

# INF3050 Réseaux Informatiques

Bassem Haidar

# Plan du cours

---

- Introduction, Modèle OSI et TCP-IP
- Couche Physique – Supports de transmission
- Couche Liaison – Ethernet
- **Couche Réseaux – Adressage IPv4**
- ARP - ICMP – DHCP
- Routage statique
- Couche Transport (UDP - TCP)
- Introduction a la couche application

# Couche Réseaux

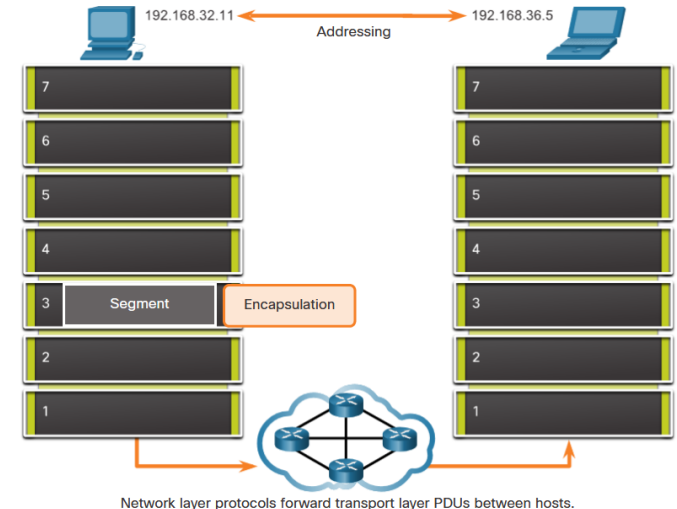
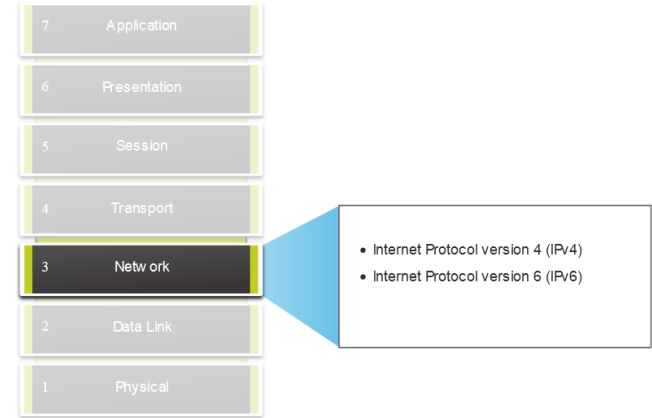
## Chapter 04

# Caractéristiques de la couche réseau

# Caractéristiques de la couche réseau

## Couche réseau

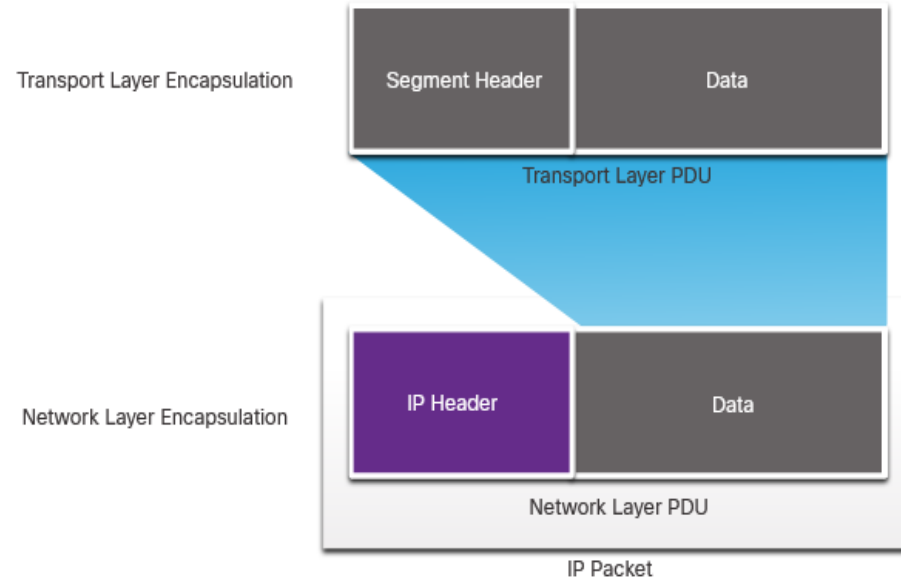
- Fournit des services qui permettent aux périphériques finaux d'échanger des données
- IP version 4 (IPv4) et IP version 6 (IPv6) sont les principaux protocoles de communication de couche réseau.
- La couche réseau effectue quatre opérations de base :
  - Adressage des périphériques finaux
  - Encapsulation
  - Routage
  - Désencapsulation



# Caractéristiques de la couche réseau

## Encapsulation de l'IP

- Le protocole IP encapsule le segment de couche transport.
- IP peut utiliser un paquet IPv4 ou IPv6 et n'affecte pas le segment de couche 4.
- Les paquets IP seront examinés par tous les périphériques de couche 3 lorsqu'ils traversent le réseau.
- L'adresse IP est identique de la source à la destination.
- Remarque: le NAT modifiera l'adressage, mais sera abordé dans un module ultérieur.



# Caractéristiques de la couche réseau

## Caractéristiques de l'IP

---

- IP est conçu pour avoir de faibles frais généraux et peut être décrit comme :
  - Sans connexion
  - Acheminement au mieux
  - Indépendant vis-à-vis des supports

# Caractéristiques de la couche réseau

## Sans connexion

- IP est Sans connexion
- L'IP n'établit pas de connexion avec la destination avant d'envoyer le paquet.
- Aucune information de contrôle n'est nécessaire (synchronisations, accusés de réception, etc.).
- La destination recevra le paquet à son arrivée, mais aucune pré-notification n'est envoyée par IP.
- S'il y a un besoin de trafic orienté de connexion, un autre protocole s'en chargera (typiquement TCP au niveau de la couche de transport).



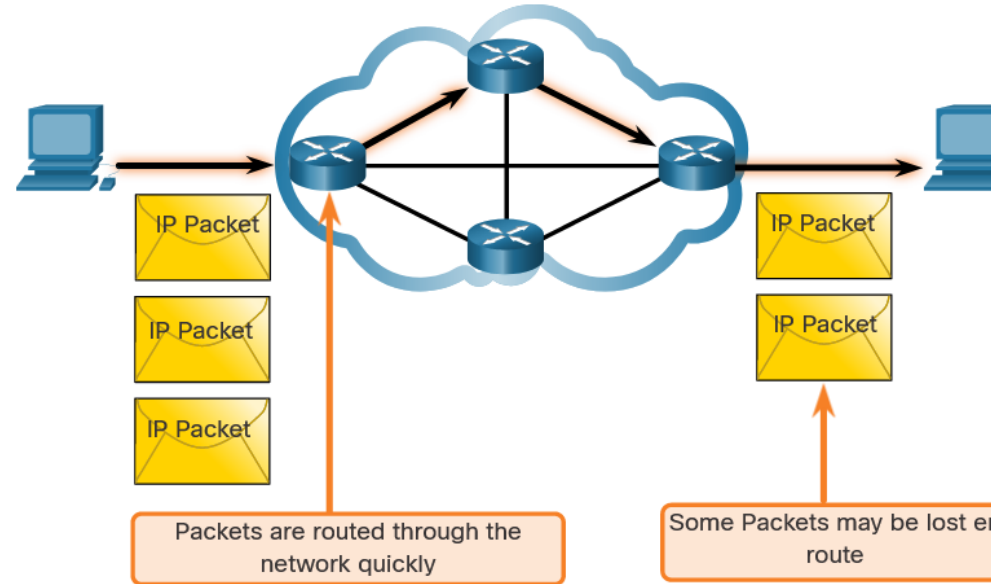
A letter is sent.



# Caractéristiques de la couche réseau

## Acheminement au mieux

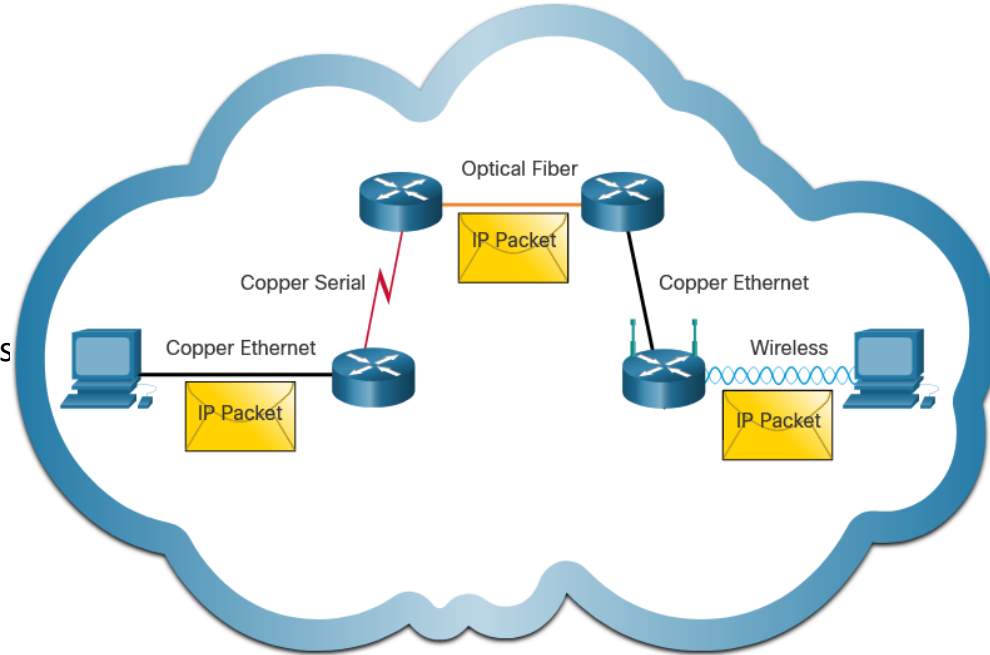
- L'IP est l'acheminement au mieux
- IP ne garantit pas la livraison du paquet.
- IP a réduit les frais généraux car il n'existe aucun mécanisme qui permet de renvoyer des données qui ne sont pas reçues.
- IP ne s'attend pas à des accusés de réception.
- IP ne sait pas si l'autre périphérique est opérationnel ou s'il a reçu le paquet.



