OFPPT

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

Direction Recherche et Ingénierie de la Formation

Examen de Fin de Formation _ CDJ _ CDS

Session Juillet 2017

Filière : Techniques des Réseaux Informatiques

Niveau : Technicien Spécialisé

Epreuve : Théorique

Barème : 40 points

Durée : 4h

« Alliance minière marocaine : AMM » est un groupe industriel dont l'activité principale est l'extraction et traitement de gisements miniers : principalement du cobalt, argent et cuivre.

Le siège de la société se trouve à Casablanca. Le groupe possède actuellement six (06) sites en activité, ces sites dépendent des mines d'extraction et de traitement.

Le groupe se charge de tout le processus d'activité depuis l'exploration et l'extraction en passant par le traitement et la valorisation jusqu'à la commercialisation.

Le système informatique de la société est amélioré constamment pour prendre en charge les dernières technologies et pour répondre efficacement aux besoins des utilisateurs.

Un progiciel de gestion intégré (ERP) permet une gestion informatisée de toutes les activités de l'entreprise (gestion des approvisionnements, gestion des ressources humaines, suivi des opérations de commercialisation ...)

Des solutions Internet permettent l'interconnexion des différents sites. Pour pallier aux problèmes de sécurité, la technologie VPN est adoptée.

Les réseaux locaux de l'entreprise utilisent des routeurs Cisco 2901 et commutateurs Cisco Catalyst 2960 (Layer 2) et 3560 (Layer 3).

Des serveurs Windows et Linux sont utilisés au niveau central et/ou par site pour assurer des rôles d'authentification, DNS et DHCP et pour héberger les applications métiers.

Votre tâche consiste en l'analyse et la proposition des solutions pour mettre à niveau le système informatique actuel de la société.

Le réseau du groupe se compose de 7 réseaux (entre siège et sites miniers).

Le réseau IP 10.0.0.0 /16 est utilisé globalement pour l'adressage. Le cahier de charge prévoit un maximum de 700 adresses IP par site.

1) ***Réaliser un découpage réseau pour affecter à chacun des réseaux ci-dessous un nombre d'adresses assurant le besoin décrit.***

N° ordre	Nom du site	Adresse réseau /longueur de préfixe
0	Siège	
1	Site-A	
2	Site-B	
3	Site-C	
4	Site-D	
5	Site-E	
6	Site-F	

Le site minier Site-D se trouve au sud du Maroc et est utilisé principalement pour l'exploitation de l'argent et du zinc.

Sur le plan fonctionnel, la mine est organisée comme suit :

- Service approvisionnement.
- Service contrôle de gestion.
- Service qualité et sécurité.
- Laboratoire.
- Service de traitement.

2) ***Reproduire et Compléter le tableau d'adressage en annexe 1 pour le Site-D***

L'administrateur local a opté pour des commutateurs multicouches pour assurer le routage inter-Vlan.

3) ***Quelles sont les caractéristiques des commutateurs multicouches ?***
4) ***Donner les commandes pour configurer les ports Fa0/1 et Fa0/2 en lien agrégé Etherchannel sans protocole de négociation sur MultilayerSW2.***
5) ***Donner la commande pour configurer le port-channel créé en mode agrégation avec l'id 77 comme id du vlan natif.***
6) ***Donner la commande(s) pour autoriser tous les Vlans sauf le Vlan 55 sur cette liaison.***
7) ***Donner les commandes nécessaires pour assurer le routage inter-vlan à l'aide de SVI entre les VLANs 11, 22 et 55 sur MultilayerSW3.***

L'interconnexion entre le siège et les différents sites est établie à base de liaison Internet à travers des connexions VPN.

Le Site-D à l'instar de la majorité des sites se trouve éloigné d'un accès ADSL disponible, pour cette raison, on utilise une connexion VSAT à 22 Mbps comme liaison principale avec technologie VPN.

Le schéma des connexions est disponible sur l'annexe 2.

