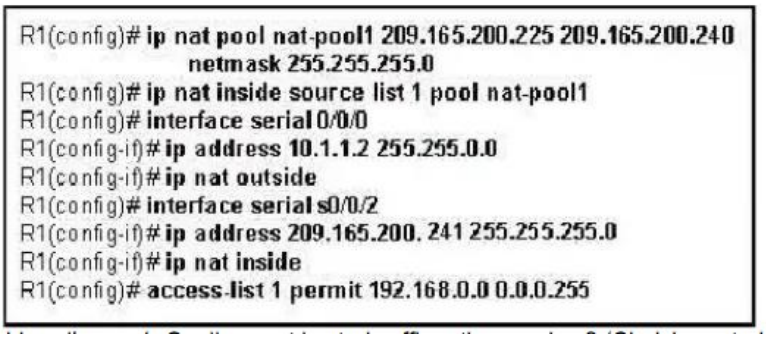
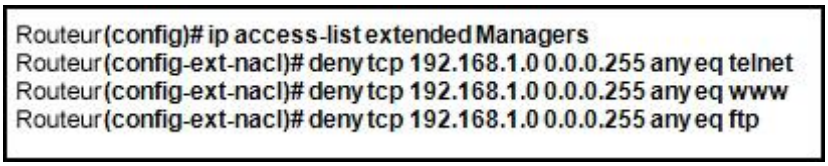
QCM:

1. Quelles sont les affirmations vraies

   - La fonction NAT avec surcharge est activée.
   - La fonction NAT dynamique est activée
   - La traduction d'adresses va échouer
   - La configuration des interfaces est incorrecte
   - Le trafic entrant dans l'interface série 0/0/2 est traduit avant de sortir de l'interface série 0/0/0.



2.



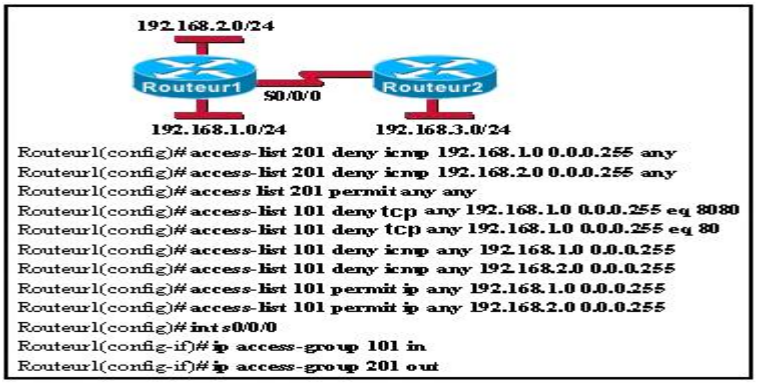
Reportez-vous à la figure. Que se passe-t-il lorsque l'administrateur réseau émet les commandes indiquées lorsqu'une liste de contrôle d'accès appelée Managers existe déjà sur le routeur ?

- Les commandes remplacent la liste de contrôle d'accès Managers qui existe déjà sur le routeur.
- Les commandes sont ajoutées à la fin de la liste de contrôle d'accès Managers qui existe déjà sur le routeur.
- Les commandes sont ajoutées au début de la liste de contrôle d'accès Managers qui existe déjà sur le routeur.
- L'administrateur réseau reçoit un message d'erreur qui stipule que la liste de contrôle d'accès existe déjà.

3. Quel est l'effet de la commande Router1(config-ext-nacl)# **permit tcp 172.16.4.0 0.0.0.255 any eq www** lors de son implémentation en entrée sur l'interface f0/0 ?
   - Tout le trafic en provenance de tout réseau et destiné à Internet est autorisé.

- Tout le trafic en provenance du réseau 172.16.4.0/24 est autorisé partout, sur tout port.
- Le trafic en provenance du réseau 172.16.4.0/24 est autorisé sur l'ensemble des destinations de port 80.
- Tout le trafic TCP est autorisé et tout autre trafic est refusé.
- La commande est refusée par le routeur car elle est incomplète.