# Caractéristiques de la couche réseau

## Indépendant vis-à-vis des supports

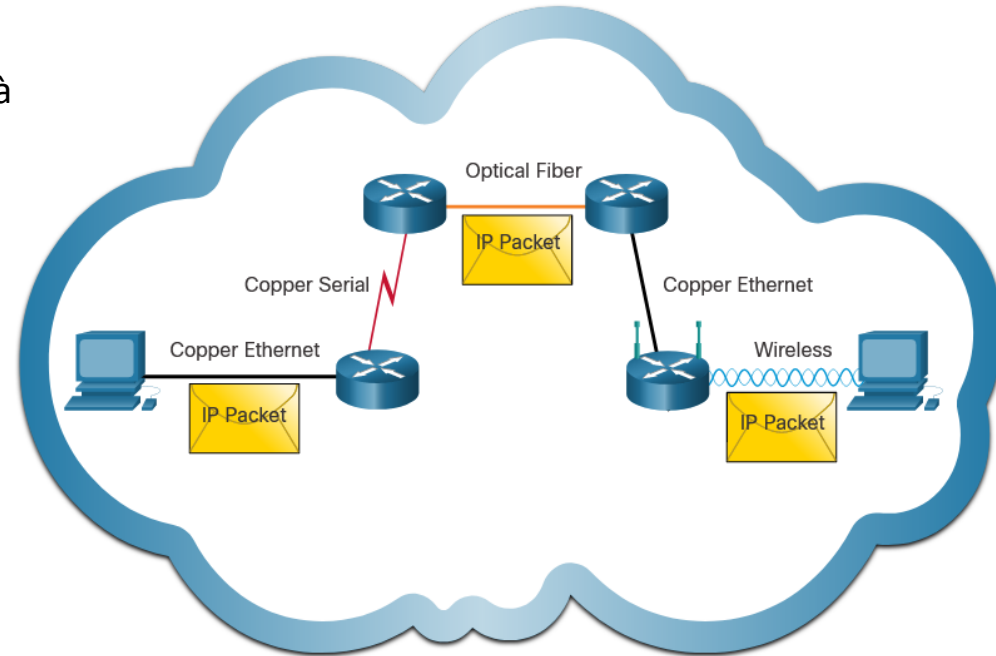
- L'IP n'est pas fiable :
  - Il ne peut pas gérer ou réparer les paquets non livrés ou corrompus.
  - L'IP ne peut pas être retransmis après une erreur.
  - IP ne peut pas se réaligner sur des paquets hors séquence.
  - IP doit s'appuyer sur d'autres protocoles grâce à ces caractéristiques.
- L'IP est indépendant vis-à-vis des supports.
  - IP ne concerne pas le type de trame requis dans la couche de liaison de données ou le type de support dans la couche physique.
  - IP peut être envoyé sur n'importe quel type de support: cuivre, fibre ou sans fil.



# Caractéristiques de la couche réseau

## Indépendant vis-à-vis des supports (suite)

- La couche réseau établira l'unité de transmission maximale (MTU).
  - La couche réseau reçoit ce message à partir des informations de contrôle envoyées par la couche de liaison de données.
  - Le réseau établit ensuite la taille MTU.
- La fragmentation est lorsque la couche 3 divise le paquet IPv4 en unités plus petites.
  - La fragmentation provoque une latence.
  - IPv6 ne fragmente pas les paquets.
  - Exemple : Le routeur passe d'Ethernet à un WAN lent avec une MTU est inférieure.



# Paquet IPv4

# Paquet IPv4

## En-tête de paquet IPv4

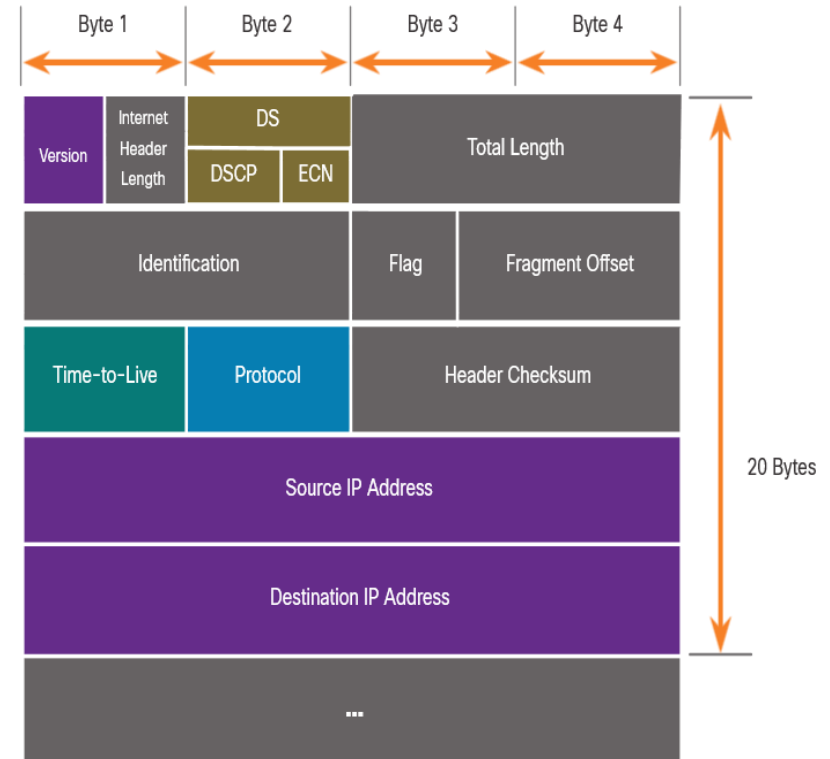
---

- IPv4 est le protocole de communication principal pour la couche réseau.
- L'en-tête réseau a de nombreux objectifs :
  - Il garantit que le paquet est envoyé vers la meilleure direction (vers la destination).
  - Il contient des informations pour la gestion de couche réseau dans différents domaines.
  - Les informations contenues dans l'en-tête sont utilisées par tous les périphériques de couche 3 qui gèrent le paquet

# Paquet IPv4

## Champs de l'en-tête du paquet IPv4

- Caractéristiques de l'en-tête réseau IPv4 :
  - C'est en binaire.
  - Contient plusieurs champs d'information
  - Le diagramme est lu de gauche à droite, 4 octets par ligne
  - Les deux champs les plus importants sont la source et la destination.
- Les protocoles peuvent avoir une ou plusieurs fonctions.



# Paquet IPv4

## Champs de l'en-tête du paquet IPv4

- Les champs importants de l'en-tête IPv4 sont :

Fonction	Description
<b>Version</b>	Ce sera pour v4, par opposition à v6, un champ de 4 bits = 0100
<b>Des services différenciés</b>	Utilisé pour la QoS: champ DiffServ — DS ou l'ancien InServ — TOS ou Type de service
<b>Somme de contrôle d'en-tête</b>	Détecter la corruption dans l'en-tête IPv4
<b>Durée de vie (Time to Live, TTL)</b>	Nombre de tronçon de couche 3. Quand il devient zéro, le routeur rejettera le paquet.
<b>Protocole</b>	Protocole de niveau suivant : ICMP, TCP, UDP, etc.
<b>Adresse IPv4 source</b>	Adresse source 32 bits
<b>Adresse IP de destination</b>	Adresse de destination 32 bits

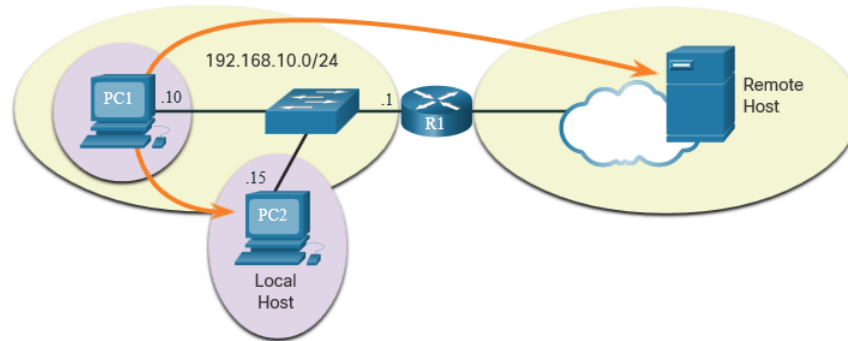
# Méthode de routage des hôtes



# Méthode de routage des hôtes

## Décisions relatives aux transmissions des hôtes

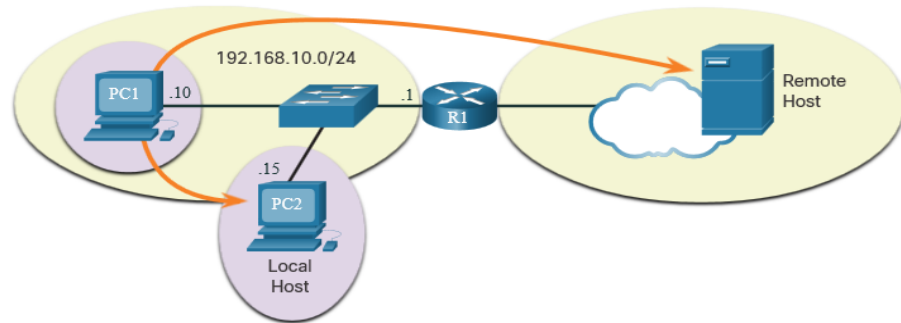
- Les paquets sont toujours créés à la source.
- Chaque unité hôte crée sa propre table de routage.
- Un hôte peut envoyer des paquets aux éléments suivants :
  - Lui-même — 127.0.0.1 (IPv4), ::1 (IPv6)
  - Hôtes locaux — la destination se trouve sur le même réseau local
  - Hôtes distants : les périphériques ne sont pas sur le même réseau local



# Méthode de routage des hôtes

## Décisions relatives aux transmissions des hôtes

- Le périphérique source détermine si la destination est locale ou distante
- Méthode de détermination :
  - IPv4 — La source utilise sa propre adresse IP et masque de sous-réseau, ainsi que l'adresse IP de destination
  - IPv6 — La source utilise l'adresse réseau et le préfixe annoncés par le routeur local
- Le trafic local est déchargé de l'interface hôte pour être géré par un périphérique intermédiaire.
- Le trafic distant est transféré directement à la passerelle par défaut sur le réseau local.



# Méthode de routage d'un hôte

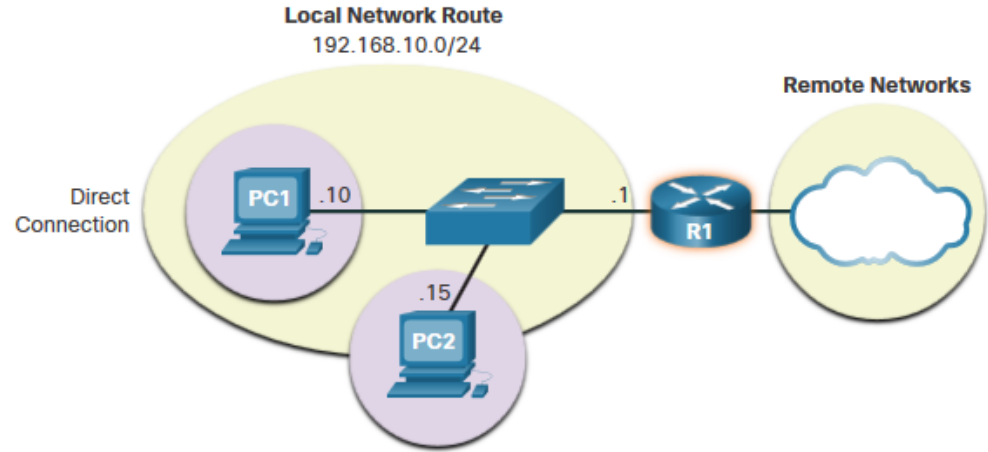
## Utilisation de la passerelle par défaut

- Un routeur ou un commutateur de couche 3 peut être une passerelle par défaut.
- Caractéristiques d'une passerelle par défaut (DGW) :
  - Il doit avoir une adresse IP dans la même gamme que le reste du réseau local.
  - Il peut accepter les données du réseau local et est capable de transférer le trafic hors du réseau local.
  - Il peut acheminer vers d'autres réseaux.
- Si un périphérique n'a pas de passerelle par défaut configuré ou une passerelle par défaut est incorrecte, son trafic ne pourra pas quitter le réseau local.