8) ***Quelles sont les caractéristiques d'une connexion Internet par VSAT ?***
9) ***Présenter les avantages des VPN en justifiant leur utilisation par le groupe.***

Du côté du siège, trois serveurs sont utilisés pour héberger des applications accessibles depuis Internet. La solution consiste à configurer une traduction NAT. Pour préserver les adresses publiques, l'administrateur décide d'exploiter les fonctions de redirection de port.

La description de la configuration à réaliser est comme suit :

Protocole	@IP privée : N° de port	@IP publique : N° de port
TCP	10.0.0.100 : 80	41.141.244.143 : 8000
TCP	10.0.0.200 : 21	41.141.244.143 : 2121

10) Donner les commandes pour configurer la NAT avec redirection de port.

Des listes d'accès sont configurés au niveau du commutateur MultiLayerSW3, l'objectif étant de :

- Permettre au Vlan 11 et Vlan22 de se connecter sur Server-A (2éme adresse VLAN serveurs) sur le port http.
- Permettre au Vlan44 et Vlan55 de se connecter au Server-B (3éme adresse VLAN serveurs) sur le port https.

11) Créer une liste de contrôle d'accès nommée « APPS-METIER » permettant de répondre à ces contraintes.

Le groupe tout entier exploite la technologie Microsoft Active Directory pour gérer l'authentification et les autorisations des utilisateurs.

Un domaine parent appelé « amm.local » est configuré au niveau du siège, alors que chaque site possède un domaine enfant à l'exemple du Site-D qui détient le domaine « siteD.amm.local »

A chaque site géographique on a fait correspondre un site Active Directory.

12) Qu'est-ce qu'un site Active Directory ?

Le tableau suivant récapitule les maîtres d'opérations et services A.D présents par contrôleur de domaine.

		Contrôleur de schéma	Maître d'attribution des noms de domaine	Maître RID	Maître d'infrastructure	Emulateur PDC	Catalogue global
Siège	DC-1	X	X				X
	DC-2			X	X		X
	DC-3					X	
Site-D	DC-4			X	X	X	
	DC-5						

13) Quel est le rôle d'un serveur de catalogue global dans une organisation Active Directory ?

L'exploitation de rapports sur l'utilisation de la bande passante du réseau Internet a révélé un constat lié à une forte utilisation de la liaison Internet au moment des ouvertures de session.

14) Comment expliquer ce constat ?

15) Quelle solution peut-on proposer pour régler ce problème ?

Un nouveau point d'exploitation loin de quelques kilomètres sera utilisé au niveau du Site-D, un petit bureau temporaire a été mise en place contenant quelques ordinateurs et autres équipements. En termes de connectivité réseau, le choix a été porté sur la mise en place de ponts Wifi. (Voir annexe3)

Un pont Wifi est installé de chaque côté, il fournit une interface RJ45 pour la connexion locale, de l'autre côté la connexion envers l'autre pont utilise la bande de fréquence 5 GHZ évitant bon nombre d'interférences qui peuvent toucher la fréquence 2.4 GHZ.

16) Expliquer les interférences pour la bande 2.4 GHZ. Donner des exemples de dispositifs causant ces problèmes.

17) Quelles sont les normes 802.11 compatibles avec la bande de fréquence 5 GHZ ?

L'administration locale a décidé d'installer un contrôleur de domaine en local pour le nouveau point d'exploitation, ce dernier étant moins sécurisé et ne bénéficiera pas d'une présence permanente d'un administrateur.

18) Quelle solution peut être adoptée concernant l'installation du nouveau contrôleur de domaine ?

Le serveur Server-D (5éme adresse VLAN serveurs) est un serveur linux, il assure le rôle de serveur secondaire pour la zone « siteD.amm.local ». Le serveur est adressé de manière statique.

19) Donnez le contenu du fichier de configuration d'interface correspondant au serveur. (Indiquer essentiellement l'interface, le type de protocole, l'adresse IP, le masque, et le type de démarrage automatique).

