc des sous-réseaux. Le nombre de bits à 1 qui diffère est de 2 bits (11000000 = 192).
  - On a donc $2^2$=4 sous réseaux en RFC 1878.
  - En RFC 950, on évite d'utiliser le sous réseau 0 (00) et (11). Déprécié depuis la RFC 1878, Il reste donc 4 sous réseaux utilisables (00 à 11).
  - La partie Hôte qui reste est donc de 6 bits, donc 62 machines possibles.
  - 96 = $01100000_2$ on a donc $01_2$ pour le sous réseau et $100000_2$ ($32_{10}$) pour l'hôte, c'est donc la 32ème machine du sous réseau 1.

| Partie Réseau de la Classe 192.168.1 | Partie Hôte de la Classe 96 | |
|---|---|---|
| 11000000.10101000.00000001. | 01 | 100000 |

JFA 50

# Les sous réseaux (Synthèse)

R 2.04

***2ème Exemple :***

- Adresse IP : 191.198.174.2/19
- masque de réseau : 255.255.224.0
  - Classe d'Adresse :
  - Masque de Réseau :
  - Adresse de Réseau :
  - Masque de sous Réseau :
  - Adresse de sous Réseau :
  - Nombre de sous réseaux :
  - Nombre de machines par sous réseaux :
  - C'est la ème machine du sous réseau .

| Partie Réseau de la Classe | Partie Hôte de la Classe | |
|---|---|---|
| . . | . | . |

JFA 51

# Les sous réseaux (Synthèse)

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

***2ème Exemple :***

- Adresse IP : 191.198.174.2/19
- masque de sous-réseau : 255.255.224.0
  - Classe d'Adresse : Classe B
  - Masque de Réseau : 255.255.0.0
  - Adresse de Réseau : 191.198.0.0
  - Masque de sous réseau : 255.255.224.0
  - Adresse de sous Réseau : 191.198.160.0
  - Nombre de sous réseaux : 8
  - Nombre de machines par sous réseaux : 8192-2 = 8160
  - C'est la 3586ème machine du sous réseau 5.

| Partie Réseau de la Classe 191.198 | Partie Hôte de la Classe 174.2 | |
|---|---|---|
| 10111111.11000110. | 101 | 01110.00000010 |

JFA 52

# Méthode de calcul du sous réseau :

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

Il faut faire un ET Logique bit à bit entre l'adresse IP et le masque de sous réseau :

Adresse IP : 191.198.174.2

masque de réseau : 255.255.224.0

- Soit en binaire :

  10111111.11000110.10101110.00000010 -> Adresse IP en binaire
  & 11111111.11111111.11100000.00000000 -> Masque de sous réseau
  = 10111111.11000110.10100000.00000000 -> Adresse de sous réseau

- Soit en décimal : 191.198.160.0
- Pour le calcul du numéro de sous réseau en binaire :

  10111111.11000110.10101110.00000010 -> Adresse IP en binaire
  & 00000000.00000000.11111111.11111111 -> NON Masque de réseau
  & 11111111.11111111.11100000.00000000 -> Masque de sous réseau
  = 00000000.00000000.10100000.00000000 -> No de sous réseau en binaire

- Soit en décimal : 5

https://fr.wikipedia.org/wiki/Sous-r%C3%A9seau

JFA 53

# Méthode de calcul du numéro de l'hôte :

R 2.04

Il faut faire un ET Logique bit à bit entre l'adresse IP et le complément du masque de sous réseau :

Adresse IP : 191.198.174.2

masque de réseau : 255.255.224.0

- Soit en binaire :

  10111111.11000110.10101110.00000010 -> Adresse IP en binaire

  & 00000000.00000000.00011111.11111111 -> NON masque sous réseau

  = 00000000.00000000.00001110.00000010 -> Numéro de l'Hôte

- Soit en décimal : 0.0.14.2
- On calcule donc le numéro de machine :
- 14*256+2 = 3586

https://fr.wikipedia.org/wiki/Sous-r%C3%A9seau

JFA 54

# Exercices:

R 2.04

***Exercice 1 :***

Détermination du nombre de bits à utiliser pour l'ID sous-réseau.
Dans cet exercice, vous devez déterminer combien de bits sont nécessaires pour créer le nombre de sous-réseaux demandés.

| | NB de sous-réseaux | Nb de bits à réserver |
|---|---|---|
| Cas 1 : | 84 sous-réseaux : | |
| Cas 2 : | 145 sous-réseaux : | |
| Cas 3 : | 7 sous-réseaux : | |
| Cas 4 : | 1 sous-réseau : | |
| Cas 5 : | 15 sous-réseaux : | |

JFA 55

# Solutions :

R 2.04

***Exercice 1 :***

Détermination du nombre de bits à utiliser pour l'ID sous-réseau.
Dans cet exercice, vous devez déterminer combien de bits sont nécessaires pour créer le nombre de sous-réseaux demandés.

| | NB de sous-réseaux | Nb de bits à réserver |
|---|---|---|
| Cas 1 : | 84 sous-réseaux : | 7 bits ($2^7 = 128$) |
| Cas 2 : | 145 sous-réseaux : | 8 bits ($2^8 = 256$) |
| Cas 3 : | 7 sous-réseaux : | 3 bits ($2^3 = 8$) |
| Cas 4 : | 1 sous-réseau : | 1 bits ($2^1 = 2$) |
| Cas 5 : | 15 sous-réseaux : | 4 bits ($2^4 = 16$) |

***Solution Ex1 :***

Il faut trouver la puissance de 2 qui est immédiatement supérieure au nombre de sous-réseaux.
Et la puissance nous donne le nombre de bits à réserver.

JFA 56

# Exercice 2:

R 2.04

Pour les adresses suivantes :

- 145.245.45.225 (1)
- 202.2.48.149 (2)
- 97.124.36.142 (3)
- 172.24.245.25
- 212.122.148.49

Donnez :

1. La classe d'adresse.
2. Le masque réseau par défaut.
3. L'adresse réseau.
4. Le masque modifié si les réseaux comportent respectivement :
   (1) 60, (2) 15 et (3) 200 sous-réseaux.
5. L'adresse du sous-réseau et son numéro.
6. Le numéro de la machine sur le sous-réseau.
7. Les intervalles d'adresses utilisables pour les trois premiers sous-réseaux.

JFA 57

## Solution 2:

R 2.04

| Adresse IP | Classe Adr. | Masque Rés. | Adr. Réseau | Masque Sous R | Adr Sous Res. | N° SR | N° Hôte |
|---|---|---|---|---|---|---|---|
| 145.245.45.225 | Classe B | 255.255.0.0 | 145.245.0.0 | 255.255.252.0 | 145.245.44.0 | 11 | 481 |
| 202.2.48.149 | Classe C | 255.255.255.0 | 202.2.48.0 | 255.255.255.240 | 202.2.48.144 | 9 | 5 |
| 97.124.36.142 | Classe A | 255.0.0.0 | 97.0.0.0 | 255.255.0.0 | 97.124.0.0 | 124 | 9358 |
| 172.24.245.25 | Classe B | 255.255.0.0 | 172.24.0.0 | 255.255.255.0 | 172.24.245.0 | 245 | 25 |
| 212.122.148.49 | Classe C | 255.255.255.0 | 212.122.148.0 | 255.255.255.224 | 212.122.148.32 | 1 | 17 |

https://www.sebastienadam.be/connaissances/exercices/adressage_ip_v4/masque_reseau_1.php

JFA 58

## Exercice 3:

R 2.04

Une société dispose d'un réseau de 254 machines réparties en 7 sous-réseaux.
La répartition des machines est la suivante :

- Sous-réseau 1 : 38 machines
- Sous-réseau 2 : 33 machines
- Sous-réseau 3 : 52 machines
- Sous-réseau 4 : 35 machines
- Sous-réseau 5 : 34 machines
- Sous-réseau 6 : 37 machines
- Sous-réseau 7 : 25 machines

Les adresses IP étant des adresses privées, on vous demande :

- De choisir l'identifiant (l'adresse) du réseau
  - De définir le nombre de bits consacrés aux identifiants (adresses) de sous-réseaux et de machines
  - De calculer le nombre de sous-réseaux potentiels et le nombre maximum de machines par sous-réseau
  - De définir les identifiants (adresses) de chaque sous-réseau
  - De définir le masque de sous-réseau
  - De calculer les adresses des premières et dernières machines configurées dans chacun des sous-réseaux

JFA 59

## Solution 3:

R 2.04

Nombre de sous-réseaux : 7
Nombre de bits nécessaires : 4 bits (14 sous-réseaux potentiels)
Nombre maximum de machines : 52
Nombre de bits nécessaires : 6 bits (62 machines potentielles par sous-réseau)
Nombre de bits nécessaire pour ID sous-réseau et ID hôte : 4 + 6 = 10
On ne peut pas travailler en classe C, nous adopterons donc des adresses de classe B et nous consacrons 1 octet pour ID sous-réseau et 1 octet pour ID hôte
ID réseau : 172.16.0.0
Masque de sous-réseau 255.255.255.0

JFA 60

## Solution 3:

R 2.04

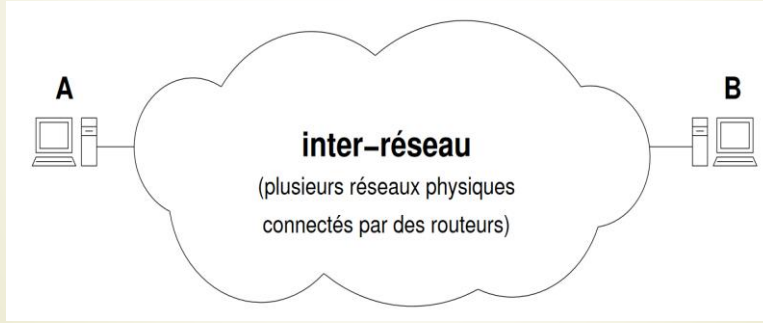
| Adresse IP | ID sous-réseau | Première machine | Dernière machine configurée | Broadcast | ID sous-réseau |
|---|---|---|---|---|---|
| SR1 : 38 machines | 172.16.1.0 | 172.16.1.1 | 172.16.1.38 | 172.16.1.255 | 172.16.1.0 |
| SR2 : 33 machines | 172.16.2.0 | 172.16.2.1 | 172.16.2.33 | 172.16.2.255 | 172.16.2.0 |
| SR3 : 52 machines | 172.16.3.0 | 172.16.3.1 | 172.16.3.52 | 172.16.3.255 | 172.16.3.0 |
| SR4 : 35 machines | 172.16.4.0 | 172.16.4.1 | 172.16.4.35 | 172.16.4.255 | 172.16.4.0 |
| SR5 : 34 machines | 172.16.5.0 | 172.16.5.1 | 172.16.5.34 | 172.16.5.255 | 172.16.5.0 |
| SR6 : 37 machines | 172.16.6.0 | 172.16.6.1 | 172.16.6.37 | 172.16.6.255 | 172.16.6.0 |
| SR7 : 25 machines | 172.16.7.0 | 172.16.7.1 | 172.16.7.25 | 172.16.7.255 | 172.16.7.0 |

https://ecursus.univ-antilles.fr/pluginfile.php/189499/mod_resource/content/1/TD2_r%C3%A9seau_corr.pdf

JFA 61

## Le Routage

- La communication en IP se fait par un acheminement de paquets (datagrammes) d'une machine source vers une machine destination B.
- Problème : Comment atteindre la machine B en ne connaissant que son adresse IP ?

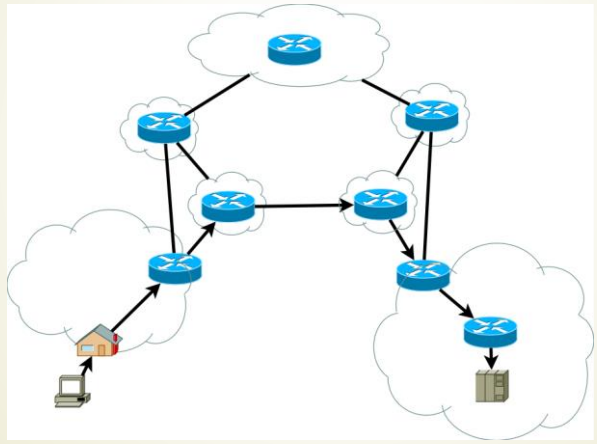



IUT GRAND OUEST NORMANDIE iNFO
R 2.04

JFA 62

## Le Routage

- La communication se fait de proche en proche de la machine source, de routeur à routeur, vers la machine de destination.



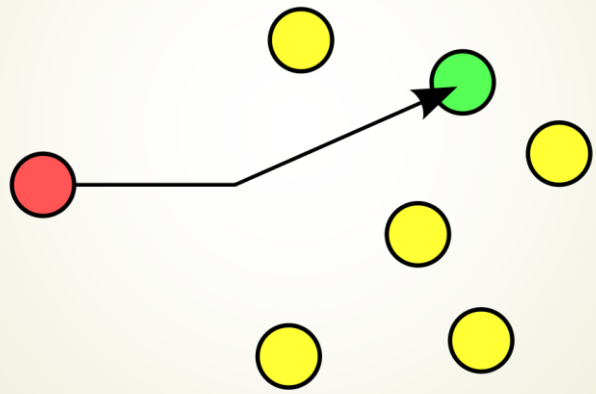
https://upload.wikimedia.org/wikipedia/commons/4/49/Internet-transit.svg

IUT GRAND OUEST NORMANDIE iNFO
R 2.04

JFA 63

## Les Types de la communication

- *unicast*, qui consiste à acheminer les données vers une seule destination déterminée,

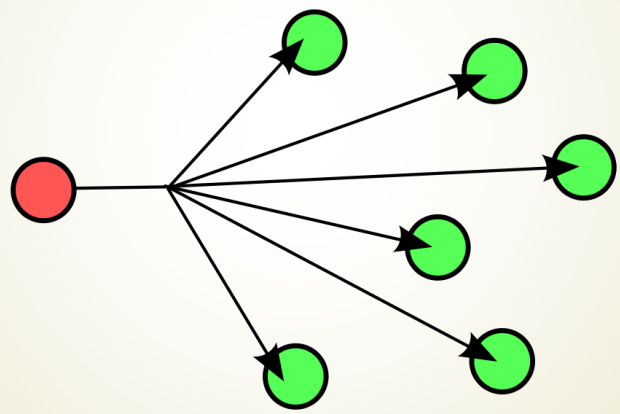


https://fr.wikipedia.org/wiki/Unicast

JFA 64

## Les Types de la communication

- *broadcast* qui consiste à diffuser les données à toutes les machines du réseau local,



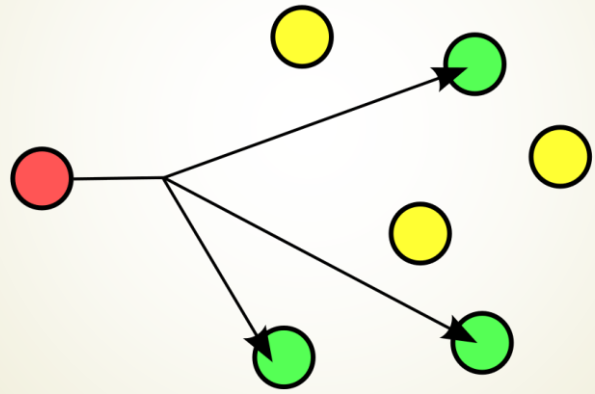
https://fr.wikipedia.org/wiki/Unicast

JFA 65

## Les Types de la communication

R 2.04

- *multicast* qui consiste à délivrer le message à un groupe de machines inscrites et regroupées par fonction, type, …



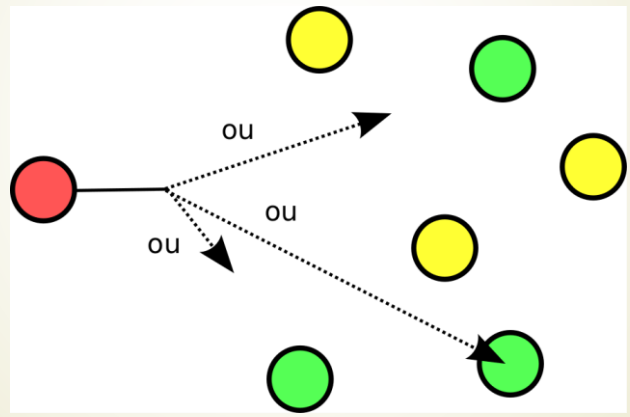
https://fr.wikipedia.org/wiki/Unicast

JFA 66

## Les Types de la communication

R 2.04

- *anycast* qui consiste à délivrer les données à un seul membre d'un groupe, généralement le plus proche, ou le plus efficace au sein du réseau.

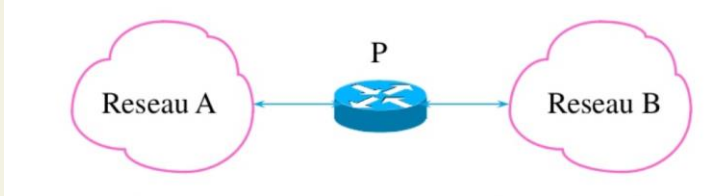



https://fr.wikipedia.org/wiki/Unicast

JFA 67

## Le Routeur

- On va utiliser des routeurs pour faire la connexion inter-réseau
- Routeur : C'est un dispositif réseau qui relie au moins 2 réseaux.