# Comment un hôte achemine

## Un hôte achemine vers la passerelle par défaut

- L'hôte connaîtra la passerelle par défaut (DGW) statiquement ou via DHCP dans IPv4.
- Une DGW est une route statique qui sera une route de dernier recours dans la table de routage.
- Tous les périphériques sur le LAN auront besoin de la DGW du routeur s'ils ont l'intention d'envoyer du trafic à distance.



# La méthode de routage des hôtes

## Les tables de routage des routeurs

- Sous Windows, utilisez les commandes `route print` ou `netstat -r` pour afficher la table de routage PC
- Trois sections affichées par ces deux commandes :
  - Liste des interfaces - toutes les interfaces potentielles et l'adressage MAC
  - Table de routage IPv4
  - Table de routage IPv6



IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r
```

### IPv4 Route Table

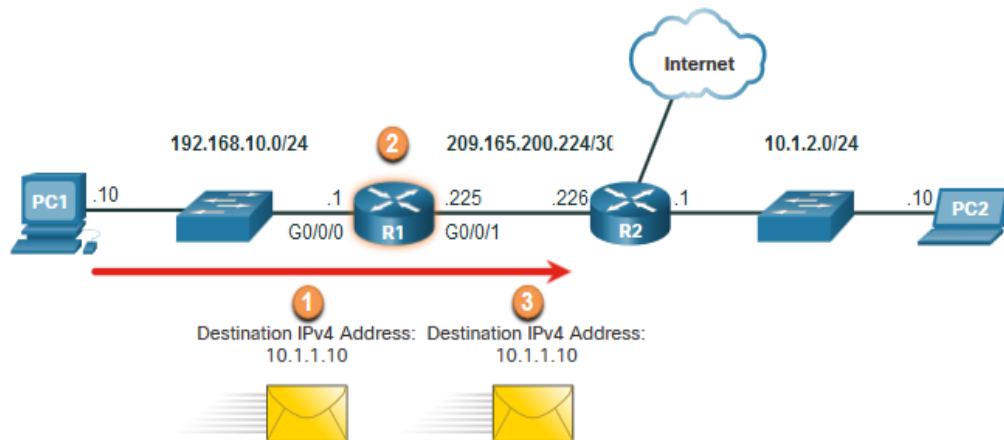
#### Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	192.168.10.0	255.255.255.0	On-link	192.168.10.10	281
	192.168.10.10	255.255.255.255	On-link	192.168.10.10	281
	192.168.10.255	255.255.255.255	On-link	192.168.10.10	281
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
	224.0.0.0	240.0.0.0	On-link	192.168.10.10	281
	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	255.255.255.255	255.255.255.255	On-link	192.168.10.10	281

# Présentation au routage

# Présentation au Routage La décision relatives à la transmission de paquet du routeur

- Que se passe-t-il lorsque le routeur reçoit la trame du périphérique hôte?



R1 Routing Table

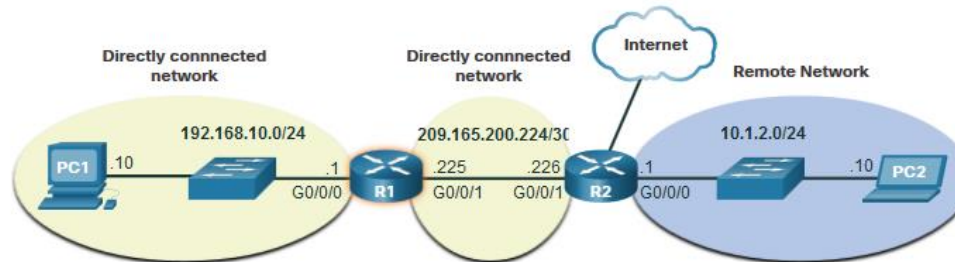
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
<b>10.1.1.0/24</b>	<b>via R2</b>
Default Route 0.0.0.0/0	via R2

1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

# Présentation au Routage

## La table de routage du routeur IP

- Il existe trois types d'itinéraires dans la table de routage d'un routeur:
- Directement connecté — Ces routes sont automatiquement ajoutées par le routeur, lorsqu'une interface est configurée avec une adresse IP et qu'elle est activée
- Routes distantes — Ce sont les routes que le routeur n'a pas de connexion directe et peuvent être apprises:
  - Manuellement — avec un itinéraire statique
  - Dynamiquement — en utilisant un protocole de routage pour que les routeurs partagent leurs informations entre eux
- Route par défaut - cela transfère tout le trafic vers une direction spécifique s'il n'existe aucune autre route jusqu'à un réseau souhaité dans la table de routage.

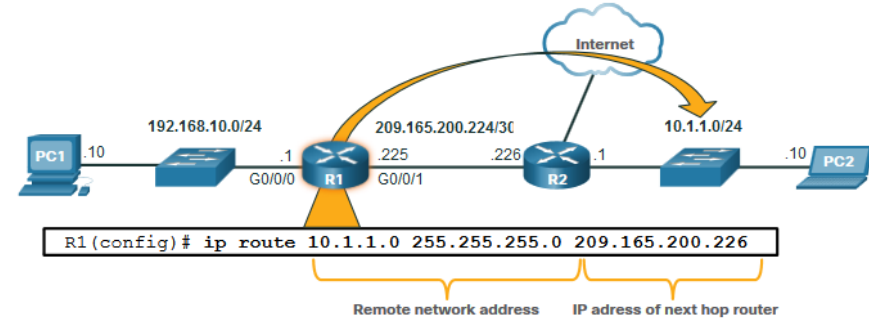




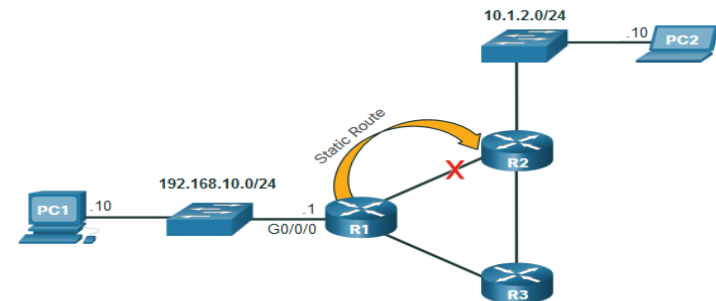
# Présentation au Routage

## Routage Statique

- Caractéristiques de routage statique :
  - Doit être configurées manuellement.
  - Doit être ajusté manuellement par l'administrateur en cas de modification de la topologie
  - Idéal pour les petits réseaux non redondants
  - Souvent utilisé conjointement avec un protocole de routage dynamique pour configurer un chemin par défaut



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.

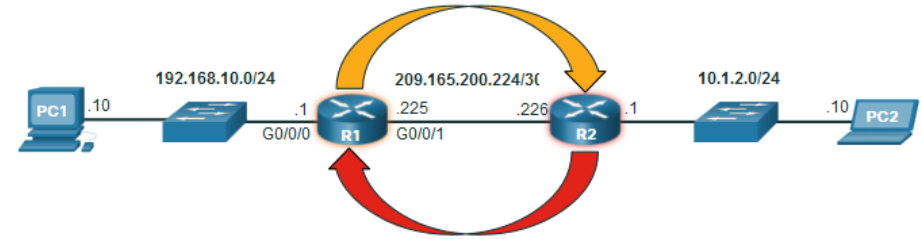


If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

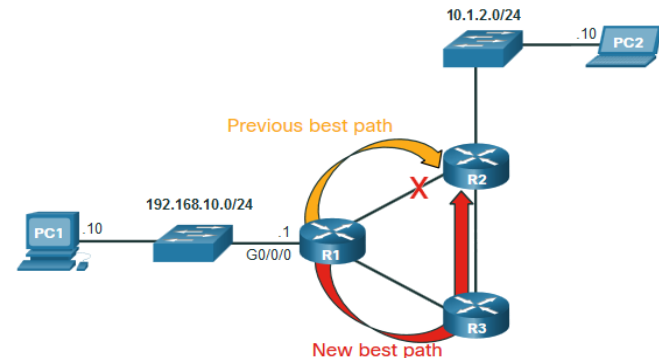
# Présentation au Routage

## Routage Dynamique

- Routes dynamiques automatiquement:
  - Découvrir les réseaux distants
  - Assurer l'actualisation des informations
  - Sélectionner le chemin le plus approprié vers un réseau de destination
  - Trouver de nouveaux meilleurs chemins lorsqu'il y a une modification de topologie
  - Le routage dynamique peut également partager des routes statiques par défaut avec les autres routeurs.



- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

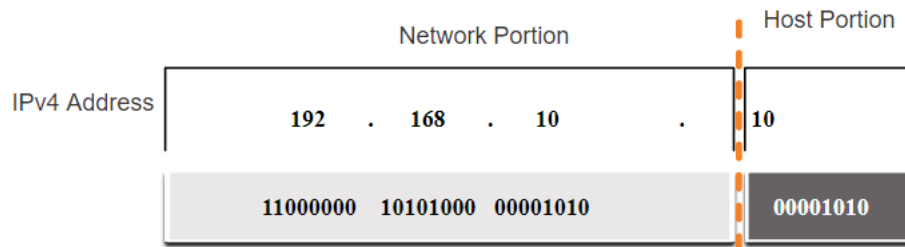