Les directives suivantes ont été extraites du fichier de configuration BIND (les variables ip1, ip2, ip3 représentent des adresses IP).

```
forwarders { ip1 ; } ;
listen-on { 127.0.0.1; ip2; };
allow-recursion {ip3;};
notify yes ;
```


20) Expliquer les différentes directives.

21) Quelle directive doit être ajoutée à une zone DNS sous Linux pour autoriser la mise à jour dynamique de la zone ?

22) Si l'administrateur devait configurer une zone de recherche inversée pour le sous-réseau 10.20.0.0 /16, quelle serait le nom de cette zone ?

Les stratégies de sécurité de l'entreprise prévoient l'utilisation de la journalisation à des fins de surveillance et de sécurité.

Le serveur Server-D assure aussi le rôle de serveur syslog. On doit s'assurer que le service de syslog nommé **syslogd** démarre pour les niveaux d'exécution : multi-utilisateurs sans X11 et multi-utilisateurs avec X11.

23) Donner la commande permettant de s'assurer du démarrage du service syslogd pour les deux niveaux d'exécution cités.

L'administrateur a exécuté la commande suivante :

```
C1(config)# logging trap warning
```

24) Quels sont les noms des différents niveaux de sévérité qui seront envoyés au serveur Syslog ?

La ligne suivante provenant d'un routeur a été extraite du journal du serveur syslog.

```
*mai 28, 17:25:34.2525: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

