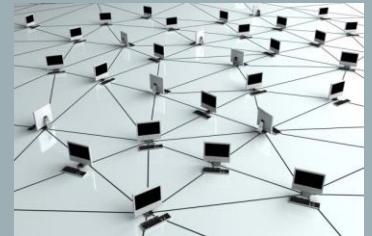


Optez pour une transformation digitale intelligente

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE VOTRE BUSINESS.



FONDAMENTAUX RESEAUX - ROUTAGE -



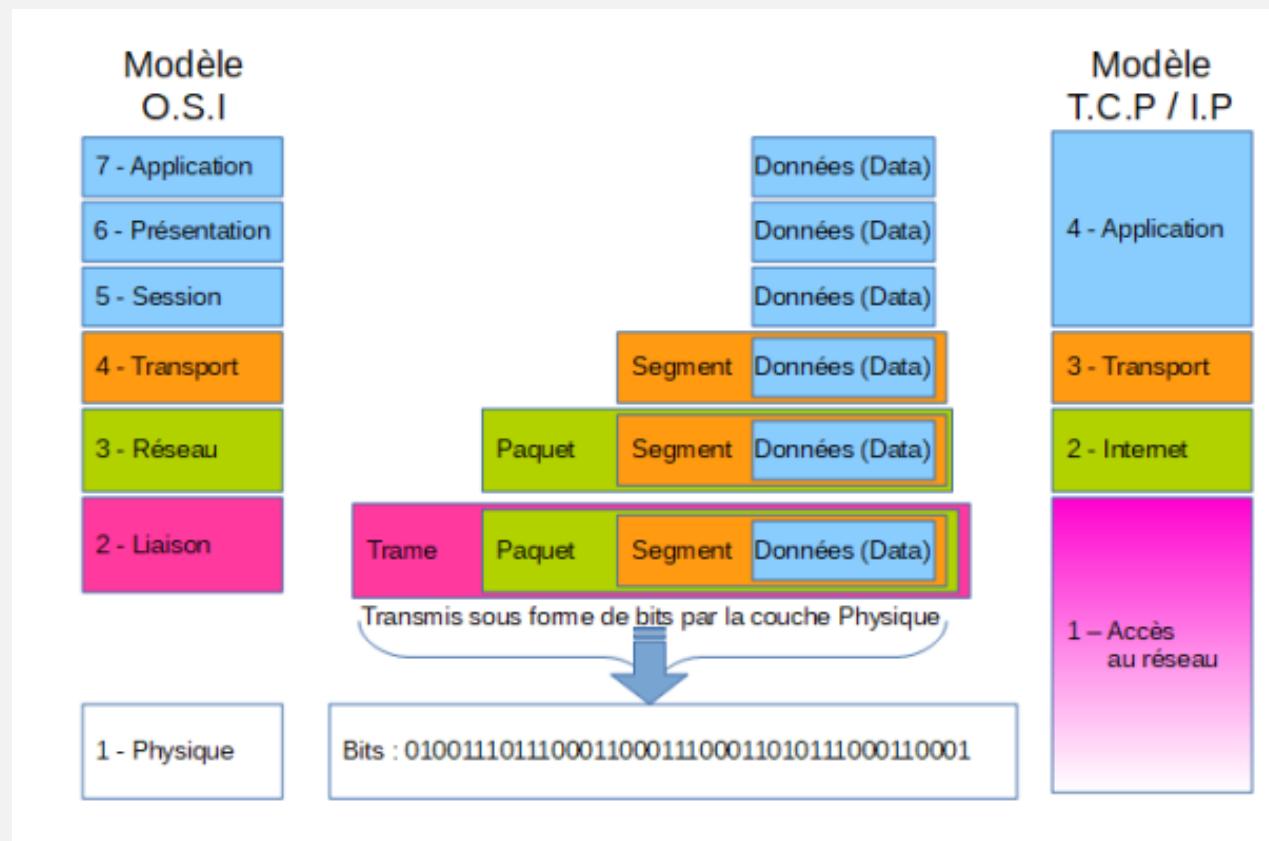
SOMMAIRE

1. TRAME ETHERNET.
2. ENTÊTE IP.
3. ENTÊTE TCP.
4. ENTÊTE ICMP.
5. ROUTAGE.
6. ROUTAGE DYNAMIQUE.
7. LES PROTOCOLES DE ROUTAGE À VECTEUR DE DISTANCE.
8. LES PROTOCOLES DE ROUTAGE À ETAT DE LIEN.

5 - TRAME ETHERNET

Rappels Hexadécimal – Trame Ethernet niveau 1 et 2 – Entête IP
– Entête TCP – Entête ICMP – Démonstration Wireshark

RAPPEL : MODELE OSI & TCP/IP



5- I L'HEXADÉCIMAL

- Le système d'hexadécimal est un système d'écriture informatique **en base 16**.
 - Il utilise donc 16 symboles de 0 à 9, puis de A à F.
 - Il va nous servir pour comprendre la construction des adresses mac et aussi les adresses de type Ipv6.
 - Chaque caractère en hexadécimal est codé sur 4 bits.
-
- Exemple
 - **Ipv6 : 2a01:e0a:33b:47b0:798f:ade8:50ae:9b75**
 - **Mac : 18-ID-EA-9A-21-62.**

5- I L'HEXADÉCIMAL

hexadécimal	Décimal	binnaire
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

En hexadécimal, on est toujours en 4 bits :

2 exemples :

hexadécimal : E1A0
binnaire : 1110 0001 1010 0000

hexadécimal : E0C1
binnaire : 1110 0000 1100 0001

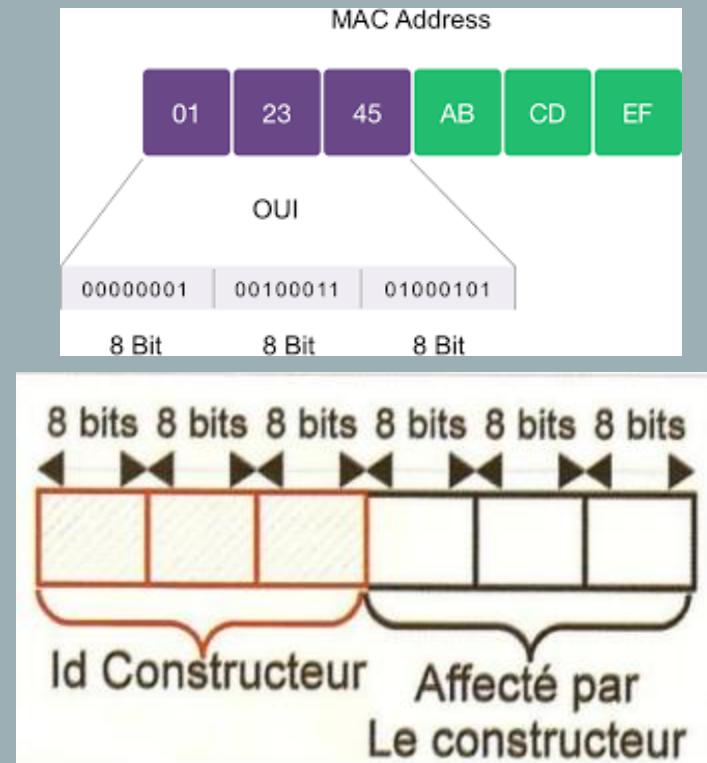
5-2 RAPPEL ADRESSE MAC

```
Carte réseau sans fil Wi-Fi :  
  
    Suffixe DNS propre à la connexion . . . . .  
    Description . . . . . : Intel(R) Dual Band Wireless-AC 8265  
    Adressse physique . . . . . : 18-1D-EA-9A-21-62 ←  
    DHCP activé. . . . . : Oui  
    Configuration automatique activée. . . . . : Oui  
    Adresse IPv6. . . . . : 2a01:e0a:33b:47b0:798f:ade8:50ae:9b75(préféré)  
    Adresse IPv6 temporaire . . . . . : 2a01:e0a:33b:47b0:18ba:cf91:a40c:56d(déprécié)  
    Adresse IPv6 de liaison locale. . . . . : fe80::798f:ade8:50ae:9b75%17(préféré)  
    Adresse IPv4. . . . . : 192.168.0.28(préféré)  
    Masque de sous-réseau. . . . . : 255.255.255.0  
    Bail obtenu. . . . . : samedi 11 septembre 2021 15:27:28  
    Bail expirant. . . . . : lundi 13 septembre 2021 04:40:58  
    Passerelle par défaut. . . . . : fe80::e69e:12ff:fe1d:67e4%17  
                                192.168.0.254  
    Serveur DHCP . . . . . : 192.168.0.254  
    IAID DHCPv6 . . . . . : 270015978  
    DUID de client DHCPv6 . . . . . : 00-01-00-01-26-84-BB-8F-48-2A-E3-1D-85-DD  
    Serveurs DNS. . . . . : 192.168.0.254  
    NetBIOS sur Tcpip. . . . . : Activé
```

CARACTERISTIQUE ADRESSE MAC

- MAC (**Media Adress Control**)
 - Adresse Physique
 - Elle est contenu dans le matériel.
 - *Identifiant unique du composant.*
 - Les adresses mac sont codées en hexadécimal.
 - Elles sont codés en 48 bits.
 - Exemple écriture :
 - 40-A3-CC-6D-43-91
 - 40:A3:CC:6D:43:91
 - 40A3.CC6D.4391
 - Accessible sur pc en tapant :
 - Sur Windows => **Ipconfig /all**
 - Sous Linux => **ifconfig**

5-2 RAPPEL ADRESSE MAC



LISTE OUI

Voici le résultat de la recherche de la correspondance entre le code Ethernet demandé et le constructeur :

- Code : 181DEA
- Constructeur : Intel Corporate

Vous avez des questions ou des remarques sur une correspondance ? Alors n'hésitez pas, rendez-vous sur les commentaires en bas de page.

COMPOSITION DE L'ADRESSE MAC

- L'adresse mac est composée en 2 parties :

- **OUI (Organizationaly Unique Identifier) :**

- Identifiant du constructeur du matériel (carte réseau). => <https://www.frameip.com/ethereum-oui-ieee/>
- **L'OUI** est codée sur les 24 *premiers* bits.
- Un constructeur peut avoir plusieurs OUI. Il dispose alors d'une plage d'OUI réservé pour le matériel produit.

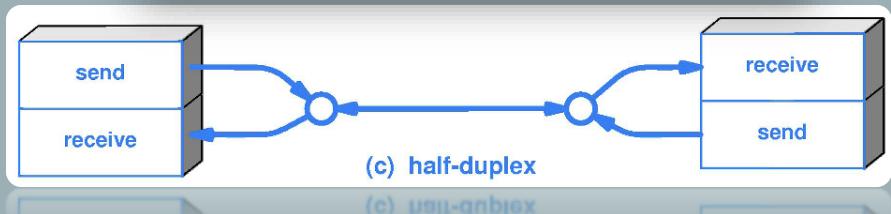
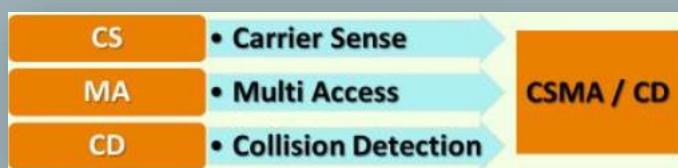
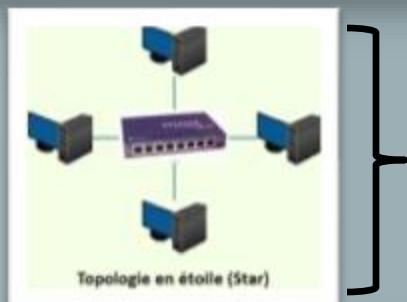
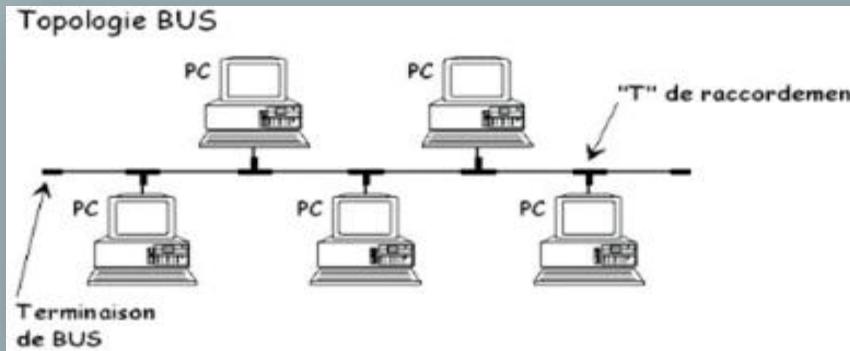
- **NIC (Network Interface Controller) :**

- **Le NIC** est codée sur les 24 derniers bits de l'adresse mac.
- Normalement numéro unique sinon c'est une collision.
- Une adresse peut être modifiée de manière temporaire grâce à des logiciels (hackers).

5-3 ETHERNET

- Ethernet est un protocole de communication entre au moins 2 machines dans un réseau local.
- La notion de trame Ethernet est principalement présente dans la couche liaison du modèle OSI (couche 2).
- Une trame est un conteneur dans lequel les données sont placées pour la transmission. Elle contient de nombreuses informations.
- La couche de liaison (couche 2) de données s'occupe de la livraison locale de trames entre dispositifs présents sur un même réseau.
- Les trames de liaison (Ethernet) ne franchissent pas les limites du réseau local.
- Le routage inter-réseau et l'adressage globale sont gérés par des couches supérieures (notamment la 3).
- La livraison de trames par des appareils de couche 2 est établie par l'utilisation d'adresses non-ambiguës de matériel (adresses Mac).

5-3 ETHERNET

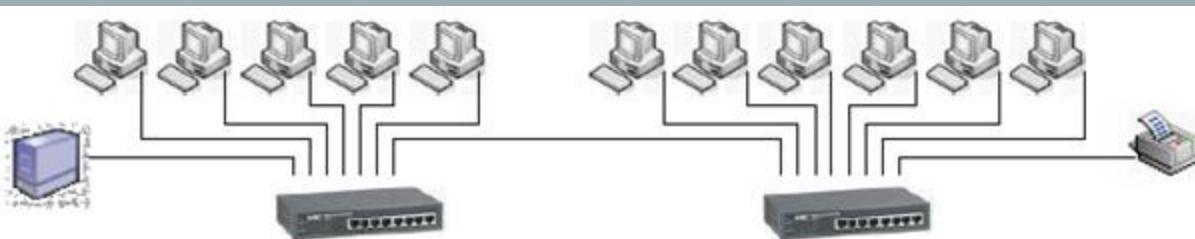


Historique

- Ethernet utilisait à l'origine dans des typologies de réseau « BUS » avec câble coaxiaux.
 - Mode de propagation => **Mode de diffusion (Broadcast)**.
 - Puis vers des typologies en étoiles mais avec des hubs et des câbles torsadés.
 - Le canal de communication est en half-duplex.
 - Pour gérer les risques de collision, le protocole CSMA/CD est utilisé (**Transmission trame – Réception trame – Détection de collision – Reprise après collision**).
- Avec cette méthode (CSMA/CD), toutes les stations d'extrémité « écoutent » le câble réseau pour savoir quand elles sont autorisées à envoyer des données.
- Lorsque la station d'extrémité détecte qu'aucun autre hôte n'est en cours de transmission, elle tente à son tour d'envoyer ses données.
- Malheureusement, des collisions peuvent se produire.

Evolution vers Ethernet commuté

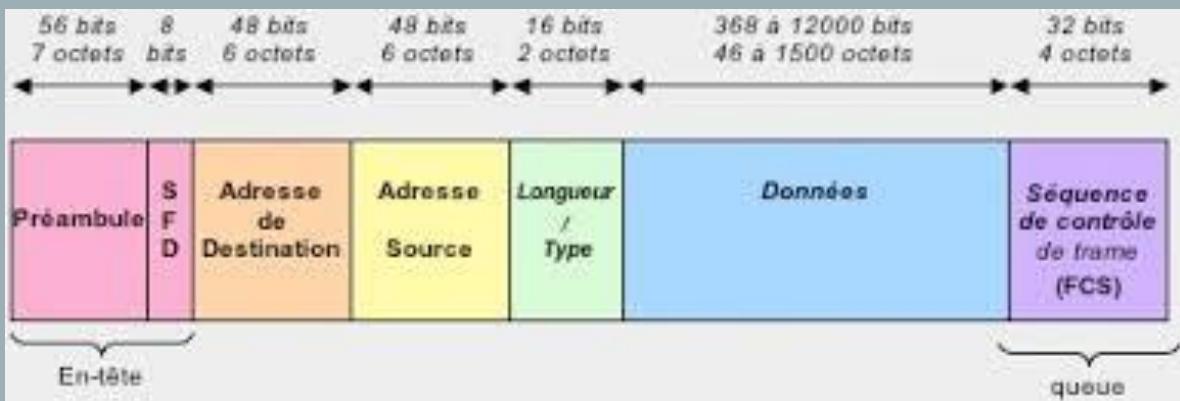
5-3 ETHERNET



- Utilisation d'un commutateur (Switch) avec câbles à paires torsadées (voir fibre optique).
- Mode de propagation => Point à point.
- Topologie en étoile sans le hub mais avec un switch.
- Les communications entre 2 équipements sont isolées.
- La communication peut se faire en full-duplex.
- Il n'y a plus de risque de collision.
- Plus besoin du système CSMA/CD

DETAILS D'UNE TRAME ETHERNET

5-4 L'EN-TÊTE ETHERNET OU TRAME ETHERNET

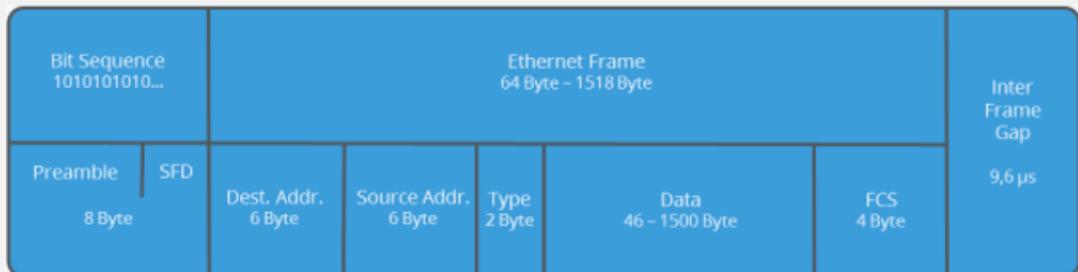


Trame Ethernet					
@destination 6 octets	@source 6 octets	protocole 2 octets	données 46 à 1500 octets	PAD	CRC 4 octets

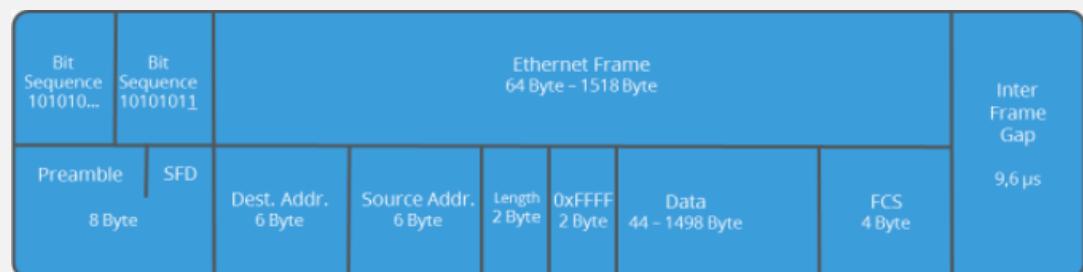
- Préambule**: Ce champ est codé sur 7 octets et permet de synchroniser l'envoi. Chacun des octets vaut 10101010 et cette série permet à la carte réceptrice de synchroniser son horloge. On prévient que c'est une trame de type ethernet.
- SFD (Start Frame delimiter)**: Ce champ est codé sur 1 octet (8 bits) et indique à la carte réceptrice que le début de la trame va commencer.
- Adresse mac destination**: cela va identifier qui est le destinataire de la trame et donc des données. Si, c'est la bonne machine, la trame et les données seront lues. Sinon, la trame sera rejetée.
- Adresse mac source**: Cela va identifier qui est l'émetteur de la trame.
- Type**: Le type de protocole qui va être utilisé au niveau 3. 0x0800 :Ipv4 – 0x86DD :Ipv6 – 0x0806:ARP.
- Données**: La charge utile => Les informations que l'on souhaite communiquer.
- FCS (Frame Check Séquence) ou CRC (cyclic redundancy check)**: Un algo est lancé à la création de la trame par l'émetteur. Cette séquence va générer une signature qui va être inscrite dans les champs du FCS. Le destinataire va effectuer le même travail et ainsi comparer les signatures au moment où il va recevoir la trame.

5-4 LES DIFFÉRENTES TRAMES ETHERNET

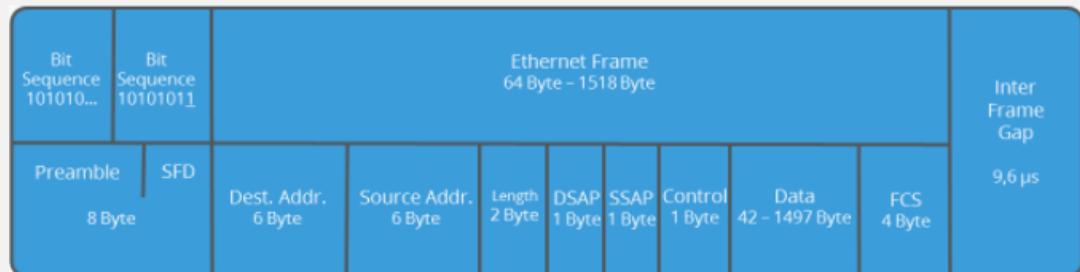
Au fil du temps, les trames ont évolués afin de transporter des données de plus en précises.



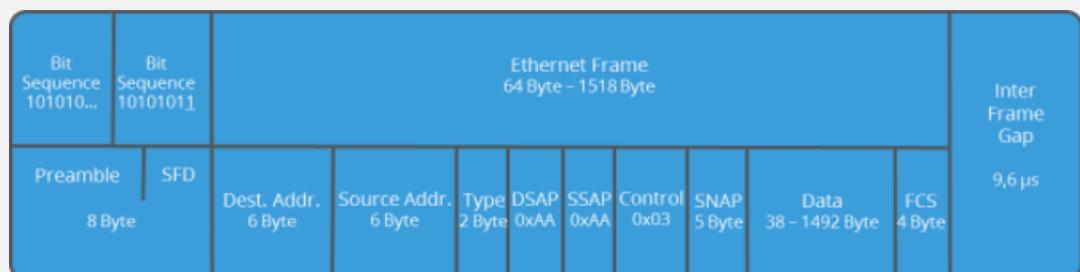
Trame Ethernet II : Pas d'indication sur la longueur des données mais plus sur le type de protocole de la couche supérieure.



Trame Ethernet 802.3raw : version hors standard.
Développé par Novell. Risque de problème de comptabilité.



Trame Ethernet IEEE 803.3 : version IEEE. Version **la plus populaire et la plus utilisée des trames**. Les champs DSAP et SSAP sont également inclus. DSAP désigne le protocole supérieur destinataire des données et SSAP désigne le protocole qui a émis la trame LLC.



Trame Ethernet IEEE 803.3 SNAP : Le champ SNAP est rajouté. Le champ SNAP (Subnetwork Access Protocol) permet de définir plus de 256 protocoles. Il fournit 2 octets pour le numéro de protocole. Le fabricant peut également intégrer un identifiant unique (3 octets).