- Le routeur P interconnecte le Réseau A au Réseau B, Il possède donc une connexion sur chacun des réseaux auquel il est connecté.
- C'est lui qui va transférer les paquets (datagrammes) circulant sur le Réseau A et destinés au Réseau B, et inversement.

https://www.slideshare.net/Pronetis/c6-rseaux-introduction-au-routage

JFA 68

## Le Routage

- Le routage => prise de décision pour l'envoi du datagramme.
- Question : l'IP de destination appartient-elle au même réseau que l'IP de l'émetteur ?
  - Oui : la remise est dite direct.
    - A peut envoyer directement le datagramme à B, en utilisant le service d'envoi de trame du réseau local.
  - Non : la remise est dite indirect.
    - A ne peut que confier le datagramme à un routeur.
    - On utilise alors l'adresse de la passerelle ou Gateway pour sortir du réseau,
    - A son tour, le routeur devra appliquer le même algorithme.
- dans ce cas, le choix fait par le routeur est prépondérant, sinon le datagramme sera perdu !

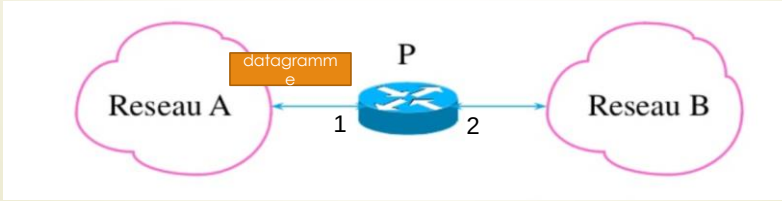
JFA 69

# Le Routage

R 2.04

Fonctionnement :

- Le routeur (ou l'hôte) reçoit un datagramme sur son entrée 1 sur le Réseau A
- Il regarde avec l'adresse IP et le masque de réseau, si il fait partie du Réseau A.
- Si Oui, il ne fait rien, la machine du Réseau A interceptera directement le paquet,
- Si Non, il regardera si il connaît le chemin pour atteindre le réseau demandé. Pour cela, il utilisera sa table de routage.




https://www.slideshare.net/Pronetis/c6-rseaux-introduction-au-routage

JFA 70

# Analyse de la table de Routage

R 2.04

La table de routage contient :

- les interfaces de l'hôte considéré,
- les adresses des sous-réseaux (auxquels le routeur est directement connecté), les routes statiques (configurées par l'administrateur), les routes dynamiques (apprises dynamiquement).
- Les masques correspondants
- Les passerelles et interfaces à contacter pour les joindre,
- une route par défaut (0.0.0.0)
- La métrique : le coût de la route (Nb sauts, Bande passante, charge, délai, …)

| Adresse destination | Masque | Passerelle | Interface | Métrique |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.0.1 | 192.168.0.100 | 1 |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 192.168.0.0 | 255.255.255.0 | 192.168.0.100 | 192.168.0.100 | 1 |
| 192.168.0.100 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 192.168.0.1 | 255.255.255.255 | 192.168.0.100 | 192.168.0.100 | 1 |

JFA 71

## Analyse de la table de Routage

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- L'adresse IP 0.0.0.0 signifie « la route par défaut »
- L'adresse IP 127.0.0.1 signifie l'adresse de Loop Back, c'est l'adresse locale de la machine,
- L'adresse IP 192.168.0.100 est l'adresse de la machine
- L'adresse IP 192.168.0.0 est l'adresse du réseau local à la machine,
- L'adresse IP 192.168.0.1 est l'adresse de la passerelle (Gateway)

| Adresse destination | Masque | Passerelle | Interface | Métrique |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.0.1 | 192.168.0.100 | 1 |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 192.168.0.0 | 255.255.255.0 | 192.168.0.100 | 192.168.0.100 | 1 |
| 192.168.0.100 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 192.168.0.1 | 255.255.255.255 | 192.168.0.100 | 192.168.0.100 | 1 |

JFA 72

## Analyse de la table de Routage

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

Quand plusieurs routes sont possibles :

- la route *la plus précise* sera utilisée, c'est-à-dire celle qui aura le préfixe réseau le plus long,
- Si plusieurs routes avec le même préfixe existent, l'arbitrage a lieu en fonction du type de route :
  - les routes directement connectées auront la priorité sur les autres,
  - les routes statiques et dynamiques sont départagées par une *distance administrative* définie par l'administrateur.
  - Si tous les paramètres sont égaux, le routeur pourra distribuer le trafic entre ces routes ou n'en utiliser qu'une seule.
- La route par défaut indiquera comment acheminer le trafic qui ne correspond à aucune entrée dans la table de routage. En l'absence de route par défaut, le routeur éliminera le datagramme dont la destination n'est pas connue.

JFA 73

# Construction de la table de Routage

R 2.04

***Méthode de construction de la table de routage :***

- *Etape 1 :*
  Indiquer les **réseaux auxquels la machine est connectée**.
- *Etape 2 :*
  Indiquer **la route par défaut**.
- *Etape 3 :*
  Indiquer tous les autres réseaux que je ne peux pas joindre avec les deux étapes précédentes.
- *Etape 4 :*
  Indiquer l'adresse de la passerelle dans mon réseau,

JFA 74

# Exemple de Construction de la table de Routage

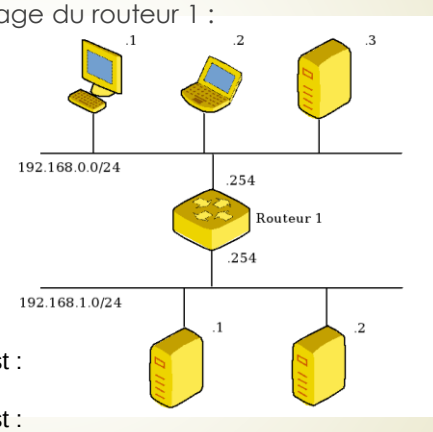
R 2.04

***Méthode de construction de la table de routage :***

Construction de la table de routage du routeur 1 :

***Etape 1 :***

| Table de routage du routeur 1 | |
|---|---|
| Réseau à joindre | passerelle |
| 192.168.0.0/24 | ? |
| 192.168.1.0/24 | ? |




***Etape 2 :***

Ici pas de route par défaut

***Etape 3 :***

La passerelle pour le réseau 0 est : 192.168.0.254
La passerelle pour le réseau 1 est : 192.168.1.254

https://openclassrooms.com/courses/apprenez-le-fonctionnement-des-reseaux-tcp-ip/le-routage-1

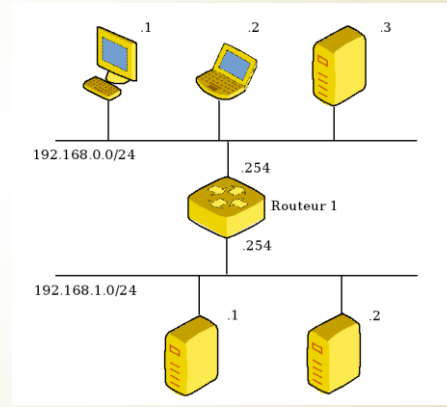
JFA 75

# Exemple de Construction de la table de Routage

R 2.04

***Table de routage du routeur 1***

| Destination | Masque | Passerelle | Interface |
|---|---|---|---|
| **127.0.0.0** | /8 | 127.0.0.1 | 127.0.0.1 |
| **192.168.0.0** | /24 | 192.168.0.254 | 192.168.0.254 |
| **192.168.1.0** | /24 | 192.168.1.254 | 192.168.1.254 |
| **192.168.0.254** | /32 | 127.0.0.1 | 127.0.0.1 |
| **192.168.1.254** | /32 | 127.0.0.1 | 127.0.0.1 |



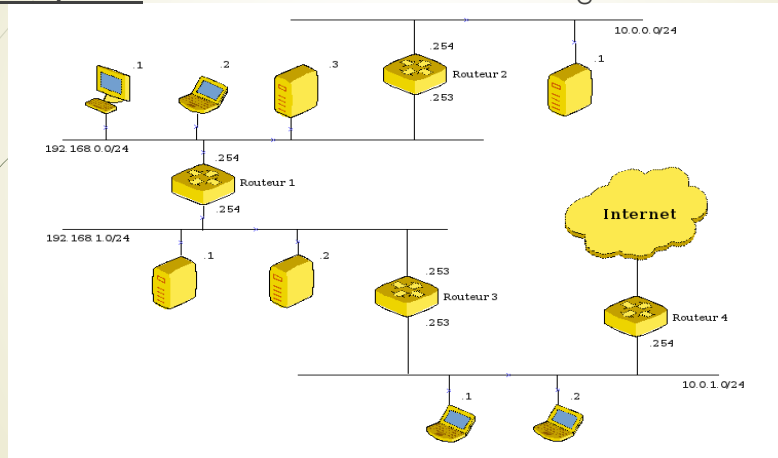

https://openclassrooms.com/courses/apprenez-le-fonctionnement-des-reseaux-tcp-ip/le-routage-1

JFA 76

# Exemple 2 de Construction de la table de Routage

R 2.04

***Exemple 2:*** Construction de la table de routage du routeur 1 :




https://openclassrooms.com/courses/apprenez-le-fonctionnement-des-reseaux-tcp-ip/le-routage-1

JFA 77

# Exemple 2 de Construction de la table de Routage des routeurs

R 2.04

***Exemple 2:*** Tables de routage des routeurs:

Table de routage du routeur 1

| Réseau à joindre | passerelle |
|---|---|
| 192.168.0.0/24 | 192.168.0.254 |
| 192.168.1.0/24 | 192.168.1.254 |
| 0.0.0.0/0 | 192.168.1.253 |
| 10.0.0.0/24 | 192.168.0.253 |

Table de routage du routeur 2

| Réseau à joindre | passerelle |
|---|---|
| 10.0.0.0/24 | 10.0.0.254 |
| 192.168.0.0/24 | 192.168.0.253 |
| 0.0.0.0/0 | 192.168.0.254 |

JFA 78

# Exemple 2 de Construction de la table de Routage des machines

R 2.04

***Exemple 2:*** Tables de routage des machines:

Table de routage de 192.168.0.1

| Réseau à joindre | passerelle |
|---|---|
| 192.168.0.0/24 | 192.168.0.1 |
| 0.0.0.0/0 | 192.168.0.254 |
| 10.0.0.0/24 | 192.168.0.253 |

Table de routage de 10.0.1.2

| Réseau à joindre | passerelle |
|---|---|
| 10.0.1.0/24 | 10.0.1.2 |
| 0.0.0.0/0 | 10.0.1.254 |
| 192.168.1.0/24 | 10.0.1.253 |
| 192.168.0.0/24 | 10.0.1.253 |
| 10.0.0.0/24 | 10.0.1.253 |

Table de routage de 10.0.1.2 Compressée

| Réseau à joindre | passerelle |
|---|---|
| 10.0.1.0/24 | 10.0.1.2 |
| 0.0.0.0/0 | 10.0.1.254 |
| 192.168.0.0/**23** | 10.0.1.253 |
| 10.0.0.0/24 | 10.0.1.253 |

Table de routage de 10.0.0.1

| Réseau à joindre | passerelle |
|---|---|
| 10.0.0.0/24 | 10.0.0.1 |
| 0.0.0.0/0 | 10.0.0.254 |

JFA 87

## Synthèse pour la construction de la table de routage :

R 2.04

La table de routage doit contenir un certain nombre de lignes par défaut :

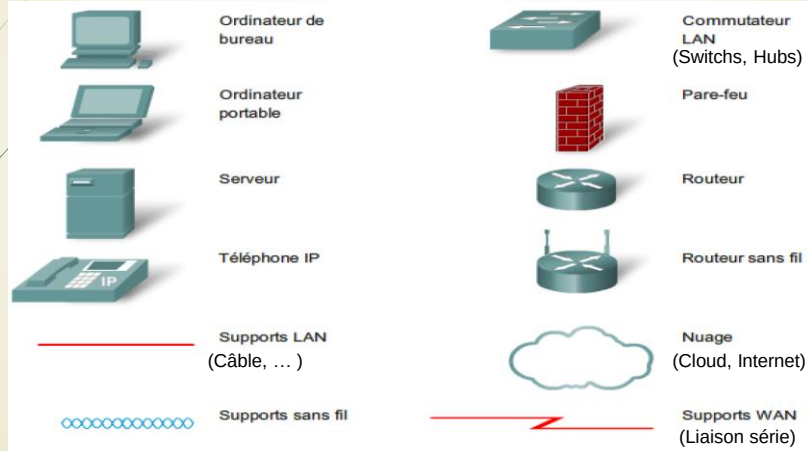
- La première ligne correspond à la passerelle vers la sortie du réseau ou vers internet , la destination est 0.0.0.0 avec un masque 0.0.0.0, cela veut dire tous les réseaux avec n'importe quel masque.
- La 2éme ligne correspond à l'adresse de boucle local (LoopBack) 127.0.0.1 (elle est toujours la même)
- La 3éme ligne et suivantes correspond à l'adresse des réseaux connectés directement au périphérique étudié.
- Les lignes suivantes correspondent aux réseaux autres que l'on connait et comment les atteindre.
- Les dernières lignes correspondent aux adresses IP du périphérique vers l'adresse de boucle locale (LoopBack) . :

JFA 88

## Représentation des symboles utilisés en réseau

R 2.04

- Symboles Courants pour les réseaux de données :




http://silanus.fr/sin/formationSTI2D/ModuleReseau/res/reseau4.png

JFA 89

# Protocole ARP

R 2.04

- ***Problème :***
  - La couche 2 utilise les adresses MAC,
  - la couche 3 utilise les adresses IP,

Comment faire correspondre les adresses MAC ET IP ?

- Le protocole ARP permet d'obtenir une adresse MAC en fonction d'une adresse IP.

JFA 90

# Protocole ARP

R 2.04

***Exemple :***

- Un routeur 1 veut envoyer un paquet vers l'adresse 10.0.0.45 du réseau 3. Le routeur regarde dans sa table de routage pour savoir où il va devoir envoyer le paquet.
- Sa table de routage lui dit que pour atteindre le réseau 10.0.0.0/255.0.0.0, il faut passer par le routeur dont l'adresse IP est 172.16.0.254.
- Le nouveau travail du routeur est donc d'envoyer le paquet vers 172.16.0.254.

JFA 91

# Protocole ARP

R 2.04

- Cette adresse IP étant sur son propre réseau (notre routeur a une adresse d'interface dans le réseau 172.16.0.0./255.255.0.0), il faut connaître son adresse MAC pour pouvoir lui envoyer le paquet.
- Pour connaître son adresse MAC, l'idéal serait de lui demander, mais pour lui demander, il faudrait connaître son adresse MAC !!!
- Et on tourne en rond :-(. Il faut donc trouver un moyen de s'adresser à l'adresse MAC de 172.16.0.254 sans la connaître !
- Pour cela Il s'agit du principe de broadcast !
- En envoyant ma question à tout le monde sur le réseau, je suis sûr que la machine 172.16.0.254 va la recevoir.

JFA 92

# Protocole ARP

R 2.04

- Je peux donc envoyer à tout le monde ma requête ARP demandant:

  Qui a l'adresse IP 172.16.0.254 ?

  et quelle est son adresse MAC ?
  - Toutes les machines reçoivent cette question, mais seule la machine 172.16.0.254 va me répondre :
  - Je suis 172.16.0.254 et mon adresse MAC est 04:CF:65:84:C5:E2
- J'ai ainsi pu récupérer l'adresse MAC de 172.16.0.254, et je peux désormais lui envoyer le paquet à transmettre.
- Nous avons ainsi réussi à faire la liaison souhaitée entre l'adresse IP connue et l'adresse MAC recherchée :-)
- Un problème se pose quand même, car si toutes les machines doivent envoyer des messages broadcast à tout le monde à chaque fois qu'elles souhaitent communiquer, on va vite encombrer le réseau...

JFA 93

# Protocole ARP

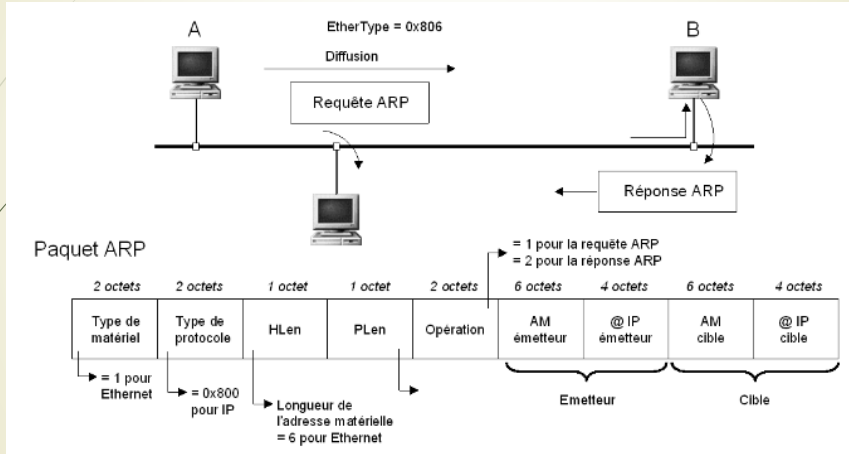
R 2.04

- Pour répondre à ce problème, ARP utilise une solution de cache local. C'est à dire que lorsqu'une requête ARP va être effectuée, la réponse à cette requête va être gardée pendant un certain temps pour pouvoir être réutilisée.
  Ce temps est paramétrable, et est souvent de l'ordre de quelques minutes.
  Ainsi, si mes machines continuent de dialoguer ensemble, il n'y aura plus besoin de faire des broadcasts ARP, il suffira d'aller chercher l'information dans le cache ARP.
- D'ailleurs, le fonctionnement de ARP veut que le système aille d'abord regarder dans le cache ARP si l'information s'y trouve, avant de faire le broadcast ARP (ce qui semble normal :-) )
- Bon, et bien nous avons maintenant en notre possession toutes les connaissances devant nous permettre de comprendre en partie le dialogue entre deux machines distantes. Allons-y !