25) Quelle commande aurait permis de configurer un routeur Cisco afin d'envoyer des messages log au serveur 10.0.13.144 ?

26) Expliquer les champs marqués dans le message syslog.

27) Pourquoi est-il important d'avoir une date et heure synchronisées sur l'ensemble des équipements réseaux ? comment un administrateur peut-il atteindre ce but facilement ?

L'administrateur soupçonne qu'une des machines a subi une attaque aboutissant à l'écoute électronique.

Les figures en annexe 4 concernent la machine victime et le routeur.

28) De quelle attaque s'agit-t-il dans ce cas ? décrire brièvement son principe.

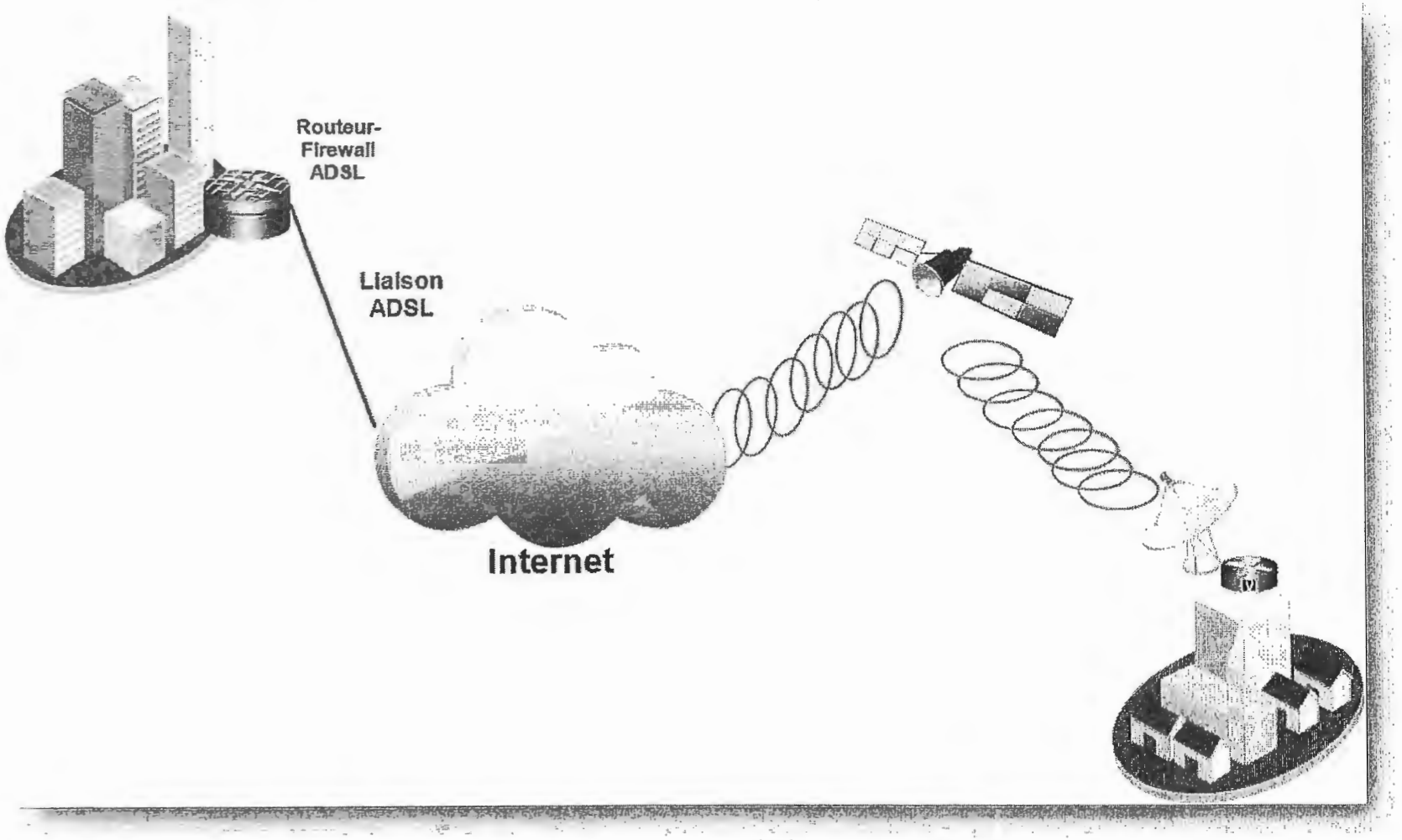
29) Citer quelques méthodes qui peuvent aider à faire face à cette attaque ?

30) Décrire une autre attaque qui peut donner lieu à l'écoute électronique.

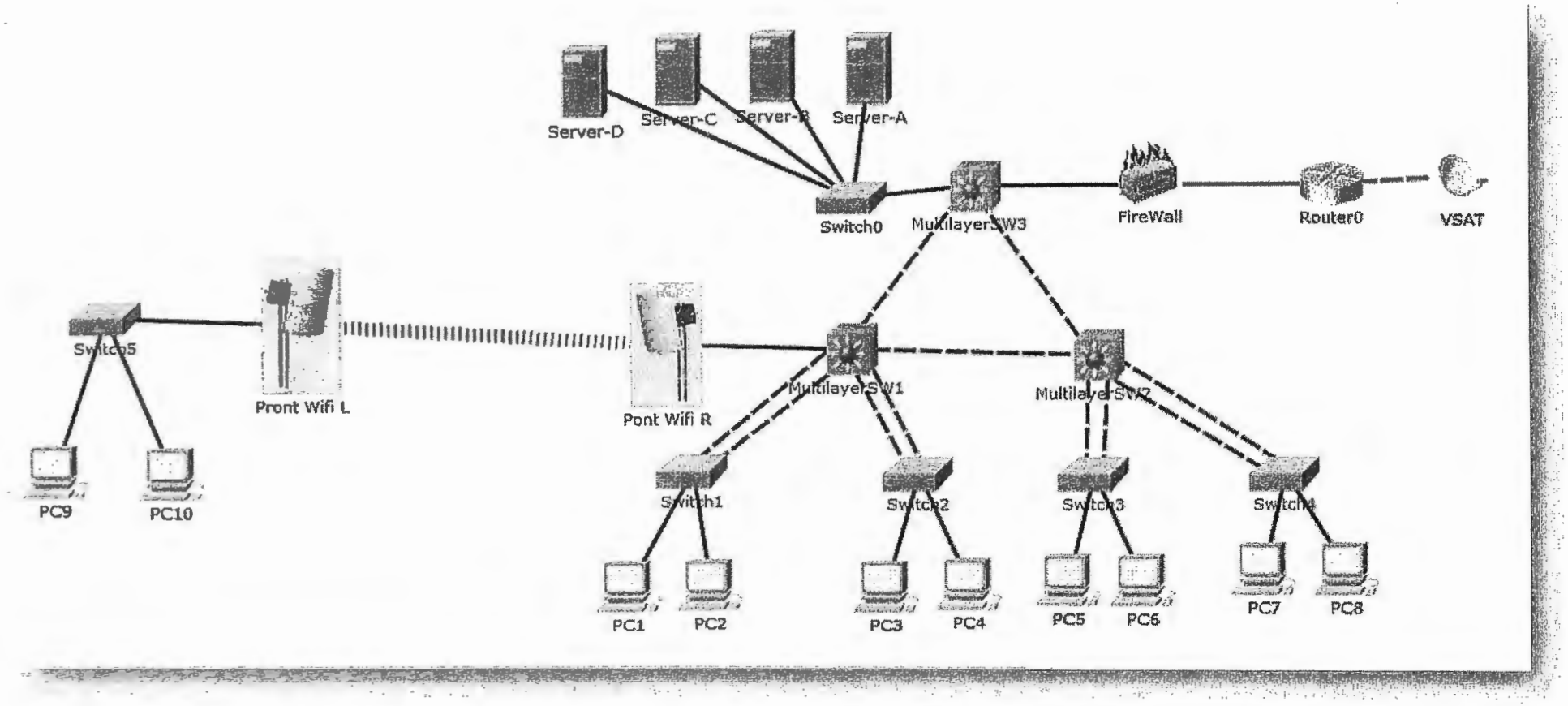
Annexe 1 : Tableau d'adressage pour Site-D :

Réseau	ID du VLAN	Adresses IP en besoin	Adresse réseau /longueur de préfixe	Première adresse utilisable	Dernière adresse utilisable
Service approvisionnement.	VLAN11	30			
Service contrôle de gestion.	VLAN22	55			
Service qualité et sécurité.	VLAN33	22			
Laboratoire.	VLAN44	17			
Service de traitement.	VLAN55	47			
Serveurs	VLAN66	5			
VLAN de Gestion	VLAN77	7			

Annexe 2 : Connexion entre le siège et Site-D :



Annexe 3 : Schéma du réseau du Site-D



Annexe 4 :

Résultats des commandes sur la machine victime :