5-5 LE SWITCH

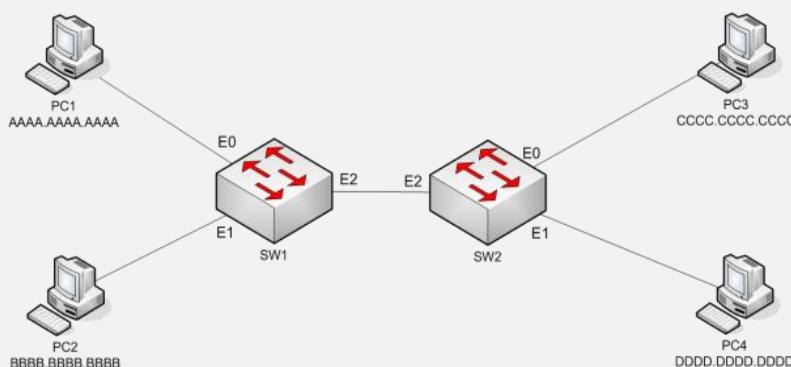


Symbole

DETAILS D'UNE TRAME ETHERNET

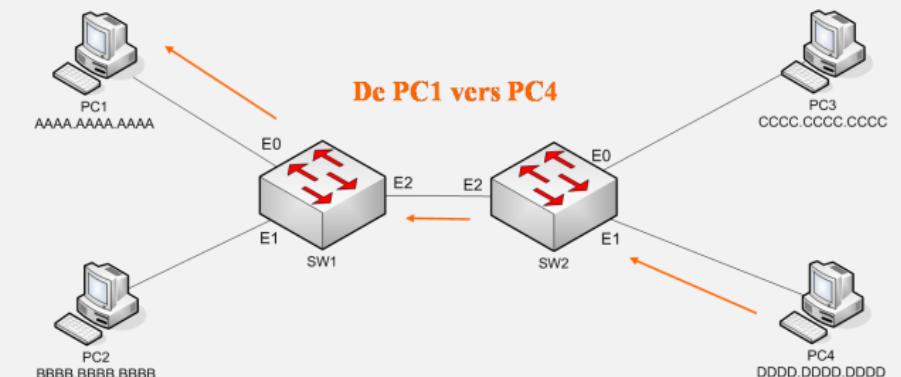
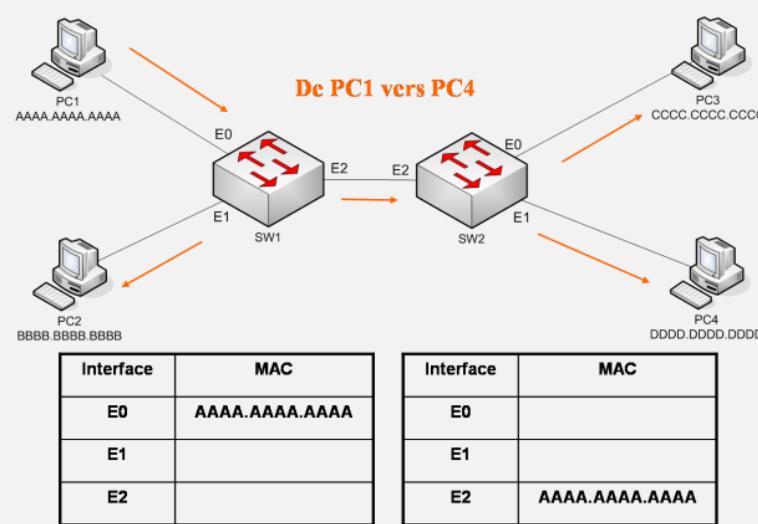
- Pérophérique réseau central (concentrateur multiport)
- C'est un équipement qui relie plusieurs segments dans un réseau informatique.
- Il créer ainsi des circuits virtuels.
- La commutation est un mode de transport de trame (comme pour le router dans la couche de niveau 3) pour un réseau local.
- Le switch n'a besoin que de la couche 1 et 2 du modèle OSI pour fonctionner.
- Il est composé de plusieurs port Rj45.
- Il transfert les paquets vers des ports spécifiques => ce qui le différencie du hub

8-5 LE FONCTIONNEMENT DU SWITCH



Interface	MAC
E0	
E1	
E2	

Interface	MAC
E0	
E1	
E2	

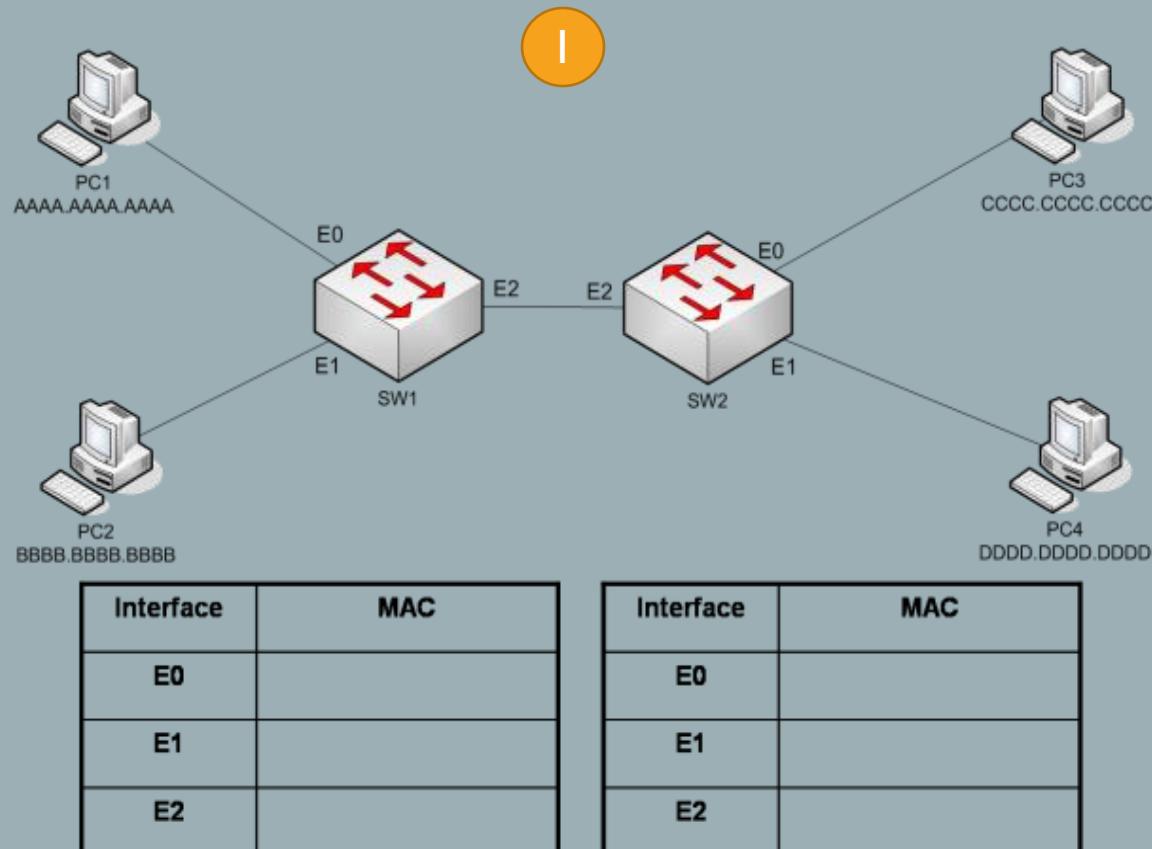


De PC1 vers PC4



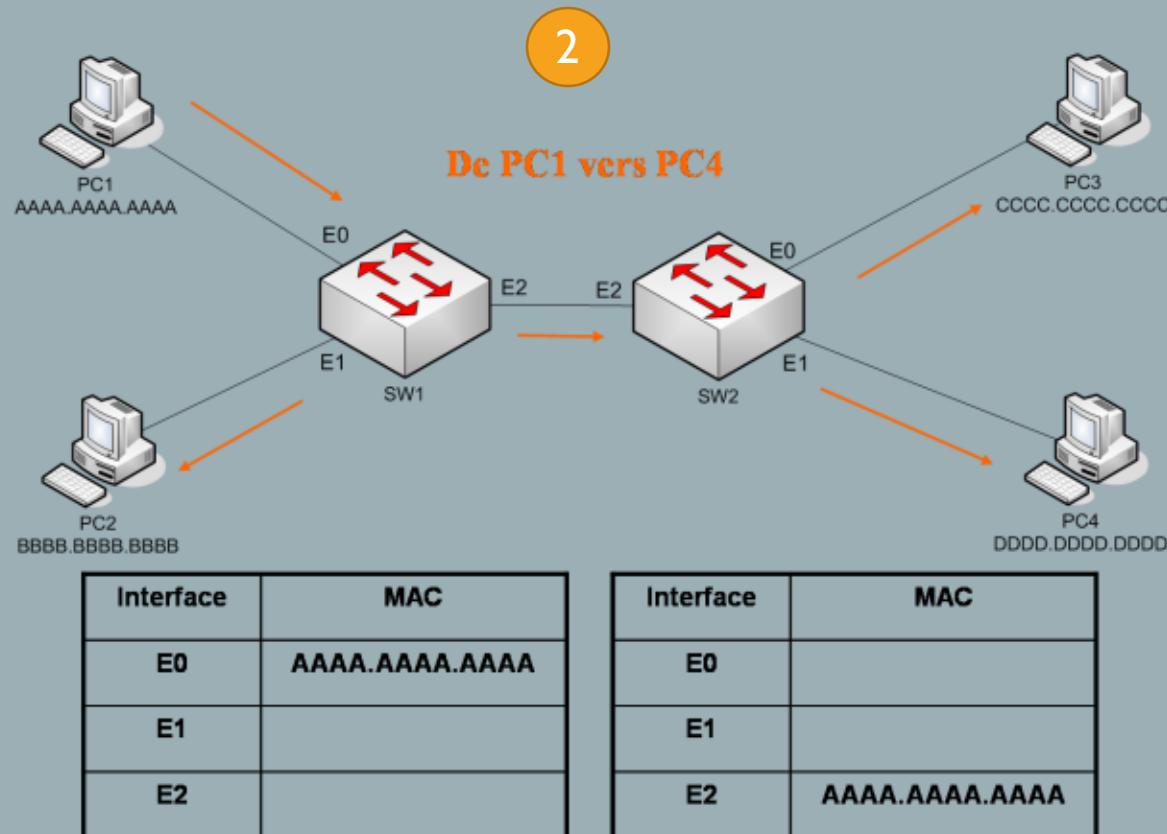
5-5 LE FONCTIONNEMENT DU SWITCH

ETAPE I : DEMARRAGE



- **Switch** : SW1 et SW2.
- **PC** : PC1, PC2, PC3 et PC4.
- **Interface** : E0, E1 et E2
- Chaque switch dispose d'une base de donnée appelé « **table CAM** » pour **Content-Addressable-Memory** ou « **table MAC** » pour **Medium Access-Control**.
- Cette table fait le lien entre le ports physiques (interfaces) et les adresses mac sources qui arrivent sur ces ports.
- Au démarrage des switch, les table sont vides.

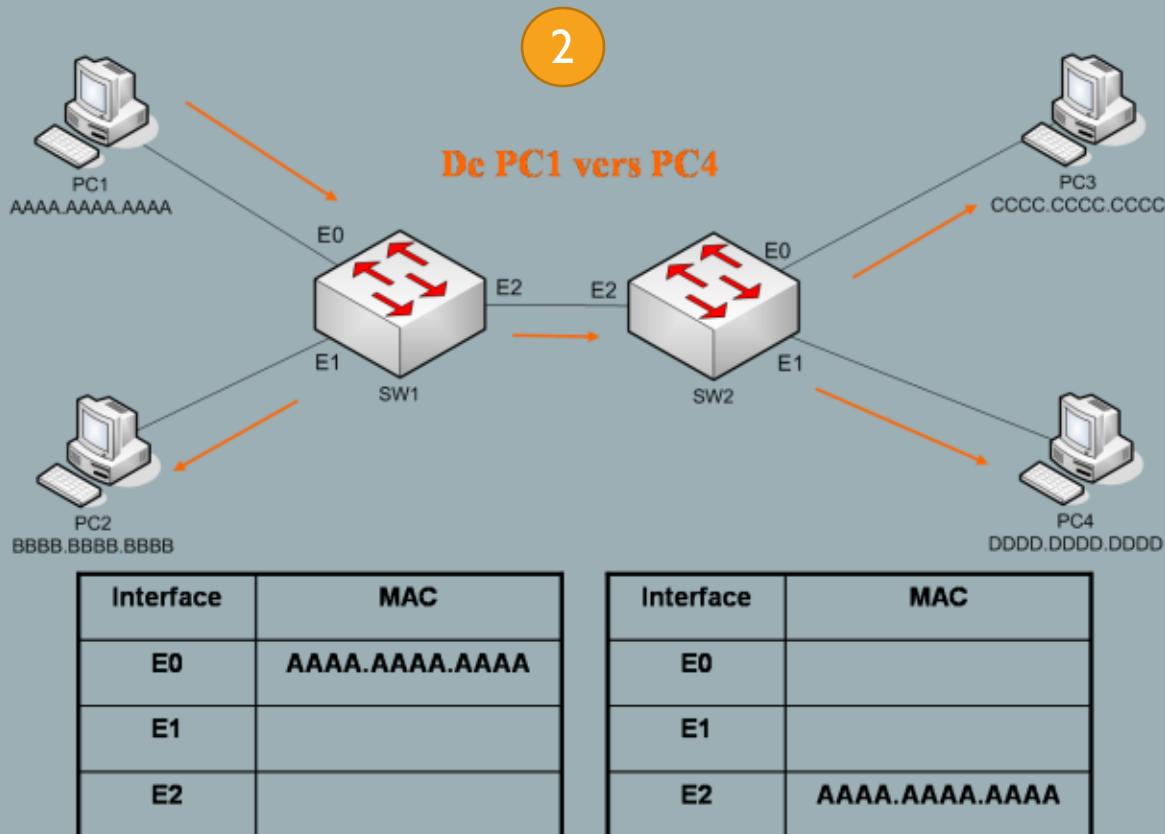
5-5 LE FONCTIONNEMENT DU SWITCH



ETAPE 2 : Le PCI initie une trame vers le PC4 (1/2).

1. La trame sort de la carte réseau de PCI avec:
 - **adresse MAC source** = AAAA.AAAA.AAAA
 - **adresse MAC destination** = DDDD.DDDD.DDDD
2. La trame arrive sur le port E0 du switch SW1
 - Le switch extrait l'adresse MAC source et l'insère dans sa table (cf schéma).
 - Maintenant le switch sait que pour joindre cette adresse MAC (AAAA.AAAA.AAAA), il doit commuter les trames vers le port E0.
 - Cette information lui servira donc pour le retour de la trame.
 - Puis le switch extrait l'adresse MAC destination (DDDD.DDDD.DDDD) et la compare à sa table: aucune entrée trouvée donc ne sachant pas où envoyer la trame, il la diffuse sur tous les ports exceptés le port de réception E0.

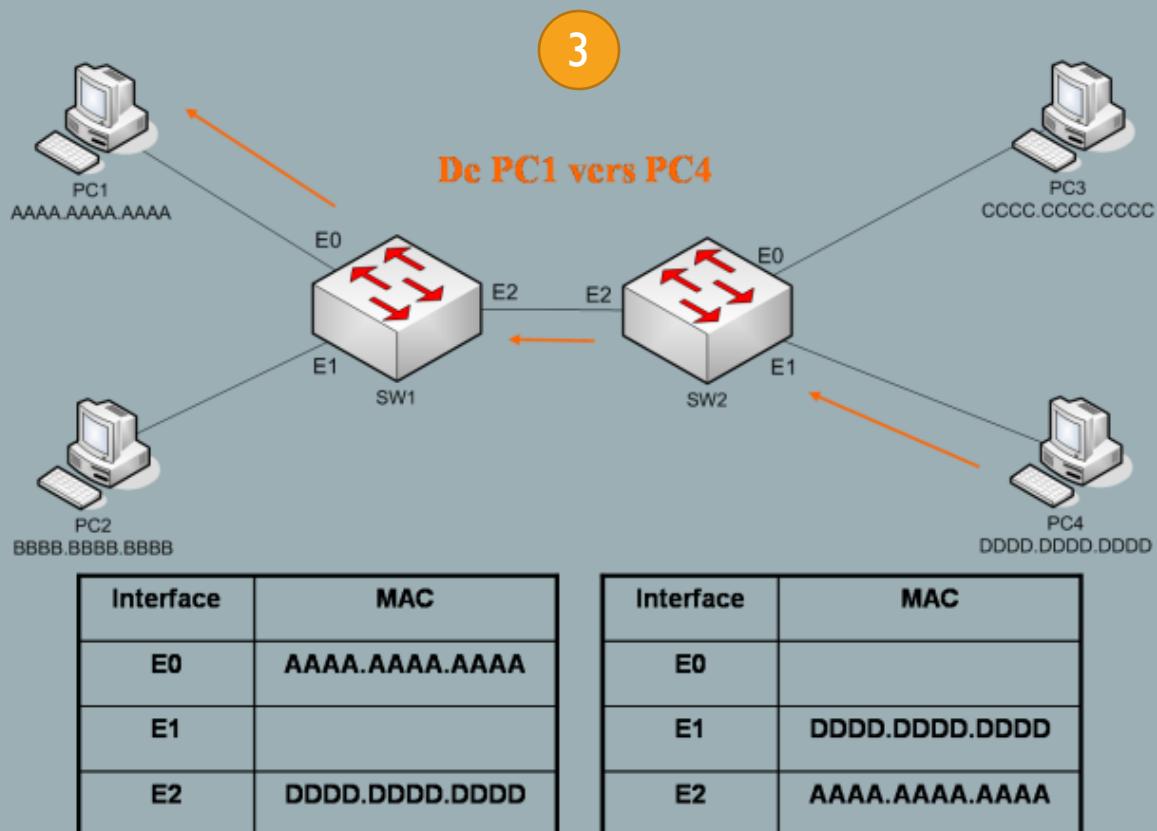
5-5 LE FONCTIONNEMENT DU SWITCH



ETAPE 2 : Le PCI initie une trame vers le PC4 (2/2).

- 3. La trame arrive sur le port E2 du switch SW2
 - Le switch extrait l'adresse MAC source et l'insère dans sa table (cf schéma). Maintenant le switch sait que pour joindre cette adresse MAC (AAAA.AAAA.AAAA), il doit commuter les trames vers le port E2. Cette information lui servira donc pour le retour de la trame.
 - Puis le switch extrait l'adresse MAC destination (DDDD.DDDD.DDDD) et la compare à sa table: aucune entrée trouvée donc ne sachant pas où envoyer la trame, il la diffuse sur tous les ports exceptés le port de réception E2.
- 4. La trame arrive sur la carte réseau du PC4: gagné pour la trame aller!

5-5 LE FONCTIONNEMENT DU SWITCH

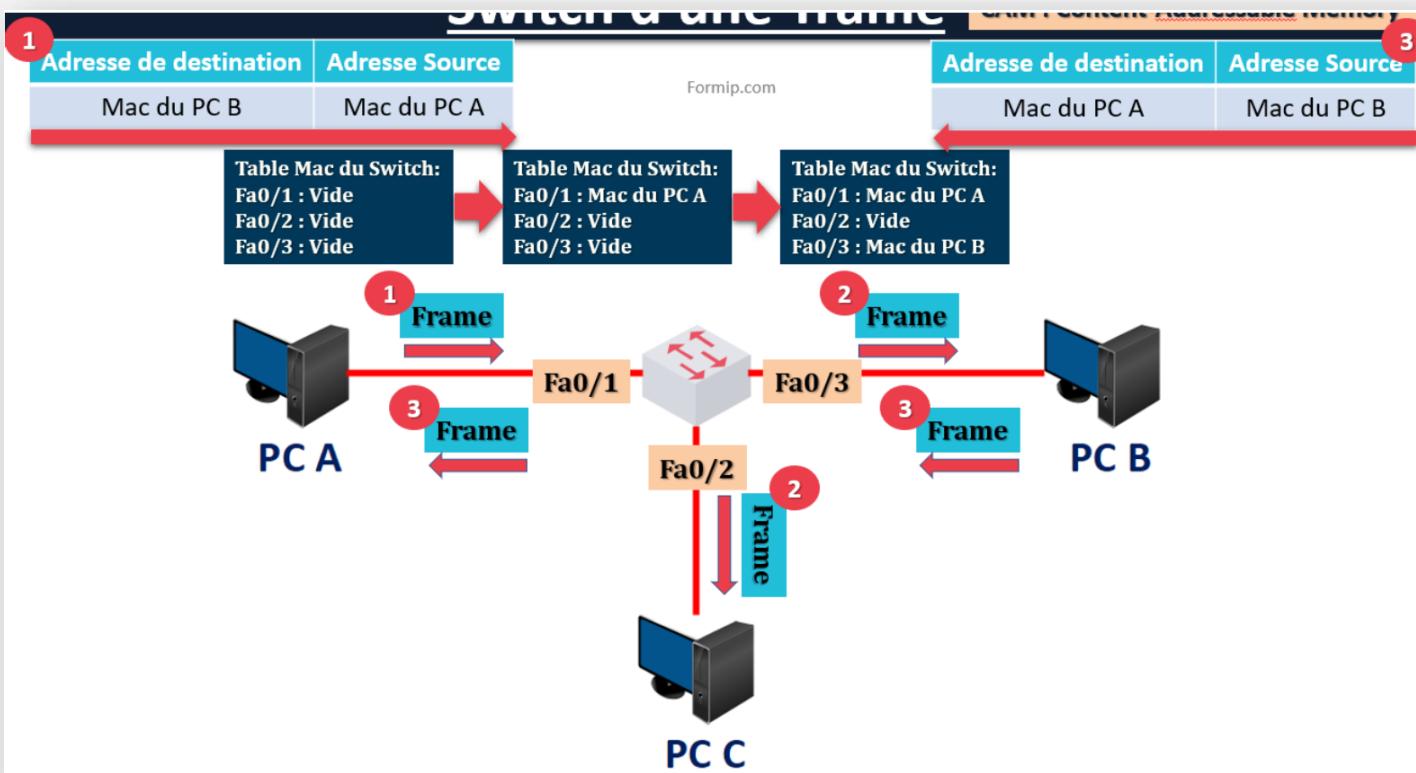


ETAPE 3 : Trame réponse envoyée par PCA4 à destination de PC1.

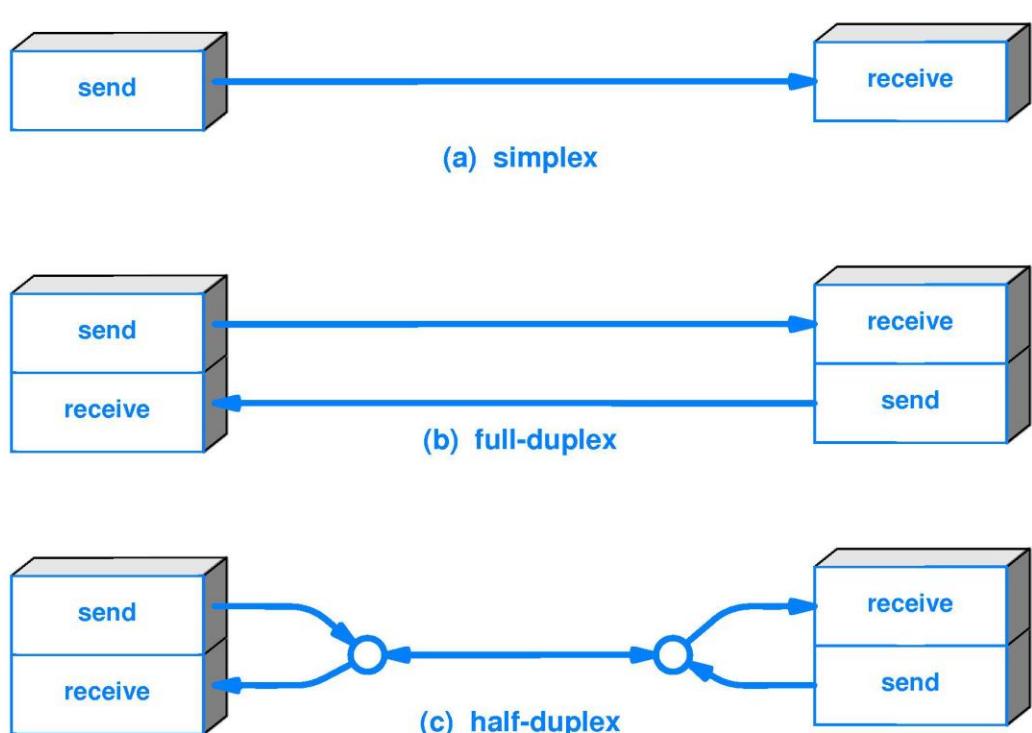
1. Le fonctionnement est le même que précédemment. On remarque que lorsque la trame arrive sur les switchs, ils insèrent l'adresse MAC source DDDD.DDDD.DDDD dans leur table.
2. Puis ils extraient l'adresse MAC destination (AAAA.AAAA.AAAA) et la compare à leur table et là ils savent où se situe cette adresse MAC; port E2 pour le switch SW2 et port E0 pour le switch SW1.
3. Ils n'ont plus qu'à commuter la trame **UNIQUEMENT** sur le port en question.

5-5 LE FONCTIONNEMENT D'UN SWITCH

Schéma synthétique



8-6 HALF-DUPLEX / FULL-DUPLEX



DETAILS DES 3 CANAUX

- **Avec Simplex :**

- Les échanges d'information se font sur un seul canal de communication et dans un même sens.

- **Avec le Half-Duplex :**

- L'information circule dans les 2 sens mais toujours sur un seul canal de communication.
- Il y a un risque de ce qu'on appelle une collision. Le contenu de chaque trame vont être altérée.

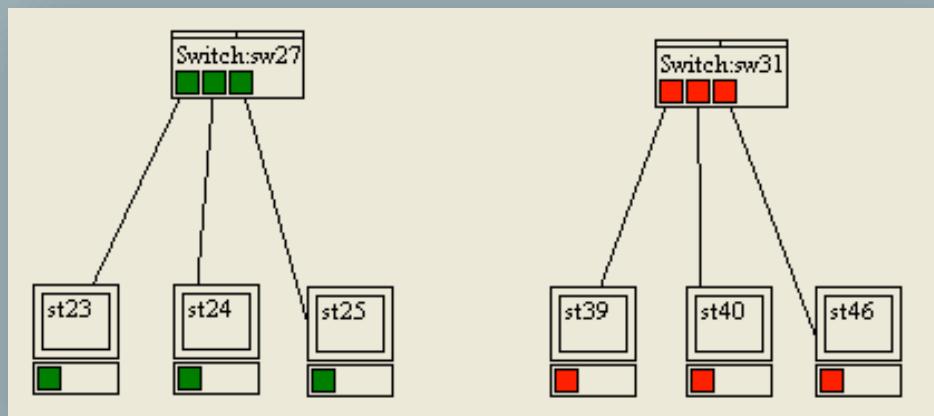
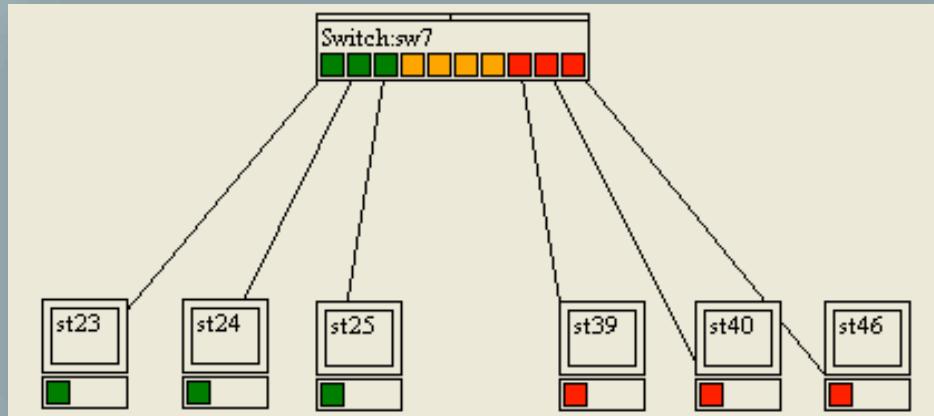
- **Avec le full-duplex :**

- L'information circule dans les 2 sens et sur des canaux différents.
- Le risque de collision est évité.

Aujourd'hui, tout fonctionne en full-duplex.

Possible half-duplex sur d'anciennes structures réseaux avec de vieux ports.

8-7 LE VLAN



C'est quoi un VLAN

- Un VLAN (Virtual Local Area Network) est un LAN (Local Area Network) virtuel.
- Un VLAN est la capacité de séparer des ports d'un switch dans des réseaux différents.
- Cela permet avec un switch d'avoir plusieurs réseaux indépendants locaux.
- L'intérêt est de pouvoir administrer différents sous réseaux avec un seul switch notamment avec une interface dédiée.

Port	PVID	Port	PVID	Port	PVID	Port	PVID
1	1	2	1	3	1	4	1
5	2	6	2	7	2	8	1
9	1	10	1	11	1	12	1
13	4	14	4	15	1	16	4
17	1	18	1	19	1	20	1
21	1	22	1	23	1	24	1
25GT	3	26GT	3				

Exemple :

- Les ports 1, 4, 8 et 24 sont dans le VLAN 1.
- Les ports 5, 6 et 7 sont rattachés au réseau VLAN 2.

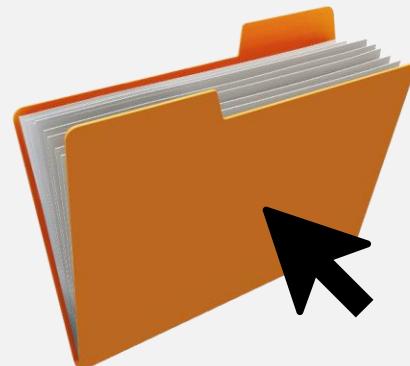


TP TIME

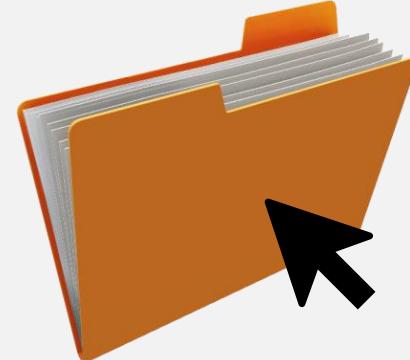
TP_ Quizz :



Quizz 1 :Intro



Quizz 2 :Couche 1



Quizz 3 :Couche 2

TRAME ETHERNET : COUCHE LIAISON

Un peu de pratique :



Avec Cisco Packet Tracer :

- *Faire communiquer 2 machines (PC).*
- *Tester la notion de sous-réseau.*
- *Installer un switch et faire communiquer des machines.*
- *Configuration avec 2 switchs.*
- *Afficher tables mac de chaque switch.*
- *Mettre en place un VLAN avec 2 sous-réseaux locaux.*
- *TP sur les vlans.*

6 - ENTÊTE IP

LE RÔLE DE LA COUCHE 3

- **L'entête IP se trouve dans la couche de niveau 3 (couche réseau).**
- **Transport de bout en bout**
 - *En dehors du réseau local.*
 - *Adressage des terminaux.*
 - *Encapsulation des données : intégration des données avec des entêtes de niveau 2 et 3.*
 - *Routage avec les adresses IP (sources et destinations).*
 - *Desencapsulation des données.*

L'ADRESSE IP

- Pour communiquer sur un réseau, il faut attribué un adresse IP a notre carte réseau.
- Elle est attribué soit:
 - **En statique**, généralement au serveur pour les retrouver facilement sur le réseau. Elle est configurée manuellement a l'installation de la machine.
 - **En dynamique**, via un serveur DHCP pour une multitude de clients .C'est une adresse ayant une date d'expiration lier a une adresse MAC.



