FEDERATION EUROPEENNE DES ECOLES
EUROPEAN FEDERATION OF SCHOOLS
Organisation non gouvernementale dotée du statut participatif auprès du Conseil de l'Europe
NGO enjoying participatory status with the Council of Europe

UE D - TECHNIQUES PROFESSIONNELLES

Master Européen d'Informatique
UC D41.1 - Réseaux, système et sécurité

Tous supports papiers et matériels sont interdits

Les réponses au QCM doivent être reportées sur la fiche optique fournie

Type d'épreuve : QCM et Exercice pratique
Durée : 3 heures
Session : Juin 2011

UC D41.1– RESEAUX, SYSTEMES ET SECURITE

PRESENTATION DE L'ETUDE DE CAS

L'étude de cas sera composée de deux parties distinctes :

- une partie « Sécurité » concernant le dossier 1,
- une partie « Réseaux et système » concernant le dossier 2.

Vous devez prévoir des copies distinctes pour chaque partie.

BAREME DE NOTATION QCM

Bonne réponse	3 points
Absence de réponse	0 point
Réponse erronée	-1 point

Nombre de points possible : **150 points**

BAREME DE NOTATION EXERCICE PRATIQUE

Dossier 1 - Sécurité	130 points
Dossier 2 - Réseaux avancés	170 points
Total	**300 points**

1/ QCM : 45 minutes

1. **Le fichier /etc/host.conf permet :**
   a. la résolution des noms
   b. la configuration des postes du réseau
   c. l'ordre de recherche pour la résolution de nom
   d. la correspondance des adresses IP avec des noms d'hôtes

2. **Si umask = 007, les droits par défaut pour les dossiers auront la valeur octale :**
   a. 0775
   b. 0665
   c. 0660
   d. 0770

3. **Lequel de ces protocoles n'est pas un protocole utilisé pour créer un VPN ?**
   a. IPSec
   b. L2PP
   c. L2TP
   d. SSL

4. **Pour monter une partition d'un disque dur de type SATA sur le lien /usbexterne, quelle proposition est correcte ?**
   a. mount -t ext3 /dev/hdb5 /usbexterne
   b. mount -t vfat /mnt/windows /usbexterne
   c. mount /dev/sdc1 /dev/sdc
   d. mount –t ext3 /dev/sdc1 /usbexterne

5. **Pour vérifier la structuration et l'intégrité des mots de passe et des champs associés des comptes Unix/Linux une commande possible est ?**
   a. verify shadow
   b. verify password
   c. pwck
   d. aucune des propositions ne convient

6. **Pour vérifier tous les systèmes de fichiers montés pendant une session, on devra consulter le fichier :**
   a. /etc/inittab
   b. /etc/mtab
   c. /etc/fstab
   d. /etc/mountab

7. **Les caractéristiques d'un lien par ls -l /bin/Leucippe donne :**
   - rwx r- - -w- 2 root presocratique 755 29 Fev. 2009 Leucippe.
   a. le lien /bin/Leucippe possède un seul lien physique
   b. root est dans le groupe "presocratique"
   c. tout processus ayant l'uid=0 est propriétaire de Leucippe
   d. le lien /bin/Leucippe possède deux liens symboliques (synonymes, raccourcis,…)

8. **Quelle proposition est fausse concernant ce même lien :**
   - rwx r- - -w- 2 root presocratique 755 29 Fev. 2009 Leucippe ?
   a. le groupe "presocratique" est le groupe du lien Leucippe
   b. le groupe "presocratique" est le groupe du propriétaire root
   c. tout processus ayant l'uid=0 est administrateur Linux/Unix
   d. les droits d'accès du lien /bin/Leucippe ne sont pas 0755 (en octal)

9. **Pour configurer SAMBA en PDC, on doit obligatoirement configurer, dans le fichier smb.conf, l'option :**
   a. security = share
   b. domain master = yes
   c. domain logons = yes
   d. domain name = <nom_domaine>

10. **Que fait la commande : echo 0 > /proc/sys/net/ipv4/ip_forward ?**
    a. elle active le routage ipv4
    b. elle inhibe le broadcast en icmp
    c. elle active le routage ipv6
    d. elle désactive le routage ipv4

11. **Pour rajouter une route par défaut à un nœud donné, vous utiliserez la commande :**
    a. # route add default 172.16.0.254 netmask 255.255.0.0
    b. # route add -net default gw 172.16.0.254 netmask 255.255.255.0
    c. # route add default gw 172.16.0.254
    d. # toutes ces propositions

