Mise en application de sous réseaux/routage

EXERCICES SUR LES ADRESSES IP

---

1. Exercices basiques

Aidez-vous du tableau suivant pour faire les exercices 1.1 et 1.2 :

128	64	32	$	)	4	2	1

1.1. Convertissez les adresses IP suivantes en binaire :

a. 145.32.59.24 => 10010001.00100000.00111011.00011000
b. 200.42.129.16 => 11001000.00101010.10000001.00010000
c. 14.82.19.54 => 00001110.01010010.00010011.00110110
d. 224.12.53.90 => 11100000.00001100.00110101.01011010

1.2. Trouvez la classe des adresses IP suivantes et vérifier la valeur en convertissant le 1er octet en décimal :

a. 10000000. 00001010. 11011000. 00100111 => 128 : Classe B
b. 11101101. 10000011. 00001110. 01011111 => 237 : Classe D
c. 01001010. 00011011. 10001111. 00010010 => 74 : Classe A
d. 11001001. 11011110. 01000011. 01110101 => 201 : Classe C
e. 10000011. 00011101. 00000000. 00000111 => 131 : Classe B

2. Classes d'adresses – Identifier bits d'hôte et bits réseau

2.1. Trouver la classe des adresses suivantes et séparer les adresses IP en deux parties :

a. 118.89.67.234 => Classe A / NestID: 118 / HostID: 89.67.234
b. 199.254.250.223 => Classe C / NestID: 199.254.250 / HostID: 223
c. 223.25.191.75 => Classe C / NestID: 223.25.191 / HostID: 75
d. 10.20.30.40 => Classe A / NestID: 10 / HostID: 20.30.40
e. 191.250.254.39 => Classe B / NestID: 191.250 / HostID: 254.39
f. 192.1.57.83 => Classe C / NestID: 192.1.57 / HostID: 83
g. 127.0.0.1 => Classe A / NestID: 127 / HostID: 0.0.1
h. 239.255.0.1 => Classe D (adresse multicast)
i. 0.0.0.0 => Invalide ou non configurée
j. 255.255.255.255 => Adresse de diffusion (broadcast)
k. 1.102.45.177 => Classe A / NetID: 1 / HostID: 102.45.177

3. Adresses particulières – adresses incorrectes

3.1. Expliquer les particularités des adresses suivantes (le masque est celui associé par défaut à la classe)

a. 191.168.1.1 => Est considérée comme incorrecte car elle ne fait pas partie des plages d'adresses valides pour la classe B,
b. 127.0.0.1 => LocalHost
c. 10.133.19.27 => Adresse privée de classe A. Les adresses commençant par 10.0.0.0 sont réservées pour une utilisation privée selon RFC 1918.
d. 1.2.3.4 : Adresse publique de classe A. Cette plage spécifique n'est plus affectée à cause de l'épuisement des adresses IPv4 publiques.
e. 224.0.0.2 : IP multicast.
f. 172.16.122.68 : IP de classe B. La plage 172.16.0.0 à 172.31.255.255 est réservée pour une utilisation privée (RFC 1918).
g. 0.137.250.17 : Adresse publique de classe A mais appartient à la plage réservée 0.0.0.0 à 0.255.255.255 définie dans RFC 11.
i. 192.252.19.4: Adresse publique de classe C valide.
j. 118.17.255.255: Adresse non valide. La partie hôte ne peut pas être 255.255 dans une adresse IP.
k. 224.0.0.9: Adresse IP multicast réservée selon IANA.
l. 169.254.192.167: Adresse de lien local selon RFC 3927. Utilisée lorsqu'aucune adresse IP n'est disponible via DHCP.
m. 131.107.109.201: Adresse publique de classe B.
n. 172.31.127.9 : Adresse IP privée de classe B réservée (RFC 1918).
o. 0.0.0.0 : Adresse IP non valide.
p. 127.131.208.51 : Adresse IP non valide car la plage 127.x.x.x est réservée pour le bouclage local
q. 192.168.0.1 : Adresse IP privée de classe C.
r. 93.1.1.0 : Adresse publique de classe A.
s. 168.192.226.13 : Adresse publique de classe B.
t. 224.0.1.24 : Adresse IP multicast.
u. 224.0.0.1 : Adresse IP multicast.
v. 172.32.14.172 : Adresse IP privée invalide car hors plage (RFC 1918)
w. 248.10.10.1 : Adresse IP invalide.
x. 201.1.1.1 : Adresse publique de classe C.
y. 192.168.129.33 : Adresse IP privée de classe C.
z. 1.0.0.127 : Adresse publique de classe A valide mais réservée comme adresse de bouclage.