JFA 94

# Protocole ARP

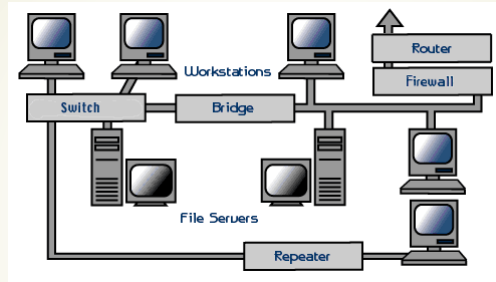
R 2.04




http://www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/MIASHS-L3/PDF/2-Le_protocole_IP.pdf

JFA 95

# L'interconnexion :




- Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Dans ce cas, des équipements spécifiques sont nécessaires.
- Sur deux réseaux de même type, il suffit de faire passer les trames de l'un sur l'autre. Si les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à une conversion de protocole avant de transférer les trames. Ainsi, les équipements à mettre en œuvre sont différents selon la configuration.

https://fcit.usf.edu/network/chap3/pics/netmap.gif

JFA 96

# Les équipements d'interconnexion :

Les principaux équipements matériels mis en place dans les réseaux locaux sont :

- Les **répéteurs**, permettant de régénérer un signal
- Les **concentrateurs** (hubs), permettant de connecter entre eux plusieurs hôtes
- Les **ponts** (bridges), permettant de relier des réseaux locaux de même type
- Les **commutateurs** (switches) permettant de relier divers éléments tout en segmentant le réseau
- Les **passerelles** (gateways), permettant de relier des réseaux locaux de types différents
- Les **routeurs**, permettant de relier de nombreux réseaux locaux de telles façon à permettre la circulation de données d'un réseau à un autre de la façon optimale
- Les **B-routeurs**, associant les fonctionnalités d'un routeur et d'un pont

JFA 97

# Le répéteur :

R 2.04

- Sur une ligne de transmission, le signal subit des distorsions et un affaiblissement d'autant plus importants que la distance qui sépare deux éléments actifs est longue. Généralement, deux nœuds d'un réseau local ne peuvent pas être distants de plus de quelques centaines de mètres, c'est la raison pour laquelle un équipement supplémentaire est nécessaire au-delà de cette distance : le répéteur.

JFA 98

# Le répéteur :

R 2.04

- Un **répéteur** (en anglais *repeater*) est un équipement simple permettant de regénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.
- D'autre part, un répéteur peut permettre de constituer une interface entre deux supports physiques de types différents, c'est-à-dire qu'il peut par exemple permettre de relier un segment de paire torsadée à un brin de fibre optique... .
- Il est très utilisé aujourd'hui en Wifi pour étendre la portée du réseau Wifi, mais il est peu utilisé en filaire.

JFA 99

# Le concentrateur ou Hub :

R 2.04


- Un **concentrateur Ethernet** (répartiteur ou **Hub**) est un équipement informatique permettant de concentrer les transmissions Ethernet de plusieurs équipements sur un même support dans un réseau local.
- Son but est de récupérer les données parvenant sur un port et de les diffuser sur l'ensemble des ports. Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé *répéteur multiports*.

https://www.dreamhardware.com/media/catalog/product/cache/1/base_image/1200x/17f82f742ffe127f42dca9de82fb58b1/e/n/en104_4_large_.jpg

JFA 100

# Le concentrateur ou Hub :

R 2.04

- Le hub possède deux types de ports ou connecteurs physiques :
  - les ports pour la connexion des machines (4, 8, 16 ou 32 ports);
  - le port pour extension du réseau auquel se connecte un autre concentrateur. Ce type de port est identique au précédent à l'exception du câblage qui est inversé (on pourra utiliser un câble croisé pour y connecter un ordinateur supplémentaire).
- Chaque équipement connecté à celui-ci partage le même domaine de diffusion ainsi que le même domaine de collision, donc une seule des machines connectées peut y transmettre à la fois. Dans le cas contraire, une collision se produit, les machines concernées doivent retransmettre leurs trames après avoir attendu un temps aléatoire.
- C'est un répéteur de données ne permettant pas de protection particulière des données et transmettant les trames à toutes les machines connectées. Ceci rend le réseau vulnérable aux attaques par Analyseur de paquets.

JFA 101

# Le concentrateur ou Hub :

R 2.04

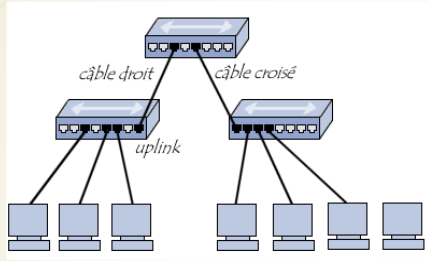
**Connexion de plusieurs hubs**

- Il est possible de connecter plusieurs hubs entre eux afin de concentrer un plus grand nombre de machines, on parle alors de connexions en cascade (*daisy chains*). Pour ce faire, il suffit de connecter les hubs à l'aide d'un câble croisé, c'est-à-dire un câble reliant les connecteurs de réception d'une extrémité aux connecteurs de réception de l'autre.
- Les concentrateurs sont en général dotés d'un port spécial appelé "*uplink*" permettant d'utiliser un câble droit pour connecter deux hubs entre eux. Il existe également des hubs capables de croiser ou de décroiser automatiquement leurs ports selon qu'il est relié à un hôte ou à un hub.
- On peut mettre au maximum 4 hubs Ethernet séparés par un câble de 100 mètres (distance maximale entre deux hubs), soit 500 mètres de distance maximum.

JFA 102

# Le concentrateur ou Hub :

R 2.04




Symbole logique :

- On distingue plusieurs catégories de concentrateurs :
  - Les concentrateurs dits "**actifs**" : ils sont alimentés électriquement et permettent de régénérer le signal sur les différents ports
  - Les concentrateurs dits "**passifs**" : ils ne permettent que de diffuser le signal à tous les hôtes connectés sans amplification
- Pour ces raisons, ce type d'appareil a tendance à tomber en désuétude au profit du commutateur réseau.

JFA 103

# Le Pont ou Bridge:

R 2.04

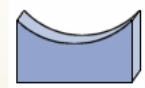

- Un **pont** est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, le pont travaille au niveau logique (couche 2 du modèle OSI), il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont.
- Ainsi, le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées au niveau local et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (notamment les collisions) sur chacun des réseaux et d'augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre brin.

JFA 104

# Le Pont ou Bridge :

R 2.04

- Un pont possède deux connexions à deux réseaux distincts. Lorsque le pont reçoit une trame sur l'une de ses interfaces, il analyse l'adresse MAC du destinataire et de l'émetteur. Il stocke ces adresses dans une table afin de se "souvenir" de quel côté du réseau ils se trouvent. Ainsi le pont est capable de savoir si émetteur et destinataire sont situés du même côté ou bien de part et d'autre du pont. dans le second le pont transmet la trame sur l'autre réseau, si jamais le pont ne connaît pas l'émetteur, il ignore le message.
- En contrepartie, l'opération de filtrage réalisée par le pont peut conduire à un léger ralentissement lors du passage d'un réseau à l'autre, c'est la raison pour laquelle les ponts doivent être judicieusement placés dans un réseau.
- Symbole logique :



# Le commutateur ou Switch :

JFA 105

R 2.04


- Un commutateur réseau, ou switch, est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et qui permet de créer des circuits virtuels (VLAN). Il s'agit d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines), il a donc la même apparence qu'un concentrateur (hub).

https://media.materiel.net/r550/oproducts/AR201301250101_g1.jpg

# Le commutateur ou Switch :

JFA 106

R 2.04

- Contrairement à un concentrateur, un commutateur ne reproduit pas sur tous les ports chaque trame qu'il reçoit : il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse de destination de cette trame. Les commutateurs sont souvent utilisés car ils encombrent moins le réseau. Dans le cas d'un réseau IP/Ethernet, un commutateur ne s'intéresse pas à la même couche OSI que le routeur, ils utilisent respectivement les adresses MAC et les adresses IP pour diriger les données. Concrètement, pour une adresse connue, une trame est toujours émise sur le même port, quel que soit l'état du trafic, une fois ses tables de routage et de communication remplies.
- Il est fréquent qu'un commutateur intègre le *Spanning Tree Protocol* qui permet de supprimer les bouclages dans un réseau.

JFA 107

# Le commutateur ou Switch :

R 2.04

***Fonctionnement :***

- Le commutateur établit et met à jour une table, il s'agit de la table d'adresses MAC, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC sources des trames reçues sur chaque port. Le commutateur construit donc dynamiquement une table qui associe des adresses MAC avec les ports correspondants.
- Lorsqu'il reçoit une trame destinée à une adresse présente dans cette table, le commutateur renvoie la trame sur le port correspondant. Si le port de destination est le même que celui de l'émetteur, la trame n'est pas transmise. Si l'adresse du destinataire est inconnue dans la table, alors la trame est traitée comme un *broadcast*, c'est-à-dire qu'elle est transmise à tous les ports du commutateur à l'exception du port de réception.

JFA 108

# Le commutateur ou Switch :

R 2.04

**Méthodes de transmission :**

La transmission des paquets peut s'opérer selon quatre méthodes :

- ***mode direct*** (*cut through*) : le commutateur lit juste l'adresse du matériel et la transmet telle quelle. Aucune détection d'erreur n'est réalisée avec cette méthode ;
- ***mode différé*** (*store and forward*) : le commutateur met en tampon, et le plus souvent, réalise une opération en somme de contrôle sur chaque trame avant de l'envoyer ;
- *fragment free* : les paquets sont passés à un débit fixé, permettant de réaliser une détection d'erreur simplifiée. C'est un compromis entre les précédentes méthodes ;
- ***commutation automatique*** (*adaptive switching*) : en fonction des erreurs constatées, le commutateur choisit automatiquement un des trois modes précédents.
- Ces quatre méthodes de transmission sont utilisées selon des critères précis.

JFA 109

# Le commutateur ou Switch :

R 2.04

**Fonctions supplémentaires :**

- *Simple Network Management Protocol* (SNMP) : permet d'interroger un équipement réseau à distance. C'est un protocole de supervision du réseau qui permet seulement l'interrogation des équipements réseaux pour récupérer les mesures que cet équipement aura effectuées au préalable ;
- *Spanning Tree Protocol* (STP) : évite les boucles dans un réseau de commutateurs interconnectés ;
- Réseaux locaux virtuels (VLAN) configurables ;
- dot1q : passage de plusieurs VLAN sur un même lien ;
- Agrégation de liens pour augmenter le débit entre deux points ;
- *IGMP snooping* et *MLD snooping* : optimisation de la diffusion *multicast* ;
- dot1x : authentification des postes ;
- QoS : traitement différencié des trames ;

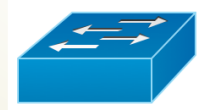
JFA 110

# Le commutateur ou Switch :

R 2.04

- Miroir de port (*port mirroring*) : réplication du trafic d'un port ou d'un VLAN sur un autre port ;
- *Jumbo frame* qui porte la taille des trames à 9 000 octets et plus ;
- Contrôle de flux : permettant d'éviter la saturation d'un équipement susceptible de recevoir un trop grand flux d'informations ;
- *Secure ports* : ports sécurisés pour lesquels on liste les équipements autorisés à communiquer via ces ports. Le commutateur ne laissera passer via le port sécurisé que les paquets destinés aux adresses autorisées ;
- Filtrage par adresse MAC : n'autorise l'accès qu'aux équipements identifiés par leur adresse MAC ;
- Commutateur empilable (*stackable switch*) : commutateur pouvant être associé à un autre commutateur pour ne former qu'un seul commutateur logique.

- Symbole logique :



JFA 111

# Le routeur :

IUT GRAND OUEST NORMANDIE iNFO

R 2.04


- Un **routeur** est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, **au mieux** selon un ensemble de règles, afin de déterminer le meilleur chemin.
- Symbole logique :

JFA 112

# Le routeur :

IUT GRAND OUEST NORMANDIE iNFO

R 2.04

- Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche.
- En plus de leur fonction de routage, les routeurs permettent de manipuler les données circulant sous forme de datagrammes afin d'assurer le passage d'un type de réseau à un autre. Or, dans la mesure où les réseaux n'ont pas les mêmes capacités en terme de taille de paquets de données, les routeurs sont chargés de fragmenter les paquets de données pour permettre leur libre circulation.
- Les premiers routeurs étaient de simples ordinateurs ayant plusieurs cartes réseau, dont chacune était reliée à un réseau différent. Les routeurs actuels sont pour la plupart des matériels dédiés à la tâche de routage, se présentant généralement sous la forme de serveurs 1U.
- Un routeur possède plusieurs interfaces réseau, chacune connectée sur un réseau différent. Il possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté.
- Le principe d'un routeur sans fil est le même que celui d'un routeur classique, si ce n'est qu'il permet à des dispositifs sans-fil de se connecter aux réseaux auxquels le routeur est connecté par des liaisons filaires.

# Le routeur :

JFA 113

**Algorithmes de routage :**

- On distingue généralement deux types d'algorithme de routage :
- Les routeurs de type vecteur de distance (distance vector) établissent une table de routage recensant en calculant le « coût » (en terme de nombre de sauts) de chacune des routes puis transmettent cette table aux routeurs voisins. A chaque demande de connexion le routeur choisit la route la moins coûteuse.
- Les routeurs de type link state (link state routing) écoutent le réseau en continu afin de recenser les différents éléments qui l'entourent. A partir de ces informations chaque routeur calcule le plus court chemin (en temps) vers les routeurs voisins et diffuse cette information sous forme de paquets de mise à jour. Chaque routeur construit enfin sa table de routage en calculant les plus courts chemins vers tous les autres routeurs (à l'aide de l'algorithme de Dijkstra).
- Dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 du modèle OSI.

IUT GRAND OUEST NORMANDIE iNFO R 2.04

# La passerelle (Gateway) :

JFA 114

- Une **passerelle** (« **Gateway** ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseau différents.
- Lorsqu'un utilisateur distant contacte un tel dispositif, ce dernier examine sa requête et, si jamais celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée une liaison entre les deux réseaux. Les informations ne sont donc pas directement transmises, mais traduites afin d'assurer la continuité des deux protocoles.
- Ce système offre, outre l'interface entre deux réseaux hétérogènes, une sécurité supplémentaire car chaque information est passée à la loupe (pouvant causer un ralentissement) et parfois ajoutée dans un journal qui retrace l'historique des événements.
  L'inconvénient majeur de ce système est qu'une telle application doit être disponible pour chaque service (FTP, HTTP, Telnet, etc).

IUT GRAND OUEST NORMANDIE iNFO R 2.04

JFA 115

# Les B-Routeurs :

R 2.04

- Un B-Routeur (*b-routeur* pour *bridge-routeur*) est un élément hybride associant les fonctionnalités d'un routeur et celles d'un pont. Ainsi, ce type de matériel permet de transférer d'un réseau à un autre les protocoles non routables et de router les autres. Plus exactement, le B-routeur agit en priorité comme un pont et route les paquets si cela n'est pas possible.
- Un B-routeur peut donc dans certaines architectures être plus économique et plus compact qu'un routeur et un pont.

JFA 117

# Interconnexions :

R 2.04

Outre le fait que les nouvelles matériel actif s'adaptent automatiquement aux câbles en reconnaissant les positions du signal, on utilisera soit un câble croisé ou droit selon le type de matériel que l'on connecte :

- **Câbles croisés :**
  - Switch à Switch
  - Hub à Hub
  - Routeur à Routeur
  - PC à PC
  - Hub à Switch
  - PC à Routeur
- **Câbles droits :**
  - PC à Hub
  - PC à Switch
  - Switch à Routeur

JFA 118

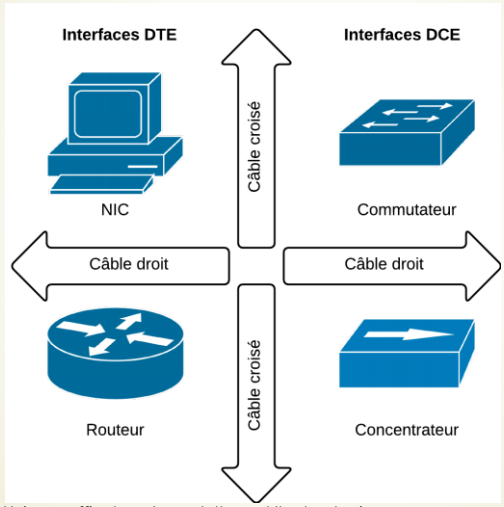
# Interconnexions :

Les commutateurs (switches) et concentrateurs (hubs) sont des périphériques DCE (Data Connexion Equipement) alors que les stations terminales et les routeurs sont des périphériques DTE (Data Terminal Equipment). Les équipements identiques DTE/DTE ou DCE/DCE se connectent avec un câble croisé (croisement de l'émission et de la réception). Les équipements de type différents se connectent avec un câble droit car l'émission/réception sur leur interfaces est déjà inversée.

