



Module 11: Adressage IPv4

Contenu Pédagogique de l'instructeur

Présentation des réseaux V7.0
(ITN)





Module 11: Adressage IPv4

Présentation des réseaux V7.0
(ITN)



Objectifs du Module

Titre du module: Adressage IPv4

Objectifs du Module: Calculer un schéma de sous-réseau IPv4 pour segmenter efficacement votre réseau.

| Titre du Rubrique | Objectif du Rubrique |
|---|--|
| Structure de l'adresse IPv4 | Décrire la structure d'une adresse IPv4, y compris la partie hôte, la partie réseau et le masque de sous-réseau. |
| Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion | Comparer les caractéristiques et les utilisations des adresses IPv4 de monodiffusion, de diffusion et de multidiffusion. |
| Les types d'adresses IPv4 | Expliquer ce que sont les adresses IPv4 publiques, privées et réservées. |
| Segmentation du réseau | Expliquer en quoi la segmentation d'un réseau permet d'améliorer la communication. |
| Sous-réseau d'un réseau IPv4 | Calculer les sous-réseaux IPv4 pour un préfixe /24. |

Objectifs du module (suite)

Titre du module: Adressage IPv4

Objectifs du Module: Calculer un schéma de sous-réseau IPv4 pour segmenter efficacement votre réseau.

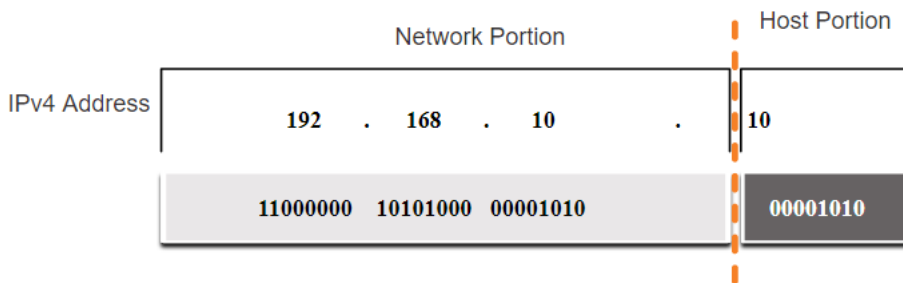
| Titre du Rubrique | Objectif du Rubrique |
|---|--|
| Sous-réseau des préfixes /16 et /8 | Calculer les sous-réseaux IPv4 pour des préfixes /16 et /8. |
| Segmentation du réseau pour répondre aux besoins | Mettre en œuvre un schéma d'adressage IPv4 à partir d'un ensemble de critères de segmentation. |
| masquage de sous-réseau de longueur variable (VLSM) | Expliquer comment créer un schéma d'adressage flexible grâce au masque de sous-réseau à longueur variable. |
| Conception structurée | Mettre en œuvre un schéma d'adressage de masque de sous-réseau à longueur variable. |

11.1 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

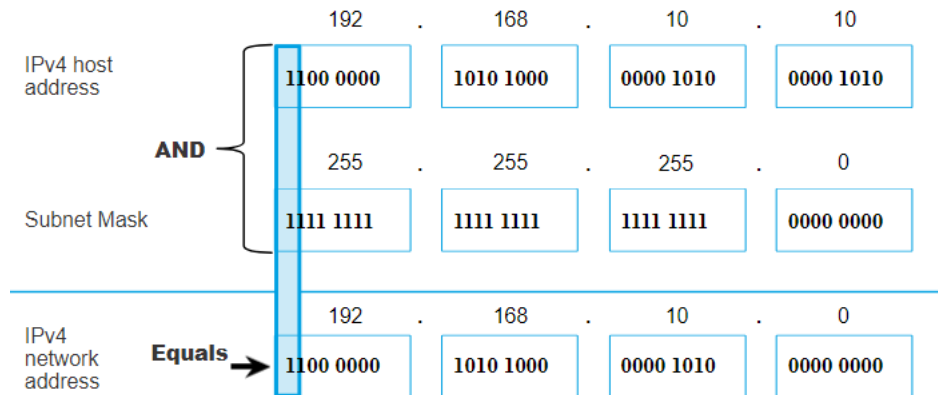
La longueur de préfixe

- Une longueur de préfixe est une méthode fastidieux 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 |

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



Démonstration vidéo - réseau, hôte et adresses de diffusion

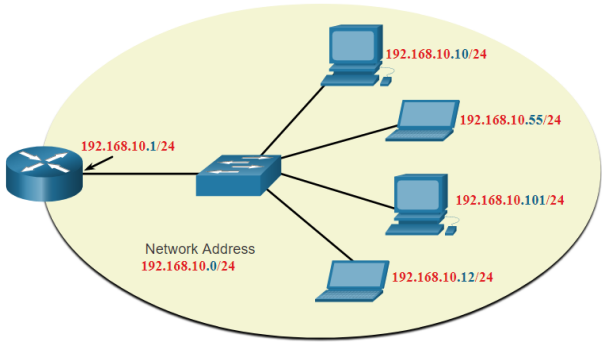
Cette vidéo présentera les points suivants :

- Adresse réseau
- Adresse de diffusion
- Première hôte utilisable
- Dernière hôte utilisable