12. **Que ne permet pas de faire un mécanisme de Filtration FireWall comme NetFilter (iptable) ?**
    a. iptable permet de faire de la translation d'adresse réseau (adresse IP) et d'adresse socket (ports)
    b. iptable peut modifier des paquets au fil de l'eau (à la volée)
    c. iptable permet de configurer le protocole IP
    d. iptable est le mécanisme, l'outil, qui par directives permet de configurer le FireWall NetFilter

13. **Quelle est la bonne syntaxe pour autoriser les réponses FTP ?**
    a. iptables -A OUTPUT -p tcp --dport ftp -j ACCEPT
    b. iptables -A INPUT -p tcp --sport ftp -j ACCEPT
    c. iptables -A INPUT -p tcp --dport ftp -j ACCEPT
    d. iptables -A OUTPUT -p tcp --dport ftp -j ACCEPT

14. **Combien de type(s) de VLAN existe(nt)-t-il(s) ?**
    a. 3
    b. 1
    c. 2
    d. 5

15. **Pour avoir le package Apache, PHP, PostGreSQL sous Linux, il faut installer une plate-forme :**
    a. LAMP
    b. LAPP
    c. WAMP
    d. WAPP

16. Donnez un équivalent en mode symbolique de la commande : #chmod –R 455 qcm.

a. chmod –R go+x,ug-w qcm
b. chmod –R ugo-r,ug-w qcm
c. chmod –R ugo+r,go+x qcm
d. chmod –R ugo+x,ug-rw qcm

17. Quelle est l'adresse de broadcast pour le réseau 169.168.1.0/28 ?

a. 169.168.1.0
b. 169.168.1.255
c. 169.168.1.15
d. 169.168.255.255

18. Quel est le nombre de bits qui représente une adresse IP version 6 ?

a. 256 bits
b. 64 bits
c. 128 bits
d. 32 bits

19. Quelle masque de sous réseaux utiliser pour avoir au maximum de 600 machines dans chaque sous réseau ?

a. 255.255.252.0
b. 255.255.240.0
c. 255.255.245.0
d. 255.255.255.0

20. Un firewall peut être un :

a. dispositif d'anti-intrusion dans une salle serveur informatique
b. dispositif bloquant les départs d'incendie dans un local informatique
c. élément matériel contrôlant les accès entre réseaux informatiques
d. logiciel de protection d'accès à des réseaux informatiques

21. Comment filtrer et contrôler les accès à internet en fonction des thèmes consultés et de l'utilisateur ?

a. mettre un proxy-cache
b. mettre un routeur
c. mettre un firewall
d. mettre des antispywares

22. Quelle commande permet de mettre sous tension une interface de routeur ?

a. Router(config-if)# enable
b. Router(config-if)# no down
c. Router(config-if)# no shutdown
d. Router(config-if)# interface up

23. Que se passe-t-il si un routeur ne trouve pas de fichier de configuration correct lors de la séquence de démarrage ?

a. la séquence de démarrage est réinitialisée
b. le routeur surveille le trafic local afin de déterminer la configuration requise pour les protocoles de routage
c. le routeur génère un fichier de configuration par défaut basé sur la dernière configuration valide
d. le routeur invite l'utilisateur à fournir une réponse pour accéder au mode setup

24. Concernant l'équilibrage de charge, quelle affirmation est exacte ?

a. l'équilibrage de la charge se produit lorsqu'un routeur envoie le même paquet à différents réseaux de destination
b. l'équilibrage de la charge se produit lorsque le même nombre de paquets sont envoyés sur les routes statiques et dynamiques
c. s'il existe plusieurs chemins avec des mesures différentes vers une destination, le routeur ne peut pas prendre en charge l'équilibrage de la charge
d. l'équilibrage de la charge à coût inégal est pris en charge par le protocole EIGRP

25. Quelles informations d'adresse un routeur modifie-t-il parmi les informations qu'il reçoit d'une interface Ethernet associée avant de les retransmettre ?

a. l'adresse source et l'adresse de destination de la couche 2
b. seulement l'adresse source de la couche 2
c. seulement l'adresse source de la couche 3
d. l'adresse source et l'adresse de destination de la couche 3

26. Que se passe-t-il sur un réseau à vecteur de distance qui n'a pas convergé ?

a. le trafic n'est pas acheminé tant que le système ne converge pas
b. les mises à jour de table de routage sont envoyées vers des destinations incorrectes
c. des entrées de table de routage incohérentes
d. rien, le routage à vecteur de distance n'a pas de convergence

