



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 Juin 2016CORRIGE

Filière : Techniques des Réseaux Informatiques

Epreuve : Théorique

Barème : 40 points

Niveau : Technicien Spécialisé

Durée : 4h30

« neem.ma » est une société marocaine de vente de produits en ligne, il s'agit d'une start-up créée en 2008 par des jeunes marocains très ambitieux.

Pour ses débuts, la société possédait un magasin de vente situé à Rabat et elle comptait sur la distribution de brochures et sur sa vitrine web comme moyens principaux de publicité et les commandes se passaient par téléphone.

Depuis son rachat en 2013 par un groupe industriel et financier et avec l'évolution du commerce électronique, la société a changé de stratégies pour s'orienter principalement vers la vente en ligne, sa boutique web a été rebaptisée pour prendre en charge la commande et le paiement en ligne.

L'épanouissement de son chiffre d'affaire et la demande ressentie des milliers de visiteurs sur tout le Maroc ont poussé la direction à adopter de grandes mesures d'accompagnement supplémentaires :

- L'ouverture de trois centres de proximités (CP) établis à Casa, Agadir et Tanger : sont des centres de relais possédants de vastes espaces de stockage pour les produits.
- « neem.ma » a signé un contrat avec une société de transport pour assurer des services de livraison à temps et satisfaisants.

La société compte actuellement des centaines de collaborateurs entre :

- Des professionnels informatiques (développeurs web et techniciens de réseaux).
- Des responsables de ventes (assurent aussi la relation client).
- Des employés chargés de produits : assurent la réception des commandes en ligne, la mise en package des produits et la communication avec la société de livraison (envoi ou retour).
- Des comptables chargés du recouvrement et du traitement des reçus de paiement faxés par les clients.
- Une équipe de direction rassemblant les décideurs et les chefs d'équipes.

Réseaux informatiques :

Il vous est demandé dans un premier temps de proposer un schéma d'adressage IP pour le site de Rabat en respectant ce qui suit :

- 18 ordinateurs et téléphones IP pour le service informatique.
- 88 ordinateurs et téléphones IP pour les chargés de produits.
- 36 ordinateurs et téléphones IP pour les responsables de ventes en plus de 18 smartphones utilisant une application spécialisée pour le suivi des commandes.
- 20 ordinateurs et téléphones IP pour les comptables.
- 24 ordinateurs et téléphones IP pour l'équipe de direction et les chefs d'équipes.

1) Vous devez utiliser l'adresse réseau 172.41.0.0 /23 pour remplir le tableau en annexe.

Pour améliorer les performances, l'administrateur a implémenté une agrégation de liaisons entre les commutateurs. Les ports Fa0/1, Fa0/2 et Fa0/3 ont été utilisés pour former une seule liaison entre les commutateurs Comm1 et Comm2.

2) Quels protocoles de négociation peuvent être activés sur les commutateurs pour établir l'agrégation de liens.

Les protocoles : LACP, PAgP

3) Donnez les modes de configuration de l'interface pour chaque protocole.

LACP : Désirable, Auto

PAgP : Active, Passive

4) Donnez les commandes à utiliser sur un Catalyst 2960 pour configurer la liaison Etherchannel sans protocole de négociation.

```
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#channel-group 1 mode on
```

L'isolation des hôtes se fait à base de VLANs, pour une meilleure gestion, l'administrateur utilise le protocole VTP pour une configuration VLAN cohérente, ci-dessous le résultat de la commande *show vtpstatus*

```
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Transparent
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

5) Quelle version de VTP est utilisée sur ce réseau ?

Version 1

6) Que fait le commutateur Comm3 lorsqu'elle reçoit une annonce VTP avec un numéro de révision supérieure à celui qu'il contient ?

Le commutateur n'est pas concerné par les annonces VTP du domaine, il est en mode transparent

7) Expliquer le mode de fonctionnement VTP du commutateur Comm3 ?

les commutateurs transparents transmettent les annonces VTP aux clients et serveurs VTP. Les réseaux locaux virtuels créés, renommés ou supprimés sur un commutateur transparent sont uniquement associés à ce commutateur.

L'administrateur implante des liaisons redondantes entre les commutateurs en présence d'un protocole spanning-tree pour éliminer les boucles de routage. La figure suivante présente le résultat de la commande **show spanning-tree** exécutée sur le commutateur **Comm1** :

```
VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 16385
Address 000A.F301.C13A
Cost 9
Port 27(Port-channel 4)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 00E0.A318.5EA6
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/7 Desg FWD 19 128.7 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Fa0/6 Desg FWD 19 128.6 P2p
Po4 Root FWD 9 128.27 Shr
Po3 Altn BLK 8 128.28 Shr
```

8) Quel protocole Spanning-tree est activé sur le commutateur Comm1 ?

Le protocole rapidpvst+

9) Donnez la commande utilisée pour activer ce protocole sur le commutateur ?