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



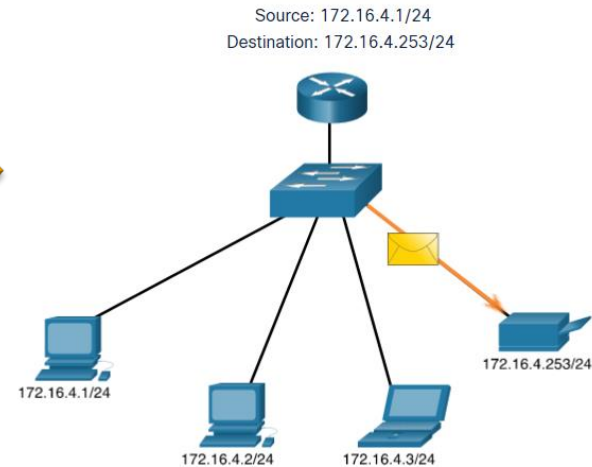
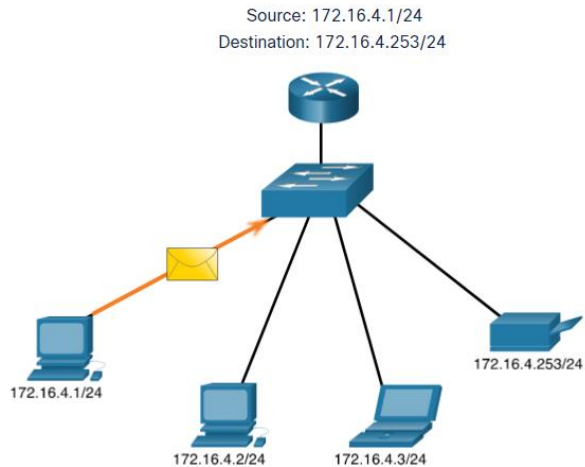
| | Partie réseau | Partie hôte | Bits d'hôte |
|--|--|-----------------|----------------|
| Masque de sous-réseau . 255.255.255.0 or /24 | 255 255 255 11111111 111111 111111 | 0 00000000 | |
| Adresse réseau 192.168.10.0 or /24 | 192 168 10 11000000 10100000 00001010 | 0 00000000 | All 0s |
| First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

11.2 Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Monodiffusion

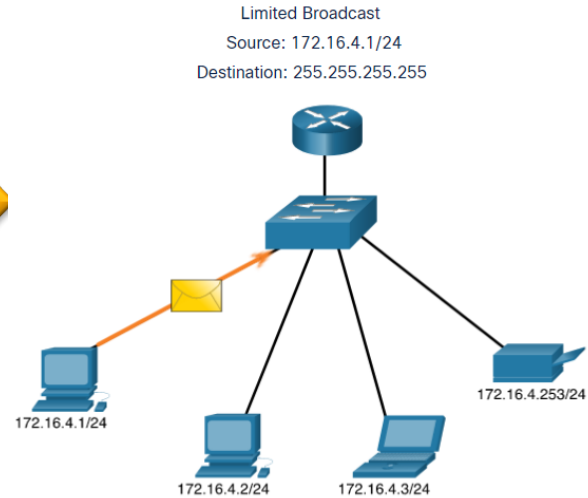
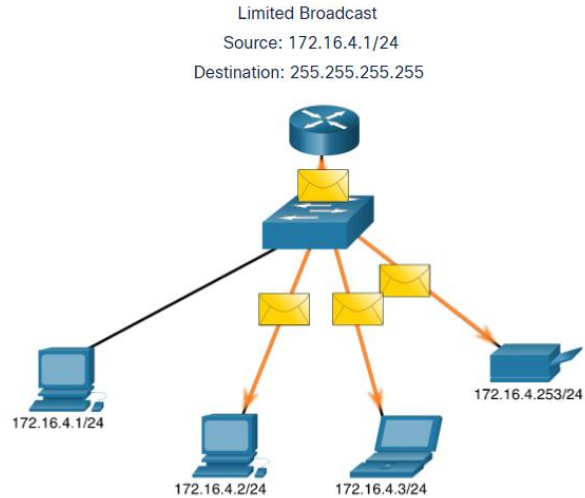
- La transmission monodiffusion envoie un paquet à une adresse IP de destination.
- Par exemple, le PC à 172.16.4.1 envoie un paquet monodiffusion à l'imprimante à 172.16.4.253.



Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Diffusion

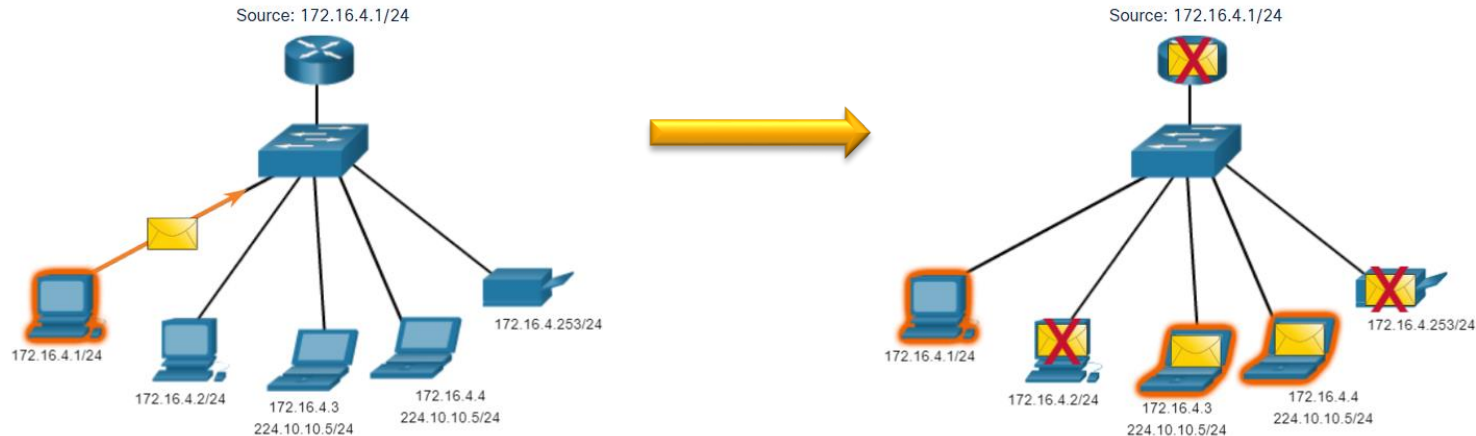
- La transmission de diffusion envoie un paquet à toutes les autres adresses IP de destination.
- Par exemple, le PC à 172.16.4.1 envoie un paquet de diffusion à tous les hôtes IPv4.



Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

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.



11.3 Types d'adresses IPv4

Les adresses IPv4 publiques et privées

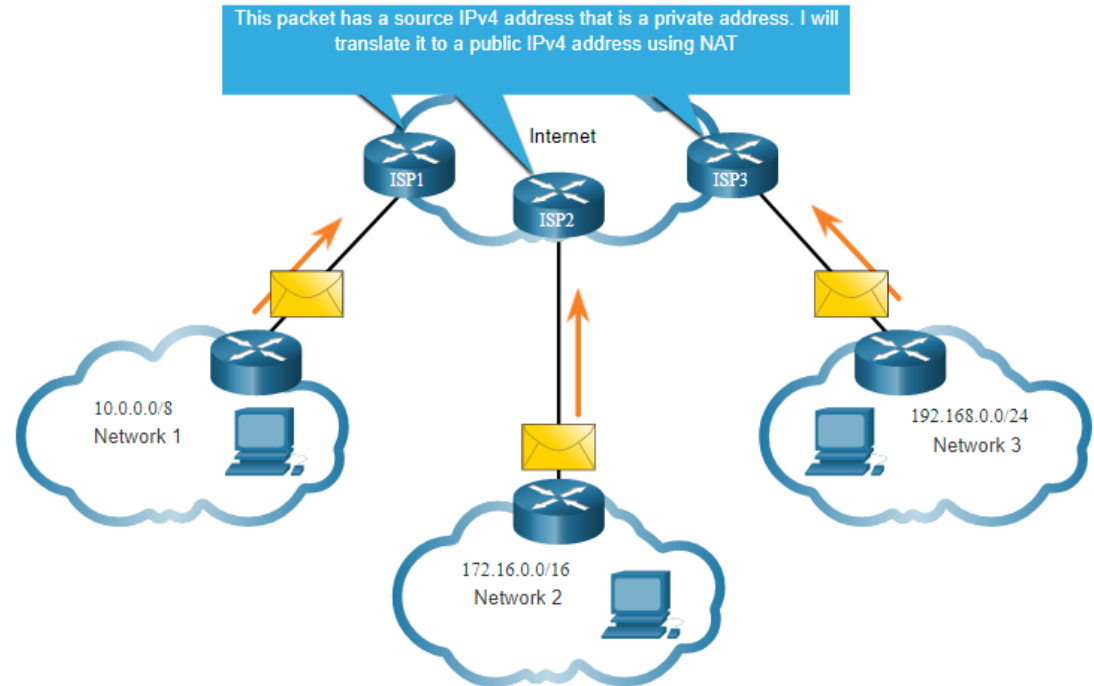
- Selon la définition de la RFC 1918, les adresses IPv4 publiques sont acheminées globalement entre les routeurs des FAI (fournisseurs d'accès à Internet).
- Certains blocs d'adresses appelés adresses privées sont utilisés par la plupart des entreprises pour attribuer des adresses IPv4 aux hôtes internes.
- 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 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.

```
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
```

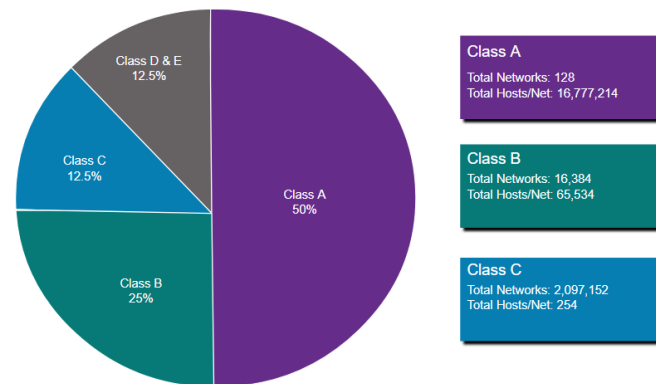
Adresses link-local

- 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.

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.

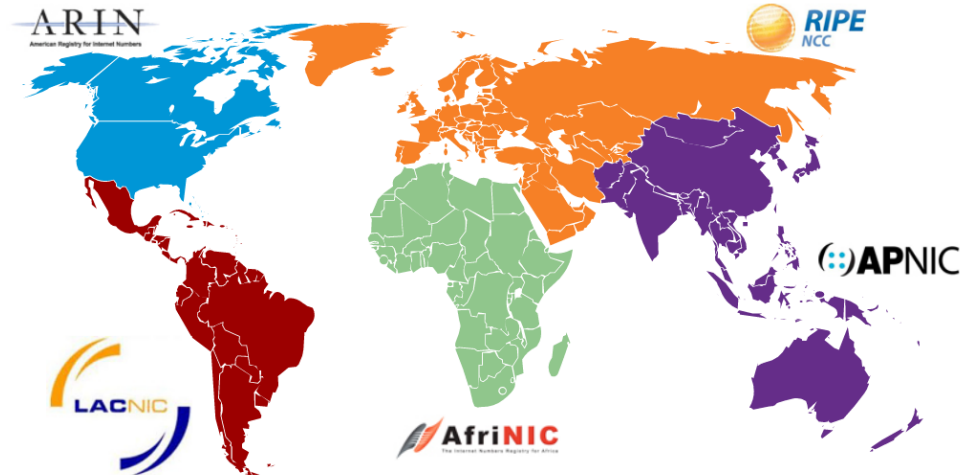


L'allocation d'adresse par classe a été remplacée par l'adressage sans classe qui ignore les règles des classes (A, B, C).