27. Dans le routage dynamique, les interfaces passives sont des interfaces :

a. désactivées
b. favorisées dans la mise à jour des tables de routage
c. non utilisées dans la mise à jour des tables de routage
d. de réception des tables de routage

28. Quel protocole de routage n'est pas à vecteur de distance ?

a. RIPv1
b. EIGRP
c. RIPv2
d. IS-IS

29. Quel algorithme est exécuté par les protocoles de routage à état de liens pour calculer le chemin le plus court vers les réseaux de destination ?

a. DUAL
b. Dijkstra
c. Bellman-Ford
d. Diffie-Hellman

30. Les mesures utilisées par les protocoles de routage sont :

a. une méthode propriétaire de Cisco pour convertir les distances en unité standard
b. une valeur quantitative utilisée par un protocole de routage pour mesurer une route donnée
c. une valeur composée de la quantité de paquets perdus pour tous les protocoles de routage
d. uniquement utilisés par les protocoles de routage dynamique

31. Les interfaces d'un réseau ont été configurées avec des adresses IP, mais aucun protocole de routage ou route statique n'a encore été configurée. Quelles routes sont présentes dans la table de routage ?

a. routes par défaut
b. routes de diffusion
c. réseaux directement connectés
d. aucune route, la table de routage est vide

32. Quelles sont les différences entre Multicast et Broadcast ?

a. il n'y en a pas, c'est la même chose
b. le Broadcast est un envoi global et le Multicast est un envoi vers un groupe
c. le Broadcast est un renvoi de messages et Multicast est un envoi de messages
d. le Multicast est inclus dans le routage et le Broadcast ne l'est pas

33. Un système autonome est un groupe de routeur géré par :

a. les mêmes administrateurs et utilisant le même protocole de routage
b. plusieurs fournisseurs d'accès et utilisant le même protocole de routage
c. les mêmes administrateurs et utilisant plusieurs protocoles de routage
d. plusieurs fournisseurs d'accès et utilisant plusieurs protocoles de routage

34. Définissez le protocole Spanning Tree ?

a. protocole de routage
b. protocole de résolution d'adresses
c. protocole qui garantit l'unicité du chemin et évite les boucles dans un réseau local
d. protocole de niveau trame qui acquitte les données

35. Quel sigle dans la liste ci-dessous représente un protocole d'authentification PPP ?

a. SSL
b. MsCHAP
c. MD5
d. PKI

36. Quel protocole de routage est un protocole utilisé dans le routage EGP ?

a. RIP
b. OSPF
c. IGRP
d. BGP

37. Dans SSH, le cryptage utilisé pour l'authentification est un :

a. cryptage symétrique
b. cryptage asymétrique
c. les deux propositions précédentes
d. aucune des propositions précédentes

38. L'algorithme DES :

a. utilise une clé privée et une clé publique
b. fait appel à la notion PKI
c. utilise une clé connue de tout le monde
d. utilise une clé secrète

39. Dans les algorithmes de "chiffrement symétrique" :

a. la même fonction mathématique sert à chiffrer et déchiffrer
b. on ne parle pas de clés chiffrement/déchiffrement on parle plutôt de fonctions de Chiffrement/déchiffrement
c. c'est l'inverse de la clé de chiffrement qui sert à déchiffrer
d. la même clé sert à chiffrer et déchiffrer

40. Quand à chaque caractère de l'alphabet du texte clair correspond un ensemble d'éléments du cryptogramme, la cryptographie est du type substitution :

a. simple
b. homophonique
c. polyalphabétique
d. de polygramme

41. Lequel des mots de passe suivants peut-il être considéré comme robuste ?

a. P@ssw0rd
b. jean7669
c. J*ple04>F
d. W3lc0m3

42. Une architecture PKI permet de :

a. gérer la politique de distribution des clés publiques
b. certifier l'authenticité des clés publiques de mes correspondants
c. signer les clés publiques
d. aucun des trois premiers choix

43. Parmi les suivants, quel est le meilleur moyen d'empêcher des intrusions via le réseau sans fil ?

a. désactiver la diffusion du SSID
b. filtrer les adresses MAC
c. activer le chiffrement WEP
d. activer le chiffrement WAP

44. Une fonction de hashage :

a. permet à un destinataire d'un message de vérifier l'intégrité des données et de contrôler l'identité de leur expéditeur
b. construit une empreinte d'une chaîne de données, à partir de laquelle il est impossible de revenir à la chaîne de données initiale
c. calcule un checksum sur un fichier qui permet d'assurer de son intégrité....
d. n'assure aucune des fonctions précédentes

45. Vous êtes l'administrateur réseau du domaine Windows 2008 d'Infosup. Votre réseau est constitué d'un serveur DNS, d'un serveur DHCP et de 125 ordinateurs clients sous Windows 7. Le serveur DNS est chargé de la résolution de noms au sein du réseau et transmet des requêtes de résolution de noms au serveur DNS du fournisseur d'accès Internet de l'entreprise XSA.