```
C:\WINDOWS\system32> ipconfig  /all

Configuration IP de Windows

Carte Ethernet Ethernet :
   ..............
   Adresse physique . . . . . . . . . . . . : 00-22-5F-9B-87-46
   ..............
   Addresse  IP ..... : 10.0.0.37
   Masque de sous-réseau..... : 255.255.255.0
   Default Gateway..... : 10.0.0.1
```

```
C:\WINDOWS\system32> arp -a
Adresse Internet     Adresse physique      Type
10.0.0.1               0066.6c66.cd2b      dynamique
10.0.0.39              000b.bed3.e480      dynamique
```

Résultats des commandes show sur le routeur :

```
Router-A# show interfaces gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Hardware is CN Gigabit Ethernet, address is 0001.c94b.ba01 (bia 0001.c94b.ba01)
Internet address is 10.0.0.1/24
.............
```

```
Router-A# show arp
Protocol    Address      Age (min)   Hardware Addr     Type    Interface
Internet    10.0.0.1         -       0001.C94B.BA01    ARPA    GigabitEthernet0/0
Internet    10.0.0.37        0       0066.6C66.CD2B    ARPA
GigabitEthernet0/0
```

Barème de notation

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total
1,5	*2*	*1*	*0,5*	*0,5*	*1*	*2*	*1*	*1*	*2*	*12,5*
Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Total
2	*0,5*	*1*	*1*	*1*	*1,5*	*0,5*	*1*	*1,5*	*2*	*12*
Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Total
1	*0,5*	*1*	*2*	*1*	*2*	*2*	*2*	*2*	*2*	*15,5*