3.2. Dans la liste ci-dessous, si une adresse ne peut être attribuée, soulignez la partie erronée et fournissez une explication. Le masque est celui associé par défaut à la classe.

a. 245.12.33.102 -> 245 est réservé pour une utilisation future, donc adresse invalide.
b. 123.123.123.123 -> Adresse valide de classe A.
c. 199.23.107.255 -> Adresse valide dans le contexte d'un réseau avec un masque de sous-réseau approprié. Cependant, la valeur "255" dans la partie hôte est réservée pour

l'adresse de diffusion. Donc, techniquement, cette adresse pourrait être utilisée, mais pas pour identifier un hôte individuel dans un réseau.
d. 199.23.107.0 -> Adresse valide de classe C.
e. 156.266.12.103 -> L'octet "266" dépasse la plage valide pour une adresse IP
f. 99.0.0.12 -> Adresse valide de classe A.
g. 153.0.0.0 -> Adresse valide de classe B.
h. 153.0.0.255 -> Adresse valide dans le contexte d'un réseau avec un masque de sous-réseau approprié. Cependant, la valeur "255" dans la partie hôte est réservée pour l'adresse de diffusion. Donc, techniquement, cette adresse pourrait être utilisée, mais pas pour identifier un hôte individuel dans un réseau.
i. 191.23.255.255 ->.Adresse valide de classe B.
j. 33.255.255.0 -> Est invalide car elle utilise la valeur "255" dans la partie réseau, ce qui la rend invalide en tant qu'adresse de réseau..
k. 12.0.0.0 -> Adresse de réseau valide de classe A.
l. 12.255.255.255 -> L''adresse IP 12.255.255.255 utilise la valeur "255" dans les trois octets de la partie hôte, ce qui est réservé pour l'adresse de diffusion.
m. 12.0.0.255 -> 255 n'est pas autorisé pour la partie hôte. C'est l'adresse de diffusion du réseau 12.0.0.0.
n. 127.0.0.1 -> Adresse de bouclage valide.
o. 127.23.109.122 -> 127 est réservé pour le bouclage, donc l'adresse est invalide.
p. 0.23.12.122 -> 0 n'est pas autorisé comme partie réseau, donc adresse est invalide.
q. 192.12.255.102 -> Adresse valide de classe C.
r. 191.105.0.0 -> 191 est réservé pour une utilisation future, donc l'adresse est invalide.
s. 203.123.45.255 -> Adresse de diffusion invalide pour la classe C.
t. 204.0.23.198 -> Adresse invalide car 204.0.0.0/8 est réservé.
u. 224.56.204.112 -> Adresse multicast réservée valide.
v. 223.255.255.254 -> 223 est réservé pour une utilisation future, donc l'adresse est invalide.
w. 126.0.0.1 -> Adresse invalide car 126.0.0.0/8 est réservé.
x. 177.45.123.255 -> Adresse invalide car 177.0.0.0/8 est réservé.
y. 192.168.255.255 -> Adresse de diffusion valide.
z. 246.1.23.67 -> 246 est réservé pour une utilisation future, donc l'adresse est invalide.

4. Notation CIDR Une forme plus courte de notation des adresses IP avec masque de sous-réseau est connue sous le nom de « notation CIDR » (Classless Inter-Domain Routing).