# Adressage IPv4

# Structure de l'adresse IPv4

# La structure d'une adresse IPv4

## Les parties réseau et hôte

- Une adresse IPv4 est une adresse hiérarchique de 32 bits qui se compose d'une partie réseau et d'une partie hôte.
- Lorsque vous déterminez la partie réseau et la partie hôte, il est nécessaire d'examiner le flux de 32 bits.
- Le masque de sous-réseau sert à déterminer la partie réseau d'une adresse IP.



# La structure d'une adresse IPv4

## Le masque de sous-réseau

- Pour identifier les parties réseau et hôte d'une adresse IPv4, chaque bit du masque de sous-réseau est comparé à l'adresse IPv4, de gauche à droite.

- En réalité, le processus utilisé pour identifier la partie réseau et la partie hôte est appelé l'opération AND.

	Network Portion				Host Portion
IPv4 Address	192	.	168	.	10
	11000000	10101000	00001010		00001010
Subnet Mask	255	.	255	.	0
	11111111	11111111	11111111		00000000

# La structure d'une adresse

## La longueur de préfixe

- Une longueur de préfixe est une méthode fastidieuse d'exprimer une adresse de masque de sous-réseau.
- En fait, la longueur de préfixe correspond au nombre de bits définis sur 1 dans le masque de sous-réseau.
- Elle est notée au moyen de la « notation de barre oblique », il suffit donc de compter le nombre de bits du masque de sous-réseau et d'y ajouter une barre oblique.

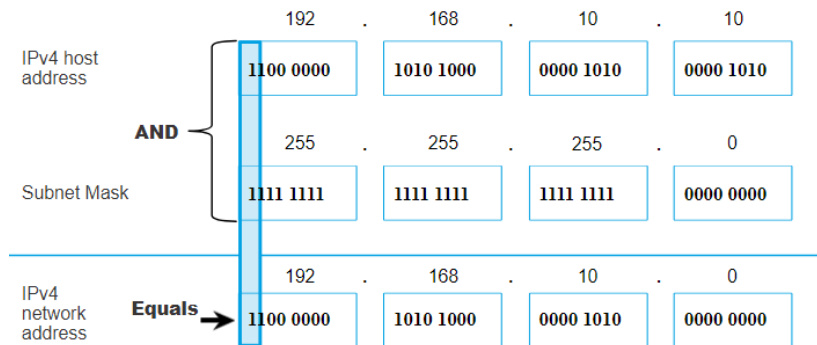
Masque de sous-réseau	Adresse 32 bits	Préfixe Longueur
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000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

# Structure d'adresse IPv4

## Détermination du réseau: AND (ET) logique

- Une opération logique AND est utilisée pour déterminer l'adresse réseau.
  - Le AND (ET) logique est la comparaison de deux bits où un 1 AND (ET) 1 produit un 1 et toutes les autres combinaisons produisent un 0.
  - $1 \text{ AND } 1 = 1$ ,  $0 \text{ AND } 1 = 0$ ,  $1 \text{ AND } 0 = 0$ ,  $0 \text{ AND } 0 = 0$
  - 1 = Vrai et 0 = Faux

Pour identifier l'adresse réseau, l'adresse IPv4 d'un hôte est soumise bit par bit à l'opération AND de manière logique avec le masque de sous-réseau

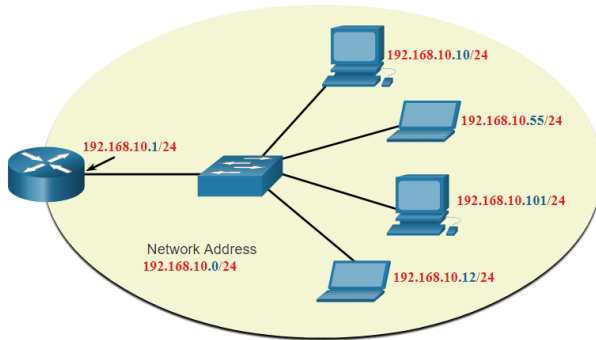




# La structure d'une adresse IPv4

## Adresses réseau, d'hôte et de diffusion

- Au sein de chaque réseau se trouvent trois types d'adresses IP:
  - Adresse réseau
  - Adresses d'hôtes
  - Adresse de diffusion



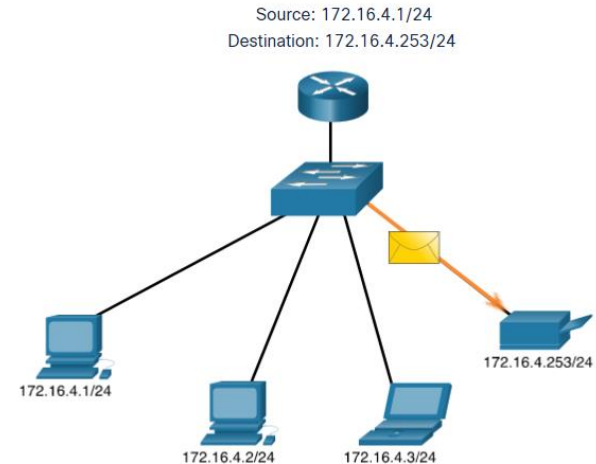
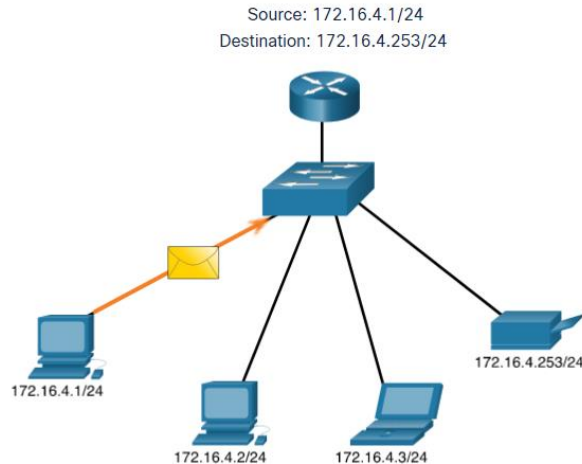
	Partie réseau	Partie hôte	Bits d'hôte
Masque de sous-réseau . <b>255.255.255.0 or /24</b>	255 255 255 11111111 111111 111111	0 00000000	
Adresse réseau <b>192.168.10.0 or /24</b>	192 168 10 11000000 10100000 00001010	0 00000000	All 0s
First address <b>192.168.10.1 or /24</b>	192 168 10 11000000 10100000 00001010	1 00000001	All 0s and a 1
Last address <b>192.168.10.254 or /24</b>	192 168 10 11000000 10100000 00001010	254 11111110	All 1s and a 0
Adresse de diffusion <b>192.168.10.255 or /24</b>	192 168 10 11000000 10100000 00001010	255 11111111	All 1s and a 0

# Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

# Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

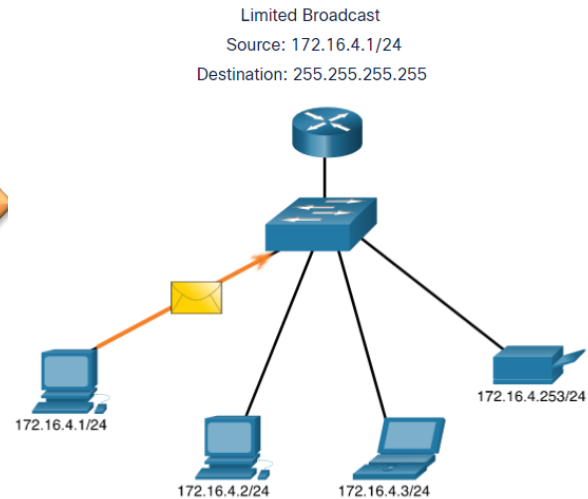
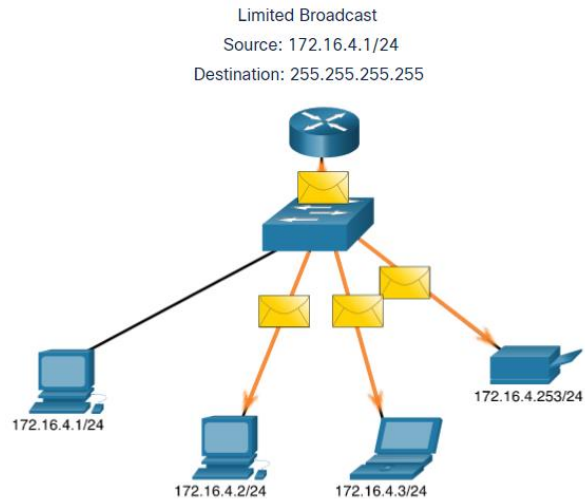
---

- La transmission monodiffusion envoie un paquet à une adresse IP de destination.
- Par exemple, le PC à 172.16.4.1 envoie un paquet monodiffusion à l'imprimante à 172.16.4.253.



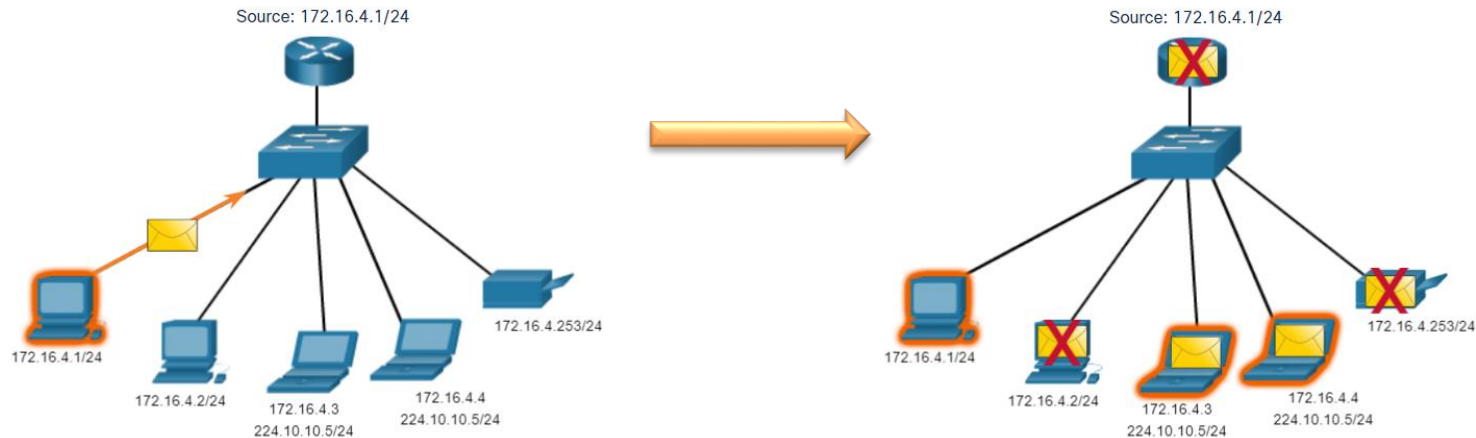
# Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

- La transmission de diffusion envoie un paquet à toutes les autres adresses IP de destination.
- Par exemple, le PC à 172.16.4.1 envoie un paquet de diffusion à tous les hôtes IPv4.



# Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

- La transmission de multidiffusion envoie un paquet à un groupe d'adresses de multidiffusion.
- Par exemple, le PC à 172.16.4.1 envoie un paquet de multidiffusion à l'adresse du groupe de multidiffusion 224.10.10.5.



# Types d'adresses IPv4

# Types d'adresses IPv4

## Les adresses IPv4 publiques et privées

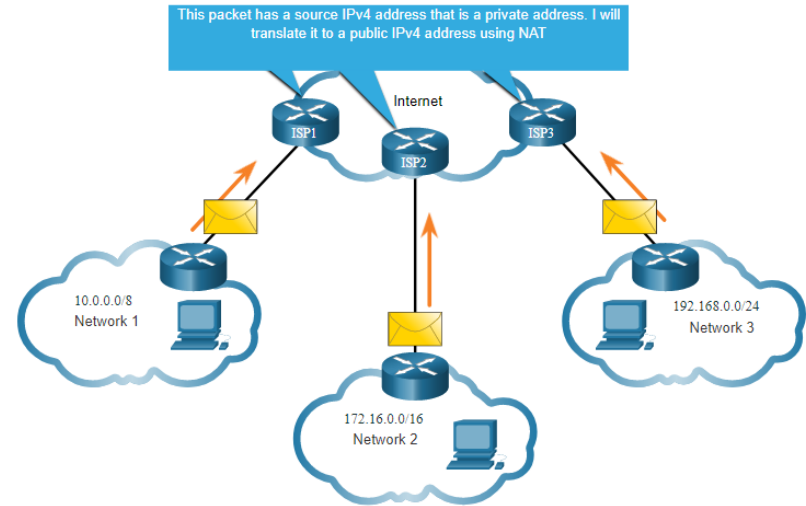
- Selon la définition de la RFC 1918, les adresses IPv4 publiques sont acheminées globalement entre les routeurs des FAI (fournisseurs d'accès à Internet).
- Certains blocs d'adresses appelés adresses privées sont utilisés par la plupart des entreprises pour attribuer des adresses IPv4 aux hôtes internes.
- Les adresses IPv4 privées ne sont pas uniques et peuvent être utilisées par n'importe quel réseau interne.
- Cependant, les adresses ne sont pas routables globalement.

Adresse réseau et préfixe	Gamme d'adresses privée RFC 1918
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

# Types d'adresses IPv4

## Routage vers l'internet

- Le processus de traduction d'adresses réseau (NAT) convertit les adresses IPv4 privées en adresses IPv4 publiques.
- NAT est généralement activé sur le routeur périphérique qui se connecte à l'internet.
- Il traduit les adresses IP privées en adresses IP publiques.





# Les types d'adresses IPv4

## Les adresses IPv4 des utilisateurs spéciaux

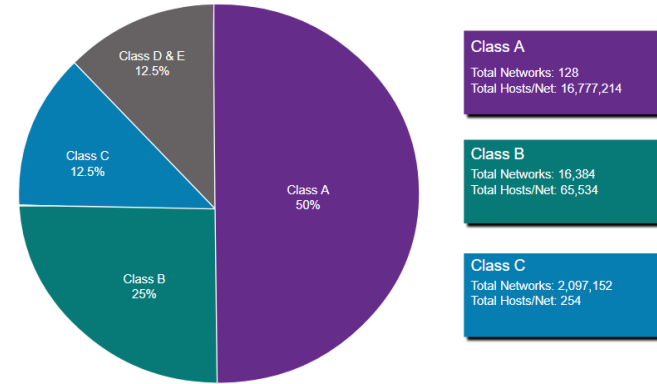
- Adresses de bouclage
  - 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
  - Généralement identifié comme 127.0.0.1
  - Utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle.
- Adresses link-local
  - 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
  - Plus connues sous le nom d'adresses APIPA (adressage IP privé automatique),
  - Elles sont utilisées par un client DHCP Windows pour se configurer automatiquement si aucun serveur DHCP n'est disponible.

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

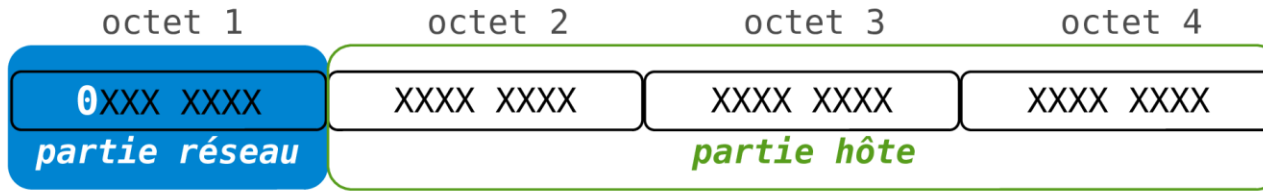
# Les types d'adresses IPv4

## Ancien système d'adressage par classe

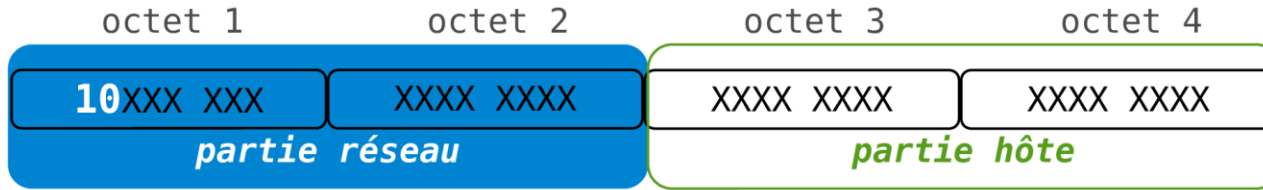
- les adresses IPv4 étaient attribuées à l'aide de l'adressage par classe tel que défini dans la RFC 790 (1981).
  - Classe A (0.0.0.0/8 à 127.0.0.0/8)
  - Classe B (128.0.0.0 /16 — 191.255.0.0 /16)
  - Classe C (192.0.0.0 /24 — 223.255.255.0 /24)
  - Classe D (224.0.0.0 à 239.0.0.0)
  - Classe E (240.0.0.0 — 255.0.0.0)
- 
- L'adressage de classe a gaspillé de nombreuses adresses IPv4.
  - L'allocation d'adresse par classe a été remplacée par l'adressage sans classe qui ignore les règles des classes (A, B, C).



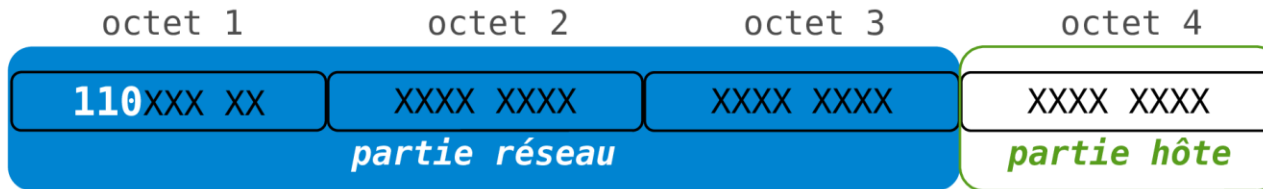
## Classe A



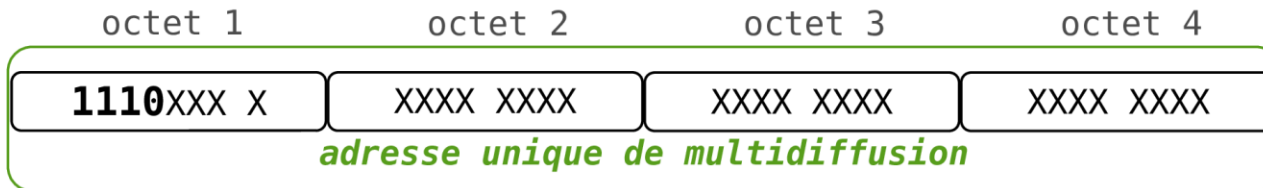
## Classe B



## Classe C



## Classe D

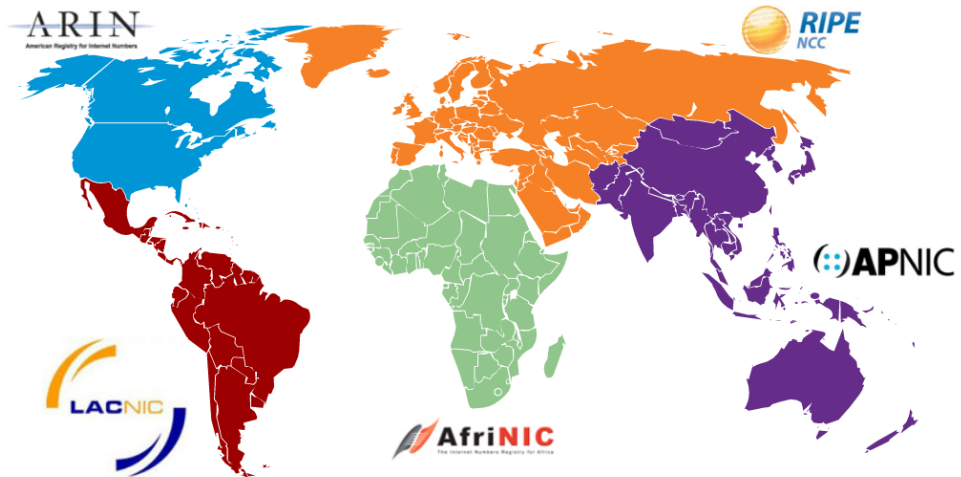


# Types d'adresses IPv4

## Attribution des adresses IP

---

- L'IANA gère les blocs d'adresses IPv4 et IPv6 et les attribue aux organismes d'enregistrement Internet locaux (RIR).
- Les RIR sont chargés d'attribuer des adresses IP à des FAI qui, à leur tour, fournissent des blocs d'adresses IPv4 aux entreprises et aux FAI de plus petite envergure.

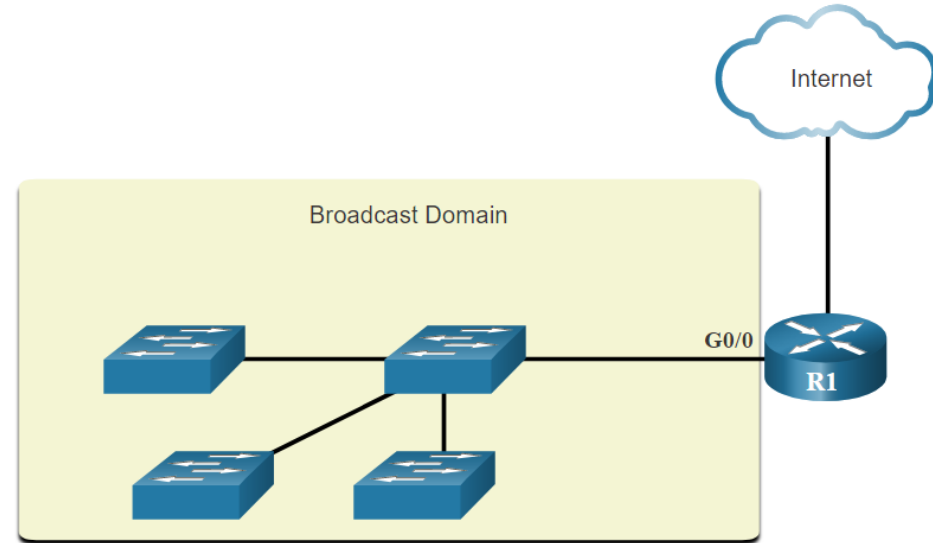


# Segmentation du réseau

# La segmentation du réseau

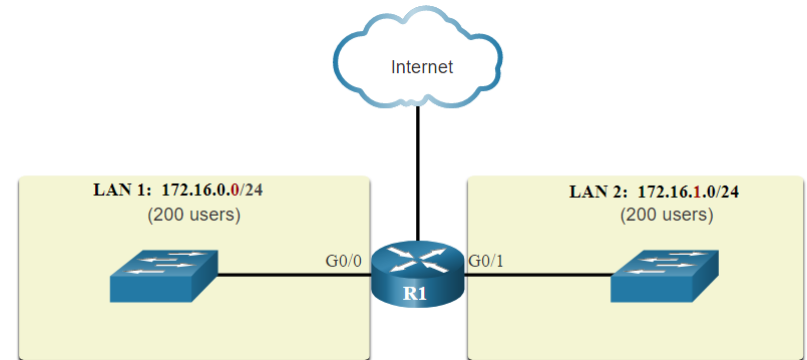
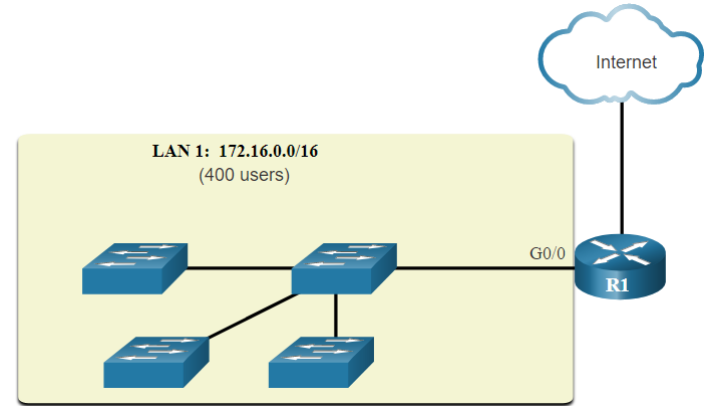
## Domaines de diffusion et de segmentation

- Plusieurs protocoles utilisent des diffusions ou des multidiffusions (par exemple, ARP utilise des diffusions pour localiser d'autres périphériques, les hôtes envoient des diffusions de découverte DHCP pour localiser un serveur DHCP.)
- Les commutateurs diffusent les messages de diffusion sur toutes les interfaces, sauf celle d'où les messages proviennent.