Un utilisateur se plaint qu'il ne peut accéder à un site de partenaire de l'entreprise. Il reçoit le message d'erreur suivant: "Serveur non trouvé ou erreur DNS". Par contre, il peut accéder à tous les autres sites internet qu'il souhaite. Vous tentez de votre côté d'accéder au site du partenaire en question et vous n'éprouvez aucune difficulté à cela.

Vous vérifiez qu'il reçoit bien les informations concernant le DNS par le serveur DHCP.

Que devez-vous faire maintenant ?

a. ouvrir une console DOS sur l'ordinateur de l'utilisateur en question et taper "ipconfig/registerdns"
b. ouvrir une console DOS sur l'ordinateur de l'utilisateur en question et taper "ipconfig/flushdns"
c. ouvrir une console DOS sur l'ordinateur de l'utilisateur en question et taper "ipconfig/refreshdns"
d. ouvrir une console DOS sur l'ordinateur de l'utilisateur en question et taper "ipconfig/renew"

46. Le réseau d'une entreprise très en vue fait face à de nombreuses tentatives d'intrusions.

L'administrateur souhaite diviser son réseau afin de placer ses serveurs sensibles dans un autre emplacement que ses serveurs accessibles depuis Internet.

Quel dispositif implémenter ?

a. une DMZ (Demilitarized Zone)
b. un pot de miel (honeypot)
c. un pare-feu (firewall)
d. un nouveau sous-réseau

47. Le câblage de votre réseau traverse des ateliers qui contiennent des équipements électriques fonctionnant à des tensions élevées. Vous êtes préoccupé par les risques d'interférence. Quel câblage conseillez-vous ?

a. le câble UTP
b. le câble STP
c. le câble coaxial
d. la fibre optique

48. Le service interne de tâche planifiée "crond", prend en charge un certain nombre de tâches sécurisées en administration : sauvegarde, lancement de services, firewall dynamique, …
On voudrait déclencher une procédure de test d'intégrité sur les partitions tous les 1ers et 3èmes mercredis du mois à minuit et 30 minutes. Indiquez la bonne directive crond :

a. `0 0 1,3 * 3 /sbin/fs_integrite C:\ D:\ E:\`
b. `0 30 * * wed /sbin/fs_integrite / /home /bin`
c. `0 0 * * 2 /sbin/fs_integrite / /home /bin`
d. `30 0 1-7,14-20 * 3 /sbin/fs_integrite / /home /bin`

49. Quel protocole d'authentification, implémenté dans l'annuaire Active Directory de Windows 2008, autorise un accès à ses objets ?

a. NT Lan Manager
b. Lightweight Directory Access Protocol
c. Kerberos
d. Secure Sockets Layer

50. Décrivez la directive noyau exécutée par le pid=1 du fichier /etc/inittab en éliminant la <u>proposition fausse</u> : 8:35:respawn:/etc/mgetty tty8.

a. respawn, lance l'écoute sur un terminal
b. respawn est un mode d'exécution persistant
c. tty8 est un lien /dev/tty8 sur un terminal
d. 35 indique qu'il se déclenche sur les niveaux d'exécution 3 et 5

2/ Exercice pratique : 2 heures 15

⇨ Dossier 1 - Sécurité

Question 1 - Sécurité Windows
Quel sens donnez-vous dans Windows aux permissions explicites, héritées et effectives ?
Pourquoi créer des unités organisationnelles (UO) dans une structure Active Directory ?
Citez 2 raisons principales.

Question 2 - Clef secrète
Votre correspondant et vous ne possédez pas encore de clef secrète pour échanger des messages confidentiels via la cryptographie symétrique. Vous choisissez une clef secrète.
Quelle est la méthode pour la lui adresser avec le plus de sécurité et commodité ?

Question 3 - Certificat numérique
Citez 6 informations différentes que l'on trouve à l'intérieur d'un certificat numérique.

Question 4 - Attaque réseau
Définissez une attaque Man in the Middle (Homme du milieu).
Citez un exemple de cette attaque et expliquez son fonctionnement.