Adresse CIDR	Adresse valide ?	Masque par défaut ?	Explications	Notation standard	Adresse Broadcast	Plage d'adresses
12.1.1.1 /8	OUI	OUI	Réseau 12.0.0.0, les bits hôtes sont différents de 0	12.1.1.1 255.0.0.0	12.255.255.255	12.0.0.1-12.255.255.254
209.207.177.100 /24	OUI	OUI			209.207.177.255	**Première adresse** : 209.207.177.1 **Dernière adresse** : 209.207.177.254
192.0.35.12 /24	OUI	OUI			192.0.35.255	**Première adresse** : 192.0.35.1 **Dernière adresse** : 192.0.35.254
120.146.80.1 /16	OUI	OUI			120.146.255.255	**Première adresse** : 120.146.0.1 **Dernière adresse** : 120.146.255.254
120.80.1.0 /8	OUI	OUI			120.255.255.255	**Première adresse** : 120.0.0.1 **Dernière adresse** : 120.255.255.254
211.104.16.17 /24	OUI	OUI			211.104.16.255	**Première adresse** : 211.104.16.1 **Dernière adresse** : 211.104.16.254
172.168.0.1 /24	OUI	OUI			172.168.0.255	**Première adresse** : 172.168.0.1 **Dernière adresse** : 172.168.0.254
96.139.84.12 /8	OUI	OUI			96.255.255.255	**Première adresse** : 96.0.0.1 **Dernière adresse** : 96.255.255.254
172.16.32.0 /24	NON	OUI			172.16.32.255	**Première adresse** : 172.16.32.1 **Dernière adresse** : 172.16.32.254

172.16.0.127 /16	NON	OUI			172.16.255.255	**Première adresse** : 172.16.0.1 **Dernière adresse** : 172.16.255.254
192.168.19.87 /8	NON	OUI			192.255.255.255	**Première adresse** : 192.0.0.1 **Dernière adresse** : 192.255.255.254
172.16.32.1 /8	NON	OUI			172.255.255.255	**Première adresse** : 172.0.0.1 **Dernière adresse** : 172.255.255.254
210.71.10.128 /16	OUI	OUI			210.71.255.255	**Première adresse** : 210.71.0.1 **Dernière adresse** : 210.71.255.254

5.1. Remplissez le tableau ci-dessous en indiquant quels hôtes peuvent dialoguer et pourquoi

Machines	Peuvent dialoguer ?	Raison
A et B	Oui	Appartiennent au même sous-réseau 172.16.11.0/24
A et F	Oui	Appartiennent au même sous-réseau 172.16.10.0/24
B et D	Oui	Appartiennent au même sous-réseau 172.16.11.0/24
C et E	Oui	Appartiennent au même sous-réseau 172.16.100.0/24
A et C	Oui	Bien que dans des sous-réseaux différents, elles sont sur le même segment sans routeur
A et D	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux différents
A et E	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux différents
B et C	Oui	Bien que dans des sous-réseaux différents, elles sont sur le même segment sans routeur
B et E	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux différents

B et F	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux différents
C et D	Oui	Bien que dans des sous-réseaux différents, elles sont sur le même segment sans routeur
C et F	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux différents
D et E	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux différents
D et F	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux différents
E et F	Oui	Même segment, donc peuvent communiquer malgré des sous-réseaux

5.2. Est-il possible de faire communiquer TOUS les hôtes de ce segment :
a) en gardant les mêmes masques ? (expliquez)
En gardant les mêmes masques, il n'est pas possible de faire communiquer tous les hôtes de ce segment. Bien qu'ils soient sur le même segment sans routeur, certaines machines appartiennent à des sous-réseaux différents avec les masques attribués actuellement. Par exemple, A et B ne peuvent pas communiquer directement avec leur masque actuel car ils sont dans des sous-réseaux différents (172.16.10.0/24 et 172.16.11.0/24).

b) en gardant les mêmes adresses ? (expliquez)
En gardant les mêmes adresses IP, il est possible de faire communiquer tous les hôtes de ce segment en modifiant les masques de sous-réseau. Puisqu'ils sont sur le même segment, un masque de sous-réseau plus large pourrait englober toutes les adresses IP dans un seul sous-réseau.