Types d'adresses IPv4

Attribution des adresses IP

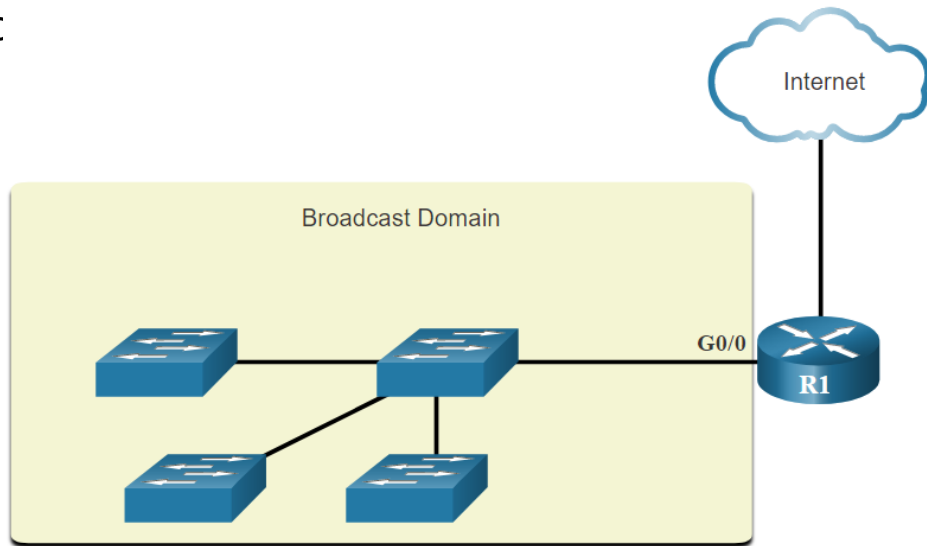
- L'IANA gère les blocs d'adresses IPv4 et IPv6 et les attribue aux organismes d'enregistrement Internet locaux (RIR).
- Les RIR sont chargés d'attribuer des adresses IP à des FAI qui, à leur tour, fournissent des blocs d'adresses IPv4 aux entreprises et aux FAI de plus petite envergure.



11.4 Segmentation du réseau

Domaines de diffusion et de segmentation

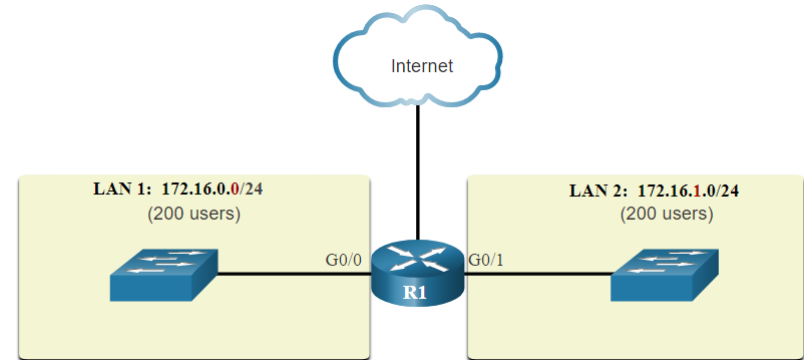
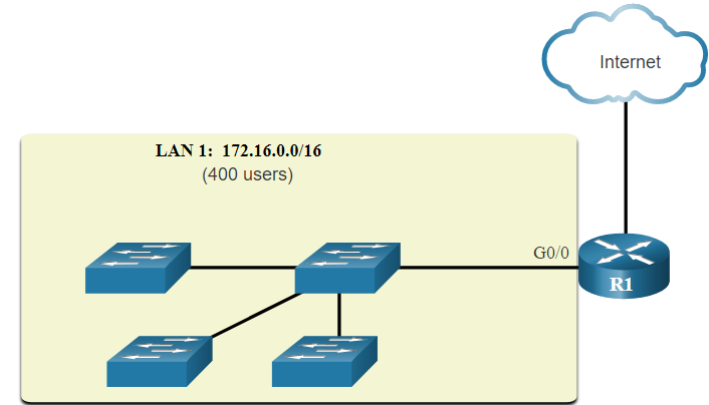
- Plusieurs protocoles utilisent des diffusions ou des multidiffusions (par exemple, ARP utilise des diffusions pour localiser d'autres périphériques, les hôtes envoient des diffusions de découverte DHCP pour localiser un serveur DHCP.)
- Les commutateurs diffusent les messages de diffusion sur toutes les interfaces, sauf C



- 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.

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.

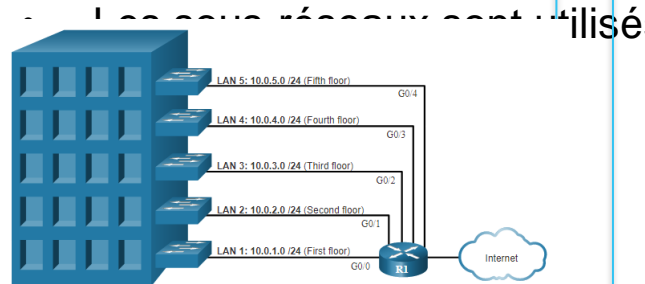


Segmentation du réseau

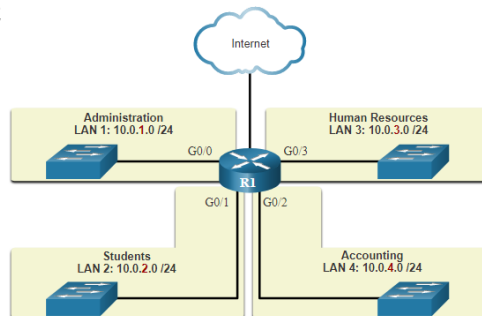
Pourquoi créer des sous-réseaux ?

- 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.