- Le seul périphérique qui arrête les diffusions est un routeur.
- Les routeurs ne diffusent pas les messages de diffusion.
- Chaque interface de routeur se connecte à un domaine de diffusion, et les diffusions sont propagées dans leur domaine de diffusion spécifique.



# Segmentation du réseau - Problèmes liés aux domaines de diffusion importants

- Dans ce type de domaine, les hôtes peuvent générer un nombre excessif de diffusion et ainsi avoir un impact négatif sur le réseau.
- La solution consiste à réduire la taille du réseau en créant de plus petits domaines de diffusion. C'est ce qu'on appelle le processus de création de sous-réseaux.
- l'adresse réseau 172.16.0.0 /16 ont été divisés en deux sous-réseaux de 200 utilisateurs chacun : 172.16.0.0 /24 et 172.16.1.0 /24.
- Les diffusions ne sont propagées qu'au sein des domaines de diffusion plus petits.

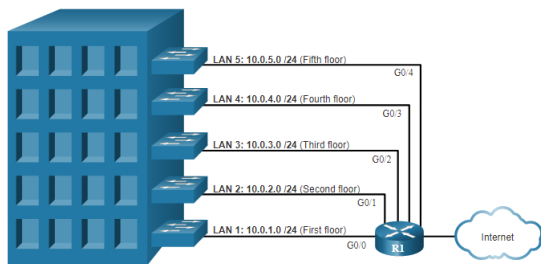


# Segmentation du réseau

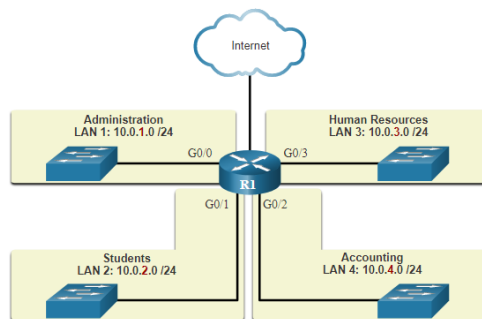
## Pourquoi créer des sous-réseaux ?

- La segmentation en sous-réseaux réduit le trafic global et améliore les performances réseau.
- Elle permet également de mettre en œuvre des politiques de sécurité entre les différents sous-réseaux.
- Le sous-réseau réduit le nombre de périphériques affectés par un trafic de diffusion anormal.
- Les sous-réseaux sont utilisés pour diverses raisons, notamment:

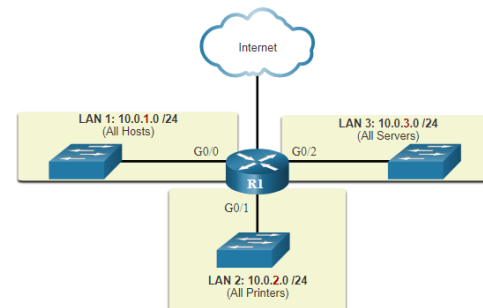
### Emplacement



### Groupe ou fonction



### Type de périphérique

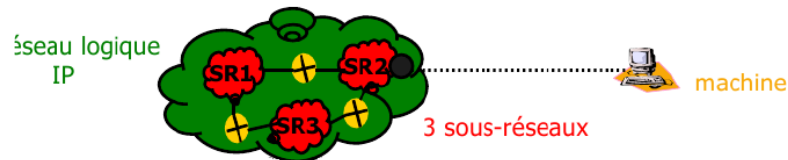




# Segmentation un réseau IPv4 en sous-réseaux

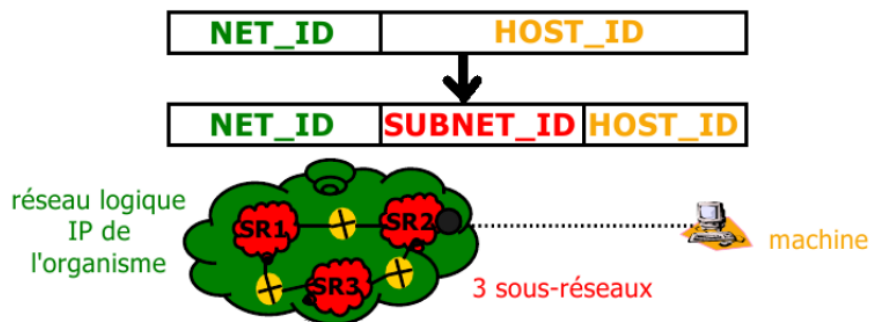
# Sous-réseaux (subnetting)

- En 1984, devant la limitation du modèle de classes, la RFC 917 (Internet subnets) crée le concept de sous-réseau.
- Ceci permet par exemple : d'utiliser une adresse de Classe B comme 256 sous-réseaux de 254 ordinateurs au lieu d'un seul réseau de 65536 ordinateurs, sans toutefois remettre en question la notion de classe d'adresse.
- d'optimiser l'utilisation et la sécurité du réseau en le segmentant
- de maîtriser l'adressage à l'intérieur du réseau
- **Conséquence : Le masque de sous-réseau ne peut plus être déduit de l'adresse IP elle-même. L'utilisation de masque de longueur variable (Variable-Length Subnet Mask, VLSM) permet une utilisation plus efficace de l'espace d'adressage**



# Sous-réseaux (subnetting)

- Pour segmenter un réseau en sous-réseaux, il faut alors décomposer la partie hostid de l'adresse IP en deux parties : une adresse de sous-réseau (subnetid) et une adresse machine (hostid).



- Par exemple, pour créer 3 sous-réseaux, il faudra prendre 2 bits dans la partie hostid et on créera donc 4 sous-réseaux :
  - 0 0 pour le sous-réseaux n°0
  - 0 1 pour le sous-réseaux n°1
  - 1 0 pour le sous-réseaux n°2
  - 1 1 pour le sous-réseaux n°3

# Sous-réseaux (subnetting)

---

- Évidemment, le masque de départ change et doit maintenant englober la partie netid et la partie subnetid. Ce nouveau masque se nomme masque de sous-réseaux.
- Exemple :
  - pour le réseau 192.168.1.0/24 découpé en 4 sous-réseaux
    - netid = 24 bits
    - subnetid = 2 bits
    - hostid =  $32 - 24 - 2 = 6$  bits
  - Le masque de sous-réseau sera :  $24 + 2 = 26$  bits soit 255.255.255.192

# Plage d'adresses des sous-réseaux

---

- Le nombre de machines adressables dans chaque sous-réseau sera de  $2^{\text{nb bits hostid}} - 2$  adresses.
- Exemple : pour le réseau 192.168.1.0/24 découpé en 4 sous-réseaux
- Le nombre de machines adressables dans chaque sous-réseau sera de :  $2^6 - 2$  adresses interdites = 62 adresses
  - sous-réseaux n°0 192.168.1.0/26 : 192.168.1.1 à 192.168.1.62 (broadcast = 192.168.1.63)