ADRESSE IP

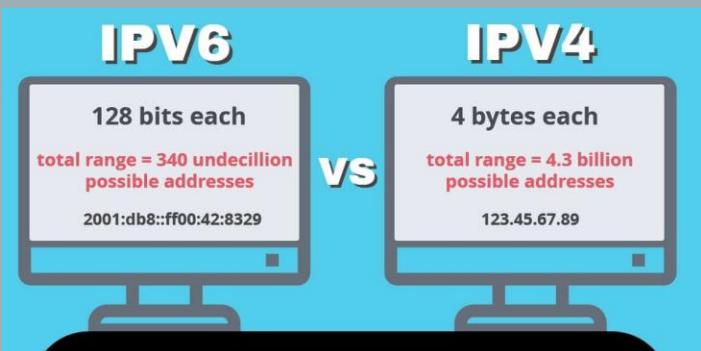
ADRESSE IP

Carte réseau sans fil Wi-Fi :

```
Suffixe DNS propre à la connexion. . . : lan
Description. . . . . : Intel(R) Dual Band Wireless-AC 8265
Adresse physique . . . . . : 18-1D-EA-9A-21-62
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . . : Oui
Adresse IPv6. . . . . : 2001:861:34c4:c970:798f:ade8:50ae:9b75(préféré)
Adresse IPv6 temporaire . . . . . : 2001:861:34c4:c970:6c5b:9da:7cae:7d8b(préféré)
Adresse IPv6 de liaison locale. . . . . : fe80::798f:ade8:50ae:9b75%17(préféré)
Adresse IPv4. . . . . : 192.168.1.63(préféré) ← Ipv4
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : lundi 13 septembre 2021 20:59:44
Bail expirant. . . . . : mardi 14 septembre 2021 20:59:42
Passerelle par défaut. . . . . : fe80::ae3b:77ff:fe5c:761c%17
                                         192.168.1.254
Serveur DHCP . . . . . : 192.168.1.254
IAID DHCPv6 . . . . . : 270015978
DUID de client DHCPv6. . . . . : 00-01-00-01-26-84-BB-8F-48-2A-E3-1D-85-DD
Serveurs DNS. . . . . : 2001:861:34c4:c970:ae3b:77ff:fe5c:761c
                                         192.168.1.254
NetBIOS sur Tcpip. . . . . : Activé
Liste de recherche de suffixes DNS propres à la connexion :
                                         lan
```

Ipv6

Ipv4



- IP : Internet Protocole.
- Adresse Logique
- Il existe 2 types d'adresse IP : Ipv4 et Ipv6
- **Ipv4 => 32 bits soit 4 octets :**
 - Exemple : 192.168.1.3.
 - 4 parties codée chacune sur 8 bits.
- **Ipv6 => 128 bits soit 8 octets :**
 - Exemple : 2001:861:34c4:c970:798f:ade8:50ae:9b75
 - 8 parties codée chacune 16.
- Accessible sur pc en tapant :
 - Sur Windows => **Ipconfig /all**
 - Sous Linux => **ifconfig**

CONVERSION IPV4 EN BINAIRE

Méthode par soustraction

Exemple pour 120 bits

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0
120							
-	64						
		56					
-	32						
			24				
-	16						
				8			

Méthode soustraction

- Chaque partie d'une adresse Ipv4 peut avoir une valeur comprise entre 0 et 255 (**soit 2^8 de possibilité => 256**).
- On peut vouloir convertir une adresse IP en binaire.
- La méthode préconisée est la méthode par soustraction :
 - Exemple avec **229 = 11100101**
 - **229 > 128 => 1**; $229 - 128 = 101$
 - **101 > 64 => 1**; $101 - 64 = 37$
 - **37 > 32 => 1**; $37 - 32 = 5$
 - **5 < 8 => 0**;
 - **5 > 4 => 1**; $5 - 4 = 1$
 - **1 < 2 => 0**;
 - **1 = 1 => 1**;

128	64	32	16	8	4	2	1
1	1	1	0	0	1	0	1

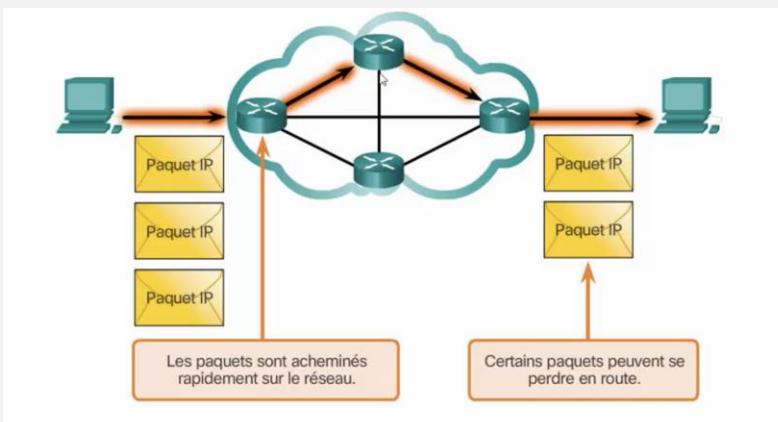
LES CARACTÉRISTIQUES DU PROTOCOLE IP

I. **Absence de connexion** : Aucune connexion avec la destination n'est établie avant l'envoi des paquets de données.

- *L'expéditeur ignore si le destinataire est présent.*
- *Si le paquet est bien arrivé.*
- *Si le destinataire peut lire le paquet.*
- *Le destinataire ignore quand le paquet va arriver.*

LES CARACTÉRISTIQUES DU PROTOCOLE IP

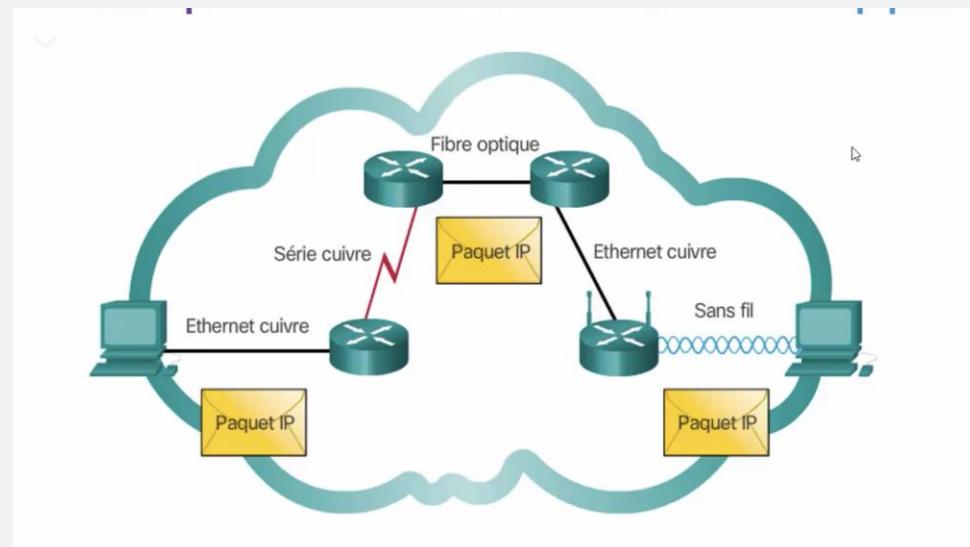
2. **Acheminement au mieux** : Le protocole IP est un protocole non fiable, il n'a aucun moyen de vérifier et de s'assurer que l'ensemble des paquets seront bien réceptionnés par le destinataire.
 - Les paquets sont acheminés rapidement sur le réseau.
 - Certains paquets peuvent être perdus durant l'acheminement.



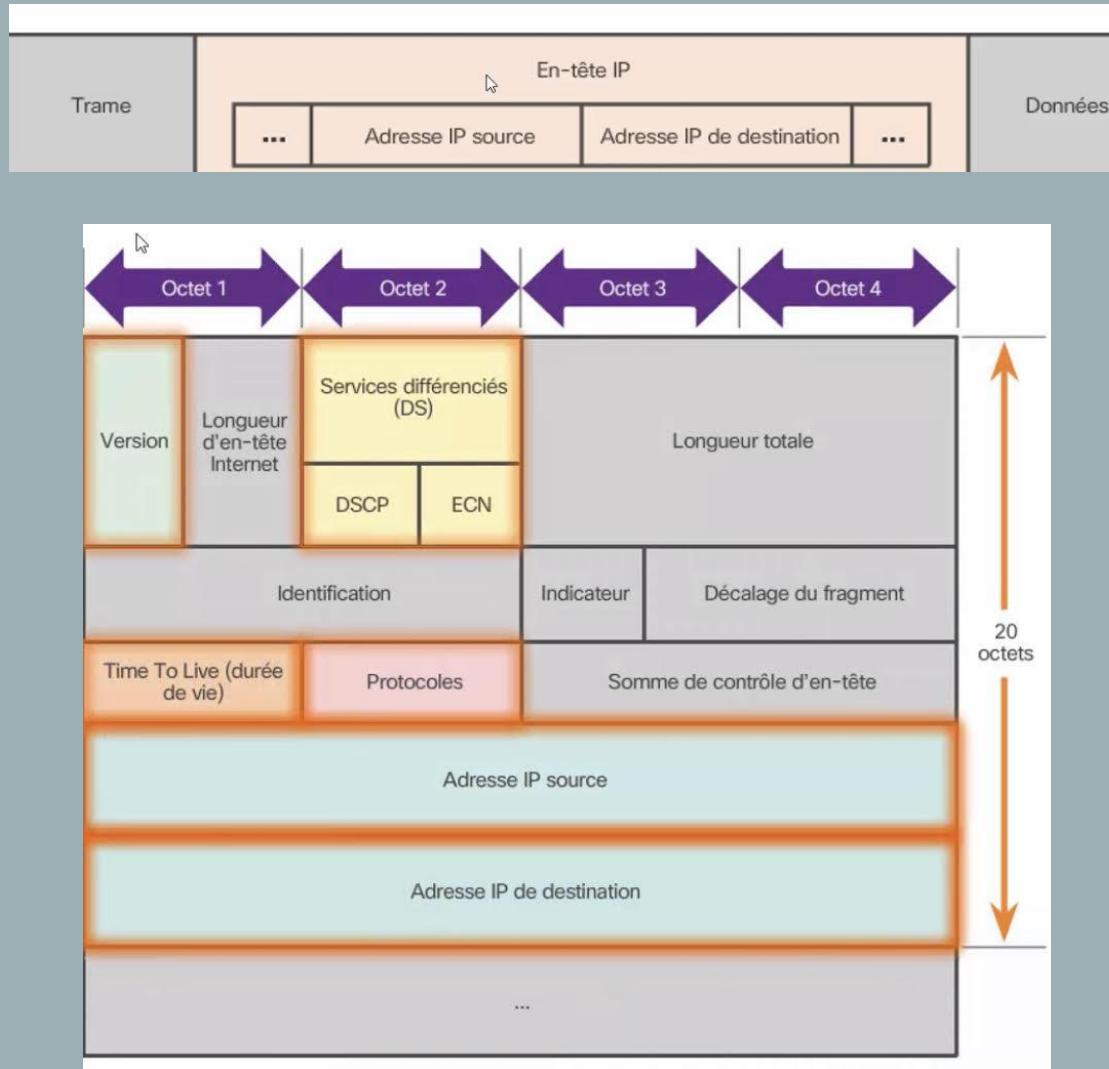
LES CARACTÉRISTIQUES DU PROTOCOLE IP

3. Indépendant du support : Le protocole IP peut fonctionner via différents supports.

- Fibre optique.
- Sans fil.
- Câble cuivré.



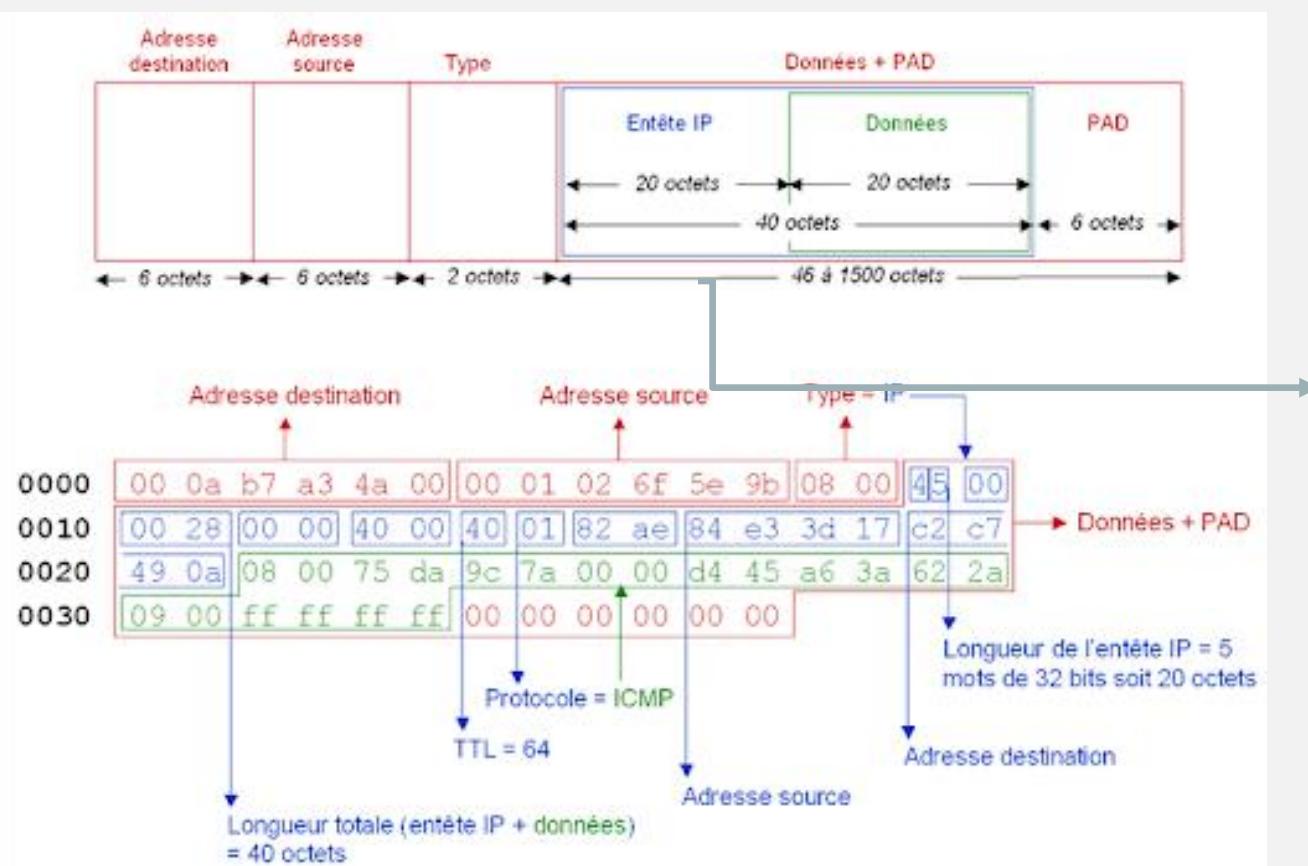
EN-TÊTE IP OU DATAGRAMME IP



Détails de l'en-tête IP

- **Version :** version du protocole IP (4 ou 6).
- **Longueur en-tête ou IHL :** 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.
- **Services différences (DS) :** Cela permet de mettre une priorité sur le trafic en fonction du type de données.
- **Longueur totale :** Longueur du datagramme entier y compris en-tête et données mesurée en octets.
- **Identification :** Valeur assignée par l'émetteur pour identifier les fragments d'un même datagramme.
- **Indicateur ou flags :** Il permet d'indiquer si le paquet a été fragmenté (Bit 0 : Réservé=0, bit 1 : DF= 1 ou 0, bit 2 : MF = 1 ou 2).
- **Décalage du fragment :** Le champ Position fragment est codé sur 13 bits et indique la position du fragment par rapport à la première trame. Le premier fragment possède donc le champ Position fragment à 0.
- **Time To Live (durée de vie du paquet) :** Limite la durée de vie du paquet. Décrémentation à chaque passage dans un routeur => évite les boucles d'un paquet sur un réseau.
- **Protocoles :** Le type de protocole de niveau 4 (TCP = 6 – UDP = 17 – ICMP = 1).
- **Somme de contrôle d'en-tête ou CheckSum :** C'est une valeur qui permet de déceler une éventuelle erreur de transmission avec une très grande probabilité.
- **Adresse IP source :** Source du paquet.
- **Adresse IP Destinataire :** Destinataire du paquet.
- **Options :** Le champ est de longueur variable. Un datagramme peut comporter 0 ou plusieurs options.
- **Padding ou bourrage :** 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.

EN-TÊTE IP OU DATAGRAMME IP



Paquet IP

version (4 bits)	longueur entête (4 bits)	type de service (8 bits)	longueur totale (16 bits, en octets)	
		identification (16 bits)	drapeau (3 bits) place du fragment (13 bits)	
durée de vie (TTL, 8 bits)	protocole (8 bits)	checksum (16 bits)		
		adresse de la source (32 bits)		
		adresse de la destination (32 bits)		
		(options)		
		données		

COUCHE 3 : RÉSEAU



- **Simulation Cisco Packet Tracer :**
- **Connexion 2 PC, 2 switchs et 1 routeur**

7 - ENTÊTE TCP

LE RÔLE DE LA COUCHE TRANSPORT

- La **couche transport** est chargée de l'établissement d'une session de communication temporaire entre 2 applications et de l'acheminement des données entre ces deux applications.
- La **couche transport** offre les services suivants :
 1. *Prise en charge des flux de données orientés connexion*
 2. *Fiabilité.*
 3. *Contrôle de flux.*
 4. *Multiplexage*

LA RESPONSABILITÉ DE LA COUCHE TRANSPORT

I – Prise en charge des données orientées connexions.

- **Suivi des conversations individuelles :**

- *La couche transport suit séparément chaque conversation transmise entre une application source et une application de destination.*

- **Segmentation des données et reconstitution des segments :**

- *La couche transport divise les données en segments qui sont plus faciles à gérer et à transporter.*

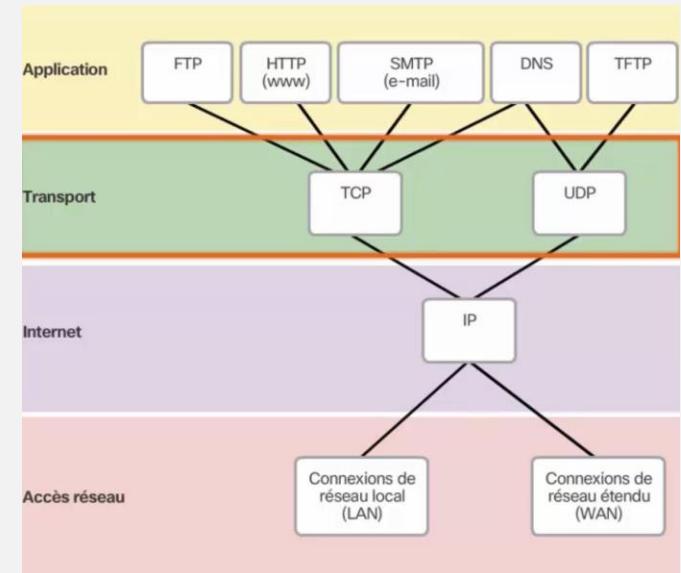
- **Identification des applications :**

- *La couche transport s'assure que même si plusieurs applications sont exécutés sur un périphérique, elles reçoivent toutes des données correctes. Identification via les ports.*

LA RESPONSABILITÉ DE LA COUCHE TRANSPORT

2 – Fiabilité de la couche transport et contrôle de flux

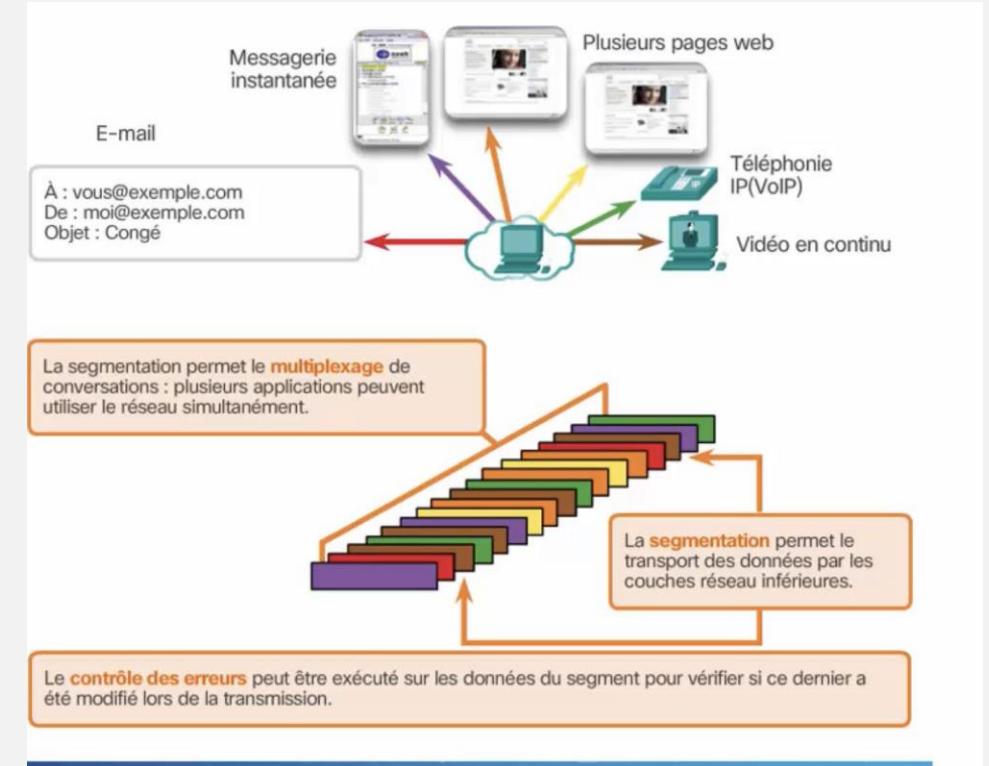
- **Certaines applications ne nécessitent pas de fiabilité. Les besoins de la couche transport varient d'une application à une autre.**
- **La suite TCP/IP fournit 2 protocoles de couche transport :**
 - **TCP (Transmission Control Protocol).**
 - **UDP (User Datagram Protocol).**
- **Le protocole IP utilise ces protocoles de transport pour permettre aux hôtes de communiquer et de transmettre des données.**
- **TCP est considéré comme un protocole de couche transport fiable, riche en fonctionnalités et qui permet de confirmer la remise des données de paquet.**
- **En revanche, le protocole UDP est un protocole de couche transport simple qui ne permet pas de garantir la fiabilité.**



LA RESPONSABILITÉ DE LA COUCHE TRANSPORT

3 – Multiplexage

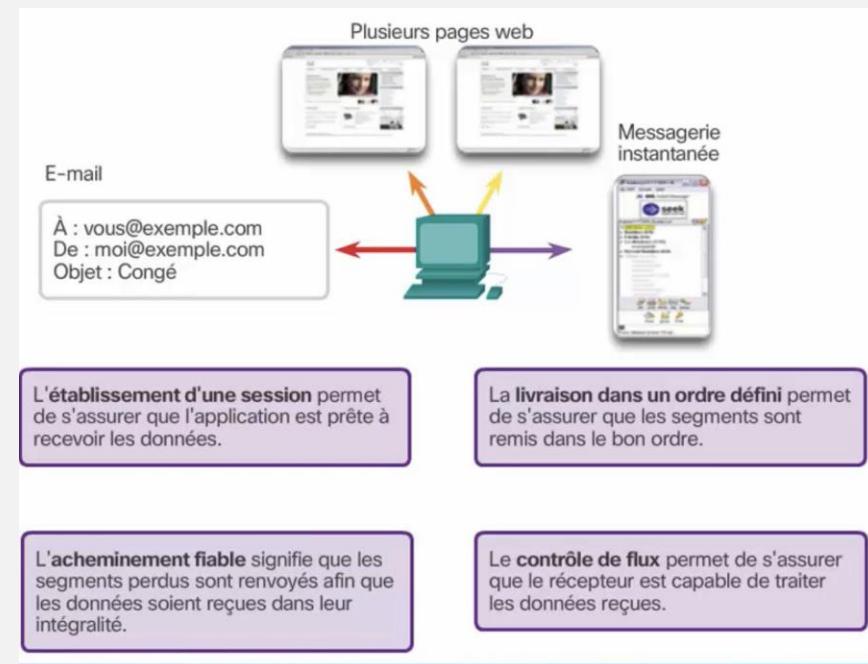
- **La segmentation des données en parties plus petites permet plusieurs communications différentes, provenant de nombreux utilisateurs, d'être imbriquées (multiplexées) sur le même réseau.**
- **La couche transport ajoute un en-tête qui contient des données binaires pour identifier chaque segment de données et permettre à divers protocoles de couche transport d'exécuter différentes fonctions relatives à la gestion de la communication.**



LE PROTOCOLE TCP - UDP

Le Protocole TCP

- La transmission de données via le protocole TCP est fiable dans la mesure où ce dernier prend en charge la confirmation de remise des paquets.
- 3 opérations simples garantissent la fiabilité avec TCP :
 - Le décompte et le suivi des segments de données transmis vers un hôte particulier depuis une application donnée.
 - Les accusés de réception des données.
 - La retransmission des données sans accusé de réception après un certain laps de temps.