- **Câble droit (straight)**
- **Câble croisé (cross-over)**

JFA 119

# Interconnexions :




https://cisco.goffinet.org/ccna/ethernet/technologie-ethernet/

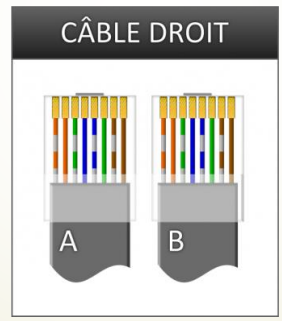
JFA 120

# Câble UTP/STP :

R 2.04

***Brochage droit d'un câble UTP/STP cat 5 sur une prise modulaire RJ45 Jack mâle :***

- Les paires d'émission (TD) et de réception (RD) sont positionnée de manière identique de part et d'autre du câble. En regardant les contacts métalliques de la fiche :



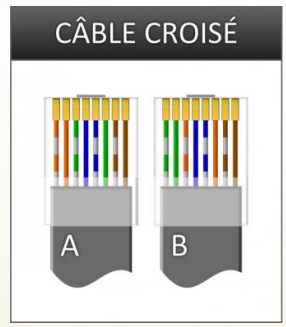

JFA 121

# Câble UTP/STP :

R 2.04

***Brochage croisé d'un câble UTP/STP cat 5 sur une prise modulaire RJ45 Jack mâle :***

- Il faut échanger les broches 1 avec 3 et 2 avec 6, c'est à dire remplacer les fils verts par les fils oranges et vice versa. En regardant les contacts métalliques de la fiche :



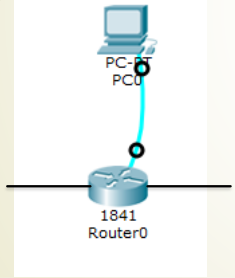
# Branchement du Routeur :

JFA 122

R 2.04

***Connexion à la console du routeur :***

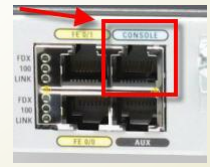
***Accès en mode direct :***




Câble Console

Prise DB9 : Série RS232

Port console Routeur



# Accéder à la console de gestion

JFA 123

R 2.04

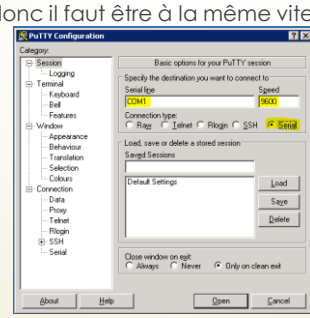
- Maintenant que votre ordinateur est physiquement connecté au switch/routeur par le câble console, il faut exécuter un **logiciel** pour afficher la console de l'équipement. La console est l'écran qui vous permet de taper des lignes de commandes (CLI) et de les envoyer à l'équipement pour que l'IOS les exécutent.
- Ce logiciel va vous permettre d'aller prendre le contrôle du port série de votre ordinateur qui je le rappelle est physiquement connecté au Switch/routeur.
- Nous allons utiliser le logiciel PUTTY car très simple d'utilisation et très puissant. Et en plus de la prise de contrôle du port série de votre ordinateur, il peut aussi utiliser les protocoles telnet et SSH pour se connecter à distance.
- Si L'ordinateur est sur le même réseau que le routeur, on peut aussi y accéder en TELNET, par son adresse IP.

# Accéder à la console de gestion

JFA 124

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- **Configuration du Putty**
  - Démarrez Putty,
  - sélectionnez le bouton "**Serial**" en haut à droite pour préciser au logiciel qu'il faut prendre le contrôle du port série de l'ordinateur **Serial line**: c'est l'identifiant de votre port série, selon les ordinateurs, il peut être **COM1, COM2, COM3**…
  - **Speed**: c'est la vitesse entre les 2 équipements. Par défaut, l'IOS Cisco est à **9600 bauds** donc il faut être à la même vitesse de l'autre coté,




# Accéder à la console de gestion

JFA 125

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- **Configuration de la liaison RS232 :**
  - cliquez sur "**Serial**" se trouvant dans le menu de gauche, tout en bas et vérifier que les paramètres sont les suivants:
    - **Data bits**: c'est le nombre de bits de données à envoyer en même temps, mettez **8 bits**
    - **Stop bits**: bit d'arrêt, mettez **1**
    - **Parity**: aucune parité à configurer
    - **Flow Control**: laissez par défaut


  - cliquez sur le bouton "**Open**",
  - une nouvelle fenêtre s'ouvre et vous êtes désormais connecté à l'IOS de votre équipement. Tapez "**Entrée**" pour récupérer la commande en ligne CLI

JFA 126

# Configuration du routeur

R 2.04

- **Configuration du routeur :**
  - Le routeur possède 2 modes de commandes, pour pouvoir modifier les paramètres, il faut passer en mode privilégié :

```
Routeur > enable (en)
Routeur #
```

  - Pour pouvoir modifier la configuration, il faut passer en mode configuration globale :

```
Routeur # configuration terminal (conf t)
Enter configuration commands, one per line. End with CTRL/Z
Routeur(config)#
```

  - Donner un nom au routeur :

```
Routeur(config)# hostname routeurFr
```

  - Pour sortir du mode configuration :

```
Routeur(config)# exit
Routeur#
```

JFA 127

# Configuration du routeur

R 2.04

- **Configuration du port d'un routeur :**
  - Vous souhaitez configurer une adresse IP au routeur, les étapes sont:
  - identifier l'interface physique du routeur (par exemple FastEthernet 0/1)
  - entrer dans le mode privilégié

```
Routeur> enable
```

  - entrer dans le mode de configuration globale du routeur

```
Routeur# conf t
```

  - entrer dans le mode de configuration de l'interface physique en question

```
Routeur(config)# interface FastEthernet 0/1
```

  - définir l'adresse IP et son masque

```
Routeur(config_if)# ip address 10.1.1.9  255.255.255.0
```

  - activer **électriquement** l'interface

```
Routeur(config_if)# no shutdown
```

  - sortir du mode de l'interface physique, et du mode configuration globale

```
Routeur(config_if)# exit
Routeur(config)# exit
```

# Configuration du routeur

JFA 128

R 2.04

- **Configuration du port d'un routeur :**
  - Pour vérifier la configuration du routeur :

```
Routeur# show running-config
```

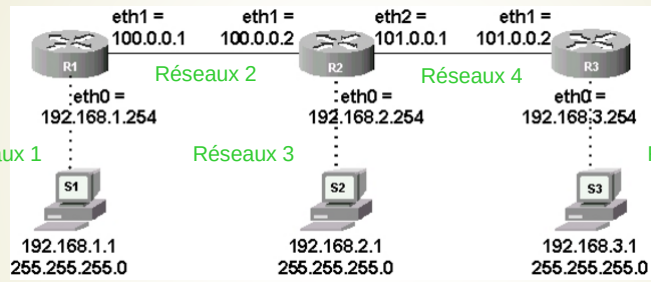
- Pour compléter les commandes utiliser la touche TAB
- Pour rappeler les commandes précédentes et les modifier, utilisez les touche flèches haut, bas, gauche et droite.
- CTRL A : permet de positionner le curseur au tout début de la ligne,
- CRTL E : permet de positionner le curseur à la fin de la ligne.
- *Il peut être pratique de copier les commandes dans un bloc note, les modifier, et les coller dans la console du routeur.*

# Routage dans un Réseau

JFA 129

R 2.04

- **Etude du schéma suivant :**




- Le routeur R1 connait le réseau 1 : 192.168.1.0 et le réseau 2 : 100.0.0.0,
- Le routeur R2 connait le réseau 2 : 100.0.0.0, le réseau 3 : 192.168.2.0 et le réseau 4 : 101.0.0.0,
- Le routeur R3 connait le réseau 4 : 101.0.0.0, et le réseau 5: 192.168.3.0

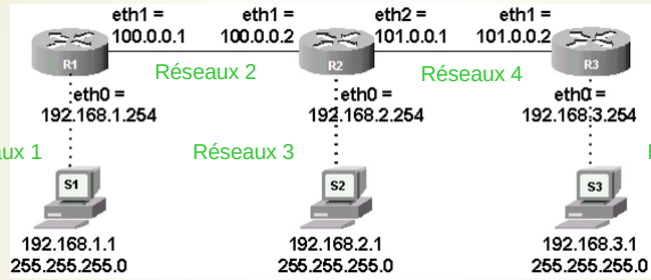
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage dans un Réseau

JFA 130

R 2.04

- **Etude du schéma suivant :**




  - Mais le Routeur 1 ne connaît pas le réseau 3, le réseau4 et le réseau 5,
  - et le Routeur 2 ne connaît pas le réseau 1 et le réseau 5,
  - Et le routeur R3 ne connaît pas le réseau 1, le réseau 2 et le réseau 3,

https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage statique en Réseau

JFA 131

R 2.04

- ***Méthode 1 : Routage statique :***
  - On peut ajouter manuellement à un routeur, les routes de notre réseau qui lui manquent, en utilisant la commande :

ip route <réseau distant> <masque réseau du réseau distant> <passerelle d'accès>

Avec :

- <réseau distant> : L'adresse IP du réseau distant que l'on cherche à ajouter,
- <masque réseau du réseau distant> : Le masque réseau du réseau distant que l'on cherche à ajouter,
- <passerelle d'accès> :
  - Le port de sortie du routeur à utiliser pour atteindre le réseau distant
  - Ou l'adresse IP du port du prochain routeur à utiliser pour atteindre le réseau distant,

***Exemples :***

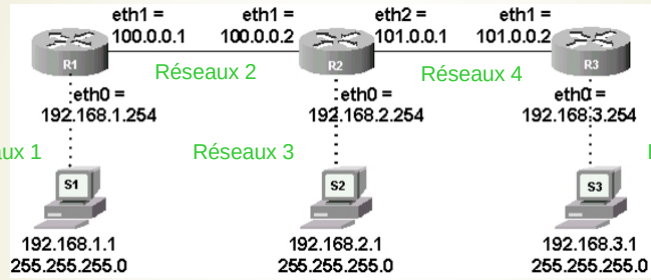
- R4(config)# ip route 192.168.2.0 255.255.255.0 FastEthernet 1/0
- R4(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

# Routage statique en Réseau

JFA 132

R 2.04

- **Méthode 1 : Routage statique : on va donc ajouter :**




- ***Sur le routeur 1 :***
  - R1 (config)# ip route 192.168.2.0 255.255.255.0 100.0.0.2
  - R1 (config)# ip route 192.168.3.0 255.255.255.0 100.0.0.2
  - R1 (config)# ip route 101.0.0.0 255.255.255.0 100.0.0.2

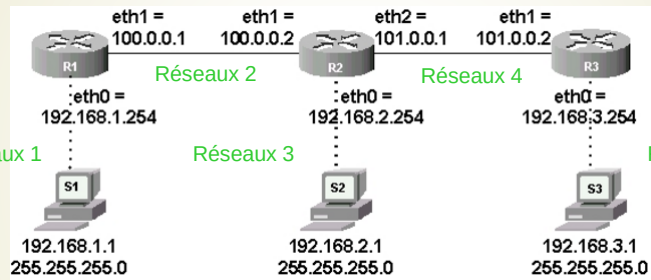
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage statique en Réseau

JFA 133

R 2.04

- **Méthode 1 : Routage statique : on va donc ajouter :**




- ***Sur le routeur 2 :***
  - R2 (config)# ip route 192.168.1.0 255.255.255.0 100.0.0.1
  - R2 (config)# ip route 192.168.3.0 255.255.255.0 101.0.0.2

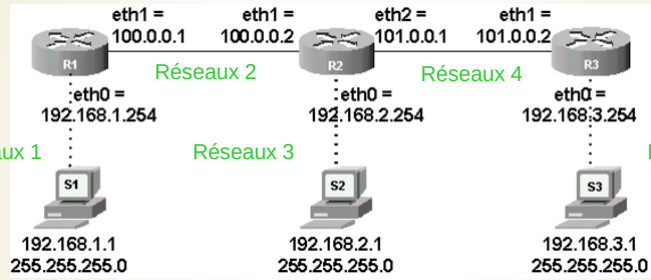
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage statique en Réseau

JFA 134

R 2.04

- **Méthode 1 : Routage statique : on va donc ajouter :**




  - ***Sur le routeur 3 :***
    - R3 (config)# ip route 192.168.2.0 255.255.255.0 101.0.0.1
    - R3 (config)# ip route 192.168.1.0 255.255.255.0 101.0.0.1
    - R3 (config)# ip route 100.0.0.0 255.255.255.0 101.0.0.1

https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage statique en Réseau

JFA 135

R 2.04

- ***Avantages :***
  - **Économie de bande passante** : Étant donné qu'aucune information ne transite entre les routeurs pour qu'ils se tiennent à jour, la bande passante n'est pas encombrée avec des messages d'information et de routage.
  - **Sécurité** : Contrairement aux protocoles de routage dynamique que nous allons voir plus bas, le routage statique ne diffuse pas d'information sur le réseau puisque les informations de routage sont directement saisies de manière définitive dans la configuration par l'administrateur.
  - **Connaissance du chemin à l'avance** : L'administrateur ayant configuré l'ensemble de la topologie saura exactement par où passent les paquets pour aller d'un réseau à un autre, cela peut donc faciliter la compréhension d'un incident sur le réseau lors des transmissions de paquets.
- ***Inconvénients :***
  - La configuration de réseaux de taille importante peut devenir assez longue et complexe, il faut en effet connaitre l'intégralité de la topologie pour saisir les informations de manière exhaustive et correcte pour que les réseaux communiquent entre eux. Cela peut devenir une source d'erreur et de complexité supplémentaire quand la taille du réseau grandit.
  - A chaque fois que le réseau évolue, il faut que chaque routeur soit au courant de l'évolution par une mise à jour manuelle de la part de l'administrateur qui doit modifier les routes selon l'évolution.

# Routage dynamique en Réseau

JFA 136

R 2.04

- ***Méthode 2 : Routage dynamique :***
  - Le routage dynamique va permet de mettre à jour de façon automatique le plan du réseau. Le choix d'un protocole de routage va permettre aux routeurs de se comprendre et d'échanger des informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Concrètement, le protocole de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleurs routes à emprunter :
  - Il est important de savoir que certains protocoles de routage calculent les routes en fonction :
    - de la vitesse des liens qui les relient (État des liens ,
    - du nombre de routeurs (Nb de sauts) à passer avant d'atteindre notre destination (Distance-vecteur),

# Routage dynamique en Réseau

JFA 137

R 2.04

- ***Méthode de Routage dynamique :***
  - Il suffit de préciser au routeur quel protocole de propagation de route on veut utiliser (***RIP***, IGRP, OSPF, IS-IS).
  - Ici, nous allons nous intéresser à RIP (Routing Information Protocol) qui est de type **vecteur distance** basé sur l'algorithme de routage décentralisé Bellman-Ford. Il permet à chaque routeur de communiquer aux autres routeurs la métrique, c'est-à-dire la distance qui les sépare du réseau IP (le nombre de sauts qui les sépare, ou « hops » en anglais). Ainsi, lorsqu'un routeur reçoit un de ces messages, il incrémente cette distance de 1 et communique le message aux routeurs directement accessibles.
  - Les routeurs peuvent donc conserver de cette façon la route optimale d'un message en stockant l'adresse du routeur suivant dans la table de routage de telle façon que le nombre de sauts pour atteindre un réseau soit minimal.

# Routage dynamique en Réseau

JFA 138

R 2.04

- ***Méthode RIP :***

Il existe deux versions de RIP, la deuxième étant une amélioration de la première.

- RIPv2 apporte les modifications suivantes à RIPv1 :
  - Le support du routage classless (CIDR).
  - La diffusion du masque réseau dans les mises à jour de routage.
  - Le support de V.L.S.M. (Variable Length Subnet Mask)
  - La diffusion des mises à jour de routage s'effectue par multicast avec l'adresse de classe D : 224.0.0.9. (Avec RIPv1 les mises à jour s'effectuent en broadcast)
  - L'authentification de la source de la mise à jour de routage par un texte en clair (actif par défaut), ou un texte crypté suivant l'algorithme MD5.
  - L'utilisation d'indicateurs de route externe (route tag) afin de pouvoir différencier les routes apprises par d'autres protocoles de routage et redistribuées dans RIP,
- Aujourd'hui, on utilise que la version 2 : RIPv2.