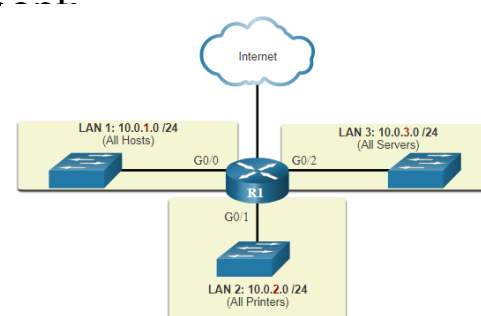
Emplacement



Groupe ou fonction



Type de périphérique



11.5 Segmentation un réseau IPv4 en sous-réseaux

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 |

Création de sous-réseaux au niveau de la limite d'octet (suite)

- 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 |

11.6 Création de sous-réseaux avec le préfixe /16 et /8

Sous-réseaux avec le préfixe /16 et /8

Créer des sous-réseaux avec un préfixe /16

- Le tableau indique les différents scénarios qui permettent de segmenter un préfixe /16 en sous-réseaux.

| Longueur de préfixe | Masque de sous-réseau | Network Address (n = network, h = host) | Nombre de sous-réseaux | Nombre d'hôtes |
|---------------------|-----------------------|--|------------------------|----------------|
| /17 | 255.255.128.0 | nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000 | 2 | 32766 |
| /18 | 255.255.192.0 | nnnnnnnnnnnnnnnnnn.nnnhhhhhhhhhhhhhh 1111111111.11000000.00000000 | 4 | 16382 |
| /19 | 255.255.224.0 | nnnnnnnnnnnnnnnnnn.nnnnnhhhhhhhhhhhh 1111111111.11100000.00000000 | 8 | 8190 |
| /20 | 255.255.240.0 | nnnnnnnnnnnnnnnnnn.nnnnnhhhhhhhhhhhh 1111111111.11110000.00000000 | 16 | 4094 |
| /21 | 255.255.248.0 | nnnnnnnnnnnnnnnnnn.nnnnnhhhhhhhhhhhh 1111111111.11111000.00000000 | 32 | 2046 |
| /22 | 255.255.252.0 | nnnnnnnnnnnnnnnnnn.nnnnnnnhh.hhhhhhhh 1111111111.11111100.00000000 | 64 | 1022 |
| /23 | 255.255.254.0 | nnnnnnnnnnnnnnnnnn.nnnnnnnnh.hhhhhhhh 1111111111.11111110.00000000 | 128 | 510 |
| /24 | 255.255.255.0 | nnnnnnnnnnnnnnnnnn.nnnnnnnnn.hhhhhhhh 1111111111.11111111.00000000 | 256 | 254 |
| /25 | 255.255.255.128 | nnnnnnnnnnnnnnnnnn.nnnnnnnnnn.nhhhhhhh 1111111111.11111111.10000000 | | 126 |

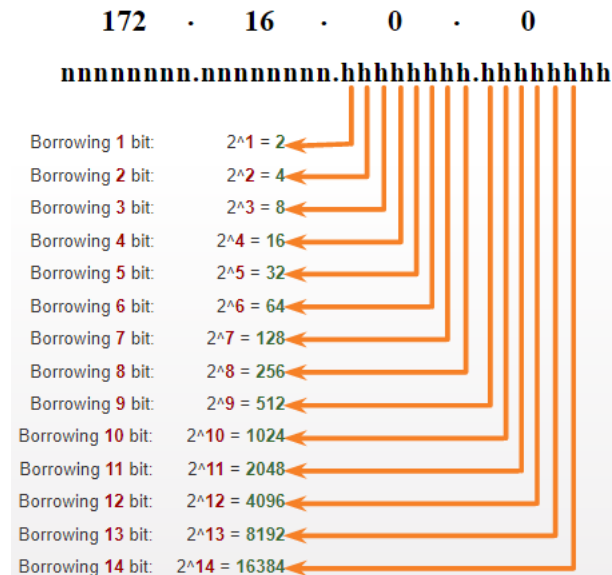
Création de sous-réseaux avec le préfixe /16 et /8

Créer 100 sous-réseaux avec un préfixe /16

Considérons une grande entreprise qui nécessite au moins 100 sous-réseaux et qui a choisi l'adresse privée 172.16.0.0/16 comme adresse de réseau interne.

- La figure indique le nombre de sous-réseaux qui peuvent être créés si l'on emprunte des bits au troisième et au quatrième octets.
- Notez qu'il y a maintenant jusqu'à 14 bits hôtes qui peuvent être empruntés (c'est-à-dire que les deux derniers bits ne peuvent pas être empruntés).

Pour obtenir les 100 sous-réseaux nécessaires à l'entreprise, il faudrait emprunter 7 bits (c'est-à-dire $2^7 = 128$ sous-réseaux) (pour un total de 128 sous-réseaux).



Créer 100 sous-réseaux avec un préfixe /8

Prenons le cas d'un petit FAI qui exige 1000 sous-réseaux pour ses clients en utilisant l'adresse de réseau 10.0.0.0/8, ce qui signifie qu'il y a 8 bits dans la partie réseau et 24 bits d'hôte disponibles à emprunter pour le sous-réseau.

- La figure indique le nombre de sous-réseaux qui peuvent être créés si l'on emprunte des bits au deuxième et au troisième octets.
- Notez qu'il y a maintenant jusqu'à 22 bits hôtes qui peuvent être empruntés (c'est-à-dire que les deux derniers bits ne peuvent pas être empruntés).



Pour obtenir les 1000 sous-réseaux nécessaires à l'entreprise, il faudrait emprunter 10 bits (c'est-à-dire $2^{10} = 1024$ sous-réseaux) (pour un total de 128 sous-réseaux).

Travaux pratiques - Formules de calcul des sous-réseaux IPv4

Au cours de ce travaux pratiques, vous réaliserez les objectifs suivants :

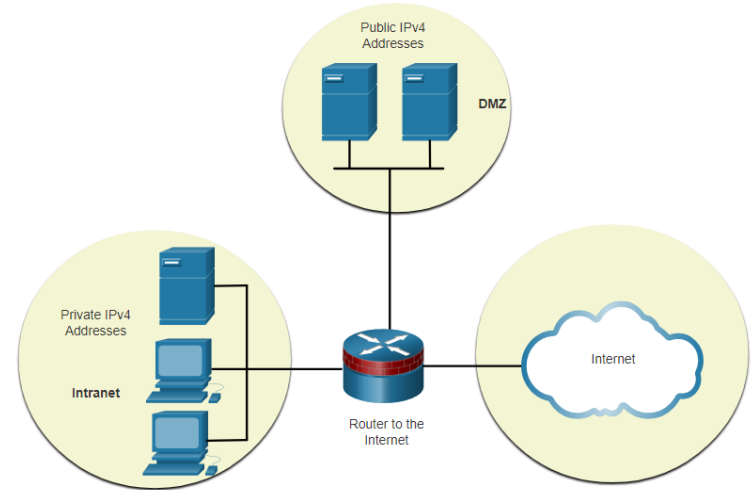
- Partie 1: Déterminer le sous-réseau d'adresses IPv4
- Partie 2: Calculer le sous-réseau d'adresses IPv4

11.7 Segmentation du réseau selon ses besoins

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.