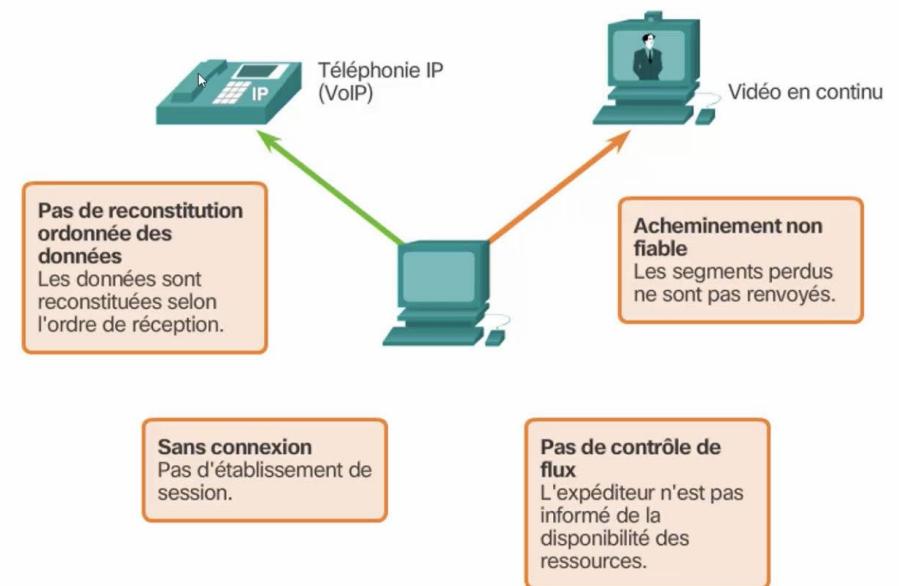


LE PROTOCOLE TCP - UDP

Le Protocole UDP

- Si la fiabilité n'est pas nécessaire UDP est un meilleur choix de protocole de transport (exemple VOIP comme skype).
- Le protocole UDP fournit des fonctions de base permettant d'acheminer des segments de données entre les applications appropriées avec peu de surcharge et de vérification des données.
- Certaines applications ne nécessitent pas de fiabilité. La fiabilité engendre une surcharge et d'éventuels retards de transmission.
- L'ajout de cette surcharge pour garantir la fiabilité de telle ou telle application peut réduire l'utilité de l'application et même en détériorer les performances.

Fonctions du protocole UDP

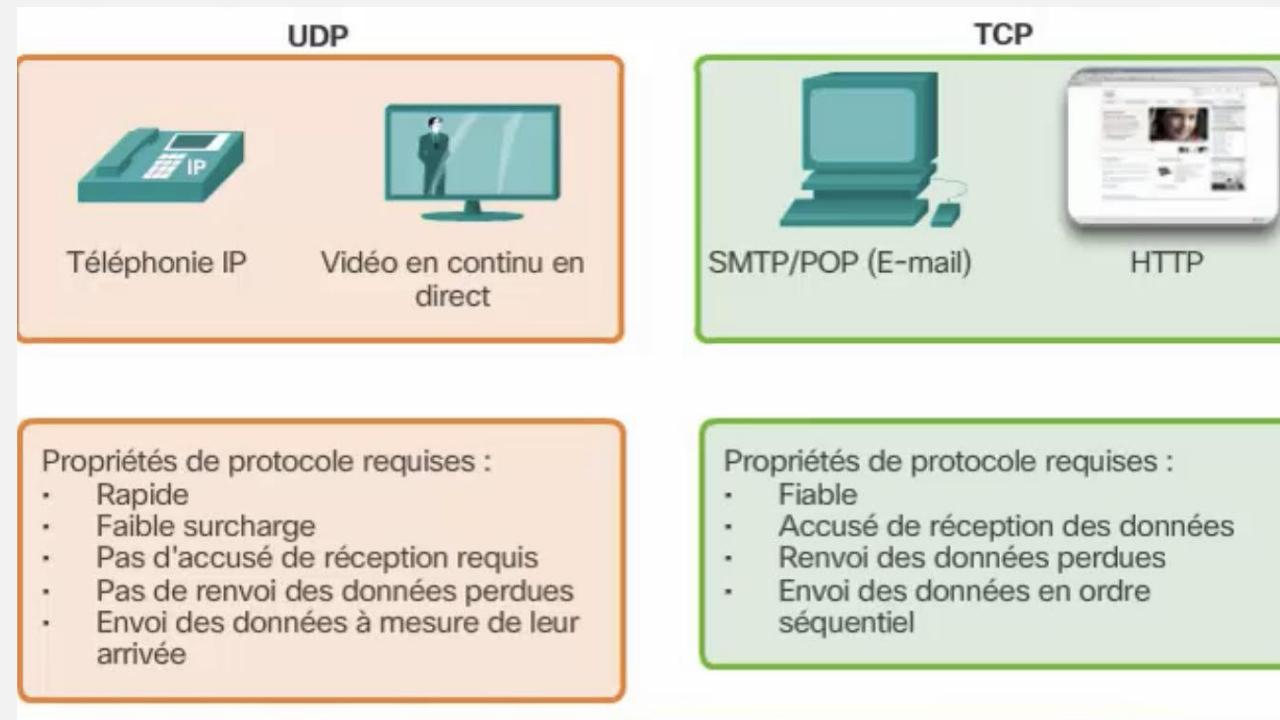


LE PROTOCOLE TCP - UDP

Comparaison entre UDP –TCP

UDP est un choix mieux adapté aux applications qui peuvent tolérer un certain niveau de perte de données

Streaming video
Streaming audio
VoIP

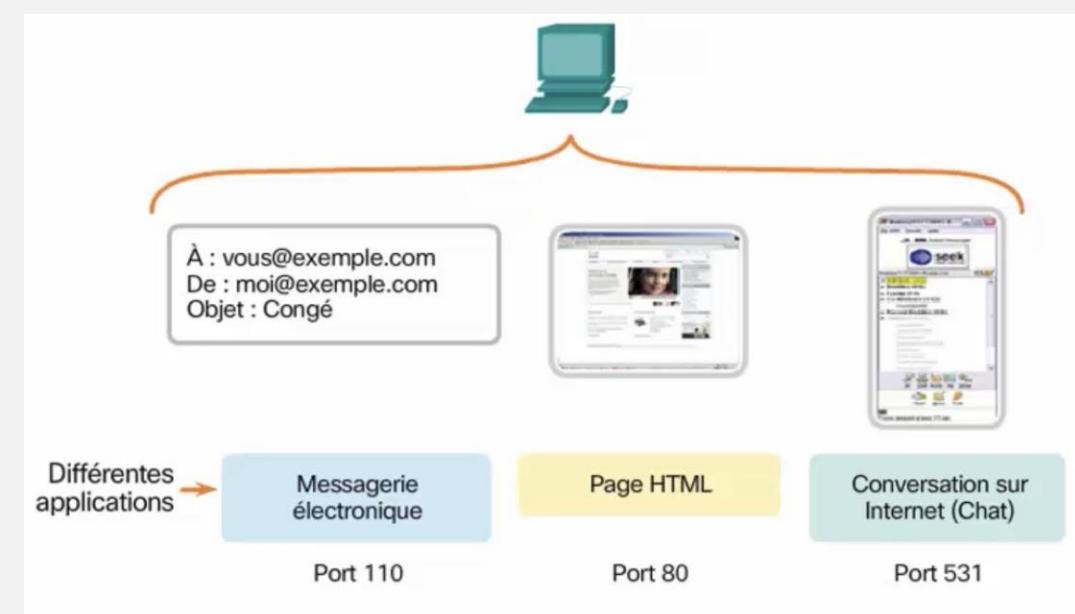


TCP est un bon choix pour les applications dont les segments doivent arriver dans un ordre bien précis et les applications qui ne tolèrent pas les pertes de données

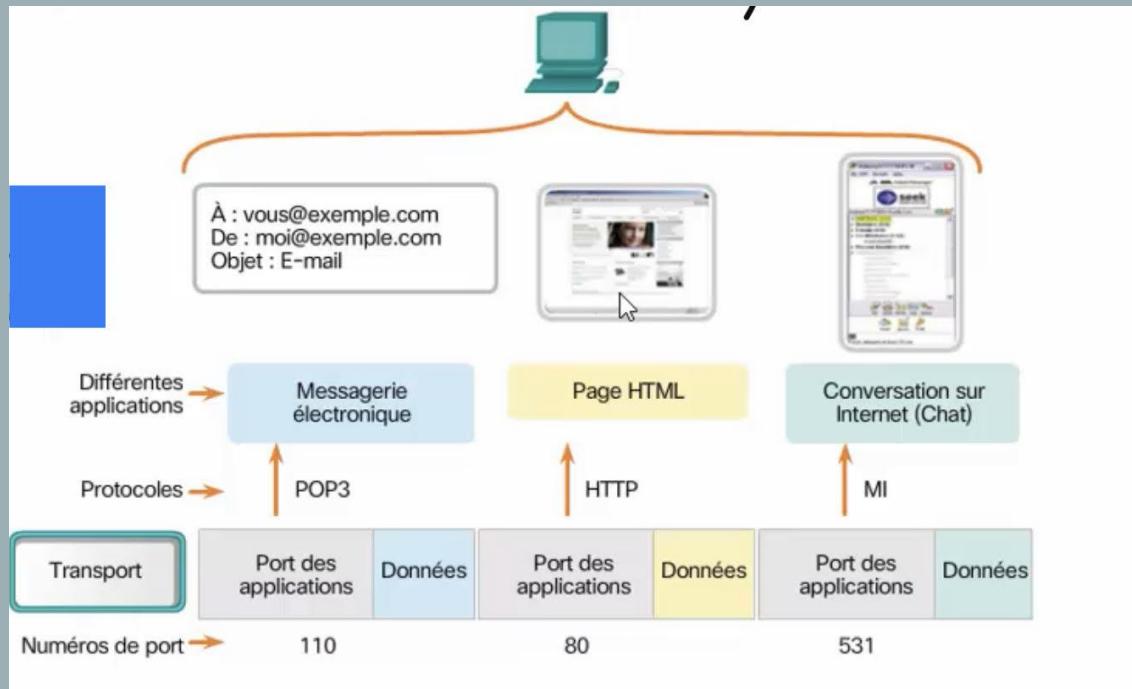
Base de données
Navigateurs web
Clients messagerie

UTILISATION DES PORTS

- La couche transport doit pouvoir séparer et gérer plusieurs communications ayant différentes exigences de transmission.
- Différentes applications envoient et reçoivent simultanément des données sur le réseau.
- Des valeurs d'en-tête uniques permettent aux protocoles UDP et TCP de gérer plusieurs conversations simultanées en identifiant ces applications.
- Ces identificateurs uniques sont **les numéros de port**.



UTILISATION DES PORTS



Numéro de port

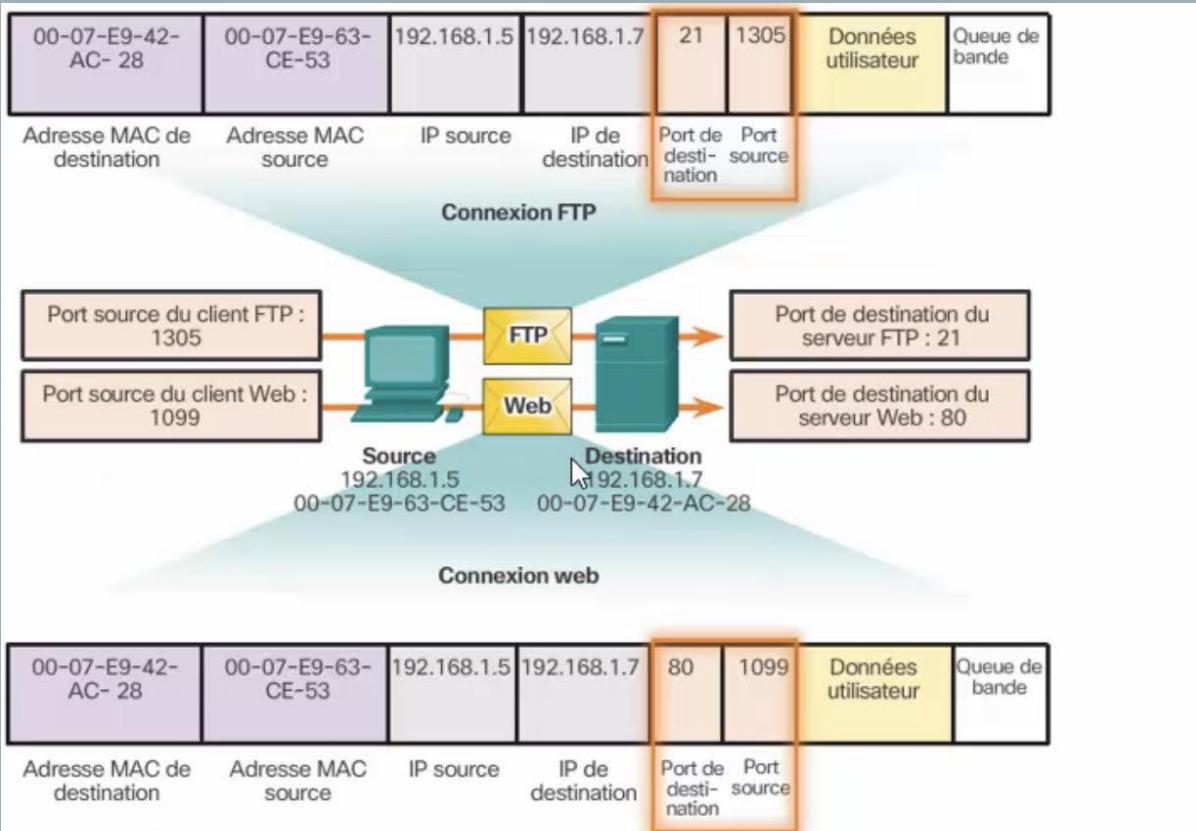
- **Port source :**

- **Le numéro du port est choisi de manière dynamique par le périphérique émetteur pour identifier une conversation entre 2 périphériques.**
- **Un client http envoie habituellement plusieurs requêtes web en même temps. Chaque conversation http est suivie en fonction des ports sources.**

- **Port destination :**

- **Sert à identifier une application ou un service qui s'exécute sur le serveur.**
- **Un serveur peut offrir plusieurs services à la fois, c'est-à-dire un service web sur le port 80 en même temps qu'un service FTP sur le port 21.**

UTILISATION DES PORTS



Paires d'interfaces de connexion

- La combinaison de l'adresse IP source et du numéro de port source, ou de l'adresse IP de destination et du numéro de port destination, est **appelée une interface de connexion**.
- **L'interface de connexion** sert à identifier le serveur et le service demandés par le client.
- **2 interfaces de connexion** forment une paire d'interfaces de connexion (192.168.1.5:1099, 192.168.1.7:80).
- **Les interfaces de connexion** permettent à plusieurs processus actifs sur un client et aux multiples connexions à un processus serveur de se distinguer les uns des autres.
- **Le numéro du port source fait office d'adresse de retour pour l'application envoyant la requête.**
- **La rôle de la couche transport** est de suivre les interfaces de connexion actives.

UTILISATION DES PORTS

Numéros de port

Plage de numéros de port	Groupe de ports
De 0 à 1023	Ports réservés
De 1024 à 49151	Ports inscrits
De 49152 à 65535	Ports dynamiques et/ou privés

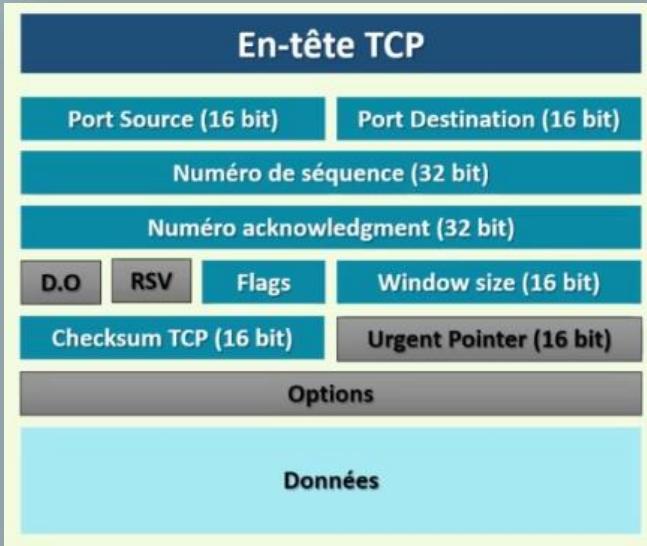
Numéros de port réservés

Numéro de port	Protocole	Application	Acronyme
20	TCP	Protocole FTP (File Transfer Protocol) (données)	FTP
21	TCP	Protocole FTP (File Transfer Protocol) (contrôle)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	-
25	TCP	Protocole SMTP (Simple Mail Transfer Protocol)	SMTP
53	UDP, TCP	Domain Name Service (service de noms de domaines)	DNS
67	UDP	Protocole DHCP (Dynamic Host Configuration Protocol) (serveur)	DHCP
68	UDP	Protocole DHCP (Dynamic Host Configuration Protocol) (client)	DHCP
69	UDP	Protocole TFTP (Trivial File Transfer Protocol)	TFTP
80	TCP	Protocole HTTP (Hypertext Transfer Protocol)	HTTP
110	TCP	Protocole POP (Post Office Protocol) version 3	POP3
143	TCP	Protocole IMAP (Internet Message Access Protocol)	IMAP
161	UDP	Protocole SNMP (Simple Network Management Protocol)	SNMP
443	TCP	Protocole HTTPS (Hypertext Transfer Protocol Secure)	HTTPS

PROCESSUS DE COMMUNICATION TCP

- Chaque processus d'application actif sur le serveur utilise un numéro de port.
- 2 services ne peuvent pas être affectés au même numéro de port d'un serveur au sein des mêmes services de la couche transport.
- Quand une application de serveur active est attribuée à un port spécifique, on considère que ce port est ouvert.
- Chaque demande de client envoyée à un port est acceptée et traitée par l'application de serveur liée à ce port.
- De nombreux ports peuvent être ouverts simultanément sur un serveur, chacun étant destiné à une application de serveur active.

ENTETE TCP



Message TCP

numéro de port source (16 bits)	numéro de port destination (16 bits)
numéro de séquence (32 bits)	
numéro d'acquittement (32 bits)	
longueur entête (4 bits)	réservé (6 bits) U A P R S F taille de fenêtre (16 bits)
checksum (16 bits)	pointeur urgent (16 bits)
(options)	
(données)	

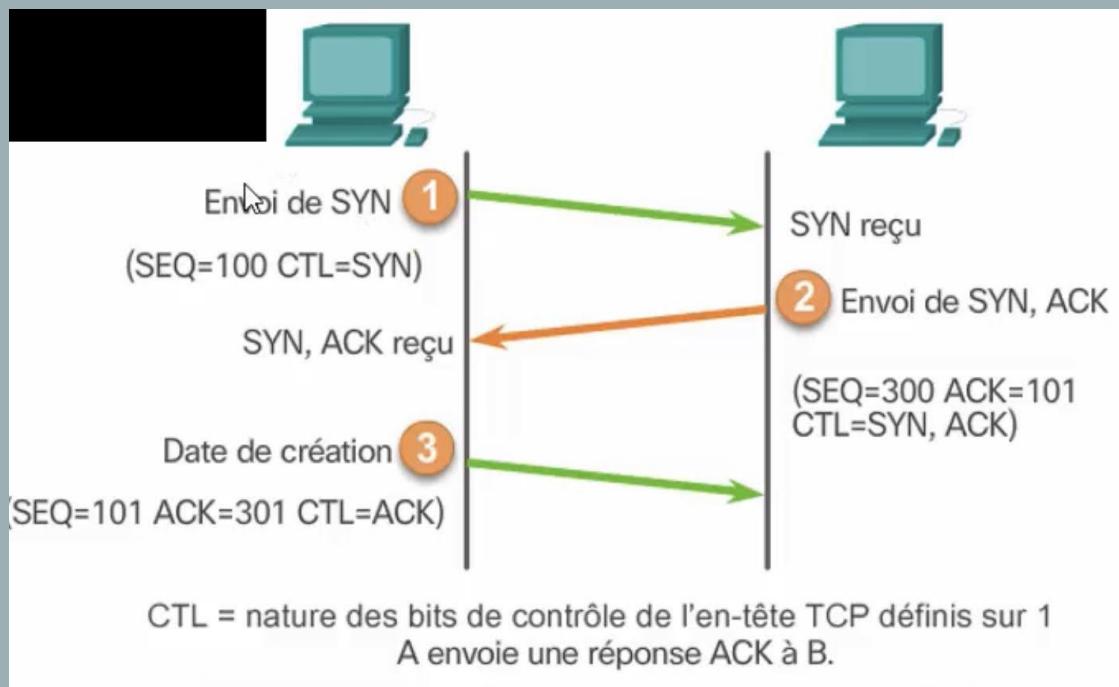
Message UDP

port source (16 bits)	port destination (16 bits)
longueur (16 bits)	checksum (16 bits)
données	

Détails de l'entête TCP

- Port source** : Le champ Port source est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine source.
- Port destination** : Le champ Port destination est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine de destination.
- Numéro de séquence** : Le champ Numéro de séquence est codé sur 32 bits et correspond au numéro du paquet. Cette valeur permet de situer à quel endroit du flux de données le paquet, qui est arrivé, doit se situer par rapport aux autres paquets.
- Numéro d'Ack ou d'accusé de réception** : Le champ Numéro de séquence est codé sur 32 bits et définit un acquittement pour les paquets reçus. Cette valeur signale le prochain numéro de paquet attendu. Par exemple, si il vaut 1500, cela signifie que tous les Datagrammes <1500 ont été reçus.
- Longueur entête** : Le champ Offset est codé sur 4 bits et définit le nombre de mots de 32 bits dans l'entête TCP. Ce champ indique donc où les données commencent.
- Réserve** : Le champ Réserve est codé sur 6 bits et il servira pour des besoins futurs. Ce champ doit être marqué à 0. Au jour d'aujourd'hui, on peut considérer que les besoins futurs se transforment en un champ non utilisé.
- Flags ou indicateurs** : Le champ URG est codé sur 1 bit et indique que le champ Pointeur de donnée urgente est utilisé - Le champ ACK est codé sur 1 bit et indique que le numéro de séquence pour les acquittements est valide - Le champ PSH est codé sur 1 bit et indique au récepteur de délivrer les données à l'application et de ne pas attendre le remplissage des tampons - Le champ RST est codé sur 1 bit et demande la réinitialisation de la connexion - Le champ SYN est codé sur 1 bit et indique la synchronisation des numéros de séquence - Le champ FIN est codé sur 1 bit et indique fin de transmission.
- Window size** : correspond au nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.
- Checksum** : Le champ Checksum est codé sur 16 bits et représente la validité du paquet de la couche 4 TCP.
- Pointeur de donnée urgente** : communique la position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence. Le pointeur doit pointer sur l'octet suivant la donnée urgente. Ce champ n'est interprété que lorsque le Flag URG est marqué à 1. Dès que cet octet est reçu, la pile TCP doit envoyer les données à l'application.
- Options – Données**.

PROCESSUS DE COMMUNICATION TCP

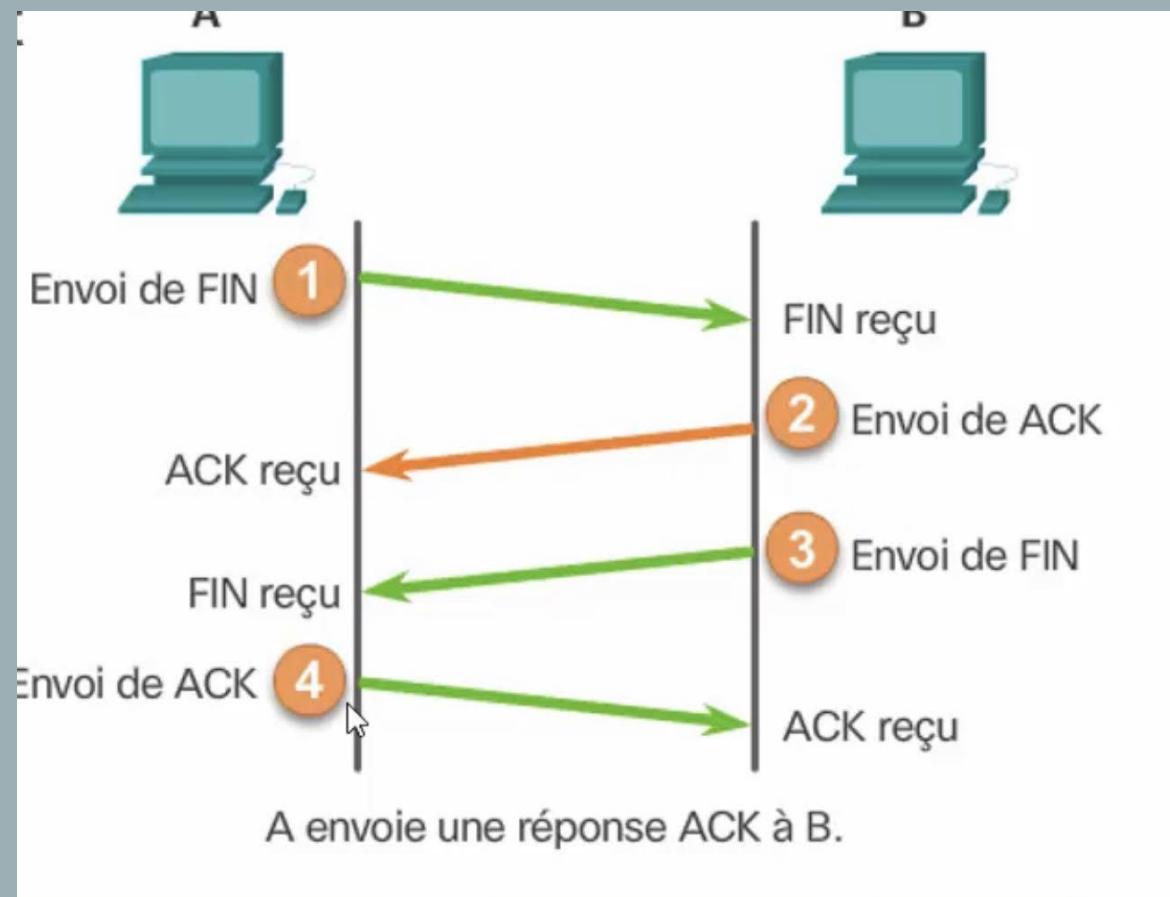


Three way handshake

Les étapes du processus de communication tcp

- **Une connexion TCP** est établie en 3 étapes :
 1. Le client demande l'établissement d'une session de communication.
 2. Le serveur accueille la session de communication client-serveur et demande l'établissement d'une session de communication serveur-client.
 3. Le client accueille la session de communication serveur-client.