***Exemples :***

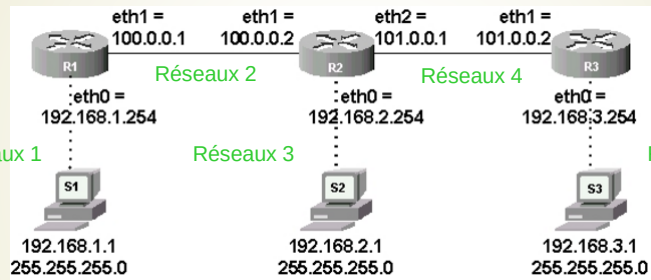
- R1 (config)# router rip
- R1 (config-router)# version 2

# Routage dynamique en Réseau

JFA 139

R 2.04

- **Méthode 2 : Routage dynamique : on va donc ajouter :**




- ***Sur le routeur 1 :***
  - R1 (config-router)# network 192.168.1.0
  - R1 (config-router)# network 100.0.0.0

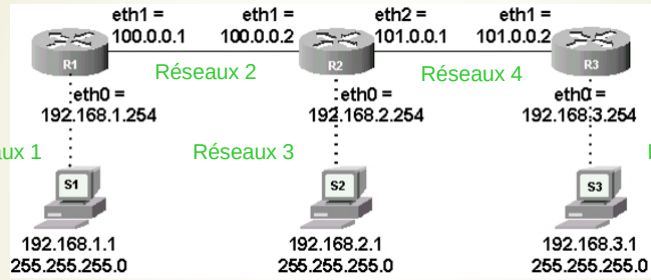
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage dynamique en Réseau

JFA 140

R 2.04

- **Méthode 2 : Routage dynamique : on va donc ajouter :**




- ***Sur le routeur 2 :***
  - R2 (config-router)# network 192.168.2.0
  - R2 (config-router)# network 100.0.0.0
  - R2 (config-router)# network 101.0.0.0

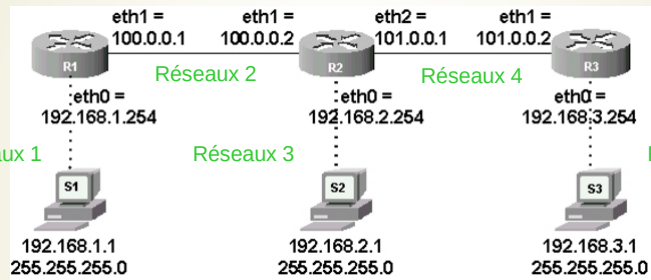
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage dynamique en Réseau

JFA 141

R 2.04

- **Méthode 2 : Routage dynamique : on va donc ajouter :**




- ***Sur le routeur 3 :***
  - R3 (config-router)# network 192.168.3.0
  - R3 (config-router)# network 101.0.0.0

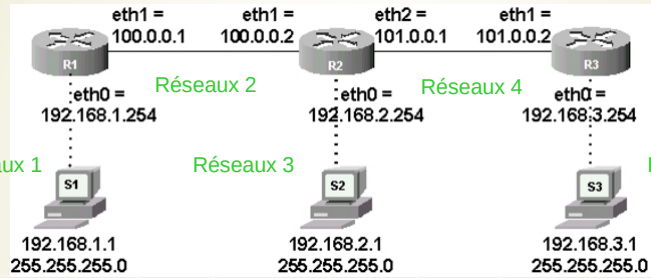
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage dynamique en Réseau

JFA 142

R 2.04

- Méthode 2 : Routage dynamique : progression à t = 0s




| Table de Routage R1 | Metric | Table de Routage R2 | Metric | Table de Routage R3 | Metric |
|---|---|---|---|---|---|
| 192.168.1.0 | 1 | 192.168.2.0 | 1 | 192.168.3.0 | 1 |
| 100.0.0.0 | 1 | 100.0.0.0 | 1 | 101.0.0.0 | 1 |
| | | 101.0.0.0 | 1 | | |

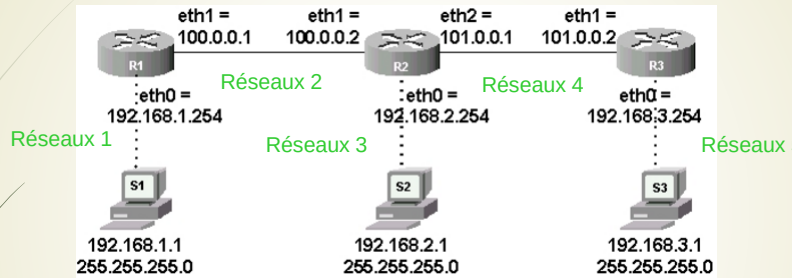
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage dynamique en Réseau

JFA 143

R 2.04

- Méthode 2 : Routage dynamique : progression à t = 30s




| Table de Routage R1 | Metric | Table de Routage R2 | Metric | Table de Routage R3 | Metric |
|---|---|---|---|---|---|
| 192.168.1.0 | 1 | 192.168.2.0 | 1 | 192.168.3.0 | 1 |
| 100.0.0.0 | 1 | 100.0.0.0 | 1 | 101.0.0.0 | 1 |
| 192.168.2.0 | 2 | 101.0.0.0 | 1 | 192.168.2.0 | 2 |
| 101.0.0.0 | 2 | 192.168.1.0 | 2 | 100.0.0.0 | 2 |
| | | 192.168.3.0 | 2 | | |

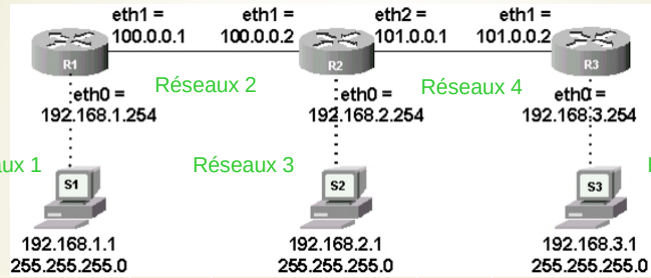
https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage dynamique en Réseau

JFA 144

R 2.04

- **Méthode 2 : Routage dynamique : progression à t = 1mn**




| Table de Routage R1 | Metric | Table de Routage R2 | Metric | Table de Routage R3 | Metric |
|---|---|---|---|---|---|
| 192.168.1.0 | 1 | 192.168.2.0 | 1 | 192.168.3.0 | 1 |
| 100.0.0.0 | 1 | 100.0.0.0 | 1 | 101.0.0.0 | 1 |
| 192.168.1.0 | 2 | 101.0.0.0 | 1 | 192.168.2.0 | 2 |
| 101.0.0.0 | 2 | 192.168.1.0 | 2 | 100.0.0.0 | 2 |
| 192.168.3.0 | 3 | 192.168.3.0 | 2 | 192.168.1.0 | 3 |

https://inetdoc.developpez.com/tutoriels/routage-dynamique-protocole-rip/images/topo22.png

# Routage dynamique en Réseau

JFA 145

R 2.04

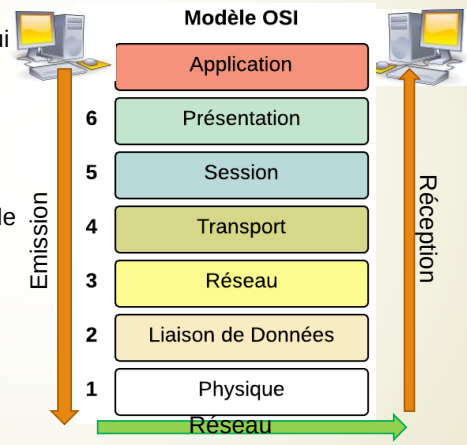
- ***Avantages :***
  - Une **maintenance réduite** par l'automatisation des échanges et des décisions de routage
  - Une **modularité** et une **flexibilité** accrue, il est plus facile de faire évoluer le réseau s'il se met à jour automatiquement.
  - Sa **performance** et sa mise en place ne dépendent pas de la taille du réseau
- ***Inconvénients :***
  - Il peut être plus compliqué à mettre en place lors de son initialisation
  - Il consomme de la bande passante par les messages que les routeurs s'envoient périodiquement sur le réseau (+/- 30 s),
  - La diffusion automatique de message sur le réseau peut constituer un problème de sécurité car un attaquant peut obtenir des informations sur la topologie du réseau simplement en écoutant et en lisant ces messages d'information du protocole de routage et même en créer afin de se faire passer pour un membre du réseau.
  - Le traitement des messages réseau et le calcul des meilleures routes à emprunter représentent une consommation de CPU et de RAM supplémentaire qui peut encombrer certains éléments du réseau peu robuste.

# Normalisation : Modèle OSI

JFA 146

R 2.04

- Dans le but de Normaliser les communications réseau, on a définit un modèle pour garantir l 'évolution et l'interopérabilité des matériels,
  - Le modèle OSI est une norme qui structure la communication entre les différents éléments et protocoles du réseau.
  - Les communications ont été découpées en différentes couches, chaque couche a un rôle bien défini,
  - Les données traversent les différentes couches, de l'application jusqu'au média réseau, et à l'arrivée font le chemin en sens inverse,




# Normalisation : Modèle OSI

JFA 147

R 2.04

***Règles du Modèle OSI :***

- Chaque couche a un rôle particulier.
- Chaque couche est indépendante ;
  - Les informations utilisées par une couche ne pourront pas être utilisées par une autre couche : Cela va permettre de garantir l'évolution des communications dans le temps.
  - Rendre les couches indépendantes garantit qu'elles sont modifiables : Cela veut dire qu'on pourra changer un protocole associé à une couche sans avoir besoin de changer toutes les couches du modèle OSI.
- Chaque couche ne peut communiquer qu'avec une couche adjacente (au-dessus ou au-dessous).
  - Lors de l'envoi (de la réception) de données chaque couche prépare les données pour la couche suivante. Ainsi toutes les couches vont être parcourues pour l'émission, et pareil pour la réception en sens inverse.
  - On peut ainsi garantir que tous les rôles associés à chaque couche, et donc nécessaires à la communication, vont être remplis !

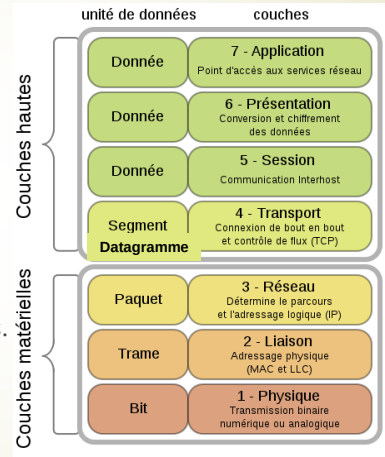
# Normalisation : Modèle OSI

JFA 148

R 2.04

***Communication inter couches :***

- On peut diviser le modèle en 2 groupes :
  - La couche haute est plutôt orientée application et bibliothèque système,
  - La couche basse est plutôt orientée communication et est fournie par le système d'exploitation et le matériel. Elle est transparente pour les données.
- On pourra remarquer que le nom de l'unité de données change en fonction de la couche !



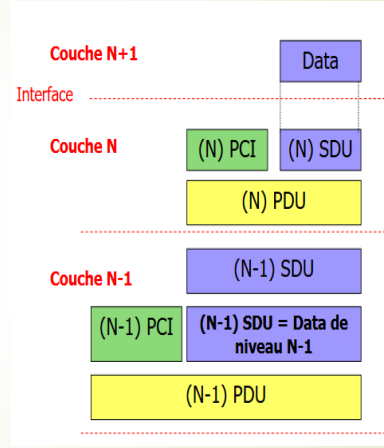

# Normalisation : Modèle OSI

JFA 149

R 2.04

***Les unités de Données :***

- Une donnée arrive de la couche N+1,
- En traversant l'interface, elle devient le SDU (Service Data Unit) de la couche N,
- On lui ajoute un bloc d'information de contrôle de protocole (PCI : Protocol Control Information), qui peut-être mis en entête et/ou en fin du SDU, suivant la couche,
- Le total devient le PDU (Packet Data Unit) c'est-à-dire l'unité de protocole de niveau N, et par conséquent le SDU de la couche N-1 !
- ***Ce procédé s'appelle l'encapsulation !***



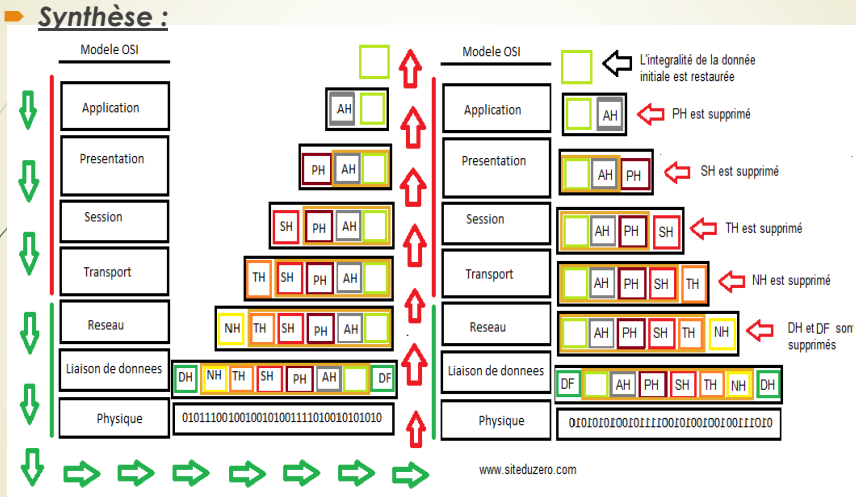

http://slideplayer.fr/slide/517930/

# Normalisation : Modèle OSI

JFA 150

R 2.04

- ***Synthèse :***



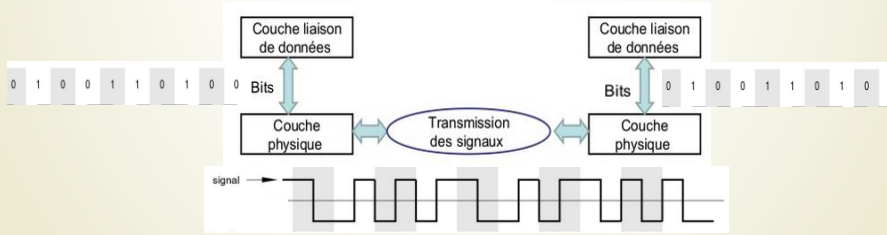

http://sdz.tdct.org/sdz/medias/uploads.siteduzero.com_files_284001_285000_284770.png

# Normalisation : Modèle OSI

JFA 151

R 2.04

- ***La couche Physique :***
  - La couche physique est chargée de la transmission effective des signaux électriques ou optiques entre les différents interlocuteurs.
  - Son service est généralement limité à l'émission et la réception d'un bit ou d'un train de bits continu (notamment pour les supports synchrones comme la fibre optique).
  - Cette couche est chargée de la conversion entre bits et signaux électriques ou optiques réalisé généralement par un circuit électronique qui va utiliser un encodage en bande de base : (NRZ, Miller, Manchester différentiel, …).




https://fr.slideshare.net/imisoliter/chap2-physique

# Modèle OSI : Couche 2

JFA 152

R 2.04

- ***La couche Liaison de données :***
- La **couche de liaison de données** transforme une transmission **brute** en une ligne sans erreurs de transmission jusqu'à la couche réseau. Pour cela **les données brutes sont découpées en trames** (Frames) comprises entre 100 et 1000 octets. Puis elles sont envoyées de manière séquentielles.
- Dans le cas où la connexion est fiable, le destinataire confirme la bonne réception de chaque trames en envoyant des **trames d'Acquittement (Acknowledgement)**, c'est à dire de bonne réception.
- C'est également **dans cette couche que se passe une partie de la régulation du trafic**.
- Enfin c'est dans cette même couche que la gestion des erreurs est gérée pour les trames.
- Exemples de protocoles de liaison de données. :
  - Ethernet pour les réseaux locaux (multi-nœuds),
  - le protocole point à point (PPP)

# Modèle OSI : Couche 2

JFA 153

R 2.04

- ***L' adressage des machines :***
- Pour la couche 2, ce sont les adresses MAC qui sont utilisées
  Les adresses MAC sont codées sur 6 octets, soit 48 bits donc $2^{48}$ = ... plusieurs milliers de milliards d'adresses possibles !
  Elles sont la plupart du temps écrites par octet sous forme hexadécimale, séparés par le caractère ":"
  Ce qui donne par exemple 3C:AB:35:48:FF:D2 qui est une adresse MAC.
- Nous pouvons ainsi identifier chaque interface de machine individuellement. Il nous faut maintenant définir les règles qui permettront aux machines de dialoguer. Pour cela nous allons définir un langage de communication, aussi appelé protocole.

# Modèle OSI : Couche 2

JFA 154

IUT GRAND OUEST NORMANDIE iNFO

R 2.04

- ***Le protocole Ethernet :***
- Le protocole Ethernet définit le format des messages échangés. Le message de base utilisé par Ethernet est la trame. La trame est composée d'un en-tête et d'une "charge utile" contenant les informations à transmettre.
  L'en-tête Ethernet contient les informations nécessaires au bon fonctionnement de la couche 2 qui pourront permettre la transmission des informations. Nous y retrouvons notamment les adresses MAC des machines participant au dialogue.

# Modèle OSI : Couche 2

JFA 155

IUT GRAND OUEST NORMANDIE iNFO

R 2.04

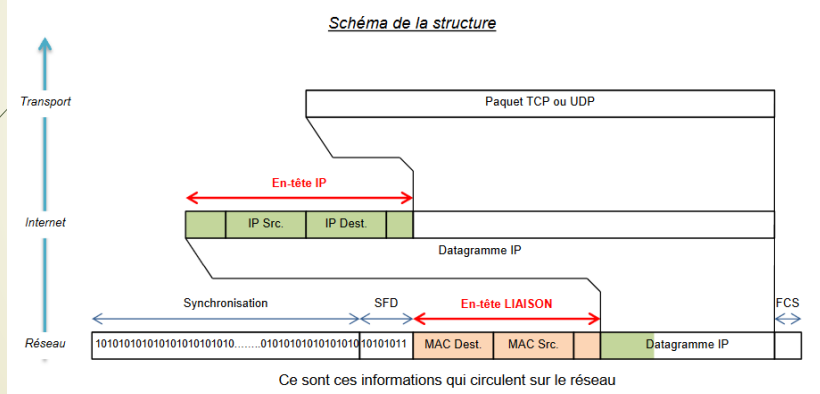
- ***Format d'une trame Ethernet:***
- La description suivante ne prend en compte que les informations qui nous intéressent et n'est pas le format complet d'une trame Ethernet.
- La trame est composée d'une en-tête contenant les informations du protocole Ethernet, et d'un payload contenant les informations à transporter.
- Trame Ethernet : Nous allons voir plus en détail ce que contient l'en-tête Ethernet.

# Modèle OSI : Couche 2

JFA 156

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- Nous allons voir plus en détail ce que contient l'en-tête Ethernet :




Ce sont ces informations qui circulent sur le réseau

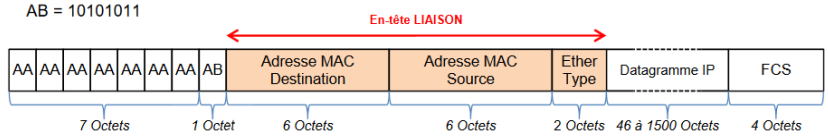
# Modèle OSI : Couche 2

JFA 157

IUT GRAND OUEST NORMANDIE – iNFO – R 2.04

- Trame Ethernet :

AA = 10101010
AB = 10101011




**Préambule** : (7 octets) Permet la synchronisation des horloges de transmission. Il s'agit d'une suite de 1 et de 0 soit 7 octets à la valeur 0xAA

**SFD** : (1 octets) "Starting Frame Delimiter". Il s'agit d'un octet à la valeur 0xAB. Il doit être reçu en entier pour Valider le début de la trame.