Question 5 - Pare-feu Netfilter
Expliquez l'objectif de ces commandes :

```
Iptables –A INPUT –p tcp –i eth0 –s 10.30.40.200 –d 10.30.40.100  --sport 110 –j ACCEPT
Iptables –A OUTPUT –p tcp –o eth0 –s 10.30.40.100 –d 10.30.40.200  --dport 110 –j ACCEPT
Iptables –A INPUT –p tcp –i eth0 –s 10.30.40.200 –d 10.30.40.100  --sport 25 –j ACCEPT
Iptables –A OUTPUT –p tcp –o eth0 –s 10.30.40.100 –d 10.30.40.200  --dport 25 –j ACCEPT
Iptables –P INPUT DROP
Iptables –P OUTPUT DROP
```

Question 6 - Sécurité sur les Sessions
Mettez un mécanisme de sécurisation de surcharge de session sur certains services de session de flux commandes à distance type rsh, telnet, ssh,…

On vous demande de fabriquer un outil en script Shell, appelé "monolog" qui n'autorisera qu'une session par login.
En sécurité cela peut servir à limiter la charge du serveur en nombre de sessions, ou à éviter qu'une administration distante n'autorise qu'un administrateur à la fois sur un serveur sensible…
Pour ce script, vous avez le choix soit de :

- bloquer tout de suite la nouvelle session, avant qu'on ait pu prendre la main sur le Shell,
- faire une post-analyse, une fois que la deuxième session a lieu, de prévenir à l'écran que cette session va être fermée, en laissant éventuellement un timeout suffisant

Ce script pourra être destiné à un login particulier.

Exemple
monolog guest
Le login guest, et seulement lui, ne peut ouvrir qu'une session.

monolog
Tous les logins sont concernés.

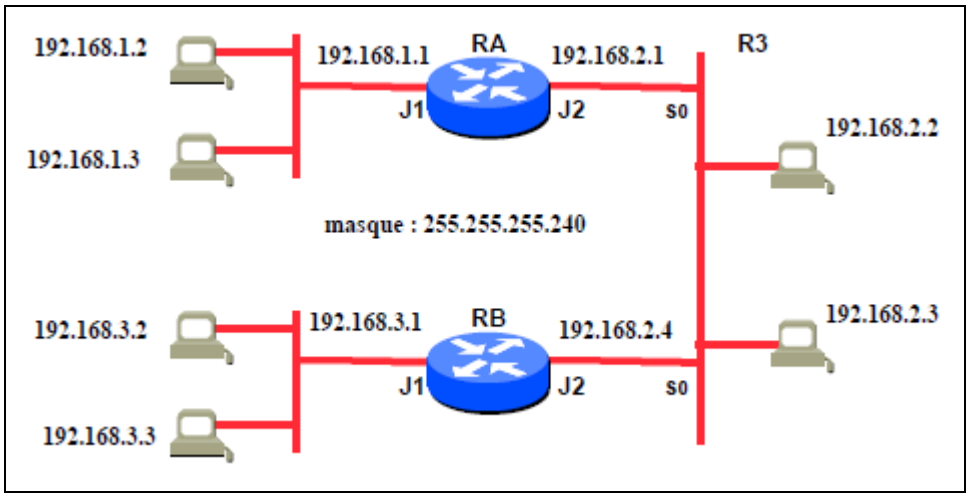
NB
Vous devez fournir le code du script dans un des cas décrits au-dessus, au choix, et surtout, expliquer comment l'administrateur met en place un tel mécanisme dans un système Linux/Unix autour d'un ou plusieurs comptes (les fichiers qui sont modifiés…).

Attention également, le mécanisme doit se déclencher à l'ouverture de la 2ème session, même si vous ne cassez pas cette session tout de suite.

Question 7 - Chiffrement asymétrique
Si vous perdez votre clef privée, pouvez-vous encore envoyer des mails chiffrés ? Et en recevoir ?
Pouvez-vous encore signer des mails, vérifiez des signatures de mails que vous recevez ?
Que doit-on faire pour être capable d'effectuer à nouveau toutes les opérations ?