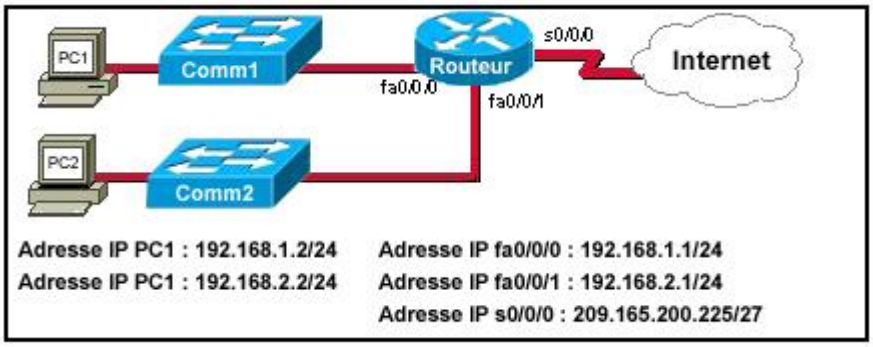
4.



Lisez l'exposé. Quelle affirmation décrit correctement la manière dont le Routeur 1 traite une requête FTP entrant dans l'interface s0/0/0 et destinée à un serveur FTP à l'adresse IP 192.168.1.5 ?

- Il fait correspondre le paquet entrant à l'instruction access-list 101 permit ip any 192.168.1.0 0.0.0.255, continue à comparer le paquet aux autres instructions dans la liste de contrôle d'accès 101 afin d'assurer qu'aucune autre instruction n'interdit FTP, puis il autorise le paquet dans l'interface s0/0/0.
- Il fait correspondre le paquet entrant à l'instruction access-list 201 permit any any, puis l'autorise dans l'interface s0/0/0.
- Il fait correspondre le paquet entrant à l'instruction access-list 101 permit ip any 192.168.1.0 0.0.0.255, ignore les autres instructions de la liste de contrôle d'accès 101, puis il autorise le paquet dans l'interface s0/0/0.
- Il atteint la fin de la liste de contrôle d'accès 101 sans correspondance à aucune condition et abandonne le paquet car l'instruction access-list 101 permit any any ne figure pas dans la liste.

5.



Reportez-vous au schéma. L'administrateur réseau crée une liste de contrôle d'accès standard pour interdire au trafic en provenance du réseau 192.168.1.0/24 d'atteindre le réseau 192.168.2.0/24, tout en autorisant l'accès à Internet à tous les réseaux. Sur quelle interface de

routeur et dans quelle direction la liste doit-elle être appliquée ?

- Interface fa0/0/0, entrant
- Interface fa0/0/0, sortant
- Interface fa0/0/1, entrant
- Interface fa0/0/1, sortant

6. Reportez-vous à l'illustration. Un administrateur réseau a configuré l'ACL 9 comme indiqué. Les utilisateurs sur le réseau 172.31.1.0 /24 ne peuvent pas transférer le trafic via le routeur CiscoVille. Quelle est la cause la plus probable de la défaillance de la circulation ?

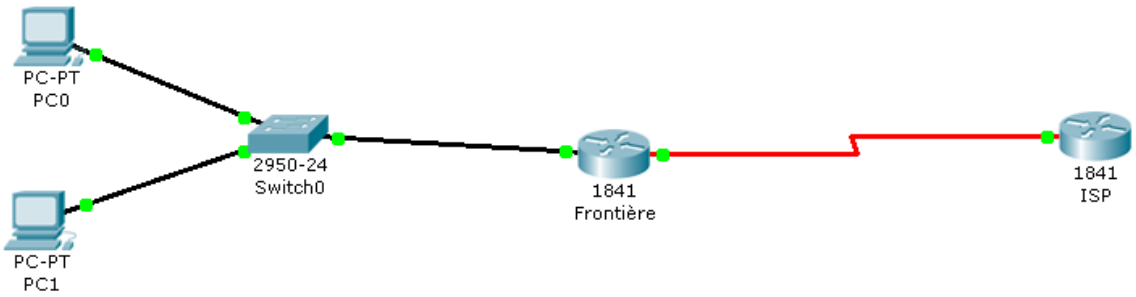
```
CiscoVille#
CiscoVille# configure terminal
CiscoVille(config)# access-list 9 permit 172.29.0.0 0.0.0.255
CiscoVille(config)# access-list 9 permit 172.30.0.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 172.31.0.0 0.0.255.255
CiscoVille(config)# access-list 9 permit 172.31.1.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 192.168.1.0 0.0.0.255
CiscoVille(config)# access-list 9 permit any
CiscoVille(config)# interface fastethernet0/1
CiscoVille(config-if)# ip access-group 9 in
CiscoVille(config-if)# end
```


- L'instruction permit spécifie un masque générique incorrect.
- Le numéro de port du trafic n'a pas été identifié avec le mot-clé eq .
- La séquence des ACEs est incorrecte.
- Le mot-clé établi n'est pas spécifié.