**En-tête** : (14 octets)
- Adresse MAC du destinataire (6 octets)
- Adresse MAC de l'émetteur (6 octets)
- EtherType (Type de protocole) (2 octets)

*Exemples de valeurs du champ EtherType* →

| EtherType | Protocole |
|---|---|
| 0x0800 | IPv4 |
| 0x0806 | ARP |
| 0x809B | AppleTalk |
| 0x8035 | RARP |
| 0x86DD | IPv6 |

**FCS** : (4 octets) Frame Check Sequence. Ensemble d'octets permettant de vérifier que la réception s'est effectuée sans erreur.

http://www.mysti2d.net/polynesie2/ETT/C044/31/SerruresBioIP/index.html?Cours4.html

# Modèle OSI : Couche 2

JFA 158

R 2.04

- L'adresse MAC source est l'adresse de la machine qui envoie la trame.
- L'adresse MAC destination est celle de la machine qui doit recevoir la trame
- Le protocole sup est le protocole utilisé par la couche supérieure (la couche 3 dans notre cas puisque Ethernet est un protocole de couche 2) Ceci est utile car quand la couche 2 reçoit le message, elle doit savoir à quel protocole de couche 3 envoyer les informations reçues (il est possible sur une machine d'utiliser plusieurs protocoles pour une même couche)

# Modèle OSI : Couche 2

JFA 159

R 2.04

- ***Dialogue entre deux machines***
  - Prenons l'exemple d'une machine A qui veut envoyer le message "Bonjour" à une machine B située sur le même réseau.
  - Il lui suffit de connaître l'adresse MAC de B pour lui envoyer le message. Ainsi, en lui envoyant la trame suivante, elle devrait pouvoir lui envoyer le message:

    ++++++++++++++++++++++++++++++++++----------

    | @MAC A| @MAC B | protocole sup | XXXXX | Bonjour |

    ++++++++++++++++++++++++++++++++++----------
  - B reçoit la trame et voit que c'est son adresse MAC qui est en destination, elle lit donc le reste des informations. Il s'agit des informations des couches supérieures (XXXXX), et enfin, du message "Bonjour"
  - Nous avons donc réussi grâce à la couche 2 à faire dialoguer deux machines connectées sur un même réseau.
  - Nous verrons plus tard comment faire communiquer deux machines appartenant à des réseaux différents.

# Modèle OSI : Couche 3

JFA 160

R 2.04

- ***La couche Réseau :***
  - La couche réseau a pour rôle d'acheminer les informations d'un réseau à un autre. C'est ce que l'on appelle le routage. Les réseaux sont donc reliés entre eux par des machines que l'on appelle routeurs. Ces routeurs vont donc recevoir les paquets sur un réseau, et les renvoyer sur l'autre. Ils ont donc une connexion sur chaque réseau. Tous les réseaux ne pouvant pas être reliés entre eux, il va souvent falloir passer par des réseaux intermédiaires pour pouvoir envoyer un paquet d'un réseau à un autre.
  - La couche réseau a d'autres fonctionnalités …
  - La **couche réseau** est donc en charge des opérations du sous-réseau. C'est ici que va se dérouler le **routage des paquets** (packets) : quelle route vont emprunter les paquets pour aller de la source à la destination et surtout par quel chemin. **Le routage peut être statique ou alors dynamique**.
  - Si **trop de paquets sont présents sur le réseau, il se forme des bouchons** (bottlenecks). Pour éviter ce genre de cas de congestion, cette couche dispose de mécanismes bien spécifiques.
  - C'est également dans cette couche que la Qualité de Service (**Quality of Service**, QoS) est gérée.

# Modèle OSI : Couche 3

JFA 161

R 2.04

- ***Pourquoi encore une adresse alors que nous avons déjà l'adresse MAC ?***
  - Il est nécessaire de différencier les adresses de couche 2 et de couche 3, car elles n'ont pas le même rôle.
  - L'adressage MAC en couche 2 permet d'identifier les machines SUR UN MEME RESEAU.
  - L'adressage IP en couche 3 permet d'adresser les machines SUR DES RESEAUX DISTINCTS.
  - Les adresses de couche 2 sont en rapport avec le matériel réseau utilisé (le protocole de couche 2 est géré au niveau de la carte connectée au réseau et non pas par le système d'exploitation comme les couches supérieures) il est donc difficile de modifier les adresses MAC qui sont censées être codées directement sur la carte réseau.
  - Cela est notamment dû au fait que chaque adresse MAC doit être unique sous peine de conflit matériel, et que cette adresse doit être accessible très tôt lors du boot d'une machine.

# Modèle OSI : Couche 3

JFA 162

R 2.04

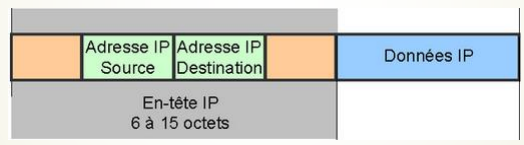
- Les adresses de couche 3 quant à elles demandent une certaine souplesse d'utilisation car on ne connait pas à priori l'adresse du réseau sur lequel une machine va se trouver.
- Il y a donc une incompatibilité d'utilisation d'une adresse de couche 2 pour une adresse de couche 3, et vice versa.
- Enfin, les protocoles réseau évoluant au fil du temps, il est nécessaire que chaque couche soit indépendante des autres.

# Modèle OSI : Couche 3

JFA 163

R 2.04

- ***Format d'un datagramme IP***
  - De la même façon qu'avec Ethernet, la couche IP (couche 3) va nécessiter un certain nombre d'informations pour pouvoir effectuer les tâches qui lui incombent comme le routage. A la manière de la trame Ethernet, le datagramme IP se compose d'une en-tête IP, et d'une charge utile contenant les informations à transporter (données IP).

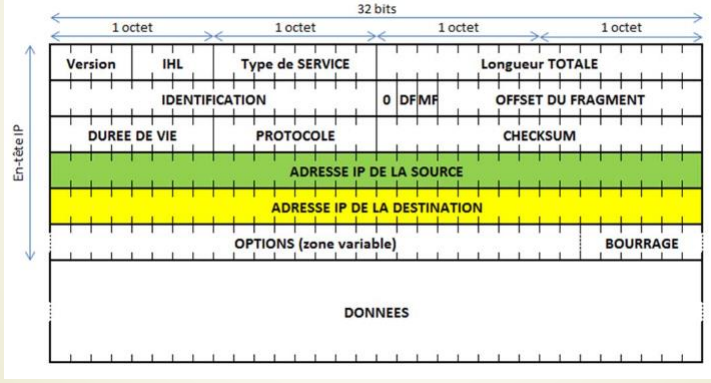


# Modèle OSI : Couche 3

JFA 164

R 2.04

- Nous allons voir plus en détail ce que contient l'en-tête IP, même si nous ne décrivons pas l'ensemble de l'en-tête, mais juste les informations qui nous intéressent.




http://www.mysti2d.net/polynesie2/ETT/C044/31/SerruresBioIP/index.html?Cours4.html

# Modèle OSI : Couche 3

JFA 165

R 2.04

**Version** : (4 bits) il indique le numéro de version du protocole IP utilisé (généralement 4).

**IHL** : (4 bits) Internet Header Lenght (Longueur d'entête). Spécifie la longueur de l'en-tête du Datagramme en nombre de mots de 32 bits. Ce champ ne peut prendre une valeur inférieure à 5.

**Type de service** : (8 bits) Donne une indication sur la qualité de « service » souhaitée pour l'acheminement des données.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Priorité | | | D | T | R | C | x |

| *Bits 0-2* | **Priorité** | 010➔Immédiate 001➔Normale 000➔Basse | |
|---|---|---|---|
| *Bit 3* | **D** | 0 = Retard standard | 1 = Retard faible |
| *Bit 4* | **T** | 0 = Débit standard | 1 = Haut débit |
| *Bit 5* | **R** | 0 = Taux d'erreur standard | 1 = Taux d'erreur faible |
| *Bit 6* | **C** | 0 = Coût standard | 1 = Coût faible |
| *Bit 7* | **x** | Réservé | |

**Longueur totale** : (16 bits) Longueur du datagramme entier y compris en-tête et données mesurée en octets.

**Identification** : (16 bits) Valeur assignée par l'émetteur pour identifier les fragments d'un même datagramme.

# Modèle OSI : Couche 3

JFA 166

R 2.04

| | | |
|---|---|---|
| **Flags** : | (3 bits) | Commutateurs de contrôle :<br>- Bit 0 Réservé, doit être laissé à 0<br>- Bit 1 (DF - Don't fragment) 0= Fragmenté 1= Non fragmenté<br>- Bit 2 (MF – More Fragment) 0= Dernier fragment 1= Fragment |
| **OFFSET** : | (13 bits) | Décalage du premier octet du fragment par rapport au datagramme complet non fragmenté. Cette position est mesurée en blocs de 8 octets (64 bits). |
| **Durée de vie** : | (8 bits) | Temps en secondes pendant lequel le datagramme doit rester dans le réseau. Si ce champ vaut 0, le datagramme doit être détruit. Ce temps diminue à chaque passage du datagramme d'une machine à l'autre. |
| **Protocole** : | (8 bits) | Protocole porté par le datagramme (au-dessus de la couche IP) |

| Valeur | Protocole |
|---|---|
| 1 | ICMP |
| 6 | TCP |
| 17 | UDP |
| Etc | etc |

| | | |
|---|---|---|
| **Checksum** : | (16 bits) | (Somme de contrôle) C'est une valeur qui permet de déceler une éventuelle erreur de transmission avec une très grande probabilité. |
| **IP Source** : | (32 bits) | Adresse IP de l'émetteur. |
| **IP Destination** : | (32 bits) | Adresse IP du destinataire. |
| **Options** : | (Variable) | Le champ est de longueur variable.Un datagramme peut comporter 0 ou plusieurs options. |
| **Bourrage** : | (Variable) | Le champ Bourrage n'existe que pour assurer à l'en-tête une taille totale multiple de 4 octets. Le bourrage se fait par des octets à 0. |

# Normalisation : Modèle OSI

JFA 167

R 2.04

- ***La couche transport :***
- Les fonctions de la couche transport sont multiples, mais les fonctions principales sont au nombre de deux :
  - Découper des données, de taille variable, en paquets de taille fixe.
  - Identifier les programmes destinataire/émetteur de la donnée.
- La couche de transport détermine également le type de services qu'il faudra pour la couche Session (L4). Le type de transport de connexion le plus classique est l'envoi des messages ou des octets dans le sens d'envoi. Mais il est possible d'envoyer des messages isolés sans garantie de l'ordre de réception. C'est également dans cette couche que l'envoi des messages de broadcast est fait. De manière générale le type de service proposé est déterminé quand la connexion est établie.
- La couche de transport de la source, à la différence des couches inférieures, communique directement avec la couche de transport de la machine de destination. On parle de communication de bout en bout (couche end-to-end). Dans les couches inférieures (1 à 3), des protocoles font la liaison entre les machines et leurs voisins immédiats.

# Normalisation : Modèle OSI

JFA 168

R 2.04

- **La segmentation :**
  - D'ordinaire, les ordinateurs s'échangent des données de taille variable et non-bornée : des fichiers, des pages web, des images, etc. Cependant, on a vu que le matériel réseau ne gère que des paquets de données, qui ont une taille maximale. Pour résoudre cette incompatibilité apparente, on est obligé de les découper en paquets de taille fixe, qui ne peuvent pas dépasser une taille maximale (le MTU). Dans le jargon du réseau, ces paquets de taille fixe de couche transport sont appelées des datagrammes ou des segments.
  - Lors de l'envoi d'une donnée sur le réseau, l'équipement réseau doit segmenter les datagrammes en paquets et les envoyer sur le réseau individuellement. Un problème avec cette solution est que les segments/datagrammes sont envoyés séparément et qu'ils peuvent arriver dans le désordre. UDP et TCP gèrent ce problème différemment. UDP ignore totalement l'ordre des datagrammes et ne cherche pas à les remettre dans l'ordre à la réception. Cela marche bien pour certaines données, comme la transmission de la téléphonie par IP, ou un flux vidéo. De son côté, TCP dispose de mécanismes pour remettre les segments dans l'ordre d'envoi et reconstituer fidèlement la donnée transmise.

# Normalisation : Modèle OSI

JFA 169

R 2.04

- **L'identification des processus émetteur/récepteur :**
  - Quand un ordinateur reçoit un paquet, il doit savoir à quel programme est destiné ce paquet : est-il destiné au navigateur web, à un jeu vidéo, ou au service de mise à jour de l'OS ? Pour cela, on définit ce qu'on appelle des ports logiciels : ce sont de simples numéros, que chaque application va réserver en émettant des données. Pour comprendre ce qu'est un port logiciel, on peut faire une analogie avec le courrier. Quand quelqu'un envoie une lettre, il ne précise pas seulement l'adresse postale, mais aussi la personne à laquelle elle est destinée, au cas où plusieurs personnes vivent à la même adresse. Dans le domaine du réseau, la lettre est un paquet réseau, le destinataire et l'émetteur de la lettre sont des programmes/processus, l'adresse postale est équivalente à l'adresse IP et le nom du destinataire est le port logiciel.
  - Les numéros de ports actuels font deux octets (16 bits), ce qui donne 65536 ports différents. L'IANA, l'organisme qui gère les noms de domaine, classe ces ports en trois types, illustrés dans le tableau ci-après

# Normalisation : Modèle OSI

JFA 170

R 2.04

- ***Les ports :***

| | | |
|---|---|---|
| Ports dédiés | 0 à 1023 | Ports réservés à des fonctions bien précises.<br>• 21: File Transfer Protocol (FTP)<br>• 22: Secure Shell (SSH)<br>• 25: Simple Mail Transfer Protocol (SMTP)<br>• 53: Domain Name System (DNS) service<br>• 80: Hypertext Transfer Protocol (HTTP)<br>• 110: Post Office Protocol (POP3)<br>• 143: Internet Message Access Protocol (IMAP)<br>• 443: HTTP Secure (HTTPS) |
| Ports réservés | 1024 à 49151 | Ports réservés à des applications propriétaires. |
| Ports dynamiques | 49152 à 65535 | Ports libres, non-réservés, utilisables à la demande. |

# Normalisation : Modèle OSI

JFA 171

R 2.04

- ***Les ports :***

Les pare-feu permettent d'interdire la communication sur certains ports et de filtrer les segments/datagrammes selon le numéro de port. Ils laissent passer les segments/datagrammes sur les ports logiciels autorisés, mais ils détruisent les segments/datagrammes envoyés/reçus sur les ports interdits. Cela permet d'éviter la réception ou l'envoi de segments/datagrammes dangereux, ou du moins non-souhaités. Par exemple, on peut configurer un pare-feu pour n'autoriser que les ports 80, 25, 110, 143 et 443 : seule la consultation de sites web et de mail sera possible. En général, les ports dynamiques font partie de ceux filtrés en priorité.

# Normalisation : Modèle OSI

JFA 172

IUT GRAND OUEST NORMANDIE – INFO – R 2.04

## Le protocole UDP:

UDP se contente du minimum syndical qu'on attend d'un protocole de couche transport : il gère les ports logiciels, mais ne vérifie pas que la donnée est bien arrivée à bon port, pas plus qu'il ne remet les datagrammes dans leur ordre d'envoi. Il est donc très adapté dans les situations où on se moque que les données arrivent dans l'ordre et où les pertes de données sont acceptables. Typiquement, un flux vidéo, un podcast, des jeux vidéos en ligne sont des utilisations les plus courantes de UDP.

UDP se contente d'ajouter un en-tête particulièrement simple aux datagrammes. Cet en-tête contient diverses informations, toutes codées sur deux octets. Il a une taille fixe, de 64 bits, soit 8 octets, quel que soit le paquet. On y trouve naturellement le port de l'application émettrice ainsi que le port de destination, deux informations essentielles pour tout protocole de la couche transport. L'en-tête contient aussi la longueur totale du paquet, en-tête compris, et des octets de contrôle d'erreur optionnels.

| Port Source (16 bits) | Port Destination (16 bits) |
|---|---|
| Longueur (16 bits) | Somme de contrôle (16 bits) |
| Données (longueur variable) | |

La seule subtilité de ce protocole tient dans le calcul de la somme de contrôle, que nous n'aborderons pas ici. Nous allons simplement dire que ce calcul se base sur l'en-tête IP, chose qui est en contradiction avec l'indépendance des couches ! Heureusement, UDP et IP sont pris en charge par le système d'exploitation, ce qui réduit quelque peu les problèmes engendrés par cette méthode de calcul.

# Normalisation : Modèle OSI

JFA 173

IUT GRAND OUEST NORMANDIE – INFO – R 2.04

## Le protocole TCP:

Le protocole TCP peut être vu comme un UDP sous stéroïdes. Non seulement il utilise des ports logiciels, mais il ajoute aussi des fonctionnalités qu'UDP n'a pas. Parmi ces fonctionnalités, on trouve la gestion des connexions, les accusés de réception et la détection des pertes de données et la gestion de l'ordre de réception. Ces fonctionnalités sont indispensables pour de nombreuses applications, comme les navigateurs web, le transfert de mails, et bien d'autres. Il n'est donc pas étonnant que TCP soit le protocole de couche transport le plus utilisé, loin devant UDP.