PROCESSUS DE COMMUNICATION TCP

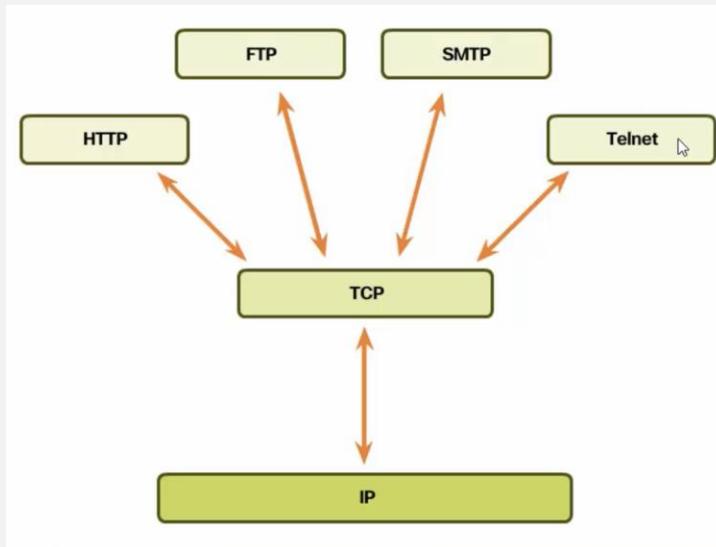


Le processus de fin de session de communication

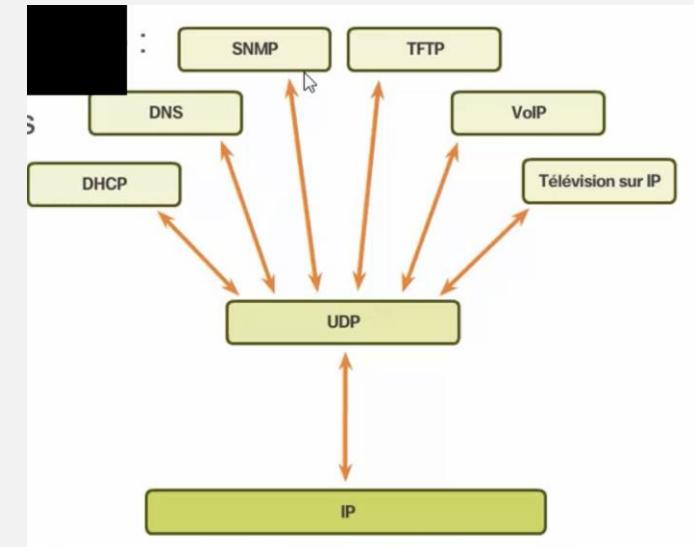
- **L'indicateur « FIN TCP » permet de mettre fin à une connexion TCP:**
 1. Quand le client n'a plus de données à envoyer dans le flux, il envoie un segment dont l'indicateur FIN est défini.
 2. Le serveur envoie un segment ACK pour informer de la bonne réception du segment FIN afin de fermer la session du client au serveur.
 3. Le serveur envoie un segment FIN au client pour mettre fin à la session du serveur au client.
 4. Le client répond à l'aide d'un segment ACK pour accuser réception du segment FIN envoyé par le serveur.
 5. Quand la réception de tous les segments a été confirmée, la session est fermée.

LES APPLICATIONS QUI UTILISENT TCP / UDP

APPLICATION TCP



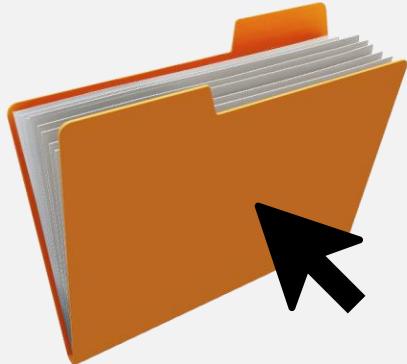
APPLICATION UDP





TP TIME

TP_ Quizz :



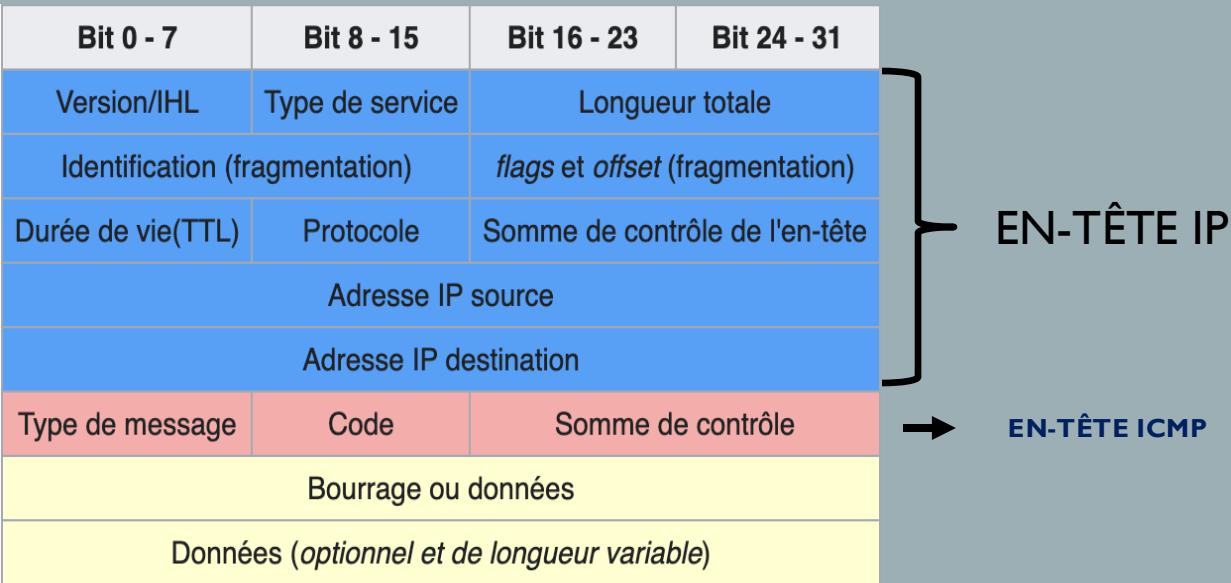
Quizz 4 : Couche réseau

8 - ENTÊTE ICMP

8- I LE PROTOCOLE ICMP

- Le protocole **ICMP** (Internet Control Message Protocol) permet de gérer les informations relatives aux erreurs du protocole IP.
- Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des Datagrammes en erreurs.
- **ICMP** gère les événements pour IP,TCP et UDP.
- **ICMP** se situe au même niveau que le protocole **IP** (couche réseau).
- Les messages d'erreur **ICMP** sont transportés sur le réseau sous forme de Datagramme, comme n'importe quelle donnée.

8-2 ENTÊTE ICMP



- **Type (8 bits) :**
 - Type du message.
 - + de 20 types de messages ICMP différents.
 - 2 grandes catégories :
 - ✓ message généré à la suite d'une erreur
 - ✓ message d'administration.
- **Code (8 bits) :**
 - sous-type du message ICMP
- **Checksum (16 bits) :**
 - protège la totalité du message.
 - procédé de calcul identique à celui de IPTCP, UDP:
 - somme de mots de 16 bits en complément à 1.
 - Obligatoire.
- **La structure du reste du message dépend du type (1 mot minimum).**

8-2 ENTÊTE ICMP

Exemple Ping

ICMP echo request and reply



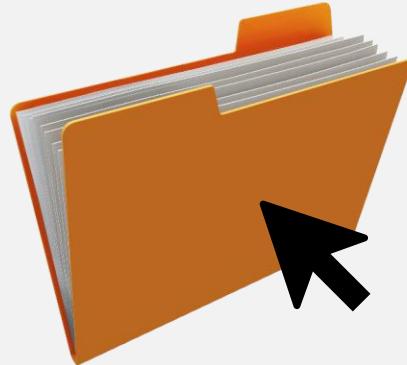
Type de message ICMP

Type	Code	Description
0 - Réponse d'echo	0	Réponse d'ECHO (Réponse au message de type 8)
1 et 2 - Réservés		Reservés
	0	Le réseau n'est pas accessible
	1	La machine n'est pas accessible
	2	Le protocole n'est pas accessible
	3	Le port n'est pas accessible
	4	Fragmentation nécessaire mais impossible à cause du drapeau (<i>flag</i>) DF
	5	Le routage a échoué
	6	Réseau inconnu
	7	Machine inconnue
	8	Machine non connectée au réseau (inutilisé)
	9	Communication avec le réseau interdite
	10	Communication avec la machine interdite
	11	Réseau inaccessible pour ce service
	12	Machine inaccessible pour ce service
	13	Communication interdite (filtrage)
	14	Priorité d'hôte violé
	15	Limite de priorité atteinte
3 – Destinataire inaccessible		
4 – Extinction de la source	0	Extinction de la source (<i>source quench</i>)
	0	Redirection pour un hôte
	1	Redirection pour un hôte et un service
	2	Redirection pour un réseau
	3	Redirection pour un réseau et un service
5 – Redirection		
8 – Demande d'echo	0	Demande d'ECHO (utilisé par la commande ping)
	0	Temps de vie du datagramme dépassé
	1	Temps de ré-assemblage des fragments du datagramme dépassé
11 – Temps dépassé		
12 – En-tête erroné	0	Le pointeur indique l'erreur
	1	Absence d'une option obligatoire
	2	Mauvaise longueur
13 – Demande heure	0	Timestamp request
14 – Réponse heure	0	Timestamp reply
15 – Demande adresse IP	0	Demande d'adresse réseau
16 – Réponse adresse IP	0	Réponse d'adresse réseau
17 – Demande masque sous-réseau	0	Demande de masque de sous-réseau
18 – Réponse masque sous-réseau	0	Réponse de masque de sous-réseau



TRAME ETHERNET

Pratique avec Wireshark :

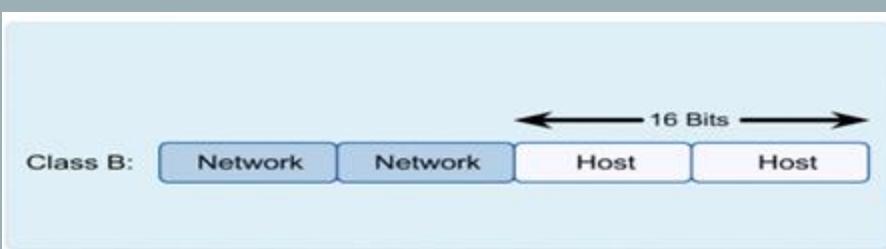
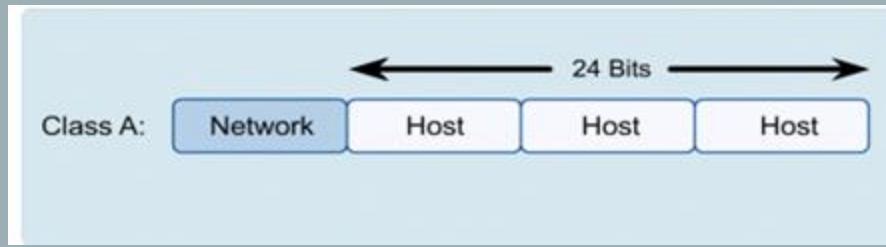


9 - ROUTAGE

Rappels réseaux, masques et calculs de masques

VLSM fonctionnement et principe

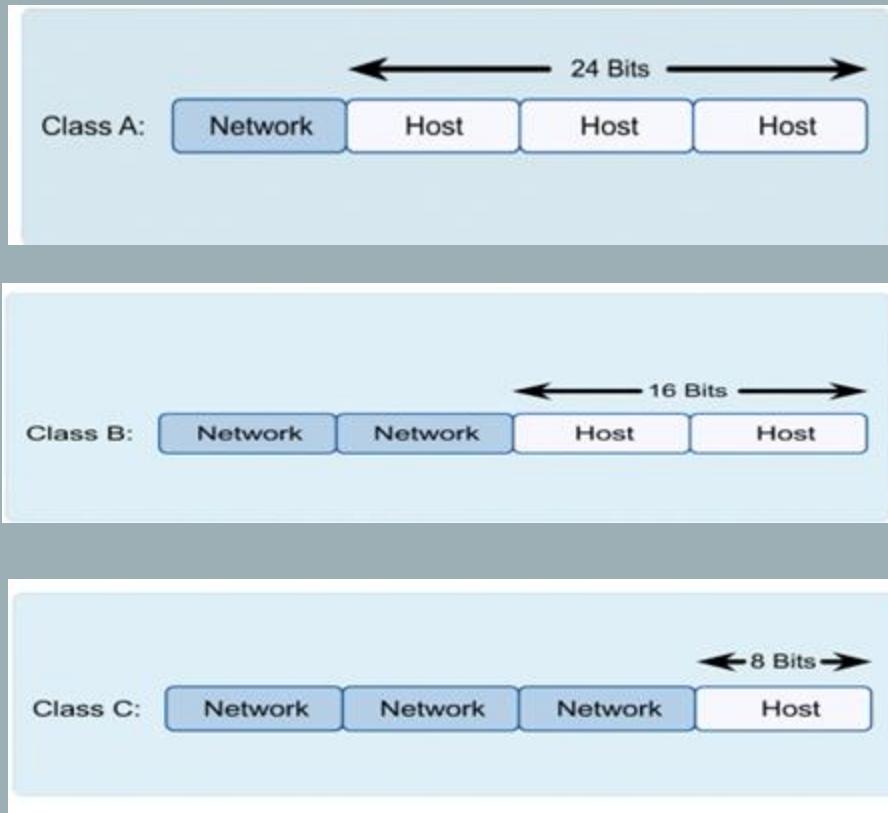
LES MASQUES DE SOUS-RÉSEAUX



Détails du masque réseau

- **L'adresse IP** est donc composée de deux parties :
 - La partie réseau.
 - La partie hôte.
- **Le masque de sous réseau** permet de savoir qu'elle est la partie des 32 bits qui est utilisé pour identifier le réseau.
- 2 types d'écriture pour le masque de sous-réseau :
 - 192.168.1.12 /24 (24 premiers bits pour le masque)
 - **255.255.255.0**
- On va pouvoir obtenir grâce à **l'adresse IP** et à au **masque réseau**:
 - La plage d'adresse disponible ou utilisable sur un réseau.
 - L'adresse du réseau (Plus petite adresse sur le réseau)
 - L'adresse de broadcast (Plus grande adresse sur le réseau)

LES MASQUES DE SOUS-RÉSEAUX



Détails du masque réseau

• Exemple :

- Adresse IP : 110.17.14.8 /23

- Soit en binaire :

0110 1110.0001 0001.0000 1110 .0000 1000

- Pour 23 => 255.255.254.0.

- Soit en binaire :

1111 1111.1111 1111.1111 1110 . 0000 0000

• Adresse réseau :

0110 1110.0001 0001.0000 1110 .**0000 0000**

- Soit une adresse : 110.17.14.0

• Adresse de broadcast :

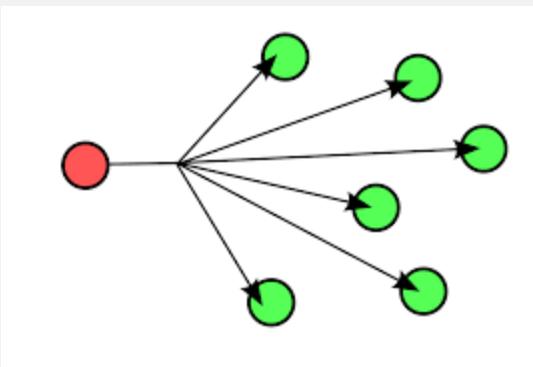
0110 1110.0001 0001.0000 1111 .**1111 1111**

- Soit une adresse : 110.17.15.255

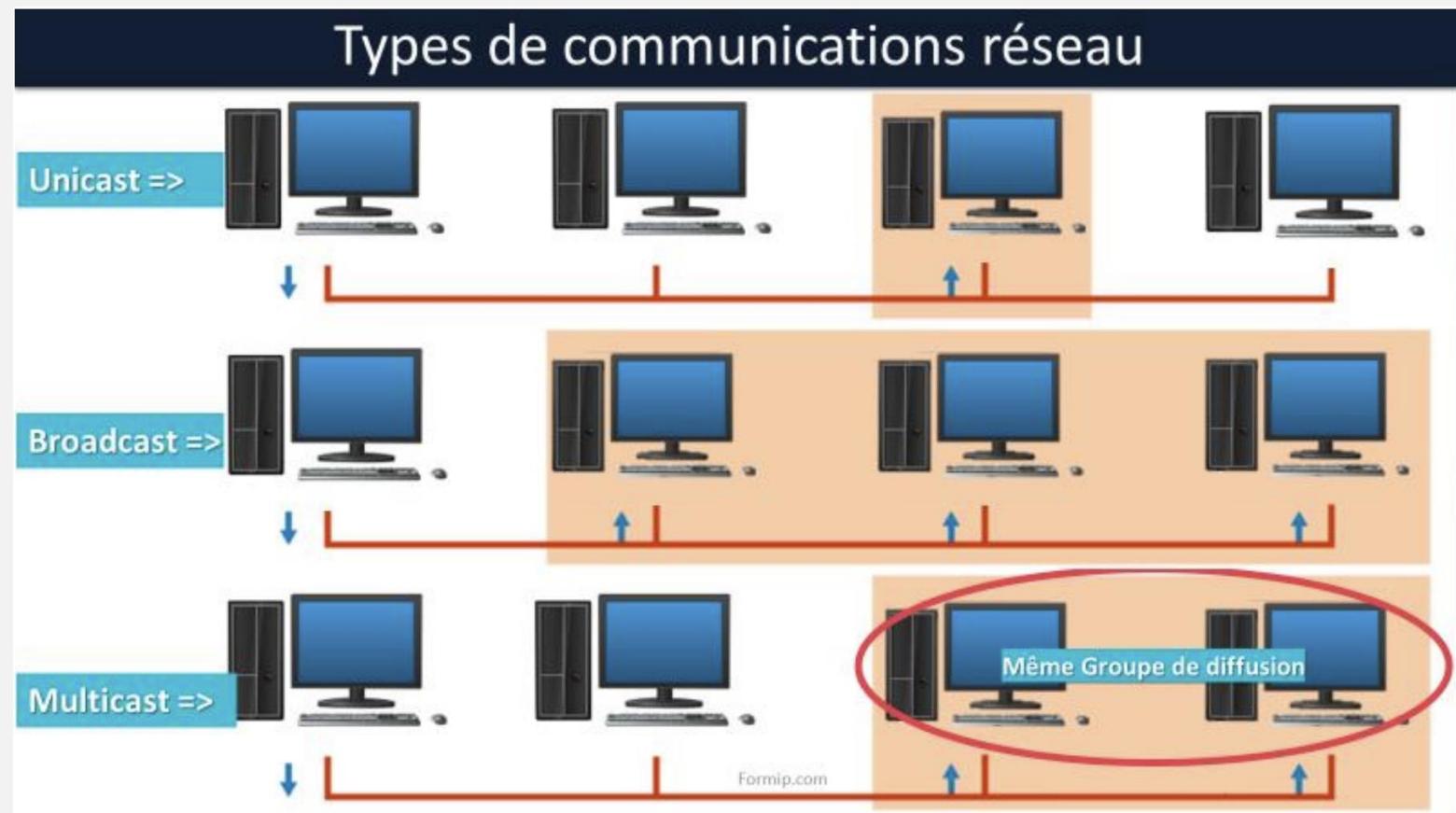
• Plage d'adresse : Entre 110.17.14.0 et 110.17.15.255

L'ADRESSE DE BROADCAST

- Une adresse de broadcast va permettre à une machine de communiquer avec toutes les machines de son sous-réseau.
- Seules les machines qui appartiennent au sous-réseau vont recevoir une copie du paquet envoyé.

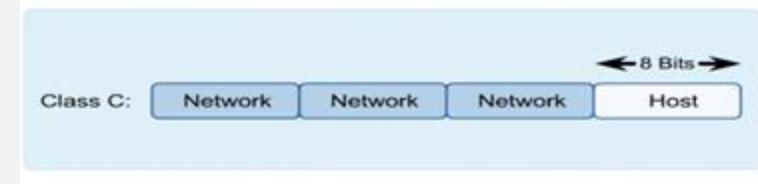
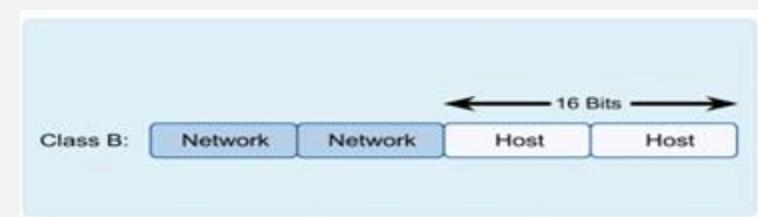
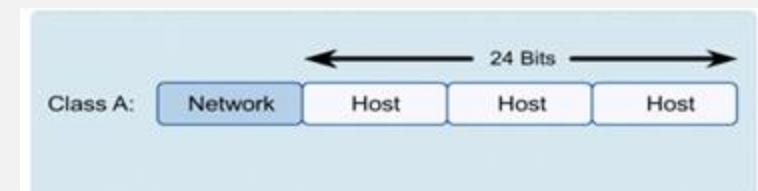


LES TYPES DE COMMUNICATION



LES CLASSES D'ADRESSE IP

Classe	Diffusion	de	à	Masque	Masque en bits (CIDR)
Classe A	Monodiffusion	0.0.0.0	126.255.255.255	255.0.0.0	/8
Classe B	Monodiffusion	128.0.0.0	191.255.255.255	255.255.0.0	/16
Classe C	Monodiffusion	192.0.0.0	223.255.255.255	255.255.255.0	/24
Classe D	Multidiffusion LoopBack APIPA Broadcast address	224.0.0.0 127.x.y.z 169.254.x.y 255.255.255.255	239.255.255.255 127.255.255.255 169.254.255.255	Non défini 127.0.0.0 169.254.0.0 255.255.255.255	Non défini /8 /16 /32
Classe E	Réservé	240.0.0.0	255.255.255.255	Non défini	Non défini



LES ADRESSES IPV4 PRIVÉES

- Les adresses IP privées ne sont pas routable sur internet contrairement aux adresses IP publiques (unique).
- Il existe plusieurs plages d'adresses IP privées regroupées par classe :
 - **Classe A** : de 10.0.0.0 à 10.255.255.255 (16 777 216 hôtes)
 - **Classe B** : de 172.16.0.0 à 172.31.255.255 (1 048 576 hôtes)
 - **Classe C** : de 192.168.0.0 à 192.168.255.255 (65 536 hôtes)
- Ces plages sont réservées pour la configuration de réseaux privés

LE ROUTER

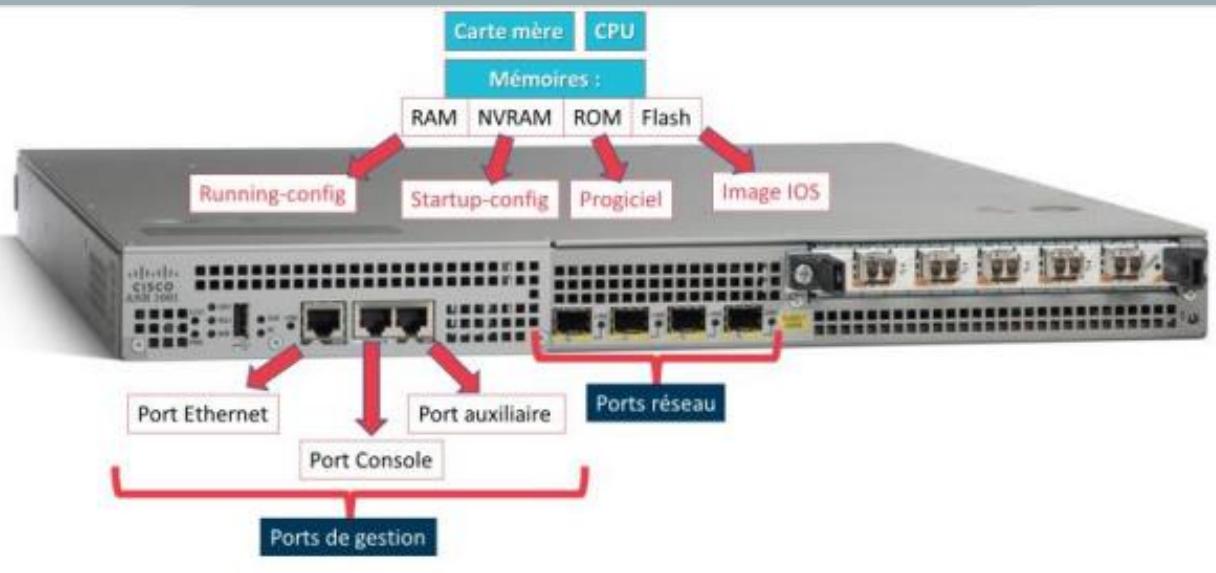


Le symbole

Le routeur

- Matériel spécialisé ou ordinateur équipé de logiciels adéquats, assurant la transmission de données entre plusieurs réseaux.
- Les routeurs opèrent au niveau de la couche 3 du modèle OSI.
- Il possède plusieurs interfaces reliées à différents réseaux.
- Il se charge aussi de déterminer le chemin d'acheminement d'un paquet.
- Son rôle est de transmettre les paquets d'un réseau à un autre.
- Il joue le rôle de passerelle entre 2 réseaux.
- Quand un paquet traverse un routeur, on dit qu'il fait **un saut**.
- Un routeur aiguille les paquets grâce à sa table de routage.
- Chaque routeur possède sa propre table de routage.

LES COMPOSANTS D'UN ROUTER



Les éléments d'un routeur

- **Carte mère :** Cœur de notre routeur. Elle concentre le fonctionnement des principaux composants de notre routeur
- **CPU :** Il exécute les instructions. Il est présent sur la carte mère.
- **Mémoires :**
 - **RAM :** Elle stocke les informations pendant le fonctionnement du routeur. La running-config y est stocké. Les informations disparaissent à l'extinction ou redémarrage du routeur.
 - **NVRAM :** Elle conserve son contenu quand le routeur est éteint. Elle stocke la startup-config. Elle stocke aussi le registre de configuration du logiciel pour savoir quelle image utilisée au démarrage.
 - **ROM :** Son rôle est principalement de permettre le démarrage du routeur s'il ne trouve pas d'image valide. Elle ne peut être modifiée.
 - **Flash :** Elle stocke l'image du logiciel Cisco IOS pour notre routeur.
- **Ports de gestion :**
 - **Port Ethernet :** Il va permettre de connecter notre routeur pour de l'administration à travers un autre sous-réseau (besoin IP).
 - **Port Console :** Il va permettre de connecter un PC directement à notre routeur pour l'administrer.
 - **Port Auxiliaire :** On peut y connecter un modem.
 - **Ports Réseau :** Ils vont permettre à notre routeur de connecter différents réseaux (LAN ou WAN).

LE FONCTIONNEMENT D'UN ROUTER

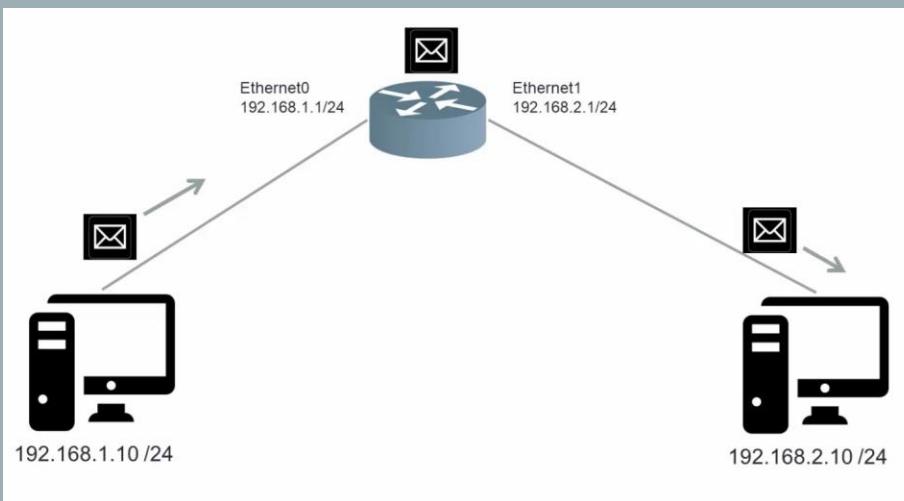
1



2



3



1

Les 2 PC sont sur le même réseau.