  - sous-réseaux n°1 192.168.1.64/26 : 192.168.1.65 à 192.168.1.126 (broadcast = 192.168.1.127)
  - sous-réseaux n°2 192.168.1.128/26 : 192.168.1.129 à 192.168.1.190 (broadcast = 192.168.1.191)
  - sous-réseaux n°3 192.168.1.192/26 : 192.168.1.193 à 192.168.1.254 (broadcast = 192.168.1.255)

# Exemples

---

1. L'adresse réseau de l'entreprise est 172.16.0.0. On désire créer 12 sous-réseaux.
  - Donner :
    - Le nombre de bits utilisés pour créer les sous réseaux
    - Le nombre de sous réseaux réellement créés
    - Le masque de sous réseau
    - Le nombre maximum d'adresses de poste pour chaque sous réseau
2. L'adresse réseau de l'entreprise est 192.168.0.0. Les différents services organisés en sous-réseaux disposent au maximum de 20 machines. Les sous-réseaux sont connectés entre eux par un routeur.
  - Donner : -
    - Le nombre d'équipements
    - Le nombre de bits à réserver pour l'adressage des machines
    - Le nombre de sous réseaux créés - Le masque de sous réseau

# Segmenter un réseau IPv4 en sous-réseaux

## Segmentation des réseaux à la limite d'octet

- Le plus simple est de segmenter les réseaux à la limite d'octet de /8, /16 et /24.
- Notez que l'utilisation de préfixes plus longs réduit le nombre d'hôtes par sous-réseau.

Longueur de préfixe	Masque de sous-réseau	Masque de sous-réseau (binaire) (n= réseau, h= hôte)	Nombre d'hôtes
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16777214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254





# Segmenter un réseau IPv4 en sous-réseaux

## Création de sous-réseaux au niveau de la limite d'octet

- Dans le premier tableau 10.0.0.0/8 est sous-réseau en utilisant /16 et dans le deuxième tableau, un masque /24.

Adresse de sous-réseau (256 sous-réseaux possibles)	Plage d'hôtes (65534 hôtes possibles par sous-réseau)	Diffusion
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.30.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.40.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.50.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.60.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.70.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Adresse de sous-réseau (65,536 sous-réseaux possibles)	Plage d'hôtes (254 hôtes possibles par sous-réseau)	Diffusion
10.0.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.2.255
...	...	...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	10.1.1.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.255
...	...	...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...	...	...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255

# Segmenter un réseau IPv4 en sous-réseaux

## Création de sous-réseaux au niveau de la limite d'octet

- Reportez-vous au tableau pour voir six façons de sous-réseau d'un réseau /24.

Longueur de préfixe	Masque de sous-réseau	Masque de sous-réseau (binaire) (n = réseau, h = hôte)	Nombre de sous-réseaux	Nombre d'hôtes
/25	255.255.255.128	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11111100	64	2

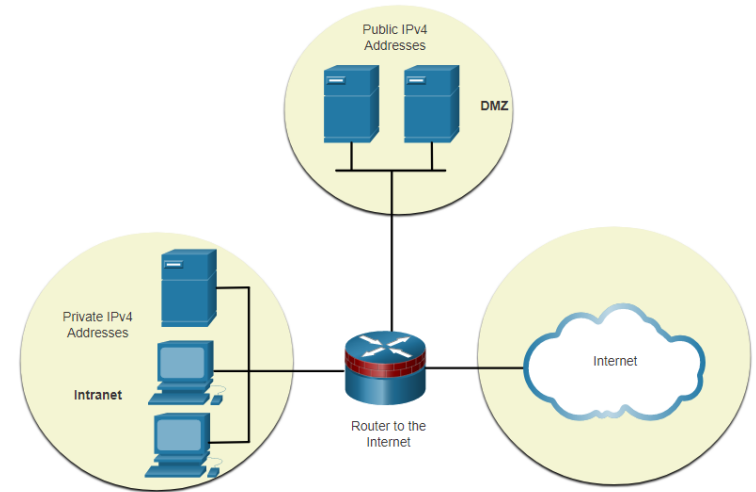
# Segmentation du réseau selon ses besoins

Sous-réseau pour répondre aux exigences

## Sous-réseau privé et espace d'adressage IPv4 public

Réseaux d'entreprises ont:


- Intranet - Réseau interne d'une entreprise utilise généralement des adresses IPv4 privées.
- DMZ — Une entreprise internet face aux serveurs. Les périphériques de la DMZ utilisent des adresses IPv4 publiques.
- Une entreprise pourrait utiliser le 10.0.0.0/8 et le sous-réseau sur la limite du réseau /16 ou /24.
- Les périphériques DMZ devraient être configurés avec des adresses IP publiques.