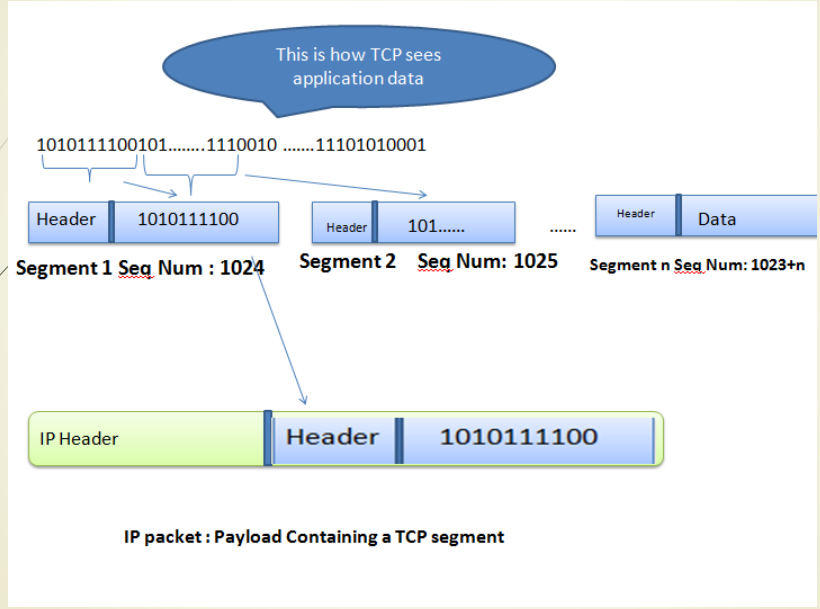
## Le séquencement des paquets :

Comme dit précédemment, TCP doit remettre les segments dans l'ordre pour reconstituer la donnée transmise. Le moyen le plus simple pour cela est de réutiliser la technique de la fenêtre glissante. Pour rappel, cette méthode demande que les paquets soient numérotés selon leur ordre d'envoi. Si un datagramme est découpé en N paquets, on peut simplement numéroter chaque paquet suivant son ordre dans la donnée initiale : le premier paquet sera le paquet numéro 1, le second paquet le numéro 2, etc. Ce numéro est transmis avec le paquet en question, à côté des numéros de ports logiciels.

# Normalisation : Modèle OSI

JFA 174

R 2.04




# Normalisation : Modèle OSI

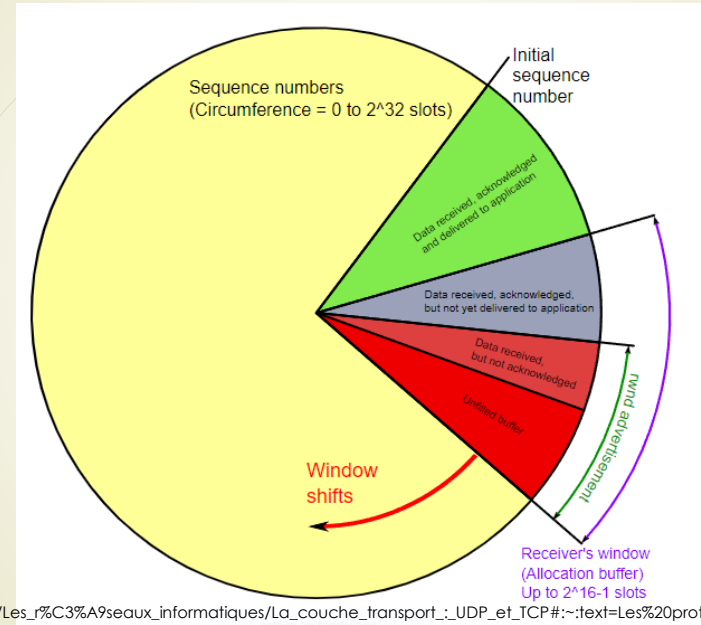
JFA 175

R 2.04

Lors de la réception, l'ordinateur doit regrouper plusieurs paquets en un seul datagramme. Pour cela, il va accumuler les paquets reçus dans une portion de mémoire, la fenêtre TCP. Cette fenêtre permet d'utiliser des mécanismes pour détecter ou empêcher les pertes de données. Seulement, la fenêtre a une taille limitée, qui est comprise entre 2 et 65536 octets. Sans précaution particulière, il est possible que la fenêtre TCP devienne pleine, notamment lors de transferts de datagrammes imposants. Pour limiter la catastrophe, le récepteur peut émettre un paquet qui indique à l'émetteur la place disponible dans sa fenêtre. Pour cela, les paquets TCP contiennent un champ nommé Window, qui indique combien d'octets peuvent encore être envoyés avant que la fenêtre soit totalement remplie (autrement dit, la place libre en octets dans la fenêtre)..

# Normalisation : Modèle OSI

JFA 176




https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/La_couche_transport_:_UDP_et_TCP#:~:text=Les%20protocoles%20de%20la%20couche,a%20le%20plus%20de%20fonctionnalit%C3%A9s.

# Normalisation : Modèle OSI

JFA 177

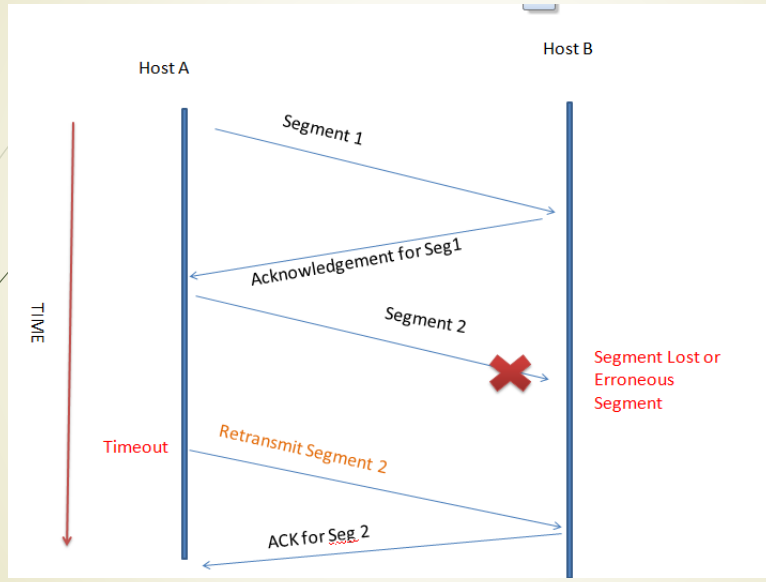
Les accusés de réception permettent de savoir si un paquet envoyé a bien été reçu. Lorsque le serveur reçoit un paquet, il envoie à l'émetteur un paquet ACK qui indique qu'il a bien reçu le paquet en question. Ces accusés de réception permettent de savoir si une donnée a été perdue lors de son transfert, que celle-ci n'est pas arrivée à destination à temps et a disparu. De telles pertes de données arrivent assez souvent, pour des raisons diverses. Chaque accusé de réception contient un numéro de séquence, qui indique que tous les paquets situés avant ce numéro de séquence ont été reçus : il permet donc d'accuser la réception de plusieurs paquets en même temps. Précisément, la fenêtre TCP commence au premier paquet non-acquitté, et contient tous les paquets suivants (acquittés ou non). La fenêtre TCP contient donc des paquets acquittés, des paquets non acquittés, et de l'espace vide.

Avec les accusés de réception, on sait qu'une donnée a disparu si on n'a pas reçu d'accusé de réception après un certain temps. Si une donnée est déclarée comme perdue, il suffit de la renvoyer en espérant que cette fois sera la bonne. Reste que la durée avant qu'on considère qu'un paquet est perdu varie suivant les circonstances. Tout dépend en réalité du serveur, de sa distance, du temps mis à transférer les données, et d'autres paramètres. Une donnée trop courte entraînera beaucoup de renvois de données inutiles, alors qu'une donnée trop longue fera attendre le client inutilement. Déterminer la durée idéale se fait par divers algorithmes logiciels, intégré dans le système d'exploitation.

# Normalisation : Modèle OSI

JFA 178

R 2.04




https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/La_couche_transport_:_UDP_et_TCP#:~:text=Les%20protocoles%20de%20la%20couche,a%20le%20plus%20de%20fonctionnalit%C3%A9s.

# Normalisation : Modèle OSI

JFA 179

R 2.04

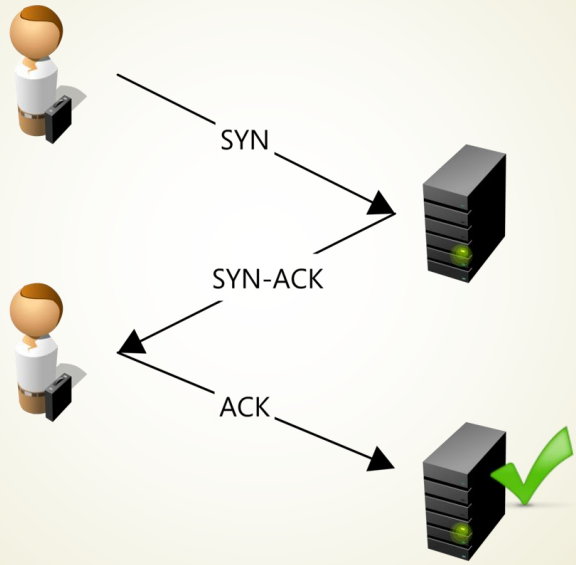
- ***Les connexions TCP :***

TCP est un protocole qui est dit en mode connecté. Ce qui signifie que tout transfert de donnée doit être précédé d'une négociation entre l'émetteur et le récepteur, cette négociation étant appelée une connexion. La connexion doit être ouverte pour que l'échange de donnée ait lieu et elle doit être fermée pour que l'échange de donnée cesse. La connexion s'effectue en trois étapes :

- le client initie la connexion au serveur en envoyant un paquet spécial (SYN) ;
- le serveur répond qu'il autorise la connexion avec un autre paquet spécial (SYN-ACK) ;
- le client envoie un accusé de réception au serveur.

# Normalisation : Modèle OSI

JFA 180

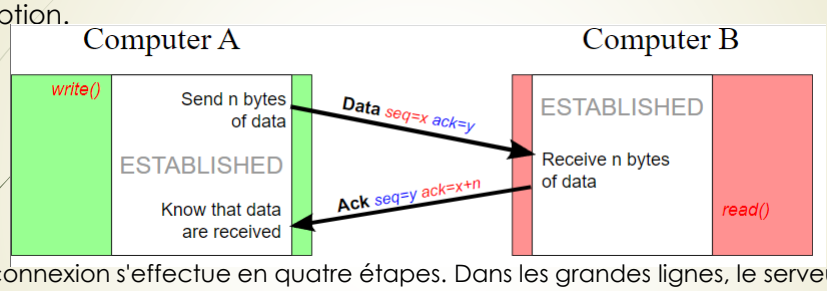



https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/La_couche_transport_:_UDP_et_TCP#:~:text=Les%20protocoles%20de%20la%20couche,a%20le%20plus%20de%20fonctionnalit%C3%A9s.

# Normalisation : Modèle OSI

JFA 181

Lors de la phase d'envoi de données, l'émetteur envoie des paquets de type DATA, et le serveur répond par des accusés de réception.

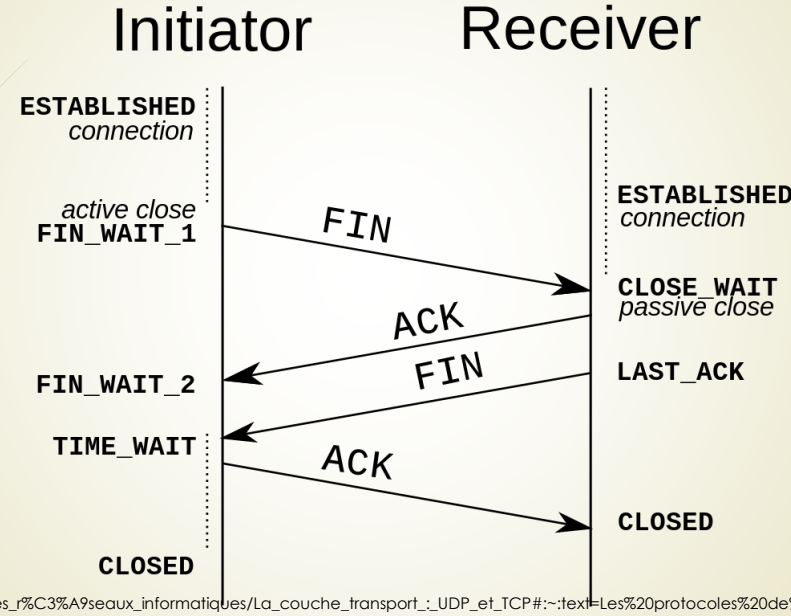



La déconnexion s'effectue en quatre étapes. Dans les grandes lignes, le serveur et le client doivent se déconnecter chacun de leur côté. Chaque demande de déconnexion d'un ordinateur est autorisée par un accusé de réception. Pour se déconnecter, ils doivent envoyer un paquet spécial nommé FIN. Dans les grandes lignes, voici comment a lieu la déconnexion :

- un ordinateur envoie une demande de déconnexion ;
- l'autre ordinateur reçoit celle-ci et renvoie l'ACK qui va avec ;
- ce dernier envoie lui aussi une demande de déconnexion ;
- et son comparse reçoit celle-ci et renvoie l'ACK qui va avec.

# Normalisation : Modèle OSI

JFA 182




https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/La_couche_transport_:_UDP_et_TCP#:~:text=Les%20protocoles%20de%20la%20couche,a%20le%20plus%20de%20fonctionnalit%C3%A9s.

# Normalisation : Modèle OSI

JFA 183

- ***Les segments TCP:***

Un segment TCP est composé d'un en-tête TCP suivi par le paquet de données de la couche application/session/présentation. Il a une taille variable, en raison de la présence d'un champ Options de taille variable à sa toute fin. Sa taille est systématiquement un multiple de 32 bits. Sa taille minimum est de 20 octets (absence de champ Options), et sa taille maximum est de 60 octets (champ Options le plus rempli possible).
Tout segment TCP commence naturellement par les ports source et destination.
Les deux champs suivants servent pour la gestion de la fenêtre glissante.

- Le numéro de séquence dit quel le numéro du segment envoyé.
- Le numéro d'accusé de réception sert dans les réponses ACK du récepteur : il indique quel est le numéro du segment accusé.

Le champ suivant donne la taille de l'en-tête, exprimée en mots de 32 bits. Il est nécessaire car l'en-tête TCP a une taille variable. Ce champ a une taille de 4 bits, de qui fait 16 valeurs différentes. allant de 0 à 15. Sachant que la taille de l'en-tête est exprimée en mots de 32 bits/4 octets, cela fait un en-tête qui fait entre 0 et 60 octets (15 * 4). Mais les valeurs inférieures à 5 sont interdites, ce qui fait un minimum de 5*4 = 20 octets. On retrouve les valeurs mentionnées au début de cette section.

# Normalisation : Modèle OSI

JFA 184

R 2.04

Les indicateurs qui suivent sont des bits qui indiquent le type du paquet, son utilité. Ils servent notamment à dire si le paquet est un paquet SYN, un paquet ACK (accusé de réception), etc. Il est composé des 8 bits suivants :

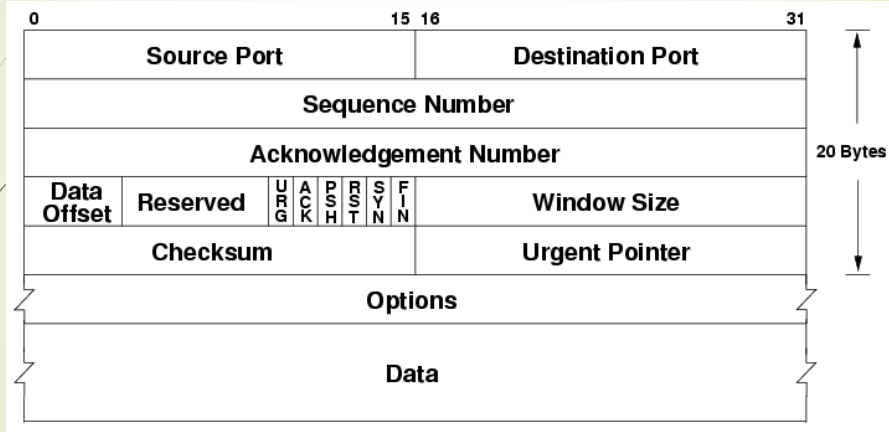
CWR : bit en lien avec la gestion de la congestion réseau ;
ECE ('Explicit Congestion Notification) : idem ;
URG : indique que le segment est de type urgent ;
ACK : indique que le segment est un accusé de réception ;
PSH : lié à la fonction PUSH ;
RST : réinitialise la connexion ;
SYN : indique que le segment est de type SYN (demande de connexion) ;
FIN : fermeture de connexion, l'émetteur n'a plus rien à envoyer.
Le champ window size indique la taille de la fenêtre glissante, à savoir le nombre de segments pouvant être reçus sans accusés de réception.

Le reste des champs est une somme de contrôle, un champ qui indique que certaines données sont urgentes à traiter, et quelques bits de bourrage ou d'options.

# Normalisation : Modèle OSI

JFA 185

R 2.04




https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/La_couche_transport_:_UDP_et_TCP#:~:text=Les%20protocoles%20de%20la%20couche,a%20le%20plus%20de%20fonctionnalit%C3%A9s.

# Normalisation : Modèle OSI

JFA 186

R 2.04

- ***La couche session :***
  - La principale fonction de cette couche est de **permettre d'établir des sessions entre les utilisateurs de machines différentes**. C'est dans ce niveau que les tokens sont gérés ainsi que la synchronisation. En effet la synchronisation permet de reprendre où la session s'était arrêtée en cas de crash...

# Normalisation : Modèle OSI

JFA 187

R 2.04

- ***La couche présentation :***
  - A la différence des autres niveaux, la couche de présentation ne **touche qu'à la sémantique et la syntaxe des informations transmises**. Ce ne sont plus des bits qui sont manipulés. Ce sont avant tout des représentations de données qui sont communiqués.