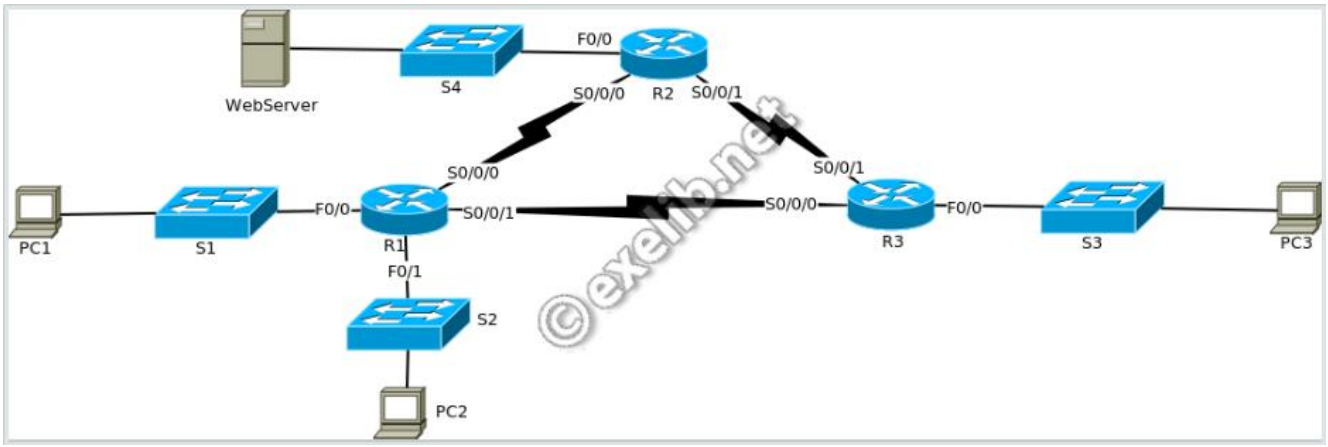
Exercice 1 :

L'entreprise **X** a un accès à l'internet (voir la figure ci-dessous). L'ISP fourni 6 adresses IP publiques de 198.18.184.95 – 198.18.184.100. Cette entreprise ayant 120 utilisateurs, qu'ils demandent l'accès à l'internet simultanément tel que l'adresse Réseau de ces 120 hosts est 192.168.255.128/26.

1) Présentez et expliquez la solution de l'accès à l'internet pour l'entreprise X.
2) Configurez le routeur de frontière entre les deux réseaux publique et privé.
3) Configurer des ACL réflexives sachant que les utilisateurs de réseau privé n'accèdent que au services HTTPS, DNS, SMTP via internet



Exercice 2 :



Tel que l'adresse réseau de LAN1 (PC1) est 192.168.10.0/24, LAN2 (PC2) : 192.168.11.0/24, LAN3 (PC3) : 192.168.30.0/24, WebServer : 192.168.20.20

1. Créer une liste de contrôle d'accès standard numérotée refusant l'accès vers le réseau 192.168.30.0/24 à partir du réseau 192.168.11.0/24.
2. Créer une liste de contrôle d'accès étendu numéroté autorisant l'accès au serveur web avec seulement le service http à partir du réseau de 192.168.10.0/24.

Exercice 3 :

Le routeur périphérique de l'entreprise dispose de trois interfaces : l'interface f0/0 est connectée au réseau interne, l'interface f0/1 est connectée à la DMZ, et l'interface s0/0/0 est connectée à Internet.

1. Mettre en place le par-feu « *Stateful Packet Inspection* » qui vérifie le trafic HTTP, HTTPS, DNS et ICMP à destination de l'Internet conformément à la figure ci-dessous :