## Segmentation du réseau selon ses besoins

### Réduire les adresses IPv4 de l'hôte inutilisées et maximiser les sous-réseaux

- Deux considérations sont à prendre en compte lors de la planification de sous-réseaux:
- Le nombre d'adresses d'hôte nécessaires pour chaque réseau.
- Le nombre de sous-réseaux nécessaires.

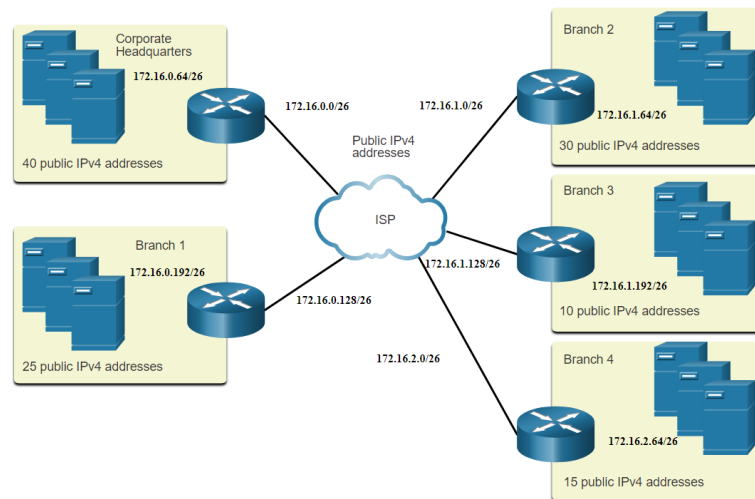
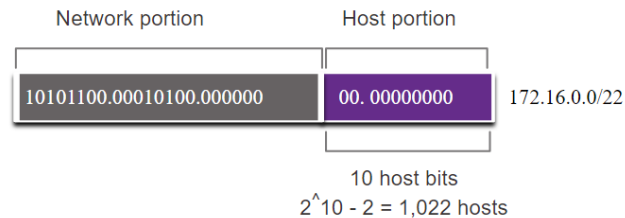


Longueur de préfixe	Masque de sous-réseau	Masque de sous-réseau (binaire) (n = réseau, h = hôte)	Nombre de sous-réseaux	Nombre d'hôtes
/25	255.255.255.128	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.nnnnnnnnn 11111111.11111111.11111111.11111100	64	2

# Segmentation du réseau selon ses besoins

## Exemple de besoins d'un réseau

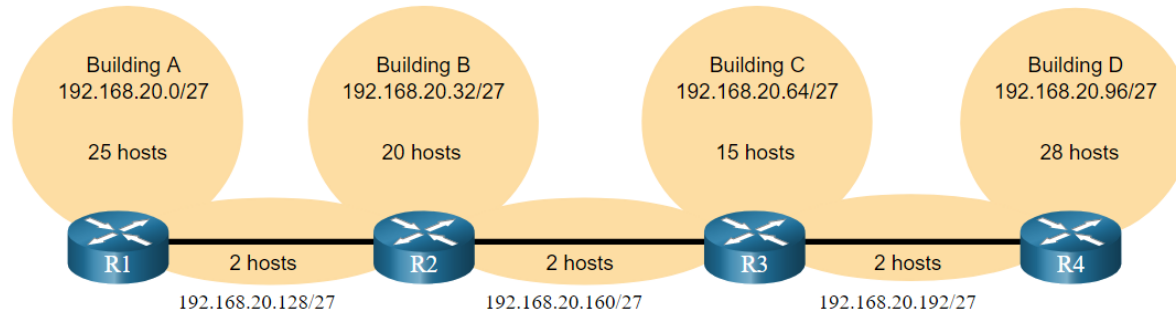
- Dans cet exemple, le siège social a attribué l'adresse réseau publique 172.16.0.0/22 (10 bits d'hôte) par son ISP (FAI) qui fournisse 1022 adresses d'hôte.
- Il y a cinq sites et donc cinq connexions Internet, ce qui signifie que l'organisation a besoin de 10 sous-réseaux avec le plus grand sous-réseau nécessite 40 adresses.
- Il a attribué 10 sous-réseaux avec un masque de sous-réseau /26 (c'est-à-dire 255.255.255.192).



# VLSM

# Conservation des adresses IPv4VLSM

- Compte tenu de la topologie, 7 sous-réseaux sont nécessaires (c'est-à-dire quatre LAN et trois liaisons WAN) et le plus grand nombre d'hôtes se trouve dans le bureau D avec 28 hôtes.
- Un masque /27 fournirait 8 sous-réseaux de 30 adresses IP hôtes et prendrait donc en charge cette topologie.

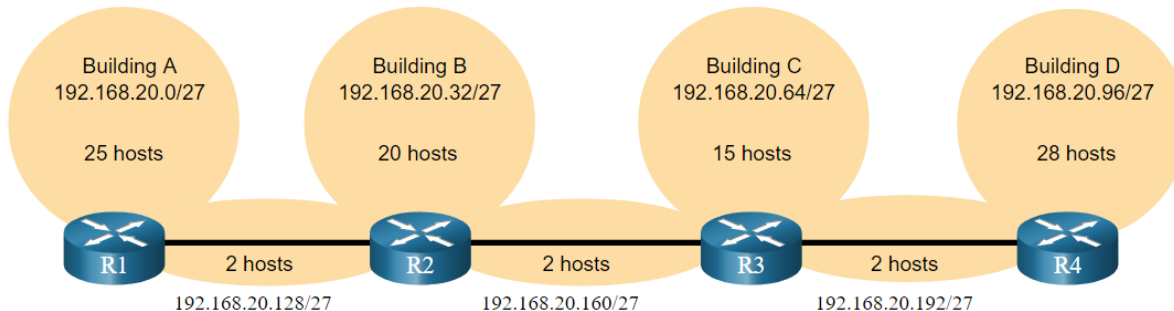




# VLSM

## Conservation des adresses IPv4 (suite)

- Cependant, les liaisons WAN point à point nécessitent seulement deux adresses et gaspillent donc 28 adresses chacune pour un total de 84 adresses inutilisées.
- L'application d'un schéma de création de sous-réseaux classique à un scénario n'est pas très efficace.
- VLSM a été développé pour éviter le gaspillage d'adresses en nous permettant de segmenter un réseau en sous-réseau.



Host portion  
 $2^5 - 2 = 30$  host IP addresses per subnet

$30 - 2 = 28$   
Each WAN subnet wastes 28 addresses

$28 \times 3 = 84$   
84 addresses are unused

# VLSM

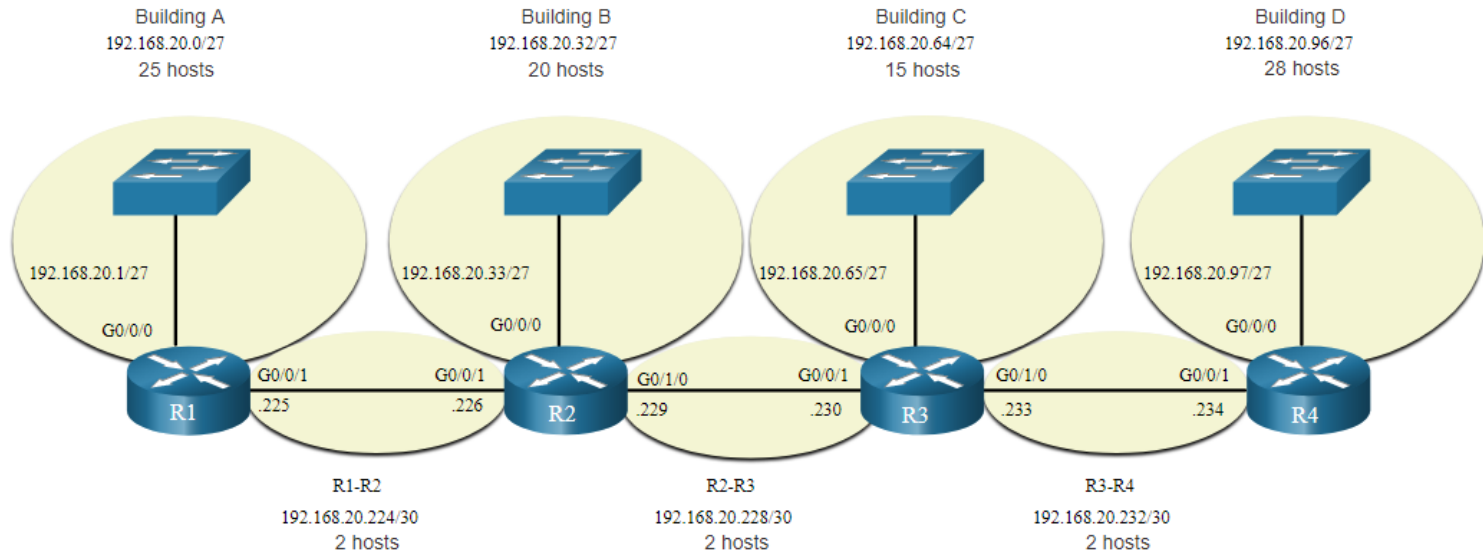
- Le côté gauche affiche le schéma de sous-réseau traditionnel (c'est-à-dire le même masque de sous-réseau) tandis que le côté droit illustre comment le VLSM peut être utilisé pour segmenter un réseau en sous-réseau et diviser le dernier sous-réseau en huit /30 sous-réseaux.
- Lorsque vous utilisez le VLSM, commencez toujours par vous assurer que les exigences en matière d'hôte du plus grand sous-réseau sont atteintes, puis continuez la segmentation de réseau jusqu'à ce que les exigences d'hôte du plus petit sous-réseau soient atteintes.
- La topologie ainsi obtenue grâce à l'application de VLSM.



# VLSM

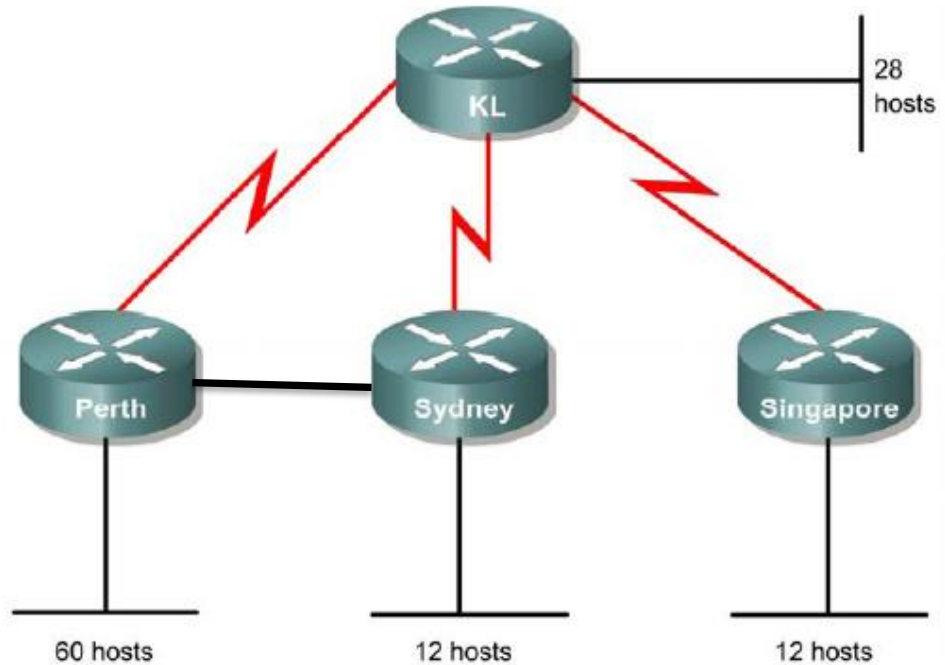
## Attribution d'adresse de topologie VLSM

- Grâce aux sous-réseaux VLSM, les réseaux LAN et les routeurs peuvent être traités sans gaspillage inutile, comme indiqué dans le diagramme de topologie logique.

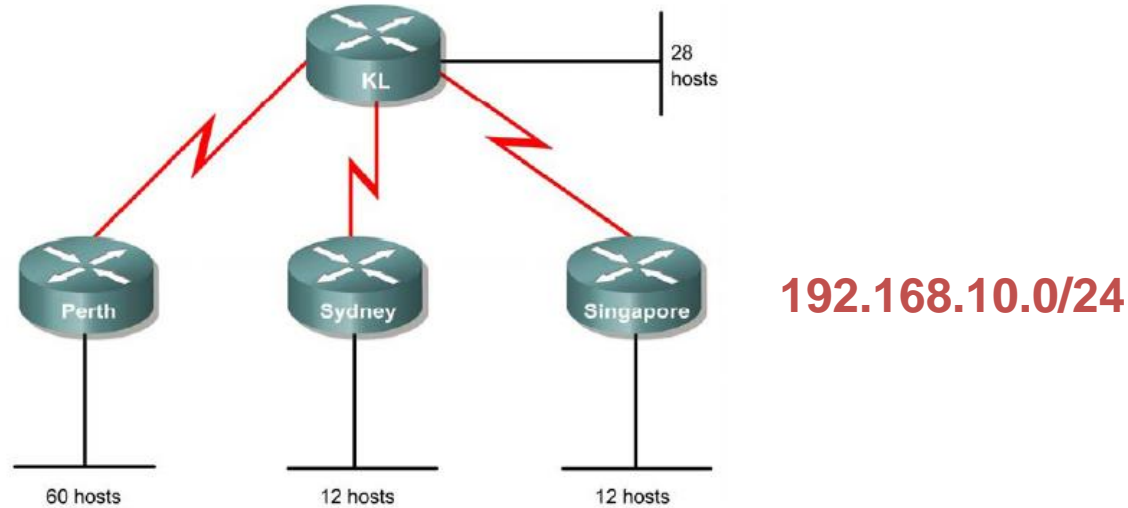


# Variable-length subnet mask (VLSM)

# Subnet with VLSM



# Regular Subnet



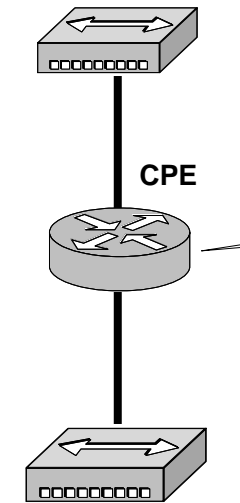
**7** subnets; The largest subnet needs **60** hosts

If **3** bits for subnet (8 subnets) → **5** bits for host (32 hosts)

If **6** bits for host (64 hosts) → **2** bits for subnet (4 subnets)

# Assignment

250 Stations

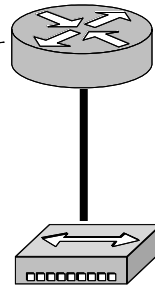


CPE

700 Stations

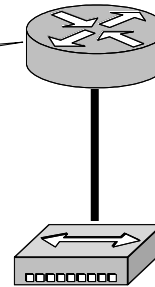
165.23.208.0/20

IE



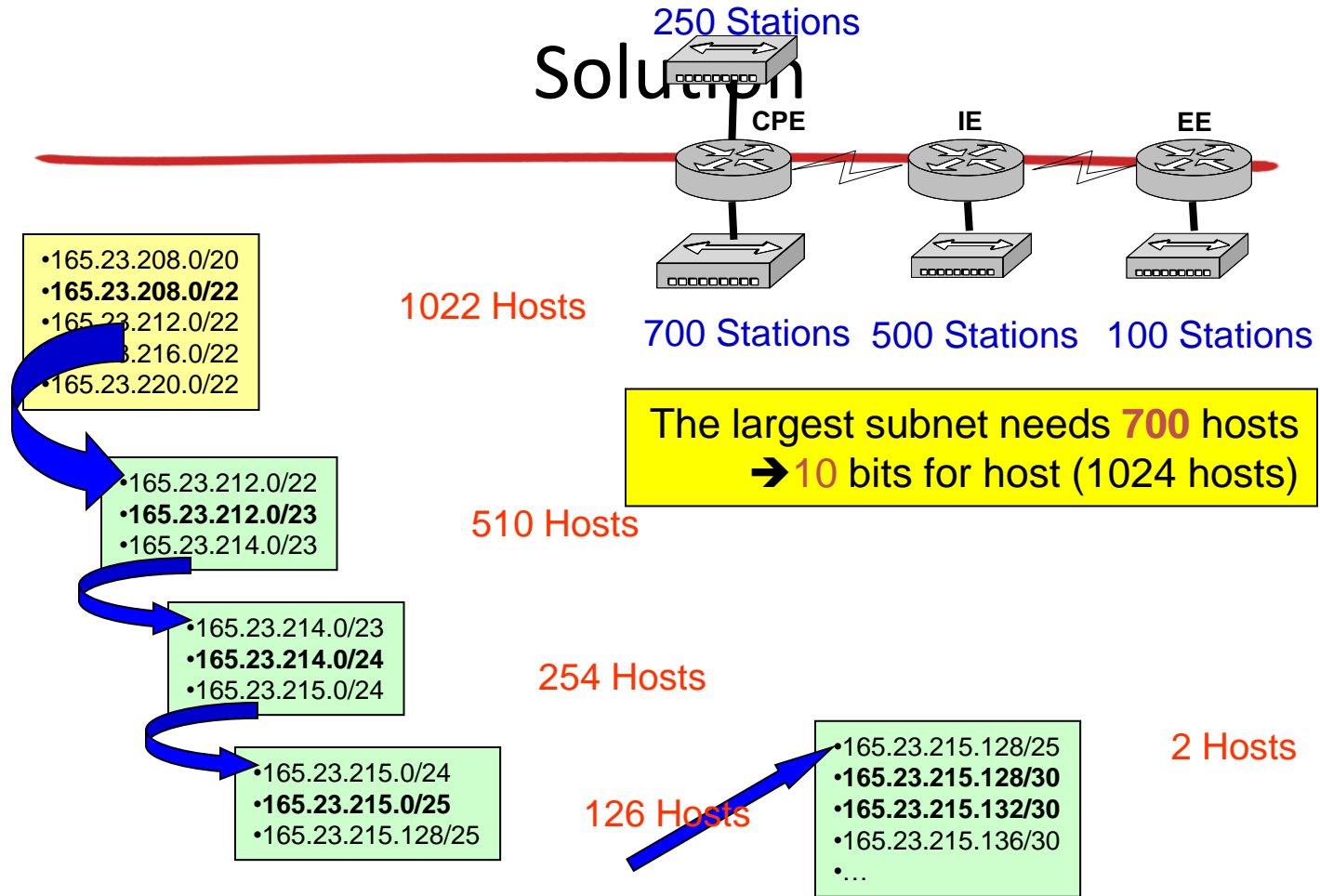
500 Stations

EE



100 Stations

# Solution





# Solution