# Normalisation : Modèle OSI

JFA 188

R 2.04

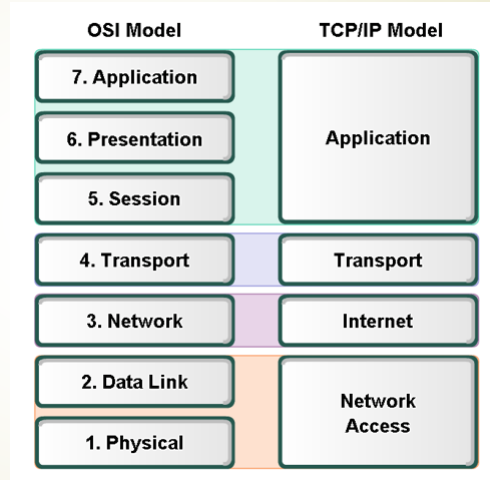
- ***La couche Application :***
  - C'est dans cette couche que vous retrouverez la plupart des **protocoles** utilisés par les utilisateurs. On peut citer notamment :
    - le protocole HTTP lors de l'accès à une page web,
    - le protocole SMTP pour les mails,
    - le FTP pour le transfert de fichiers.

# Modèle OSI versus Modèle TCP/IP

JFA 189

R 2.04

- ***Le modèle TCP/IP :***
- C'est le modèle utilisé dans le monde Internet.
- Il a été développé en 1976 avant le modèle OSI (1984),
- On a donc adapté …



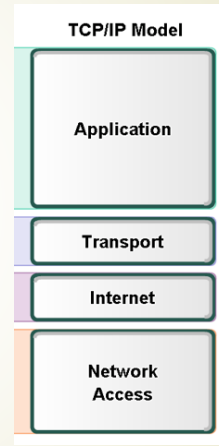

https://upload.wikimedia.org/wikipedia/commons/7/7e/Comparaison_des_mod%C3%A8les_OSI_et_TCP_IP.png

JFA 190

# Modèle TCP/IP

R 2.04

- ***La couche Accès réseau (Network Access) :***
- Cette couche "regrouper" les couches physique et liaison de données du modèle OSI. Sa seule contrainte est de permettre à un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est typique de la technologie utilisée sur le réseau local. Par exemple, Ethernet est une implémentation de la couche Accès-réseau.

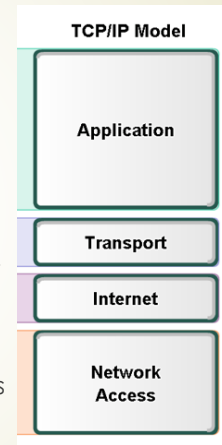



JFA 191

# Modèle TCP/IP

R 2.04

- ***La couche Internet :***
- Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion.
- Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.
- Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI. La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).
.

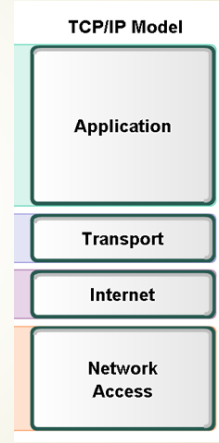


JFA 192

# Modèle TCP/IP

R 2.04

- ***La couche Transport :***
- Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.
- Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol).

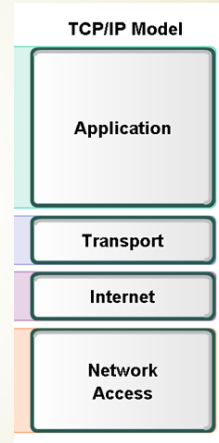



JFA 193

# Modèle TCP/IP

R 2.04

- TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine à une autre machine. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis par la couche internet pour reconstruire le message initial.
- TCP s'occupe également du contrôle de flux de la connexion.

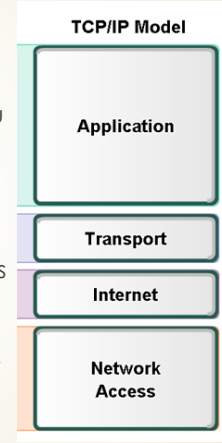


JFA 194

# Modèle TCP/IP

R 2.04

- UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion.
- Son utilisation présuppose que l'on a besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont en charge la vérification de l'ordre de remise des messages.
- Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

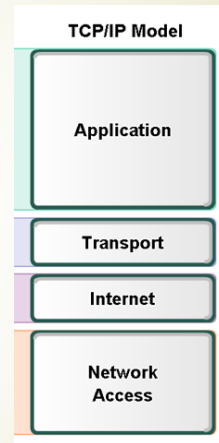



JFA 195

# Modèle TCP/IP

R 2.04

- ***La couche Application :***
- C'est la couche immédiatement supérieure à la couche transport, parce que les couches présentation et session sont apparues inutiles. Elle contient tous les protocoles de haut niveau, Telnet, TFTP (trivial FTP), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol).
- Le choix du protocole de transport à utiliser est important :
- TFTP utilisera UDP, en partant du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP.
- A l'inverse, SMTP utilise TCP, car on veut que tous les messages parviennent intégralement et sans erreurs.

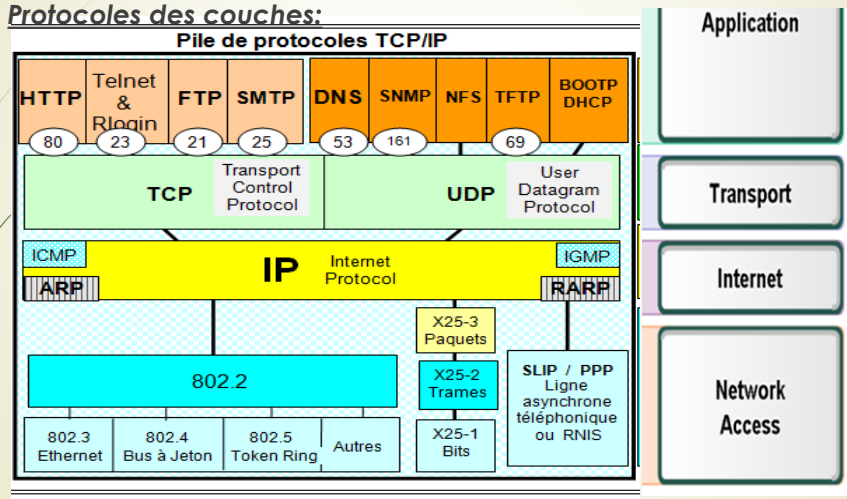


JFA 196

# Synthèse des Protocoles

R 2.04

***Protocoles des couches:***



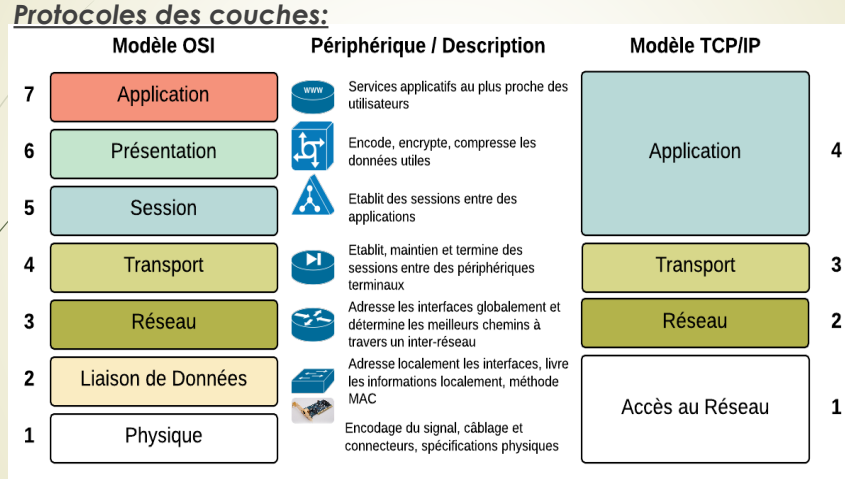

https://2.bp.blogspot.com/-NHurUmd-pzc/VUqkmaRf01I/AAAAAAAABfI/Rf3U6S-V0V0/s1600/protocoles.png

JFA 197

# Synthèse des Couches

R 2.04

***Protocoles des couches:***




http://cisco.goffinet.org/s1/OSIdetailledNewPage1.png

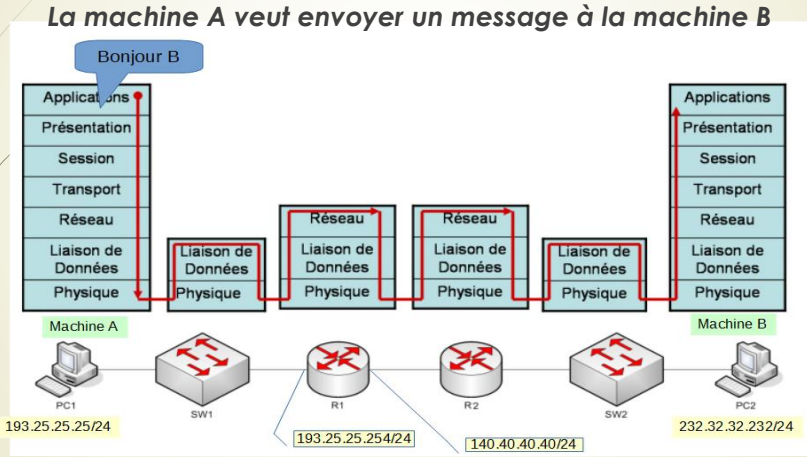
JFA 198

# Dialogue entre 2 machines

R 2.04

- ***Présentation du Dialogue :***

***La machine A veut envoyer un message à la machine B***




https://reussirsonccna.fr/wp-content/uploads/2012/02/7couches_archi11.png

JFA 199

# Dialogue entre 2 machines

R 2.04

- ***Emission du message par A :***
- La machine A veut envoyer le message "bonjour" à B. Ce message va traverser les différentes couches du modèle pour que chacune y apporte l'information nécessaire. Dans le modèle TCP/IP, les couches 5 et 6 ne sont pas utilisées Le message passe donc par la couche 4 qui, une fois son en-tête ajoutée, envoi le paquet à la couche 3.
- La couche 3 reçoit le paquet (segment TCP) et l'adresse de destination 232.32.32.32. Elle va voir dans la table de routage de la machine A à qui envoyer les informations.
- ***Table de routage de A:***

| Réseau | Masque | Interface | Passerelle |
|---|---|---|---|
| 193.25.25.0 | 255.255.255.0 | ethernet 1 | ethernet 1 |
| 0.0.0.0 | 0.0.0.0 | ethernet 1 | 193.25.25.254 |

JFA 200

# Dialogue entre 2 machines

R 2.04

- Elle n'a pas de route spécifique pour l'adresse 232.32.32.32, ce sera donc la route par défaut qui sera utilisée. A doit donc maintenant envoyer le paquet à l'interface 193.25.25.254 du routeur 1.
- A retourne voir dans sa table de routage par quel interface sortir pour envoyer le datagramme à 193.25.25.254.
- Elle doit maintenant connaître l'adresse MAC de l'interface 193.25.25.254.
- Pour cela, elle va voir dans son cache ARP si elle ne trouve pas l'information.
- Si c'est le cas, elle connaît l'adresse MAC,
- Sinon, il faut qu'elle fasse un broadcast ARP pour la trouver.
- Maintenant que la couche 3 connaît l'adresse MAC destination, elle peut envoyer le datagramme IP (en-tête IP + segment TCP) et l'adresse MAC destination à la couche 2.

JFA 201

# Dialogue entre 2 machines

R 2.04

- ***En-tête IP***


La couche 2 reçoit le datagramme et y ajoute son en-tête Ethernet.
La trame est maintenant prête à être envoyée sur le réseau.

- ***En-tête Ethernet***


La trame circule sur le réseau jusqu'à sa destination qui est l'adresse MAC de 193.25.25.254.

JFA 202

# Dialogue entre 2 machines

R 2.04

- ***Réception du message par le routeur 1 intermédiaire***

  Le routeur 1 intermédiaire reçoit la trame. La couche 2 regarde l'adresse MAC en destination, et comme c'est l'adresse MAC de l'interface 193.25.25.254, le datagramme IP est envoyé à la couche 3.

  La couche 3 reçoit le datagramme et regarde l'adresse IP de destination. Ce n'est l'adresse d'aucune des interfaces du routeur 1, donc le paquet devra être routé vers sa destination. Le routeur va donc voir sa table de routage pour voir vers qui renvoyer le paquet.

- ***Table de routage du routeur 1:***

| Réseau | Masque | Interface | Passerelle |
|---|---|---|---|
| 193.25.25.0 | 255.255.255.0 | ethernet 1 | ethernet 1 |
| 140.40.40.0 | 255.255.255.240 | ethernet 2 | ethernet 2 |
| 0.0.0.0 | 0.0.0.0 | ethernet 2 | 140.40.40.13 |

JFA 203

# Dialogue entre 2 machines

R 2.04

- Il n'y a pas de route spécifique pour l'adresse 232.32.32.32.
- C'est donc la route par défaut qui sera utilisée.
- La prochaine machine à qui envoyer le paquet est donc 140.40.40.13.
- Le routeur retourne voir dans sa table de routage par quelle interface sortir pour atteindre 140.40.40.13.
- C'est la seconde ligne de la table qui contient l'information et l'interface à utiliser est l'interface 2.
- De la même façon que précédemment, il faut trouver son adresse MAC pour lui envoyer la trame contenant les informations nécessaires. On la trouve facilement grâce aux mécanismes ARP. Le routeur 1 peut donc envoyer la trame vers le prochain routeur. Nous n'allons pas détailler la suite, le passage par chaque routeur étant identique à celui-ci.
- Les informations arrivent donc jusqu'au routeur 2 grâce aux mécanismes de routage d'Internet. Celui-ci va comme précédemment renvoyer le paquet qui ne lui est pas destiné vers la machine B qui est sur son réseau.

JFA 204

# Dialogue entre 2 machines

R 2.04

- ***Réception du message par la machine B***
- La trame arrive donc sur l'interface de la machine B. L'adresse MAC en destination est bien celle de cette interface (Cette adresse MAC aura été trouvée grâce au mécanisme ARP mis en œuvre par le routeur 2.
- La couche 2 renvoie donc le datagramme IP à la couche 3 IP.
- La couche 3 reçoit le datagramme et regarde l'adresse IP de destination.
- C'est bien l'adresse d'une des interfaces de la machine !
- La couche 3 va donc pouvoir envoyer les informations à la couche 4, qui enverra elle-même le message "bonjour" à la couche 7 applicative.

Et nous avons réussi ainsi à envoyer le message "bonjour" de la machine A à la machine B !!!

JFA 205

# Dialogue entre 2 machines

R 2.04

- ***Remarques :***
- Les adresses MAC source et destination sont modifiées à chaque passage par un routeur !
  Ces adresses MAC sont relatives à la couche 2 dont le rôle principal est le dialogue sur un réseau local. Donc les adresses MAC utilisées dans une trame doivent être en relation avec le réseau sur lequel on se situe !
- Que se passerait-il si une adresse MAC de destination était celle d'une interface située sur un autre réseau ?
  - Ca ne marcherait plus :-( car la trame serait envoyée sur le réseau local (en couche 2) et ne trouverait pas de machine ayant cette adresse MAC. La trame serait donc perdue.
    Les adresses MAC contenues dans une trame Ethernet doivent donc toujours être en rapport avec le réseau local. C'est ce qui explique qu'elles doivent être modifiées à chaque passage sur un nouveau réseau.

JFA 206

# Dialogue entre 2 machines

R 2.04

- Par contre, les adresses IP source et destination n'ont pas été modifiées durant le transport de A à B
  - Oui, et cela est encore normal ! La couche 3 concerne les informations de routage, donc sur des adresses appartenant à des réseaux distants. Ces adresses représentent donc les deux extrémités du dialogue et ne doivent pas être modifiées.
- Que se serait-il passé si on avait modifié les adresses IP source et destination à chaque passage d'un routeur ?
  - Nous aurions eu des problèmes. Le datagramme IP serait bien arrivé jusqu'au routeur 1, et l'aurait renvoyé vers le prochain routeur en mettant comme adresse IP destination 140.40.40.13. Le routeur ayant cette adresse 140.40.40.13 aurait bien reçu le datagramme, comme c'était son adresse IP de destination, il aurait pris le paquet pour lui et la communication se serait arrêtée là. la couche 4 n'aurait pas reconnu ce paquet comme appartenant à une connexion valide et l'aurait supprimé ! Il est donc impératif de ne pas modifier les adresses IP lors du transport du datagramme.
  - Le dialogue IP se fait de bout en bout entre les réseaux distants, alors que le dialogue Ethernet se fait de proche en proche sur chacun des réseaux traversés.

JFA 207

# WEBOGRAPHIE

R 2.04

- Liens Web :
- http://www.commentcamarche.net/contents/532-qos-qualite-de-service
- http://csud.educanet2.ch/3oc-info/3_Internet/3_Reseaux/page2.html
- http://si.lycee-desfontaines.eu/userfiles/image/images_cours/buscan-cr1.gif
- http://www.sen-av.net/IMG/jpg/LCD_Gestion_synoptiq1.jpg
- http://www.loriotpro.com/ServiceAndSupport/How_to/WAN_Simulation_FR.php
- http://slideplayer.com/slide/4919385/
- https://www.sebastienadam.be/connaissances/cours/adressage_ip/les_adresses_ip_v4.php
- https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html
- http://slideplayer.fr/slide/1322647/
- https://www.sebastienadam.be/connaissances/cours/adressage_ip/les_sous-reseaux.php
- https://openclassrooms.com/courses/apprenez-le-fonctionnement-des-reseaux-tcp-ip/le-routage-1
- http://www.linux-france.org/~openingault/gulliveripv6/theorie/addr.html
- http://www.lalitte.com/index.php?title=Le_routage
- http://www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/MIASS/
- https://www.it-connect.fr/routage-statique-et-routage-dynamique/
- Cours de M. JEANPIERRE L.