- Les 2 machines peuvent communiquer entre elles.
- L'envoi d'un paquet sera opérationnel.

2

Les 2 pc ne sont pas sur le même réseau.

- La communication n'est pas possible.

3

La mise en place d'un passerelle va permettre la communication entre 2 machines qui ne sont pas sur le même réseau.

- Le router dispose de 2 interfaces qui lui permettent de faire communiquer les 2 machines présentes sur 2 sous-réseaux différents.

LE FONCTIONNEMENT D'UN ROUTER

ROUTAGE SANS ROUTE PAR DÉFAUT

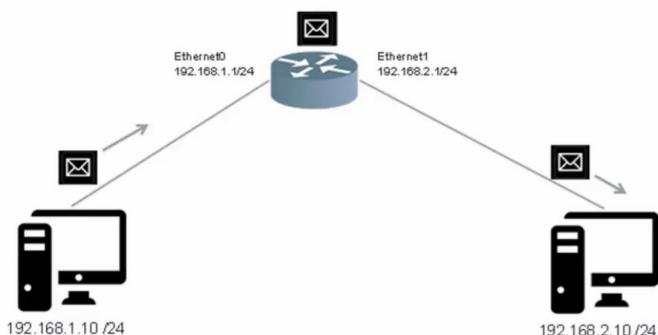


Table de routage :

Interface Ethernet0 -> Réseau 192.168.1.0 /24
Interface Ethernet1 -> Réseau 192.168.2.0 /24

Si je reçois un paquet à destination d'une machine sur le réseau 192.168.1.0/24, alors je le transmet à mon interface Ethernet0.

Si je reçois un paquet à destination d'une machine sur le réseau 192.168.2.0/24, alors je le transmet à mon interface Ethernet1.

ROUTAGE AVEC ROUTE PAR DÉFAUT

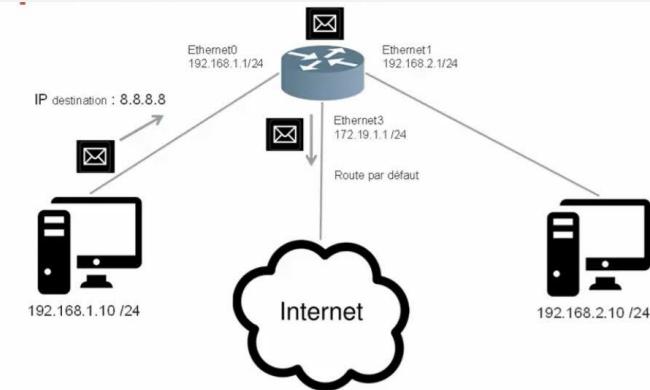


Table de routage :

Interface Ethernet0 -> Réseau 192.168.1.0 /24
Interface Ethernet1 -> Réseau 192.168.2.0 /24
Interface Ethernet3 -> Tous les autres réseaux

Si je reçois un paquet à destination d'un réseau auquel je ne suis pas connecté, je peux l'envoyer par la route par défaut via mon interface Ethernet 3.

LA TABLE DE ROUTAGE

- Une table de routage est une structure de données utilisée par un routeur ou un ordinateur en réseau et qui associe des préfixes à des moyens d'acheminer les trames vers leur destination. C'est un élément central du routage IP.
- La table de routage indique **quelle passerelle utiliser pour joindre un réseau**.
- Chaque ligne de la table de routage répertorie un réseau de destination ainsi que l'interface ou l'adresse IP qui permet de l'atteindre.
- **Toute machine connectée à un réseau possède une table de routage**, même une imprimante, un téléphone,
- La table de routage contient :
 - a. Les adresses du routeur lui-même ;
 - b. Les adresses des sous-réseaux auxquels le routeur est directement connecté ;
 - c. Les routes statiques, c'est-à-dire configurées explicitement par l'administrateur ;
 - d. Les routes dynamiques, apprises par des protocoles de routages dynamique comme BGP, OSPF, IS-IS, etc. ;
 - e. Une route par défaut.

LA TABLE DE ROUTAGE

```
[MBP-de-Mohamed:~ mohamed$ netstat -nr
Routing tables

Internet:
Destination      Gateway        Flags     Netif   Expire
default          192.168.1.254  UGScg    en0
127              127.0.0.1      UCS      lo0
127.0.0.1        127.0.0.1      UH       lo0
169.254          link#12       UCS      en0    !
192.168.1         link#12       UCS      en0    !
192.168.1.5       f8:27:93:c5:96:74  UHLWI    en0    !
192.168.1.7       9c:8c:6e:d8:5d:c6  UHLWII   en0    1018
192.168.1.15      a8:d3:f7:ee:91:ea  UHLWII   en0    566
192.168.1.51/32    link#12       UCS      en0    !
192.168.1.51      a0:78:17:75:9f:42  UHLWI    lo0
192.168.1.89      34:36:3b:5b:bf:6c  UHLWI    en0    !
192.168.1.91      1a:c6:10:30:1b:ae  UHLWI    en0    !
192.168.1.254/32   link#12       UCS      en0    !
192.168.1.254      ac:3b:77:5c:76:1c  UHLWIir  en0    1178
192.168.1.255      ff:ff:ff:ff:ff:ff  UHLWbI   en0    !
224.0.0/4          link#12       UmCS    en0    !
224.0.0.251         1:0:5e:0:0:fb   UHmLWI   en0
239.255.255.250    1:0:5e:7f:ff:fa  UHmLWI   en0
255.255.255.255/32 link#12       UCS      en0    !
```

Sous Windows : route print ou netsh int ipv4 / ipv6 sh route

Sous Unix/OS X : netstat -rn

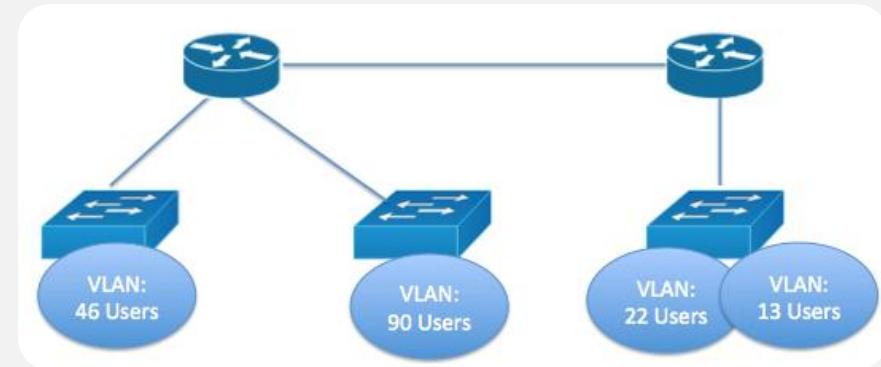
Sous Linux : ip -4 / -6 route

Sous Cisco IOS : show ip / ipv6 route

Sous Juniper JunOS: show route

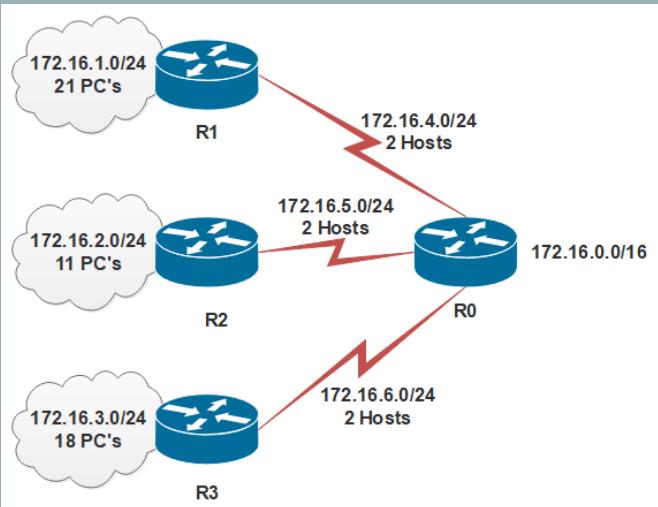
VLSM

- VLSM (Variable Length Subnet Mask) vs FLSM (Fixed Length Subnet Mask).
- Le concept est lié au fait d'économiser des adresses IP dans votre réseau (surtout pour les FAI par exemple).
- Chaque sous-réseau peut avoir un besoin d'adresse IP différent.
- Il va permettre d'adapter la quantité d'adresse IP nécessaire à chaque sous-réseaux et ainsi éviter que chaque sous-réseau dispose de la même quantité d'IP disponible alors que leurs besoins sont différents.



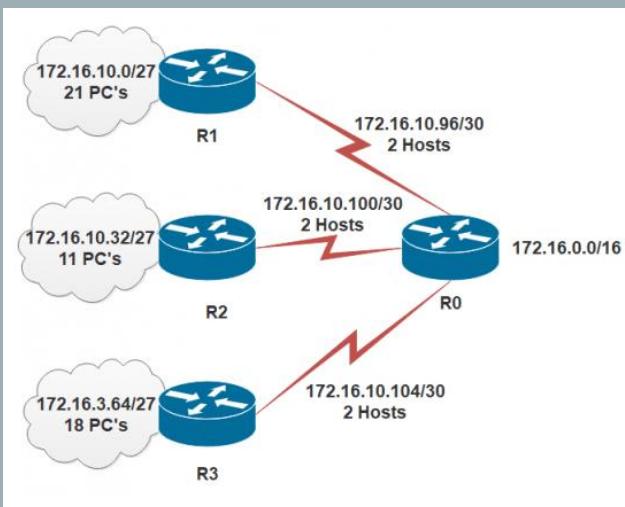
PRINCIPE DU VLSM

Détails principes



Exemple avec
FLSM

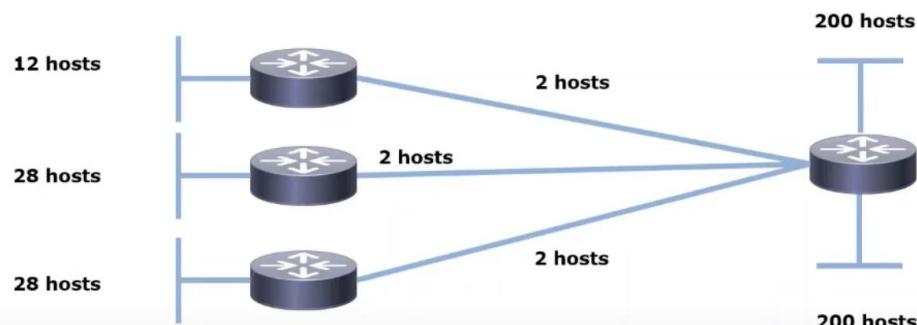
Exemple après
mise en place du
VLSM



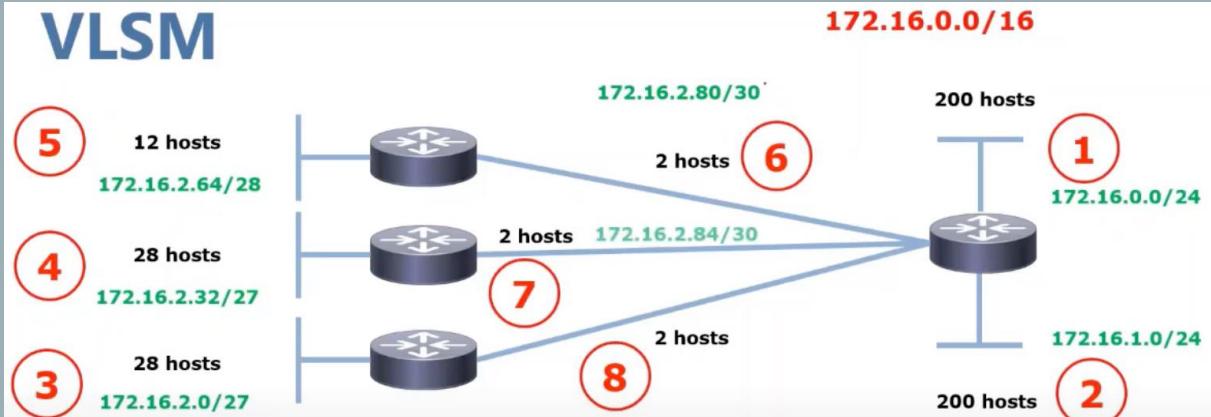
- Le principe est d'adapter le nombre d'adresse IP dans un sous-réseau en fonction de son besoin réel d'adresse IP.
- On utilisera pour cela le masque de sous-réseau pour réduire ou augmenter la part « host » dans l'adresse IP de sous-réseau.
- Le masque de sous-réseau va évoluer en fonction du besoin du sous-réseau.
- Il est important de démarrer le VLSM sur la partie réseau qui dispose du plus de besoin et d'attribuer les autres adresses IP de manière décroissante.

FONCTIONNEMENT DU VLSM

VLSM



VLSM



- On priorise par taille de sous-réseaux, soit le besoin en adresse IP par sous-réseau.
- On identifie l'adresse réseau principale (ex : 172.16.0.0/16).
- Pour le sous-réseau 1 et 2, le besoin est de 200 adresses IP. On peut donc utiliser un masque sous-réseau /24 ce qui va nous permettre d'attribuer jusqu'à 255 adresses et 253 disponibles.
- Pour le sous-réseau 3, on voit que le besoin d'adresse IP est de 28. Donc un masque sous-réseau de /24 serait trop important.
- Il faut choisir un masque sous-réseau qui va nous permettre de mobiliser uniquement le nombre d'IP nécessaire soit 28. Le masque réseau /27 va nous permettre de mobiliser uniquement 32 IP.
- Idem pour le sous-réseau 4, mais pour passer du sous réseau 3 au 4, il faudra faire un saut de 32 et démarrer la partie host du sous-réseau à 32.
- Pour passer au sous-réseau 5, on fait une fois de plus un saut de 32 car 32 IP sont mobilisés sur le sous-réseau 4.
- Pour le sous-réseau 5, il est possible de réduire le nombre d'IP mobilisable est de changer de masque de sous-réseau à /28 (partie host encore réduite) pour n'utiliser que 16 IP sur ce sous-réseau.
- On voit que pour les sous-réseaux 6, 7 et 8 le nombre d'IP nécessaire est de 2. Nous sommes dans une connexion Point à Point (entre 2 retours).
- Là aussi, pour passer du sous-réseau 5 à 6, on fait un saut de 16, on change notre masque sous-réseau pour une valeur de 30. Cela nous fournira 4 IP possibles (2 mobilisables).
- Pour les sauts entre 6 et 7, il faudra rajouter 4.

FONCTIONNEMENT DU VLSM

Tableau complet des masques réseaux

Masque de sous-réseau décimale	Masque de sous-réseau binaire	Notation en « / »	Nombre de bits d'hôtes	Nombre d'IP 2^n
255.0.0.0	1111111.0000000.0000000.0000000	/8	24	16777216
255.128.0.0	1111111.1000000.0000000.0000000	/9	23	8388608
255.192.0.0	1111111.1100000.0000000.0000000	/10	22	4194304
255.224.0.0	1111111.1110000.0000000.0000000	/11	21	2097152
255.240.0.0	1111111.1111000.0000000.0000000	/12	20	1048576
255.248.0.0	1111111.1111100.0000000.0000000	/13	19	524288
255.252.0.0	1111111.1111110.0000000.0000000	/14	18	262144
255.254.0.0	1111111.11111110.0000000.0000000	/15	17	131072
255.255.0.0	1111111.11111111.0000000.0000000	/16	16	65536
255.255.128.0	1111111.11111111.1000000.0000000	/17	15	32768
255.255.192.0	1111111.11111111.1100000.0000000	/18	14	16384
255.255.224.0	1111111.11111111.1110000.0000000	/19	13	8192
255.255.240.0	1111111.11111111.1111000.0000000	/20	12	4096
255.255.248.0	1111111.11111111.1111100.0000000	/21	11	2048
255.255.252.0	1111111.11111111.11111100.0000000	/22	10	1024
255.255.254.0	1111111.11111111.11111110.0000000	/23	9	512
255.255.255.0	1111111.11111111.11111111.0000000	/24	8	256
255.255.255.128	1111111.11111111.11111111.1000000	/25	7	128
255.255.255.192	1111111.11111111.11111111.1100000	/26	6	64
255.255.255.224	1111111.11111111.11111111.1110000	/27	5	32
255.255.255.240	1111111.11111111.11111111.1111000	/28	4	16
255.255.255.248	1111111.11111111.11111111.1111100	/29	3	8
255.255.255.252	1111111.11111111.11111111.1111100	/30	2	4

- Avec l'exemple précédent, le besoin réel était de 474 IP ($200 + 200 + 28 + 28 + 12 + 2 + 2 + 2$).
- Avec un système FLSM, on aurait $8 \times 256 =$ soit 2048 IP.
- Avec VLSM, on mobiliser 604 adresses IP sur notre réseau ($2 \times 256 + 2 \times 32 + 1 \times 16 + 3 \times 4$).
- Avec FLSM, on n'obtient $2048 - 474 = 1574$ IP inutilisées sur notre réseau.
- Avec VLSM, on $604 - 474 = 130$ IP non utilisées.

LES DIFFÉRENTS TYPES DE ROUTAGE

- **Le routage direct :** Il s'agit le plus souvent du routage dans le même réseau (LAN).
- **Le routage indirect :** Le destinataire n'est pas sur le même LAN. On doit franchir une passerelle connue d'avance ou un chemin par défaut pour acheminer le paquet :
 - **Routage statique :** Ce sont des routes créées au démarrage de la machine ou ajoutées manuellement par l'administrateur système. Il est utilisé si peu de machine et les données de routage figées.
 - **Routage dynamique :** Il est utilisé si le réseau est vaste et complexe, sujet à des changements fréquents de configuration.
 - Il existe de nombreux protocoles pour le routage dynamique :
 - a) RIP
 - b) OSPF
 - c) EIGRP

LE ROUTAGE IP STATIQUE

- Très stable.
- Fastidieux à mettre en place et risque d'erreur important, si le réseau comporte plus de 10 routeurs.
- Il est réservé au cas simple comme pour
 - un poste de travail vers un seul routeur.
 - Un petit réseau : Quelques pc vers un routeur avec route par défaut FAI.
 - Pas de possibilité de routes redondantes.

ROUTAGE



Simulation Cisco Packet Tracer :

- ***Mise en place 4 pc, 2 switch et 2 routeur = Routage statique***
- ***Mise en place d'un réseau avec les principes VLSM***

10 – ROUTAGE DYNAMIQUE

LES PROTOCOLES DE ROUTAGE

- Un protocole de routage est un ensemble de processus, d'algorithmes et de messages que les routeurs se partagent dynamiquement.
- Il y a 2 grandes familles de routage dynamiques :
 - a. Interior Gateway Protocol (Protocole de routage intérieur) => IGP.
 - b. Exterior Gateway Protocol (Protocole de routage extérieur) => EGP.
- OSPF , EIGRP , RIPv2 et IS-IS sont des protocoles de routages dynamiques de type IGP.
- Il existe deux types de protocoles de routage dynamique IGP :
 1. A vecteur de distance (Distance Vector Routing Protocole).
 2. A état de lien (Link State Routing Protocole).

LES PROTOCOLES DE ROUTAGE

- Les **protocoles de routage à vecteur de distances** construisent eux mêmes les tables de routages.
- Par contre, aucun routeur ne possède la vision globale du réseau, car la diffusion des routes se fait uniquement de proche en proche.
- Dans **un protocole de routage à état de liens**, ici, chaque routeur connaît entièrement la topologie du réseau, c'est-à-dire que les routeurs ne se fient pas qu'à leurs voisins.
- Les routeurs qui exécutent des protocoles de routage échangent des messages afin de conserver leurs tables de routage à jour.

Lorsqu'un routeur se rend compte qu'il y'a eu une modification dans le réseau, ou bien un nouvel itinéraire, alors, il en informera ses voisins qui font partiit du même protocole de routage.

LES PROTOCOLES DE ROUTAGE

Les routeurs choisissent le meilleur chemin vers les réseaux de destination en fonction de plusieurs critères :

- **La Bande passante** : c'est le débit du lien entre routeurs.
- **Le Délai**: c'est la durée que met le paquet IP à se déplacer d'un point à un autre.
- **Le Cout**: qui est une valeur prédefinie, et qu'un admin réseau peut modifier manuellement s'il le souhaite.
- **Le Nombre de sauts** : qui est le nombre de routeurs qu'un paquet IP doit parcourir avant d'arriver à sa destination.

Pour déterminer le meilleur chemin vers une destination, les protocoles de routage utilisent une métrique.

Chaque protocole de routage dispose de sa propre métrique, et de sa propre façon de calculer le chemin le plus court, à l'aide de son algorithme.

LA DISTANCE ADMINISTRATIVE

Détails

Tableau distance administrative

Origine de la route	Distance administrative
Connecté	0
Statique	1
Résumé de routes EIGRP	5
BGP externe	20
EIGRP interne	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externe	170
BGP interne	200

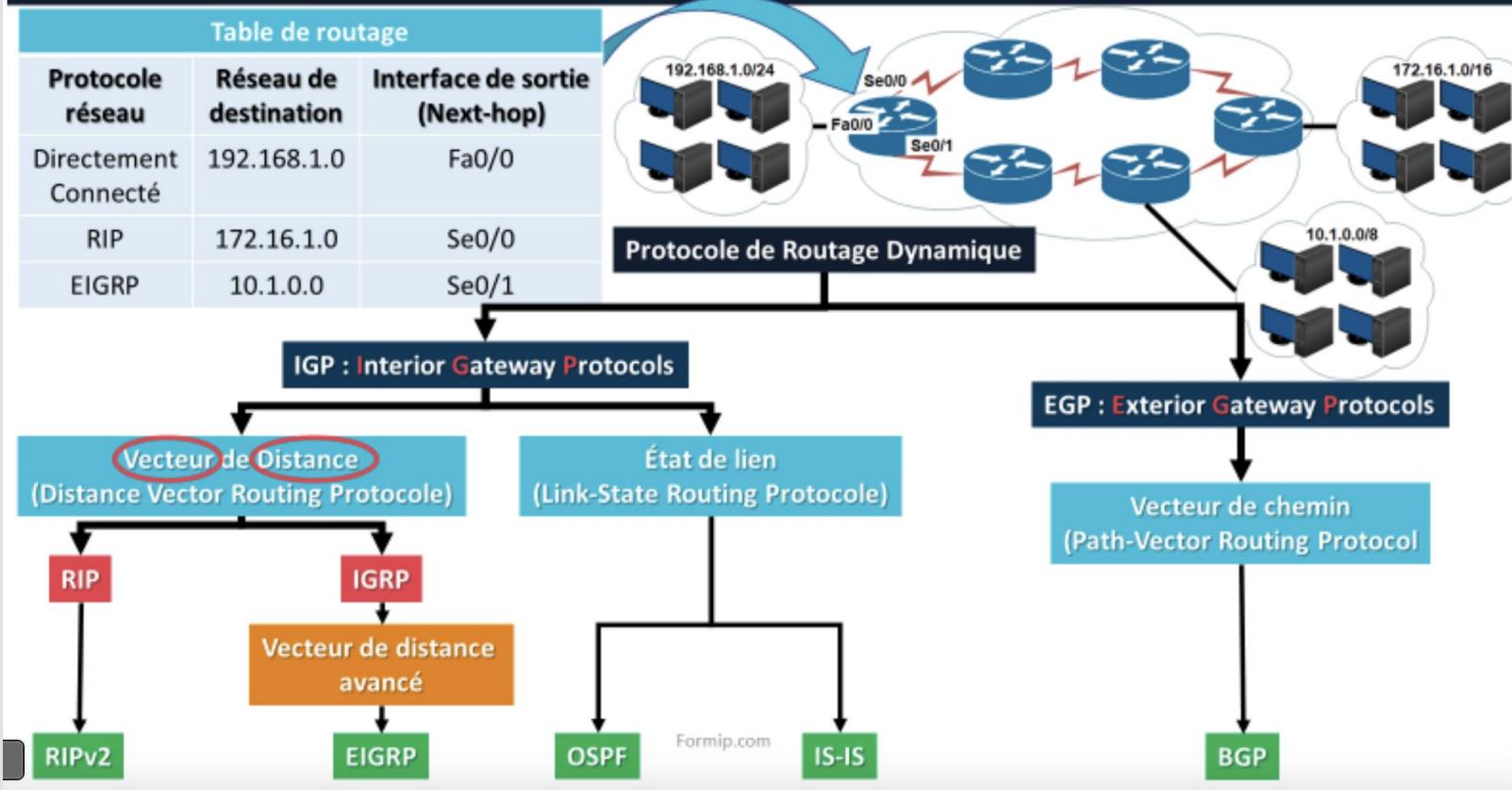
- La plupart des protocoles de routage ont des structures et des algorithmes métriques qui ne sont pas compatibles avec d'autres protocoles.
- La distance administrative est la fonctionnalité que les routeurs utilisent afin de sélectionner le meilleur chemin quand il y a deux routes ou plus vers la même destination à partir de deux protocoles de routage différents.
- Chaque protocole de routage est classé du plus fiable (crédible) au moins fiable, à l'aide d'une valeur de distance administrative.

LES PROTOCOLES DE ROUTAGE

		Interior Gateway Protocols			Exterior Gateway Protocols
		Distance Vector Routing Protocols	Link State Routing Protocols	Path Vector	
Classful		RIP	IGRP		EGP
Classless		RIPv2	EIGRP	OSPFv2	IS-IS
IPv6		RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6
					BGPv4 for IPv6

LES PROTOCOLES DE ROUTAGE

Protocoles de routage à vecteur de distance et à état de lien



II – LES PROTOCOLES DE ROUTAGE VECTEUR DE DISTANCE

RIP

- RIP (**Routing Information Protocol**) est un protocole de routage IP de type Vector Distance (à vecteur de distances) s'appuyant sur l'algorithme de détermination des routes décentralisé Bellman-Ford.
- **C'est un protocole normalisé** qui fait partie des protocoles IGP, c'est-à-dire du **routage interne**.
- **Le protocole RIP existe en 3 versions** (RIPv1, RIPv2 et Ripng pour l'IPv6).
- Il envoie à ses voisins routeurs, toutes les 30 secondes, sa table de routage complète en utilisant le **split-horizon** et **route-poisoning** :
 1. **Le split horizon** permet de transmettre à ses voisins uniquement les réseaux qui ne lui sont pas directement raccordés.
 2. **Le « Route poisoning »** permet de **supprimer les réseaux indisponibles des tables de routage**.