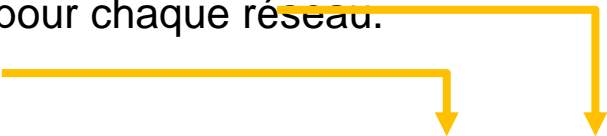


Segmentation du réseau selon ses besoins

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.

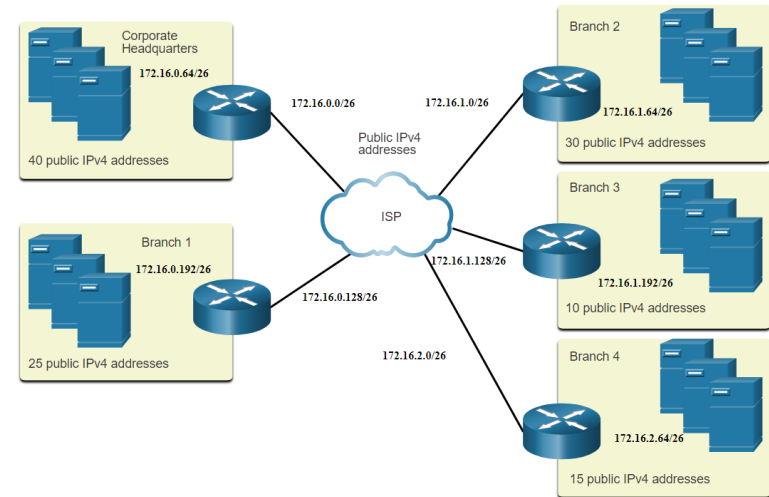
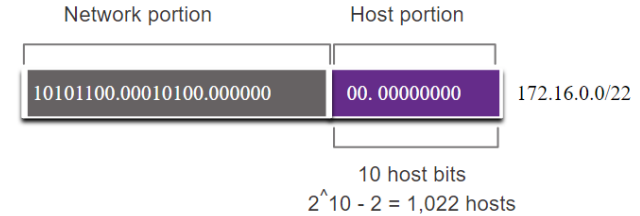


| Longueur de préfixe | Masque de sous-réseau | Masque de sous-réseau (binaire) (n = réseau, h = hôte) | Nombre de sous-réseaux | Nombre d'hôtes |
|---------------------|-----------------------|--|------------------------|----------------|
| /25 | 255.255.255.128 | nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nhhhhhhhhh 11111111 . 11111111 . 11111111 . 10000000 | 2 | 126 |
| /26 | 255.255.255.192 | nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnhhhhhhhh 11111111 . 11111111 . 11111111 . 11000000 | 4 | 62 |
| /27 | 255.255.255.224 | nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnhhhhhhh 11111111 . 11111111 . 11111111 . 11100000 | 8 | 30 |
| /28 | 255.255.255.240 | nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnnnhhhhh 11111111 . 11111111 . 11111111 . 11110000 | 16 | 14 |
| /29 | 255.255.255.248 | nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnnnnhhhh 11111111 . 11111111 . 11111111 . 11111000 | 32 | 6 |
| /30 | 255.255.255.252 | nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnnnnnhhh 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).

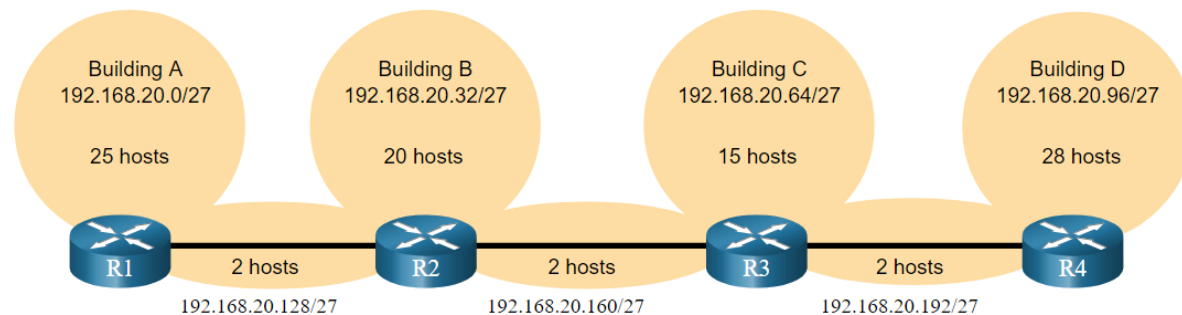


11.8 VLSM

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.

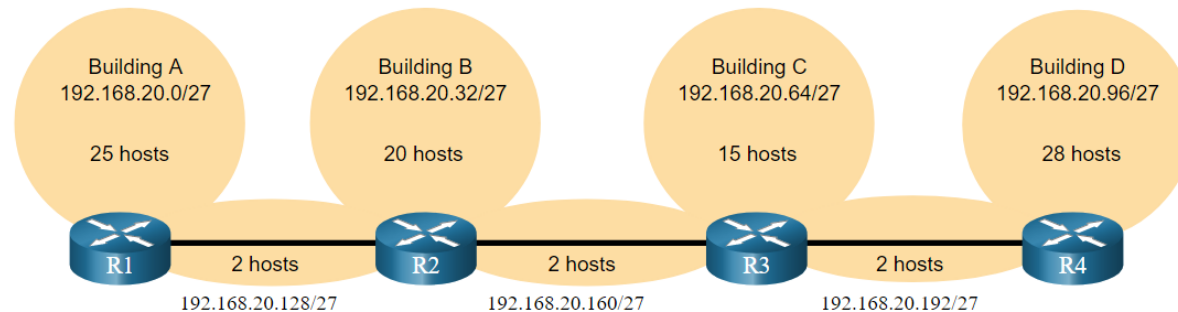
- Un masque /27 fournirait 8 sous-réseaux de 30 adresses IP hôtes et prendrait donc en charge cette topologie.