```
Switch(config)#spanning-tree mode rapid-pvst
```

Vous remarquez que lorsqu'un périphérique final est connecté au port d'un commutateur, ce port demande un temps important avant de s'activer, vous désirez voir le port s'activer automatiquement, le port doit se désactiver à la réception d'une trame BPDU.

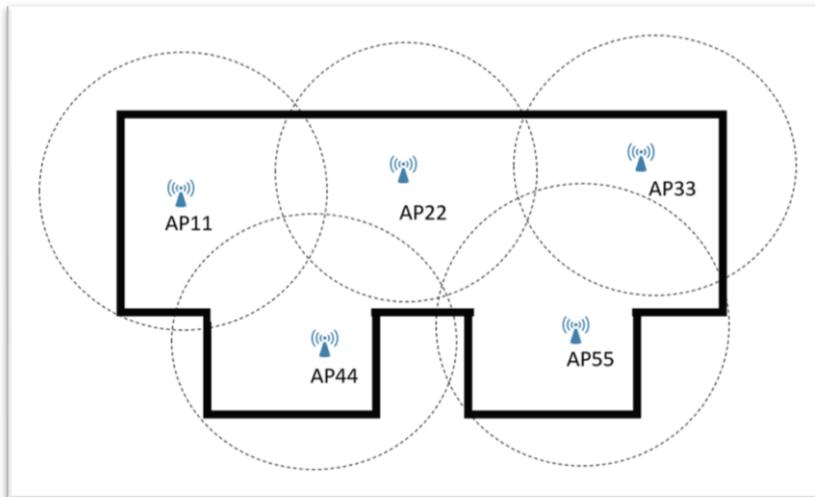
10) Quelles commandes doit-t-on exécuter sur le port Fa0/11 pour atteindre l'objectif décrit ?

```
Switch(config)#interface fastEthernet 0/11
Switch(config)#switchport mode access
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
```

Les responsables de ventes doivent se déplacer sur tout le magasin pour suivre la préparation des produits pour livraison, pour cela ils utilisent des smartphones avec une application spécialisée et se connectant au réseau WiFi.

Le réseau WiFi doit couvrir l'ensemble du magasin pour permettre l'itinérance (Roaming) entre différents points d'accès.

Le schéma suivant correspond au positionnement des points d'accès couvrant tout le magasin.



La figure ci-dessous correspond à la configuration faite sur le point d'accès AP11 :

The screenshot shows the configuration settings for AP11. The settings are as follows:

- Network mode : 802.11g only
- Network Name (SSID) : WNEEM
- Standard Channel : 1
- SSID Broadcast : Enabled

11) Quelles sont les caractéristiques de la norme activée sur le point d'accès AP11 ?

La norme 802.11g assure des débits de données plus élevés dans cette bande en utilisant la technique de modulation OFDM.

La norme IEEE 802.11g utilise la bande de fréquence 2.4 Ghz et est compatible avec les systèmes IEEE 802.11b.

12) La même configuration a été adoptée sur les autres points d'accès, spécifier pour chacun (AP22, AP33, AP44 et AP55) le canal à utiliser pour éviter les interférences entre eux (Voir annexe pour les fréquences de canaux).

Canal	1	2	3	4	5	6	7	8	9	10	11	12	13
Fréquence (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472

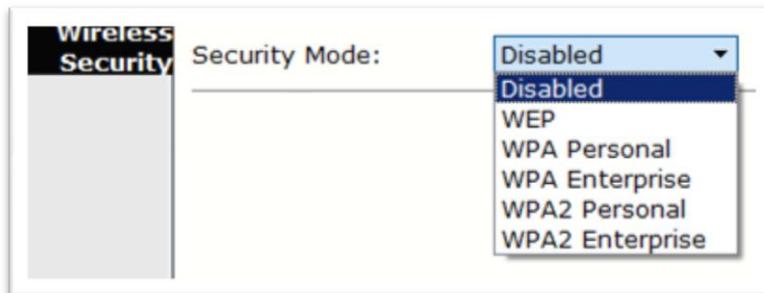
Le stagiaire doit choisir pour les points d'accès adjacents des canaux qui sont séparés par 5. (exemple : 1,6 et 11).

Les cinq points d'accès sont connectés respectivement sur les ports Fa0/1 à Fa0/5 du commutateur Comm2, l'idée est de regrouper les connexions Wifi sur le même VLAN que celui des responsables de ventes, ce VLAN porte l'ID 33.

13) Donnez les commandes nécessaires à exécuter sur le commutateur Comm2 pour aboutir à cette fin.