RIP

Exemple RIP (1/2)

192.168.10.0/24

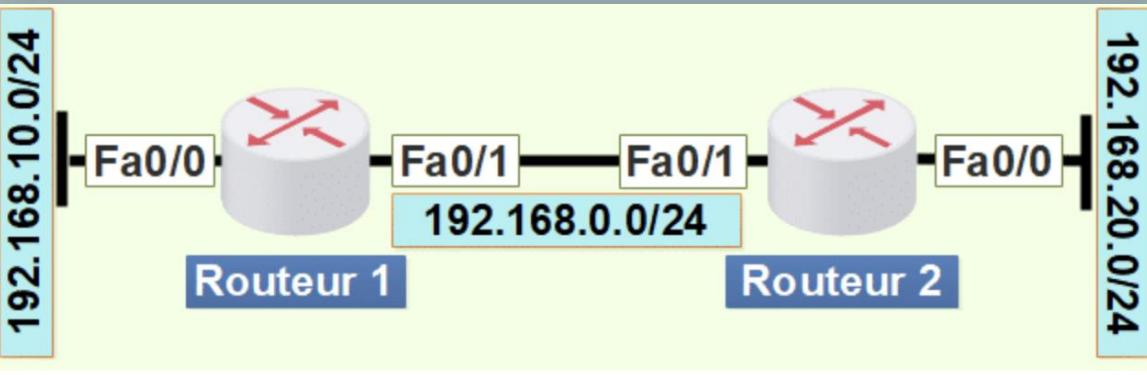


Table de routage R1

C	192.168.0.0	Fa0/1	metric_0
C	192.168.10.0	Fa0/0	metric_0
RIP	192.168.20.0	Fa0/1	metric_1

Table de routage R1

C	192.168.0.0	Fa0/1	metric_0
C	192.168.20.0	Fa0/0	metric_0
RIP	192.168.10.0	Fa0/1	metric_1

```
R1(config)# router rip  
R1(config-router)# version 2  
R1(config-router)# network 192.168.10.0  
R1(config-router)# network 192.168.0.0
```

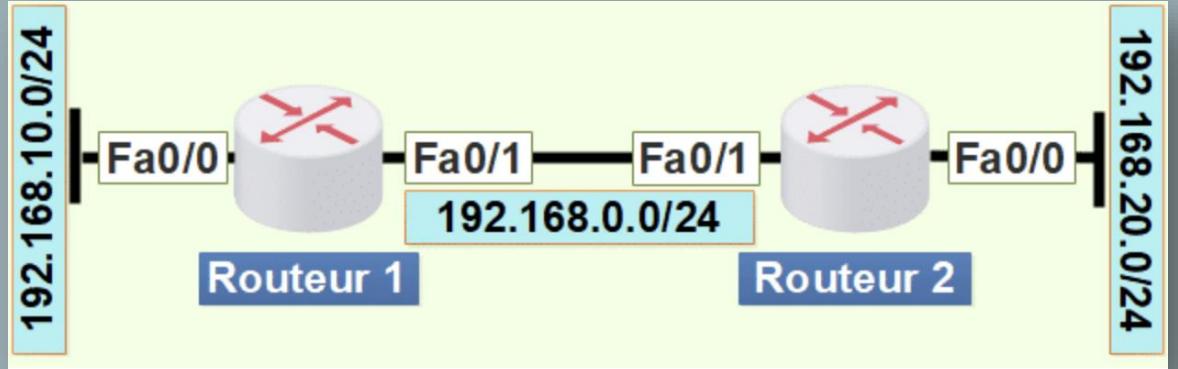
```
R2(config)# router rip  
R2(config-router)# version 2  
R2(config-router)# network 192.168.20.0  
R2(config-router)# network 192.168.0.0
```

- Avec 3 réseaux et 2 routeurs.
- Chaque Routeur connaît les 2 réseaux sur lesquels il est connecté directement (C) et le port sur lequel il peut être appelé.
- Grâce au split-horizon, les routeurs ne communiquent au routeur voisin que les informations de routage qu'il ne connaît pas (RIP).
- La métrique 0 indique qu'il n'y a pas de saut à effectuer pour accéder au réseau « 192.168.0.0 » accessible par son port Fa0/0.
- La métrique 1 indique qu'il y a 1 saut (soit un routeur) pour accéder au réseau 192.168.20.0 sur le port Fa0/1 du routeur R1.

Exemple RIP (2/2)

- Le « **Route poisoning** » va permettre de supprimer les routes indisponibles.
- Les routeurs envoient un message toutes les 30 secondes pour indiquer leurs tables de routages sont toujours opérationnelle => update.
- Si une modification intervient sur la table de routage d'un routeur, le routeur envoi un message RIP à **+ 0 à 5 secondes**.
- Et si un des routeurs ne reçoit pas de mise à jour, alors cela aura pour effet de déclencher différents types de timers :
 1. **Si au bout de 30 secondes**, il ne reçoit pas sa mise à jour, alors le *timer Invalid* se déclenche.
 2. **Après 180 secondes**, l'itinéraire est considéré comme invalide et placé dans le mode *Hold Down*.
Dans ce mode, les mises à jour de cette route seront ignorées pendant 180 secondes, à moins qu'elle obtienne une métrique plus faible (la metrique dans ce mode est 16 => infini).
 3. **Et par contre, si au bout de 240 secondes**, la route est toujours indisponible, alors elle sera **supprimée de la table de routage => mode flush**.

RIP



```
R1# show ip route
C 192.168.10.0/24 is directly connected
C 192.168.0.0/24 is directly connected
R 192.168.20.0/24 [120/1] via 192.168.0.2
```

```
R2# show ip route
C 192.168.20.0/24 is directly connected
C 192.168.0.0/24 is directly connected
R 192.168.10.0/24 [120/1] via 192.168.0.1
```

Update : Mise à jour =>30s

Invalid : Itinéraire invalide => 180s

Hold Down : Mise à jour ignoré => 180s

Flush : Suppression de la route => 240s

LES LIMITES DU RIP (RIPV1)

- Pour éviter les boucles de routage, le nombre de sauts est limité à 15. Au-delà, les paquets sont supprimés.
- Impossible de travailler avec des réseaux en VLSM
- MAJ de la table de routage par broadcast sans les netmasks (utilise les masques par défaut des classes IP).
- Aucune authentification pour protéger les informations de routage à travers le réseau.
- Le protocole RIPv2 a été créé pour répondre aux limitations du protocole RIPv1.

RIPV2

Les principales différences entre RIPv1 et RIPv2

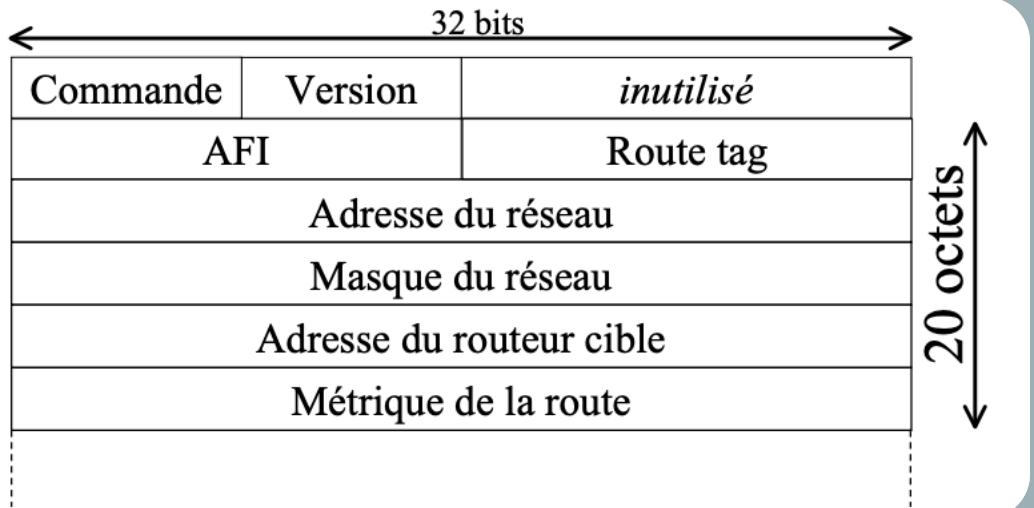
- **Transmission d'un masque de sous-réseau avec les routes.** Cette fonctionnalité permet à RIPv2 de supporter le VLSM (masque à longueur variable).
- **Authentification.** L'authentification d'une mise à jour de routage peut se faire en clair ou de manière cryptée (MD5). La première est prévue dans la RFC et l'autre a été ajoutée par Cisco
- **Inclusion l'adresse IP du prochain saut dans la mise à jour de routage.** Un routeur peut annoncer une route mais diriger tous les autres routeurs à l'écoute vers un différent routeur vers un même sous-réseau. Cette fonction est uniquement utilisée lorsqu'un routeur dispose d'une meilleure route.
- **Emploi d'indicateurs de routes externes (route tag).** RIP peut transmettre des informations sur les routes découvertes par le biais d'une source externe et redistribuées dans RIP.
- **Envoi de mises à jour de routage à une adresse Multicast.** Au lieu d'envoyer des mises à jour avec l'adresse de diffusion (Broadcast) 255.255.255.255, RIPv2 les envoie vers l'adresse de Multicast 224.0.0.9 . Cette fonctionnalité réduit la charge de traitement requise sur les hôtes qui ne prennent aucune des deux versions de RIP en charge au sein d'un même réseau.

RIPv2

Les caractéristiques RIPv1 et RIPv2

Caractéristique	RIPv1	RIPv2
Méthode et algorithme	Vecteur de distance, Bellman-Ford	<i>idem</i>
Métrique, métrique infinie	Nombre de sauts, 16	<i>idem</i>
Distance administrative	120	<i>idem</i>
Compteurs	"update" 30 sec, "invalid" 180 sec, "holddown" 180 sec, "flush" 240 sec	<i>idem</i>
Encapsulation	UDP 520	<i>idem</i>
Anti-bouclage	"Split-horizon with poison reverse", "triggered updates"	<i>idem</i>
Répartition de charge	égale (4 par défaut)	<i>idem</i>
Type	Classful	Classless
Nombre de routes par MàJ	25	25 (24 avec l'authentification)
Adresse de destination	255.255.255.255	224.0.0.9
Authentification	Non	Oui
RFC	RFC 1058	RFC2453

PAQUET RIPV2



```
▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: 00:77:3b:49:19:02 (00:77:3b:49:19:02), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
▶ Internet Protocol Version 4, Src: 192.168.3.1, Dst: 224.0.0.9
▶ User Datagram Protocol, Src Port: 520, Dst Port: 520
▶ Routing Information Protocol
```

```
  Command: Response (2)
  Version: RIPv2 (2)
  IP Address: 192.168.1.0, Metric: 1
    Address Family: IP (2)
    Route Tag: 0
    IP Address: 192.168.1.0
    Netmask: 255.255.255.0
    Next Hop: 0.0.0.0
    Metric: 1
```

Format paquet Ripv2

- **Commande** : indique si le paquet est une requête ou une réponse. La requête est une demande d'avoir la table des informations de routage. La réponse peut être non sollicitée (cas des émissions régulières faites par les routeurs) ou sollicitée par une requête.
- **Version** : 2 actuellement (la version 1 de RIP n'est plus utilisée).
- **AFI** : (Address Family Identifier) type de protocole.
- **Route tag** : marqueur qui peut être utilisé pour distinguer les routes internes (au protocole (apprises par RIP) des routes apprises par d'autres protocoles (ex. OSPF)).
- **Adresse du réseau** : Adresse IP donnant le préfixe.
- **Masque du réseau** : champ binaire dont les bits positionnés à 1 donnent la longueur du préfixe.
- **Adresse du routeur cible** : adresse IP où il faut router les paquets à destination du réseau cible.
- **Métrique** : valeur de la métrique (nombre compris entre 1 et 15).

AUTHENTIFICATION EN RIPV2

```
R2#conf t  
R2(config)#key chain TEST123  
R2(config-keychain)#key 1  
R2(config-keychain-key)#key-string cisco123  
  
R2(config)#int fa0/0  
R2(config-if)#ip rip authentication key-chain TEST123  
R2(config-if)#ip rip authentication mode md5
```

Configuration sécurité routeur 3

```
R3#conf t  
R3(config)#key chain TEST123  
R3(config-keychain)#key 1  
R3(config-keychain-key)#key-string cisco123  
  
R3(config)#interface fa0/1  
R3(config-if)#ip rip authentication key-chain TEST123  
R3(config-if)#ip rip authentication mode md5
```

```
R2#debug ip rip  
RIP protocol debugging is on  
  
*Mar 11 03:50:30.331: RIP: received packet with MD5 authentication  
*Mar 11 03:50:30.331: RIP: received v2 update from 10.2.2.3 on FastEthernet0/0  
*Mar 11 03:50:30.331: 1.0.0.0/8 via 0.0.0.0 in 2 hops  
*Mar 11 03:50:30.335: 3.0.0.0/8 via 0.0.0.0 in 1 hops  
*Mar 11 03:50:30.335: 10.1.1.0/24 via 0.0.0.0 in 1 hops
```

Configuration sécurité routeur 2

Vérification avec la commande Debug

Avec mot de passe crypté MD5

Exemple avec 2 routeurs : R2 et R3

- L'authentification des routeurs va éviter d'avoir un routeur inséré dans un réseau de manière malveillante.
- Seul les routeurs authentifiés grâce à un mot de passe pourront partager des informations de routage.
 1. Définissez un trousseau de clés avec un nom.
 2. Définissez la ou les clés du trousseau.
 3. Spécifiez le mot de passe ou la chaîne clé à utiliser dans la clé.
 4. Activez l'authentification sur une interface et spécifiez le trousseau de clés à utiliser.
 5. Indiquez si l'interface doit utiliser l'authentification MD5.

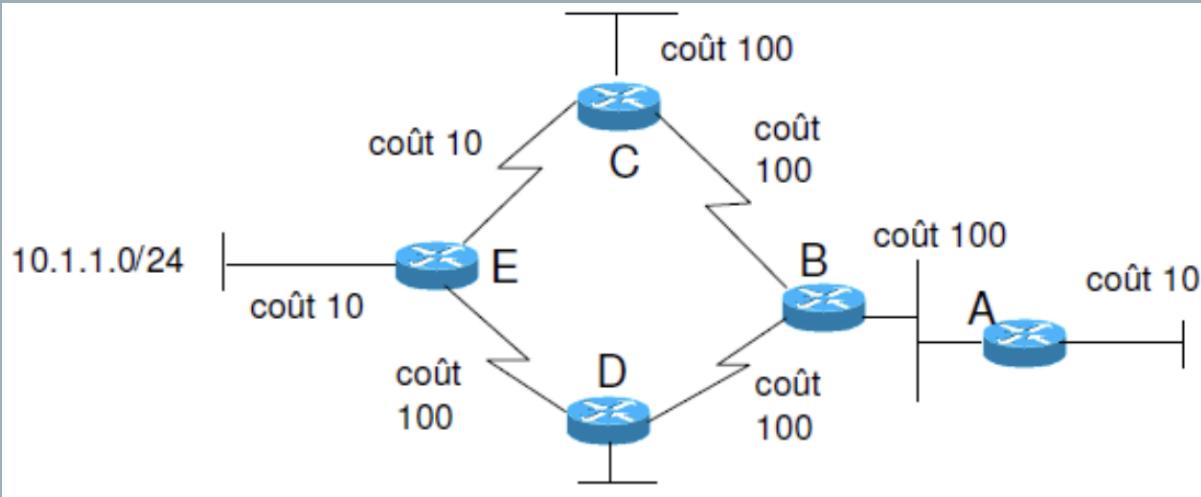
II – LES PROTOCOLES DE ROUTAGE A ÉTAT DE LIEN

OSPF

- **OSPF a été conçu pour s'affranchir des limitations de RIP :**
 - Possibilité de gérer des domaines de diamètre > 16 routeurs.
 - Amélioration du temps de convergence (changement de l'algorithme utilisé) => « temps de calcul d'un chemin ».
 - Métrique plus sophistiquée (prise en compte des débits).
 - Meilleure possibilité d'agrégation des routes.
 - Segmentation possible du domaine en aires.
- **Mais OSPF est aussi :**
 - Plus complexe (routeurs plus puissants, configuration moins simple que RIP)
- **Le protocole OSPF est un protocole de routage de type link-state ayant pour buts :**
 - Table de routage avec les meilleures routes.
 - Convergence la plus rapide possible.
- **Protocole à état de lien :**
 - Beaucoup de données sont transmises et nécessitent d'être traitées (utilisation de ressources +++).
 - Chaque routeur doit connaître ses voisins avant d'échanger avec lui des informations.

**OSPF : Open
Shortest
Path First**

FONCTIONNEMENT OSPF



- Les différentes routes pour aller de A vers 10.1.1.0/24 :
 - ✓ A vers 10.1.1.0/24 en passant par C : coût 220 (100+100+10+10)
 - ✓ A vers 10.1.1.0/24 en passant par D : coût 310 (100+100+100+10)
- Donc A mettra dans sa table de routage la route vers 10.1.1.0/24 passant par C.
- L'algorithme utilisé pour calculer les meilleures routes s'appelle « Shortest Path First Algorithm (SPF) » aussi appelé Algorithme de Djikstra.
- Les informations ne s'échangent pas en broadcast comme pour RIPv1 mais est précédée par une recherche des voisins.

LES PAQUETS OSPF



Les paquets utilisés

- **Hello packet** : permet de découvrir ses voisins et d'avertir son entourage de sa présence.
- **Database Description packets (DBD)** : contient un résumé de la base de données de chaque routeur dont les noms des routeurs connus.
- **Link-State Request Packets (LSR)** : permet de faire une demande d'informations complémentaire par rapport à sa DBD.
- **Link-State updates packets (LSU)** : décrivent les changements de topologie et contient 7 types de LSA (Link-State advertisements) différents (contenant le sous-réseau, le masque, la métrique et d'autres informations sur les sous-réseaux).
- **Link-State Acknowledgement packets (LSAck)** : accuse réception des paquets OSPF reçus.

SYNTHÈSE FONCTIONNEMENT OSPF

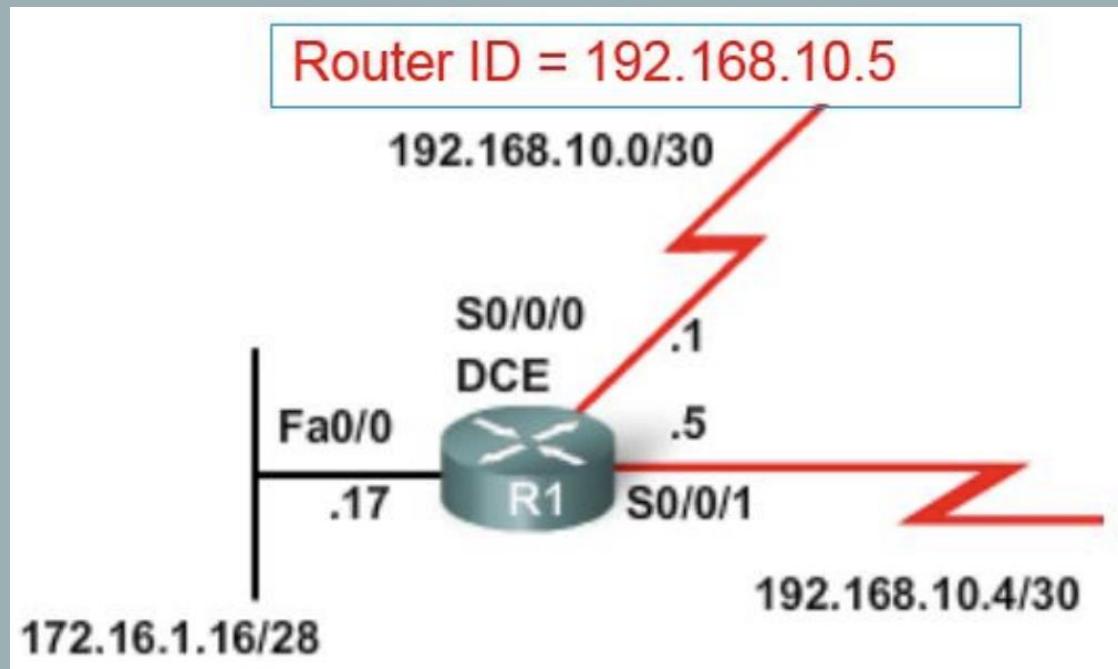
Les différentes étapes OSPF de chaque routeur :

1. Découvre son voisinage et conserve une liste de tous ses voisins
2. Utilise un protocole fiable pour échanger les informations topologiques avec les voisins (routeurs connectés directement).
3. Stocke les informations topologiques apprises dans leur BDD.
4. Exécute l'algorithme SPF pour calculer les meilleures routes.
5. Place la meilleure route vers chaque sous-réseau dans sa table de routage.

Chaque routeur possède :

- Une table de ses voisins : Neighbor Table
- Base de données de la topologie du réseau : Toplogy Database
- Une table de routage

L'IDENTIFICATION DU ROUTEUR OSPF



Un routeur est identifié par le RID (Router Identifier).

Le RID peut avoir pour valeur :

- ❖ Une valeur entrée manuellement par l'administrateur réseau
- ❖ Si le routeur possède une adresse de Loopback, il choisir la plus grande adresse de Loopback
- ❖ Sinon, il choisira la plus grande adresse IP de ses interfaces opérationnelles
- ❖ Attention : Le RID ne change pas, même si une nouvelle interface s'active. Les changements n'ont lieu que si le processus OSPF est réinitialisé (« clear ip ospf process »).

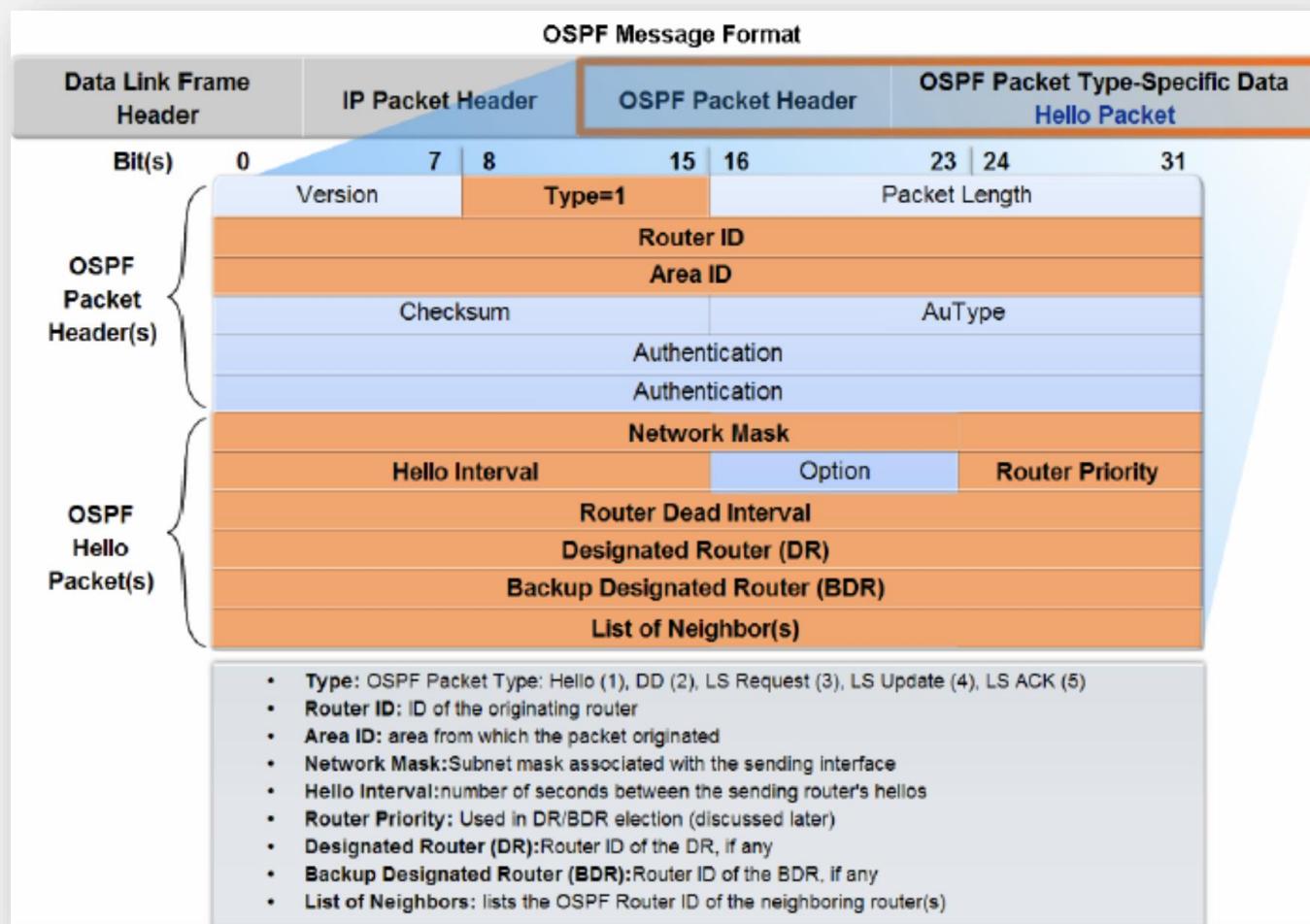
LA DÉCOUVERTE DES VOISINS OSPF (1/2)

- **Deux routeurs OSPF deviennent voisins s'ils possèdent une interface OSPF sur le même sous-réseau.**
- **Pour découvrir d'autres routeurs OSPF, le routeur diffuse par multicast un message du type OSPF Hello packet à destination de l'adresse 224.0.0.5 :**
 - Envoyés toutes les 10 secondes sur les réseaux supportant le broadcast.
 - Envoyés toutes les 30 secondes sur les autres réseaux (NBMA).
- **Ces paquets permettent de :**
 - Découvrir ses voisins.
 - Elire le Designated Router et le Backup Designated Router

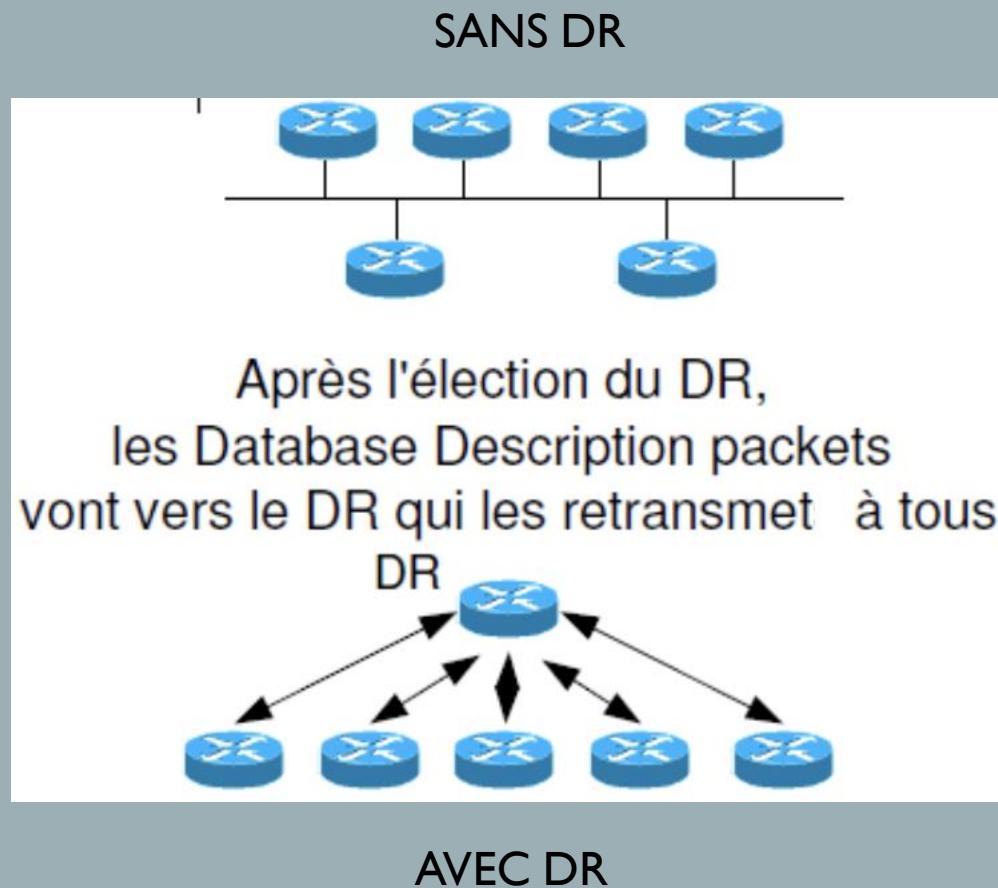
LA DÉCOUVERTE DES VOISINS OSPF (2/2)

- **Chaque routeur a besoin de savoir si le message Hello est bien arrivé à destination.**
- **Si routeur A reçoit d'un routeur B un message Hello :**
 - *Il va prévenir B qu'il a bien reçu son message Hello en ajoutant B dans la liste de ses voisins dans le prochain message Hello qu'il expédiera.*
 - *B fera de même en ajoutant A dans la liste de ses voisins dans son prochain message Hello.*
- **Dès qu'un routeur voit son propre RID dans la liste des voisins d'un paquet hello provenant d'un autre routeur, il sait qu'une « two-way communication » est établie.**
 - Des LSAs sont dès lors susceptibles d'être échangés.