Conservation des adresses IPv4 (suite)

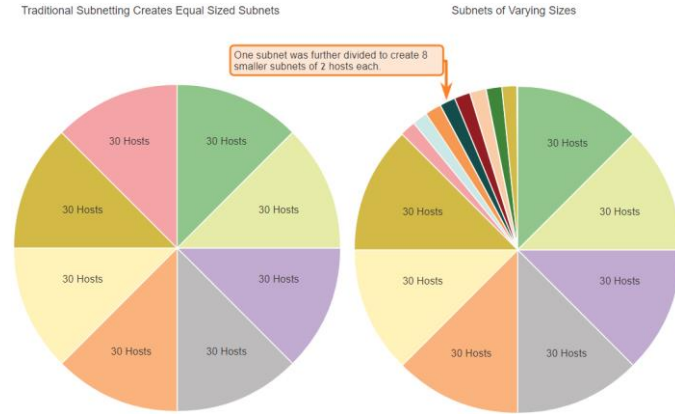
Cependant, les liaisons WAN point à point nécessitent seulement deux adresses et gaspillent donc 28 adresses chacune pour un total de 84 adresses inutilisées.

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

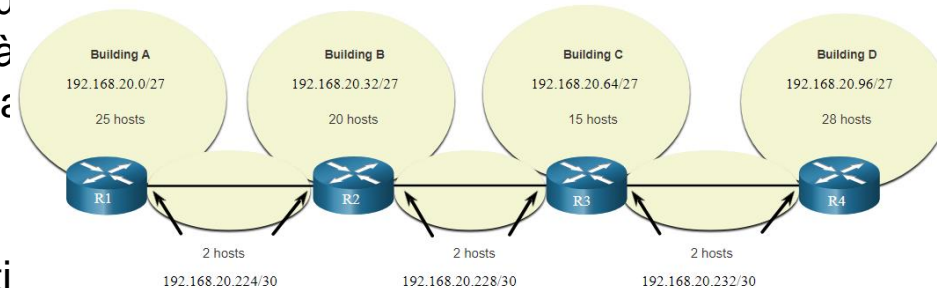


- L'application d'un schéma de création de sous-réseaux classique à un scénario n'est pas très efficace.
- VLSM a été développé pour éviter le gaspillage d'adresses en nous permettant de segmenter un réseau en sous-réseau.

- 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.



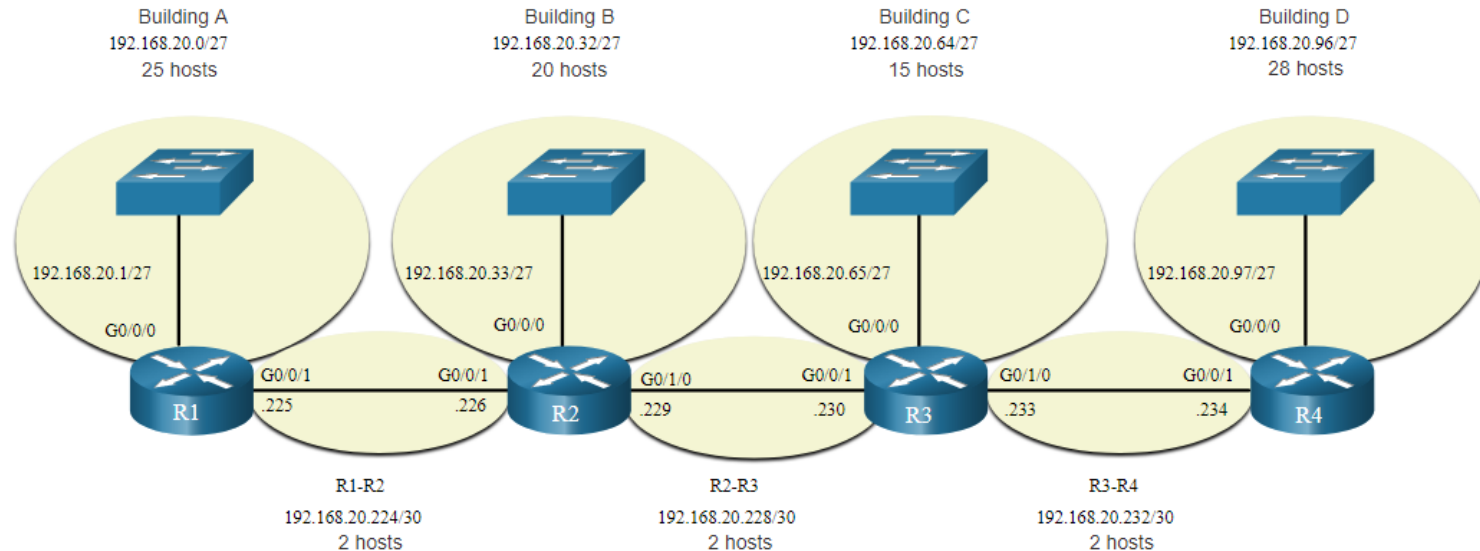
- Lorsque vous utilisez le VLSM, commencez toujours par vous assurer que les exigences en matière d'hôte du plus grand sous-réseau sont atteintes, puis continuez la segmentation de réseau jusqu'à ce que les exigences d'hôte du plus petit sous-réseau soient atteintes.