⇨ Dossier 2 - Réseaux avancés

Question 1 - Routage RIP
Soit le réseau ci-dessous, exploité en RIP V1 :



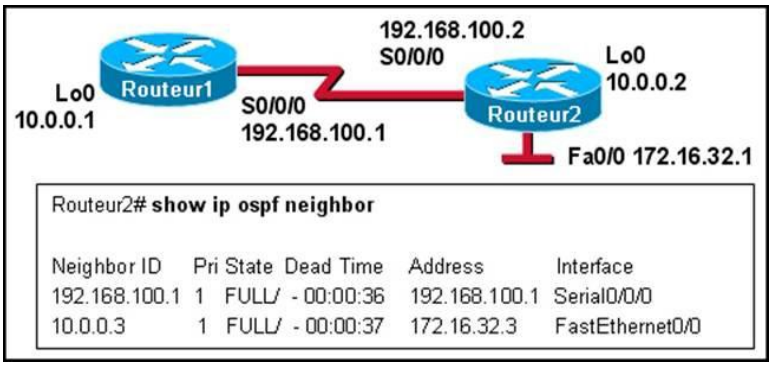
Quelles sont les tables de routage de RA et RB ?
On utilisera le format simplifié suivant :

Destination	Masque	Prochain Saut	Interface	Coût

Question 2 - Routage OSPF

L'administrateur réseau souhaite définir le numéro du processus du routeur OSPF à 100 vers le réseau 192.168.100.1.

Quelle est la commande permettant à l'administrateur d'accomplir cette opération ?



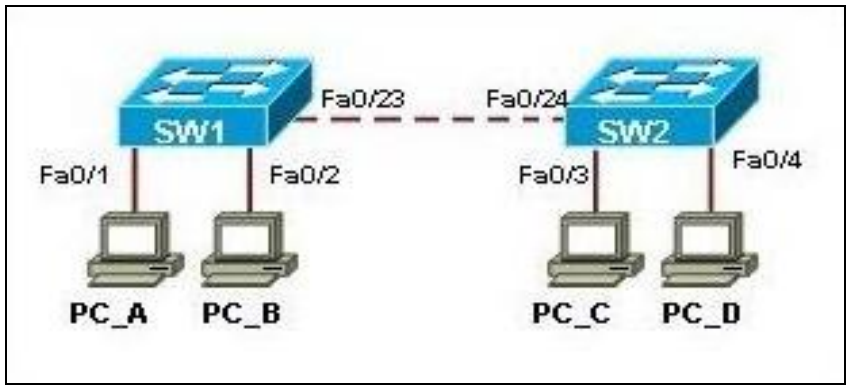
Question 3 - Table de pontage

Reportez-vous à l'illustration.

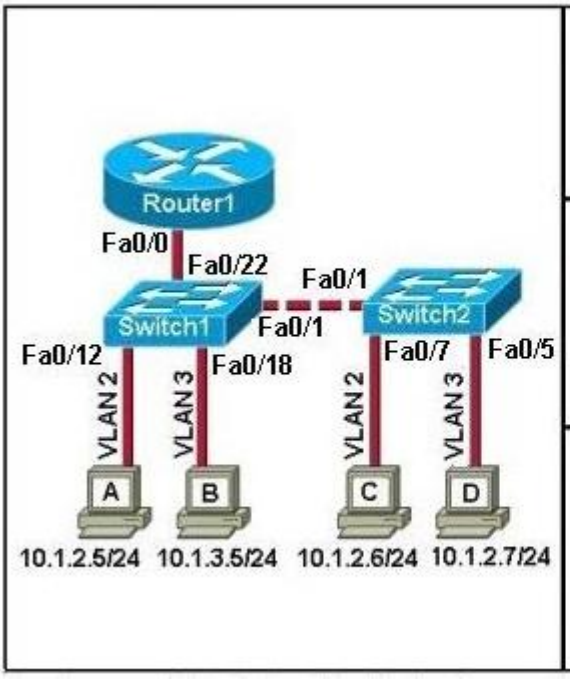
Quelle action SW1 effectue-t-il sur une trame envoyée de PC_A vers PC_C si la tables d'adresses MAC du SW1 est vide ?

Qu'en sera-t-il lors de la prochaine trame envoyée ?

Quel est le rôle du TTL dans une table de pontage et qu'advient l'association qui a un TTL égal à zéro ?



Question 4 - Agrégation de VLAN
On considère le schéma ci-dessous :



Switch1# show interface fa0/1 trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 desirable 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-20, 30, 40

Switch1# show interface fa0/22 trunk
Port Mode Encapsulation Status Native vlan
Fa0/22 desirable 802.1q trunking 1

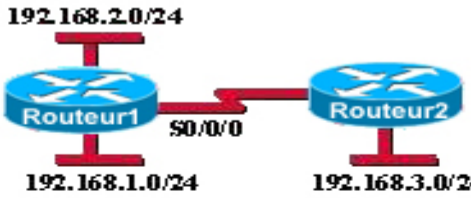
Port Vlans allowed on trunk
Fa0/22 1-20, 30, 40

Switch2# show interface fa0/1 trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 desirable 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-20, 30, 40

L'ordinateur B ne peut pas communiquer avec l'ordinateur D.
Quelle est la cause la plus probable de ce problème ?
Si l'administrateur supprime le VLAN 2 des switchs, qu'advient-il des ports membres de ce VLAN ?