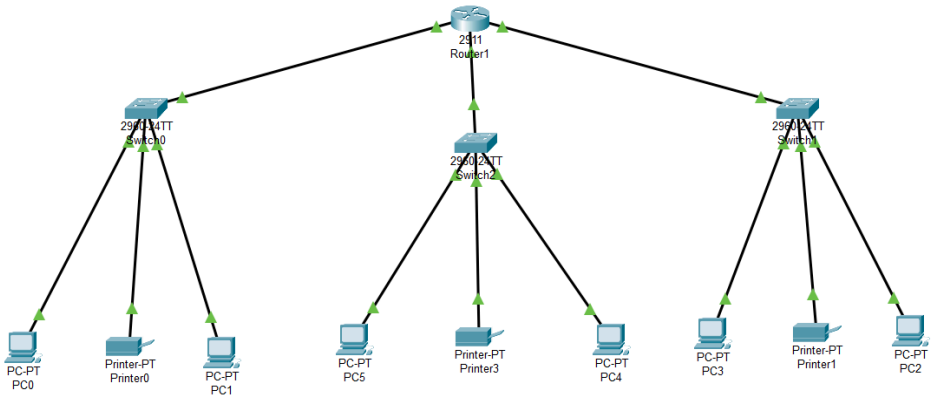
c) On souhaite que tous les hôtes (A, C, E et F) puissent se parler, mais que B ne parle qu'avec D et réciproquement car ces 2 machines contiennent des informations sensibles. Sans toucher aux adresses du schéma, on modifie les masques ainsi : 255.255.255.0 (B et D) et 255.255.0.0 (A, C, E, F)
Le but est-il atteint? Expliquez pourquoi.

c) Le but d'isoler B et D des autres hôtes est partiellement atteint, mais pas complètement.

- B et D appartiennent au sous-réseau 172.16.11.0/24 avec le masque 255.255.255.0, ils peuvent donc communiquer entre eux.
- A, C, E et F appartiennent au sous-réseau 172.16.0.0/16 avec le masque 255.255.0.0, ils peuvent donc communiquer entre eux.
- Cependant, B et D peuvent toujours communiquer avec A, C, E et F car ils sont sur le même segment de réseau sans routeur.

Pour isoler complètement B et D des autres hôtes, il faudrait les placer sur un segment de réseau séparé avec un routeur configuré pour contrôler le trafic entre les segments. Ou bien, il faudrait mettre en place des règles de filtrage réseau (pare-feu) pour bloquer les communications indésirables.

Exercice Packet Tracer routage



Se connecter avec Telnet

Telnet et SSH sont deux protocoles différents utilisés pour l'accès et la gestion à distance de systèmes et d'équipements réseau comme les routeurs.

Sécurité

- Telnet transmet les données, y compris les noms d'utilisateur et mots de passe, en texte clair non chiffré, ce qui le rend vulnérable aux écoutes et aux attaques.
- SSH (Secure Shell) utilise le chiffrement pour sécuriser la connexion et protéger les données transmises, offrant ainsi une meilleure sécurité.

Ports utilisés

- Telnet utilise le port TCP 23 par défaut.
- SSH utilise le port TCP 22 par défaut.

Autres fonctionnalités :

- Telnet permet uniquement d'ouvrir une session texte distante.
- SSH offre des fonctionnalités supplémentaires comme le transfert de fichiers sécurisé (SCP, SFTP) et le tunneling sécurisé.

En raison des risques de sécurité inhérents à Telnet, SSH est fortement recommandé pour les accès à distance aux équipements réseau. La plupart des fabricants de routeurs et de commutateurs recommandent ou imposent même l'utilisation de SSH plutôt que Telnet pour des raisons de sécurité.

Cependant, dans certains environnements hérités ou de test, Telnet peut encore être utilisé, bien qu'il soit préférable de le remplacer par SSH dès que possible pour renforcer la sécurité du réseau.