- La topologie ainsi obtenue grâce à l'application du 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.



11.9 La conception structurée

La conception structurée

Planification de l'adressage réseau

La planification des sous-réseaux nécessite de développer une solution évolutive pour un réseau d'entreprise.

- Pour élaborer un schéma d'adressage IPv4 à l'échelle du réseau, vous devez savoir combien de sous-réseaux sont nécessaires, combien d'hôtes particulier un sous-réseau requiert, quels périphériques font partie du sous-réseau, quelles parties de votre réseau utilisent des adresses privées et lesquelles utilisent des adresses publiques, et bien d'autres facteurs déterminants.

Observez les besoins de l'entreprise en termes d'utilisation du réseau et la structure appropriée des sous-réseaux.

- Effectuer une étude des besoins du réseau en examinant l'ensemble du réseau afin de déterminer comment chaque zone sera segmentée.
- Déterminez le nombre des sous-réseaux d'hôte disponibles et le nombre de sous-réseaux nécessaires.
- Déterminez les pools d'adresses DHCP et les pools VLAN de couche 2.

Attribution d'adresse de périphérique

Dans un réseau, il existe différents types d'appareils nécessitant des adresses:

- **Clients des utilisateurs finaux** - La plupart utilisent DHCP pour réduire les erreurs et la charge pesant sur le personnel de support réseau. Les clients IPv6 peuvent obtenir des informations d'adressage avec DHCPv6 ou SLAAC.
- **Les serveurs et les périphériques** doivent avoir une adresse IP statique prévisible.
- **Serveurs accessibles à partir l'internet** — Les serveurs doivent avoir une adresse IPv4 publique, le plus souvent accessible via NAT.
- **Les périphériques intermédiaires** – Des adresses sont attribuées à ces périphériques pour la gestion, la surveillance et la sécurité du réseau.
- **Passerelle** : les routeurs et les périphériques de pare-feu sont une passerelle pour les hôtes de ce réseau.

Lors du développement d'un schéma d'adressage IP, il est généralement recommandé que vous définissiez un modèle d'attribution des adresses pour chaque type de périphérique.

Packet Tracer - Pratique de conception et mise en œuvre d'un système d'adressage avec des VLSM

Dans le cadre de ce Packet Tracer, vous ferez ce qui suit :

- Étudier les besoins du réseau
- Concevoir le schéma d'adressage VLSM
- Attribuer des adresses IP aux périphériques et vérifier la connectivité

11.10 Module pratique et questionnaire

La conception structurée

Packet Tracer - Conception et mise en œuvre d'un schéma d'adressage VLSM

Dans le cadre de ce Packet Tracer, vous ferez ce qui suit :

- Concevoir un schéma d'adressage IP VLSM compte tenu des exigences
- Configurer l'adressage sur les périphériques réseau et les hôtes
- Vérifier la connectivité IP
- Résolution des problèmes de connectivité.

Packet Tracer – Conception et mise en œuvre d'un schéma d'adressage VLSM - Mode Physique

Travaux Pratiques – Conception et mise en œuvre d'un schéma d'adressage VLSM

Dans les deux activités mode physique du Packet Tracer et dans les Travaux Pratiques, vous remplirez les objectifs suivants:

- Examiner les besoins du réseau
- Concevoir le schéma d'adresses VLSM
- Câbler et configurer le réseau IPv4

Qu'est-ce que j'ai appris dans ce module?

- La structure d'adressage IP est constituée d'une adresse réseau hiérarchique 32 bits qui identifie un réseau et une partie hôte. Les périphériques réseau utilisent un processus appelé ANDing à l'aide de l'adresse IP et du masque de sous-réseau associé pour identifier les parties réseau et hôte.
- Les paquets IPv4 de destination peuvent être monodiffusion, diffusion et multidiffusion.
- Il existe des adresses IP routables globalement telles qu'assignées par l'IANA et il existe trois plages d'adresses IP privées qui ne peuvent pas être routées globalement mais peuvent être utilisées sur tous les réseaux privés internes.
- Réduisez les grands domaines de diffusion à l'aide de sous-réseaux pour créer des domaines de diffusion plus petits, réduire le trafic réseau global et améliorer les performances du réseau.
- Créer des sous-réseaux IPv4 en utilisant un ou plusieurs bits d'hôte en tant que bits réseau. Cependant, les réseaux sont plus facilement segmentés en sous-réseaux à la limite des octets /8, /16 et /24.
- Les plus grands réseaux peuvent être segmenter en sous-réseaux aux limites /8 ou /16.
- Utilisez VLSM pour réduire le nombre d'adresses hôtes inutilisées par sous-réseau.

Qu'est-ce que j'ai appris dans ce module? (Cont.)

- la méthode VLSM permet de diviser un espace réseau en parties inégales. Commencez toujours par répondre aux besoins en hôtes du plus grand sous-réseau. Poursuivez la segmentation jusqu'à ce que les besoins en hôtes du plus petit sous-réseau soient satisfaits.
- Lorsque vous créez un système d'adressage réseau, tenez compte des exigences internes, DMZ et externes. Utiliser un système d'adressage IP interne cohérent avec un modèle défini d'attribution des adresses à chaque type de périphérique.

Nouveaux termes et commandes

- longueur de préfixe
- logique AND (ET)
- adresse de réseau
- l'adresse de diffusion
- Première adresse utilisable
- Dernière adresse utilisable
- Transmission en monodiffusion, diffusion et multidiffusion
- adresse privée
- Adresses publiques
- Traduction d'adresses de réseau (NAT)
- Adresses de bouclage
- Adresse IPv4 APIPA (Automatic Private IP Addressing)
- adressage de classe (classe A, B, C, D et E)

Internet Assigned Numbers Authority (IANA)
Organismes d'enregistrement Internet locaux
Afrinic, APNIC, ARIN, LACNIC et RIPE NCC
domaines de diffusion
sous-réseaux
limite d'octet
VLSM (variable-length subnet mask)