Question 5 - Access list
On considère le schéma ci-dessous.

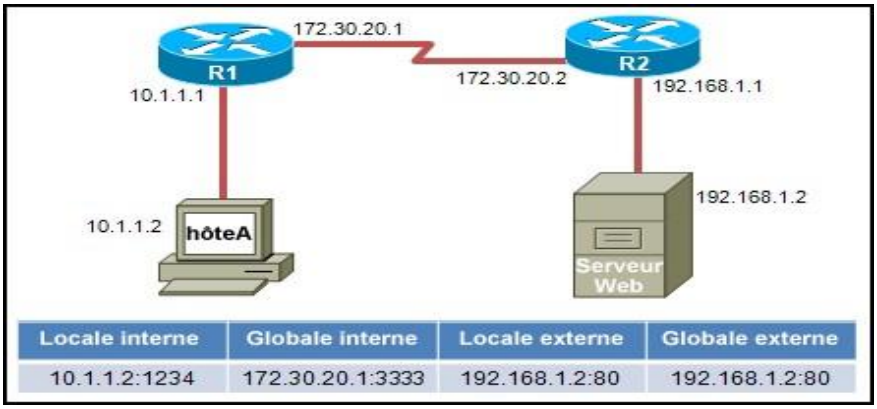



```
Routeur1(config)# access-list 201 deny icmp 192.168.1.0 0.0.0.255 any
Routeur1(config)# access-list 201 deny icmp 192.168.2.0 0.0.0.255 any
Routeur1(config)# access list 201 permit any any
Routeur1(config)# access-list 101 deny tcp any 192.168.1.0 0.0.0.255 eq 8080
Routeur1(config)# access-list 101 deny tcp any 192.168.1.0 0.0.0.255 eq 80
Routeur1(config)# access-list 101 deny icmp any 192.168.1.0 0.0.0.255
Routeur1(config)# access-list 101 deny icmp any 192.168.2.0 0.0.0.255
Routeur1(config)# access-list 101 permit ip any 192.168.1.0 0.0.0.255
Routeur1(config)# access-list 101 permit ip any 192.168.2.0 0.0.0.255
Routeur1(config)# int s0/0/0
Routeur1(config-if)# ip access-group 101 in
Routeur1(config-if)# ip access-group 201 out
```

L'administrateur réseau crée deux listes de contrôle d'accès standard (101 et 201) sur le Routeur 1.
Décrivez brièvement le rôle de ces deux ACL et leur direction appliquée.

Question 6 - NAT

On considère le schéma ci-dessous.



Locale interne	Globale interne	Locale externe	Globale externe
10.1.1.2:1234	172.30.20.1:3333	192.168.1.2:80	192.168.1.2:80

Le routeur R1 réalise la fonction NAT avec surcharge pour le réseau interne 10.1.1.0/24. L'hôte A envoie un paquet au serveur Web.