EXEMPLE HELLO PAQUET



LE DESIGNATED ROUTER (DR)



Afin de diminuer le trafic réseau entre les routeurs, dans certains cas, un DR est élu. Ainsi tous les échanges ne se font qu'avec ce routeur désigné.

- Chaque routeur possède une priorité.
- Le routeur qui envoie un message Hello avec la plus grande priorité OSPF est élu DR et le second est élu BDR.
- En cas d'égalité de priorité (si on laisse la valeur par défaut) c'est le routeur avec le plus grand RID qui est élu DR.
- Une priorité de 0 signifie que le routeur ne sera jamais élu DR ou BDR.
- Attention, si un DR est élu et qu'un routeur apparaît avec une meilleure priorité, le DR ne sera réélu qu'en cas de défaillance du DR ou du BDR :
 - ✓ Si le DR est en panne, le BDR devient DR et un nouveau BDR est élu
 - ✓ Si le BDR est en panne, un nouveau BDR est élu.

ECHANGE DES DONNÉES ENTRE ROUTEUR OSPF

- Sur une interface sans DR (liaison point to point) les mises à jour OSPF sont envoyées directement à tous les voisins.
- Lorsqu'un DR existe, les routeurs DROTHER (non DR ou BDR) envoient leurs mises à jour au DR et BDR en utilisant l'adresse multicast **224.0.0.6**.
- Le DR relaie les mises à jour à tous les routeurs OSPF en utilisant l'adresse multicast **224.0.0.5**.
- Le BDR reçoit les mises à jours, mais ne les transmet pas.
- Les routeurs voisins échangent alors leur BDD entre eux. Dès qu'un routeur a fait cet échange, il est dit en état : « Full State ».
- Un routeur « Full State » échange des LSUs avec ses voisins.
- Donc : un routeur sera « Full State » avec un DR et un BDR et en « 2 way state » avec les autres routeurs DROTHERs.

RAPPEL : LA DISTANCE ADMINISTRATIVE

Description distance administrative

- La distance administrative est la fonctionnalité que les routeurs utilisent afin de sélectionner le meilleur chemin quand il y a deux routes ou plus vers la même destination à partir de deux protocoles de routage différents.
- La distance administrative définit la fiabilité d'un protocole de routage.
- Chaque protocole de routage est classé du plus fiable (crédible) au moins fiable, à l'aide d'une valeur de distance administrative.

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

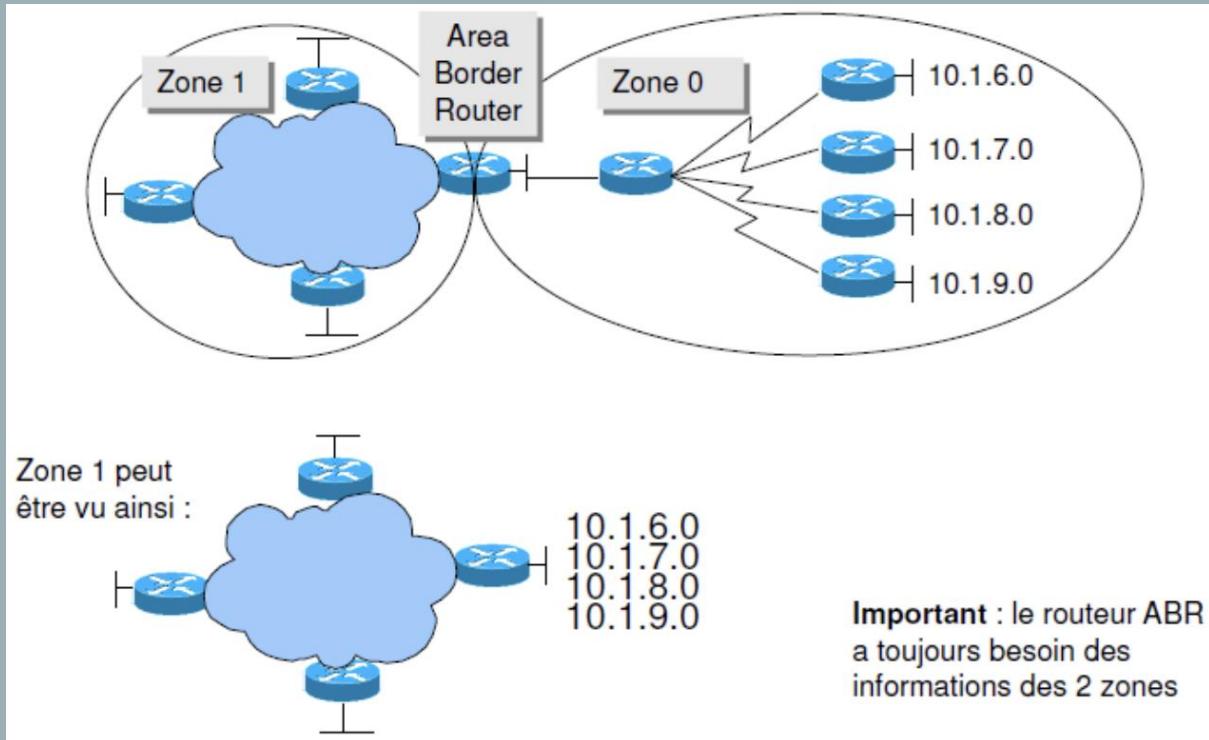
L'AUTHENTICATION OSPF

- Avec OSPF, comme avec la plupart des autres protocoles de routage (Ripv2), il est possible d'authentifier les paquets.
- 2 méthodes :
 - ❖ Authentification plaintext : transmission en clair du mot de passe.
 - ❖ Authentification message-digest (hash MD5).
- Attention : l'authentification ne chiffre pas les tables de routage.

LES ZONES OSPF

- **OSPF peut être utilisé sur de petits réseaux, ou sur des grands réseaux.**
- **Supposons maintenant que nous avons 1000 routeurs :**
 - Plus le réseau est grand, plus il faudra de mémoire pour stocker la topologie du réseau.
 - La résolution de l'algorithme SPF nécessitera plus de ressources de calcul.
 - Un simple changement de status forcera à re-exécuter sur tous les routeurs l'algorithme SPF.
- **C'est pour cela que lorsque le réseau devient trop important, on doit utiliser le mécanisme des zones OSPF.**

LES ZONES OSPF



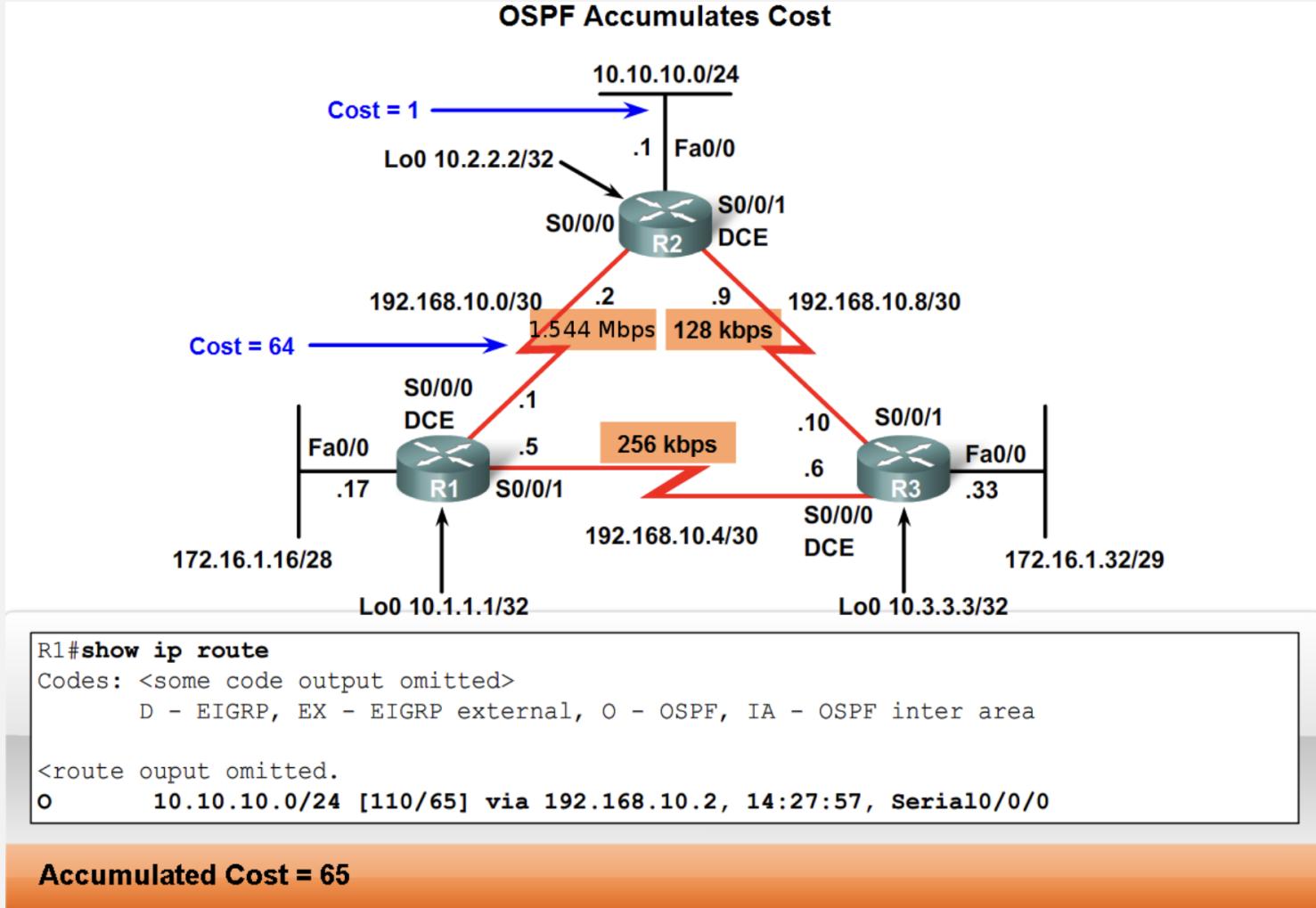
- **Les zones OSPF** permettent d'isoler des parties du réseau afin de diminuer la taille de la topologie réseau à mémoriser sur chaque routeur.
- **Dans un système sans zone**, les routeurs voient la topologie détaillé de son réseau, c'est-à-dire les routeurs, les liens vers les autres routeurs, etc... comme on peut le voir dans le premier schéma.
- **Avec la définition de zone**, chaque routeur de la zone 1, hors routeur ABR, ne voient des routeurs de la zone 2 que les sous-réseaux auxquels ils pourraient accéder.
- **Les routeurs de la zone 1 n'enregistrent plus les différentes routes possibles mais principalement les sous-réseaux accessibles dans la zone 2.**
- **Chaque routeur d'une zone dispose de la topologie détaillée de sa zone mais pas de celle des autres zones.**
- **Cela permet de réduire la taille de la bdd et des tables de routage => performance améliorée.**

LES COUTS OSPF

Interface Type	$10^8/\text{bps} = \text{Cost}$
Fast Ethernet and faster	$10^8/100,000,000 \text{ bps} = 1$
Ethernet	$10^8/10,000,000 \text{ bps} = 10$
E1	$10^8/2,048,000 \text{ bps} = 48$
T1	$10^8/1,544,000 \text{ bps} = 64$
128 kbps	$10^8/128,000 \text{ bps} = 781$
64 kbps	$10^8/64,000 \text{ bps} = 1562$
56 kbps	$10^8/56,000 \text{ bps} = 1785$
28 kbps	$10^8/28,000 \text{ bps} = 3571$
14 kbps	$10^8/14,000 \text{ bps} = 7143$

- **OSPF calcule le cout d'un lien par la formule :**
 - $10^8 / \text{bande passante.}$
- **La meilleure route sera la route avec le plus petit cout.**
- **La référence pour la bande passante est 100 Mb/s.**
- **Possibilité de la modifier avec la commande «bandwidth 'bande passant en kb'».**

LES COUTS OSPF



EIGRP

- Enhanced Interior Gateway Routing Protocol est un protocole de routage à vecteur de distance avancé ou Hybride propriétaire. Il est créé par Cisco.
- Un protocole de routage dynamique est dit être **hybride** quand celui-ci possède à la fois des fonctionnalités d'algorithmes de routage à vecteur distance et d'algorithmes de routage à états de liens
- OSPF => Mise en relation avec ses voisins.
- On utilise un algorithme DUAL.
- Utilise les métriques suivantes :
 - bande passante (par défaut)
 - le délai (par défaut)
 - la fiabilité
 - la charge (MTU)
- Il concurrence les standard OSPF.
- Distance administrative pour les routes internes: 90 (valeur par défaut).

IGRP -> EIGRP

- **EIGRP est une version avancée d'IGRP :**
 - Converge plus vite qu'IGRP
 - Tous 2 propriétaires Cisco
 - EIGRP envoie d'abord toutes ses informations de routage à un voisin et ensuite seulement des mises à jour :
 - IGRP envoie régulièrement (toutes les 90 s.) la totalité de sa table de routage
 - EIGRP fonctionne avec Novell IPX et Apple AppleTalk, en plus d'IP, contrairement à IGRP

LES AVANTAGES EIGRP

1. Il prend en compte la bande passante et le délai.
2. Vitesse de convergence instantanée grâce l'algorithme DUAL (Diffusion Update Algorithme).
3. Null besoin d'une cartographie complète => Il fait confiance à son réseau => Pas de perte de temps pour trouver le meilleur chemin.
4. Répartition de charge égale des routes, mais aussi répartition de charge inégale de routes.
5. Authentification : EIGRP permet l'utilisation de hash comme MD5 et SHA-2 pour la communication entre deux routeurs (authentification et chiffrage des messages).
6. Chaque route possède une route secondaire.

LES TABLES EIGRP

EIGRP fonctionne avec 3 tables :

Table de voisinage *EIGRP Neighbors table*

Elle va stocker l'identité des routeurs voisins dans un même sous-réseau.

Table de topologie *EIGRP topology table*

Elle va stocker la topologie du réseau après échange avec ses routeurs voisins

Table de routage

Elle va stocker les routes avec les métriques plus faibles qui sont issues de l'analyse de la topologie.

FONCTIONNEMENT EIGRP

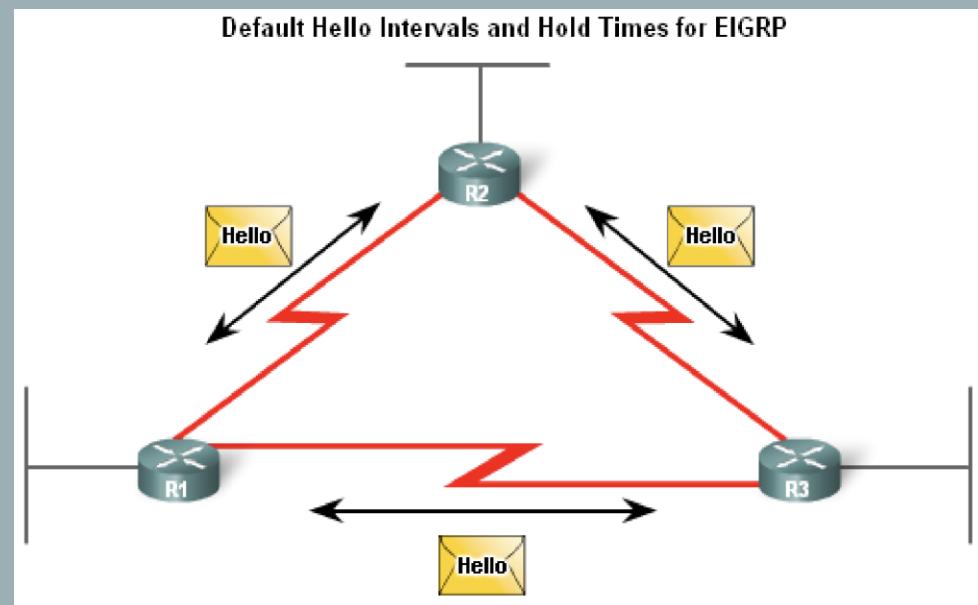
- Quand **2 routeurs se sont mutuellement découvert** voisins, ils échangent complètement leur table de routage.
- Ensuite, des messages **Hello** sont constamment échangés afin de manifester sa présence, comme OSPF. L'intervalle de temps séparant 2 messages Hello est par défaut de
 - 5 secondes sur un **LAN** ou connexion PPP
 - 60 secondes sur un **WAN** multi-points comme Frame Relay
- Quand une modification topologique est constatée, seules les nouveautés sont échangées, comme OSPF,
 - par multicast à l'adresse 224.0.0.10, si plusieurs routeurs doivent être prévenus
 - par unicast dans le cas contraire Les mises à jour sont envoyées via le protocole RTP (Reliable Transport Protocol  UDP Ou TCP).

LES TYPES DE MESSAGE EIGRP

EIGRP utilise 5 types de message :

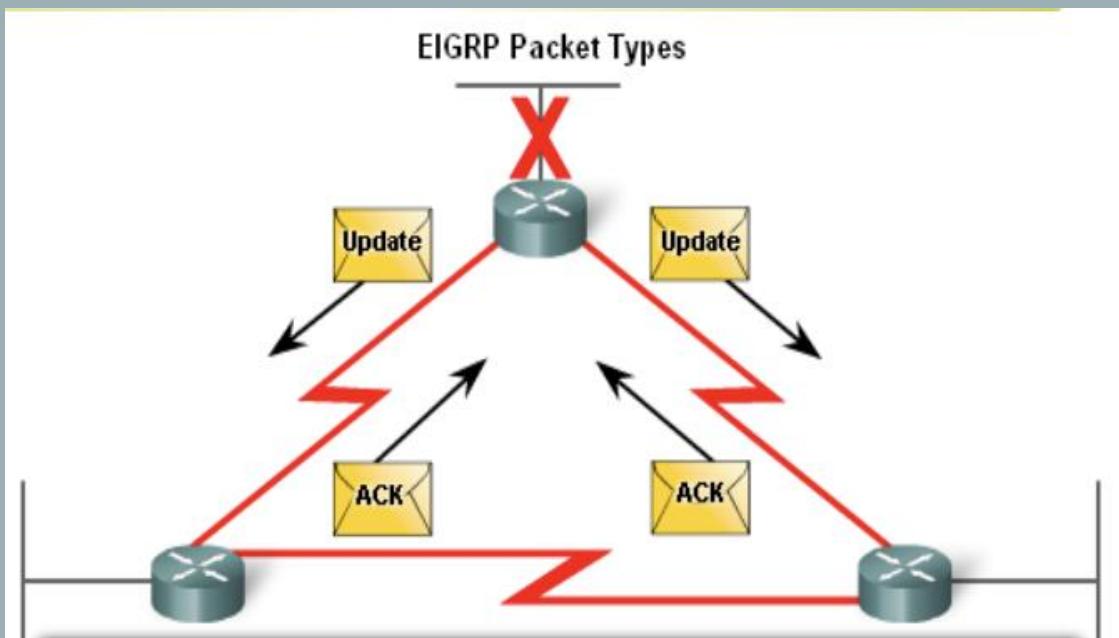
- ***Hello packets***
- ***Update packets***
- ***Acknowledgement packet***
- ***Query packets***
- ***Reply packets***

FOCUS HELLO PAQUETS



- Permet de découvrir les voisins.
- Envoie toutes :
 - Les 5 secondes sur la plupart des réseaux
 - Les 60 secondes sur le Non Broadcast Multi-access Networks (NBMA).
- C'est le temps maximum qu'un routeur peut attendre avant de déclarer un routeur absent :
 - Holdtime Par défaut : 3 fois le hello intervalle

FOCUS UPDATE PAQUETS



- EIGRP n'envoie des mises à jour que si des changements sont constatés.
- Partial update :
 - *N'inclut que les informations de routage ayant été modifiées*
- Bounded update :
 - *Quand une route change, seules les routeurs concernés par ce changement seront prévenus grâce à des partials updates.*
- EIGRP utilise des partial bounded updates pour minimiser l'utilisation de la bande passante.

LA MÉTRIQUE EIGRP

EIGRP Composite Metric

Default Composite Formula:
metric = **[K1*bandwidth + K3*delay]*256**

Complete Composite Formula:
metric = **[K1*bandwidth + (K2*bandwidth)/(256 - load) + K3*delay] * [K5/(reliability + K4)]*256**
(Not used if "K" values are 0)

```
R1#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
```

- **EIGRP utilise comme métrique une association des paramètres suivants :**
 - La bande passante, le délai, la fiabilité et la charge.
- **EIGRP calcule les métriques sur base de 5 paramètres combinés à 5 coefficients K :**

- **K1 Bande passante**
- **K2 Charge**
- **K3 Délai**
- **K4 Fiabilité**
- **K5 MTU**

LA MÉTRIQUE EIGRP

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: Link to R2
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 3d22h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Slowest bandwidth: $(10,000,000/\text{bandwidth kbps}) * 256$

Plus the sum of the delays: $+ (\text{sum of delay}/10) * 256$

= EIGRP metric

```
R2#show ip route
<output omitted>
D  192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:02:14, Serial0/0/1
```

- **Les valeurs des paramètres de calcul sont récupérables au travers des informations contenues dans les interfaces :**

- ❖ **BW** (Bande passante) en kbit.
- ❖ **DLY** (delai) en usec (microseconde).
- ❖ **Rehability** sous forme de fraction.
- ❖ **Load en 2 parties** -> **txload** (traffic envoi) et **rxload** (traffic reception)

LA MÉTRIQUE EIGRP

```
R2#show inter ser 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
<remaining output omitted>
<remaining output omitted>
```

```
R3#show inter fa 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0002.b9ee.5ee0 (bia 0002.b9ee.5ee0)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<remaining output omitted>
```

$$\text{delay} = [(20000/10) + (100/10)] * 256 = 514560$$

Résultat pour la métrique vers le sous-réseau 192.168.1.0/24

$$\text{EIGRP Metric} = \text{bandwidth} + \text{delay} = 2499840 + 514560 = 3014400$$

Calcul délai pour la métrique vers le réseau 192.168.1.0/24

```
R2#show ip route
<code output omitted>

Gateway of last resort is not set

  192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D    192.168.10.0/24 is a summary, 00:00:15, Null0
D    192.168.10.4/30 [90/21024000] via 192.168.10.10, 00:00:15, Serial0/0/1
C    192.168.10.8/30 is directly connected, Serial0/0/1
  172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D    172.16.0.0/16 is a summary, 00:00:15, Null0
D    172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:15, Serial0/0/0
C    172.16.2.0/24 is directly connected, FastEthernet0/0
C    172.16.3.0/30 is directly connected, Serial0/0/0
  10.0.0.0/30 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, Loopback1
D  192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:15, Serial0/0/1
```

```
R2#show inter ser 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
<remaining output omitted>
```

```
R3#show inter fa 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0002.b9ee.5ee0 (bia 0002.b9ee.5ee0)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<remaining output omitted>
```

$$\text{bandwidth} = (10,000,000/1024) = 9765 * 256 = 2499840$$

Calcul BW avec la plus petite BW vers le sous-réseau de destination

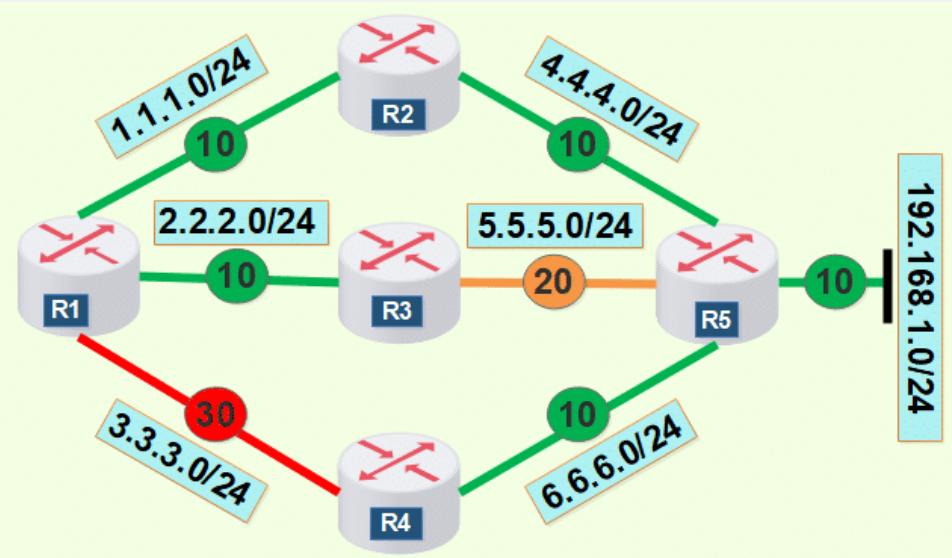
L'ALGORITHME DUAL

- **2 concepts importants** pour déterminer la meilleure route :
 - La « **Feasible Distance** » (FD) est la métrique pour un subnet du point de vue du routeur lui-même, utilisée pour choisir la meilleure route vers ce subnet.
 - La « **Reported Distance** » (RD) est la métrique pour un subnet du point de vue du routeur voisin. (La métrique annoncée par le routeur voisin).
- **Les routes sélectionnées sont :**
 - **Successor** : la route avec le plus faible FD est considérée comme la meilleure.
 - **Feasible Successor** : Il s'agit de la route de backup pour la route « Successor ». On la sélectionne à travers le RD.



La route sélectionnée sera enregistrée dans la table de routage.

L'ALGORITHME DUAL



R1	Table de Topologie	
	RD	FD
R2	20	30
R3	30	40
R4	20	50

Successor (FD la plus faible) ?

= Routeur 2

Feasible Successor ?

< 30

= Routeur 4

La « **Feasible Distance** » (FD) est la métrique pour un subnet du point de vue du routeur lui-même.,.

La « **Reported Distance** » (RD) est la métrique pour un subnet du point de vue du routeur voisin.

COMPARAISON EIGRP - OSPF