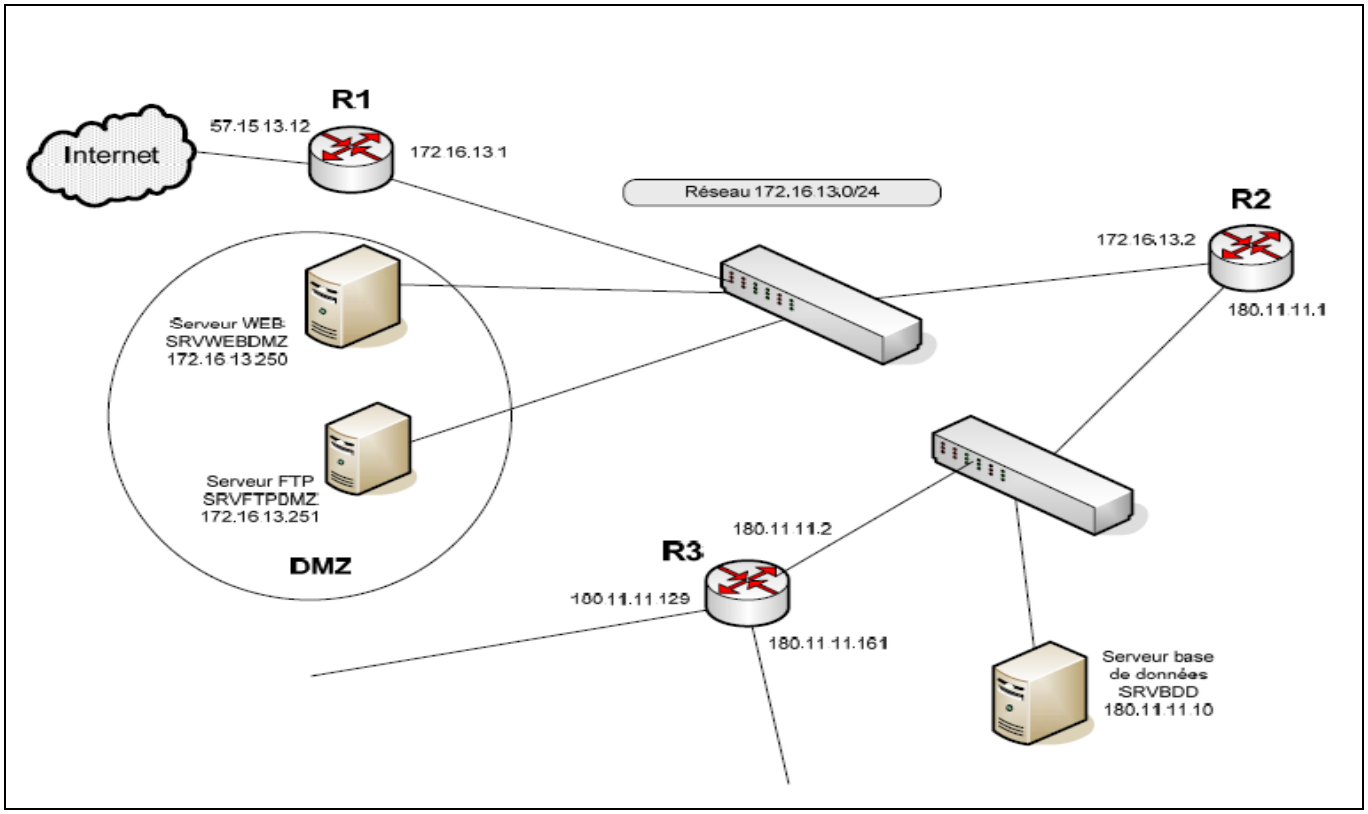
Quelle est l'adresse IP de destination du paquet renvoyé par le serveur Web ?

Question 7 - Pare-feu

Un réseau contient une zone démilitarisée (DMZ) avec le serveur web (172.16.13.250) et le serveur FTP (172.16.13.251). Un routeur pare-feu (R2) sépare la DMZ du réseau local. Le routeur R1 permet l'accès à l'Internet.
La table de filtrage du routeur R2 se présente ainsi :

N°	Interface Entrée	Interface Sortie	Adresse Source	Port Source	Adresse Destination	Port Destination	Action
10	180.11.11.1	172.16.13.2	180.11.11.10	Tous	Toutes	Tous	Refuser
20	180.11.11.1	172.16.13.2	Toutes	Tous	Toutes	80	Accepter
30	172.16.13.2	180.11.11.1	Toutes	Tous	180.11.11.10	Tous	Refuser
40	172.16.13.2	180.11.11.1	Toutes	80	Toutes	Tous	Accepter

Le schéma du réseau est ci-dessous :



Remarque : les règles sont numérotées de 10 en 10 de manière à ce que l'insertion d'une nouvelle règle soit aisée.

L'algorithme utilisé par le service de filtrage est le suivant, pour chaque paquet à traiter :

- en suivant l'ordre des règles de 1 à n, rechercher la première règle applicable,
- si une des règles est applicable, alors appliquer l'action au paquet et arrêter le parcours de la table,
- si aucune règle n'est applicable, refuser le paquet.

Indiquez le rôle de la règle numéro 10.
Indiquez le numéro des règles permettant aux postes du réseau local de demander et d'obtenir des pages web.
Écrivez les deux règles à ajouter pour permettre au serveur web de communiquer avec le SGBD interrogeable sur le port 1520, en précisant le numéro attribué à chaque règle ajoutée.

Question 8 - Trames réseaux
A quoi correspond la trame de la capture ci-dessous ?
Expliquez le processus complet correspondant.
Développez toutes les trames de ce processus.
Que signifie *source port* de l'entête UDP ?
Développez.