```
Switch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 33
```

Le point d'accès propose les choix suivants pour sécuriser l'accès au réseau Wifi :



14) Quel mode doit-on choisir pour une meilleure sécurité sachant que l'administrateur ne prévoit pas la mise en place d'un serveur d'authentification ?

WPA2 personnel

La société héberge ses serveurs publics en local, elle a opté pour l'offre d'un FAI qui a proposé un accès en fibre optique avec débit garanti symétrique de 100 Mbps.

L'offre propose aussi une liaison SDSL de secours (back-up).

15) Comment expliquer le choix des liaisons Internet symétriques ?

Comme la société possède des serveurs Internet en interne, la demande en débit est surtout importante en envoi.

Pour assurer une redondance au premier saut pour les hôtes et spécialement les serveurs publics, des chemins doubles ont été mises en place vers les routeurs se connectant à Internet.

16) Citer trois protocoles de gestion de redondance au premier saut.

HSRP
VRRP
GLBP

Des parties des résultats de la commande **show standby** et **show running-config** exécutée sur le routeur R1 est présenté ci-dessous :

<pre>RRabat1#show standby gigabitEthernet0/0.10 - Group 10 (version 2) State is Active 11 state changes, last state change 00:49:38 Virtual IP address is 172.41.0.254 Preemption enabled Active router is local</pre>	<pre>RRabat1#show running-config Interface gigabitEthernet0/0.11 Encapsulation dot1q 11 ip address 172.41.0.1 255.255.255.0 standby 10 ip 172.41.0.254 standby 10priority 105 standby 10 preempt</pre>
--	--

Standby router is 172.41.0.2 Priority 105 (configured 105)	
--	--

17) Quel protocole a été configuré sur RRabat1 ? Quel est l'état de ce routeur ?

Le protocole HSRP est le protocole activé, le RRabat1 est le routeur actif.

18) Quelle adresse IP doit être configurée au niveau des hôtes clients comme passerelle par défaut ?

L'adresse IP à utiliser est 172.41.0.254

Toutes les ressources de la société (applications métiers, services et fichiers) sont centralisées au niveau du réseau de Rabat. Par conséquent, une connexion sur base de Frame Relay permet aux utilisateurs sur les centres de proximité d'accéder à ces ressources.

19) Quelle topologie Frame Relay est la plus adaptée à cette situation ? justifier votre réponse.

La topologie à utiliser est la topologie Hub & spoke parce que toutes les ressources sont centralisées et par conséquent les centres de proximité ont juste besoin de se connecter au site de Rabat.

Des liaisons Frame Relay seront configurées entre le site de rabat et les centres de proximité, le tableau suivant récapitule les informations nécessaires :

Connexion vers	Id de la sous-interface	Adresse de liaison point à point	DLCI
Tanger	3	10.0.0.0 /30	301
Oujda	4	10.0.0.4 /30	401
Agadir	5	10.0.0.8 /30	501

20) Donnez la configuration nécessaire de l'interface Ser0/0 sur le routeur RRabat1 ?

```
Router(config)#interface serial 0/0/0  
Router(config-if)#encapsulation frame-relay
```

```
Router(config-if)#interface serial 0/0/0.3 point-to-point  
Router(config-subif)#ip address 10.0.0.1 255.255.255.252  
Router(config-subif)#frame-relay interface-dlci 301
```

```
Router(config-if)#interface serial 0/0/0.4 point-to-point  
Router(config-subif)#ip address 10.0.0.5 255.255.255.252  
Router(config-subif)#frame-relay interface-dlci 401
```

```
Router(config-if)#interface serial 0/0/0.5 point-to-point  
Router(config-subif)#ip address 10.0.0.9 255.255.255.252  
Router(config-subif)#frame-relay interface-dlci 501
```

```
Router(config)#interface serial 0/0/0  
Router(config-if)#no shutdown
```

21) Quelles commandes doivent permettre la configuration du protocole EIGRP sur le routeur RRabat1 (inclure aussi la commande de redistribution de la route par défaut et la désactivation du résumé automatique) ?

routereigrpid_processus

network adresse_réseaumasque_générique (voir tableau d'adressage)

no auto-summary

Le serveur DNS public possède l'adresse IP interne **172.41.1.196**, l'administrateur désire voir les requêtes DNS provenant d'Internet redirigées vers le serveur interne.

Adresse publique	N° de port	Adresse du serveur interne	N° de port
172.41.1.196	53	105.155.186.249	53

22) Donnez les commandes à exécuter sur le routeur RRabat1 pour configurer la traduction d'adresse adéquate avec redirection de port.

RRabat1(config)#ipnatinside source statictcp 172.41.1.196 53 105.155.186.249 53

Systemes serveurs :

Les serveurs présents dans l'entreprise sont les suivants :

Pour une gestion centralisée, la société utilise les services de domaine Active Directory, le domaine « neem.ma.intra » est déployé à l'aide de deux contrôleurs de domaine : DC1 et DC2 fonctionnant sous Windows 2008 server.

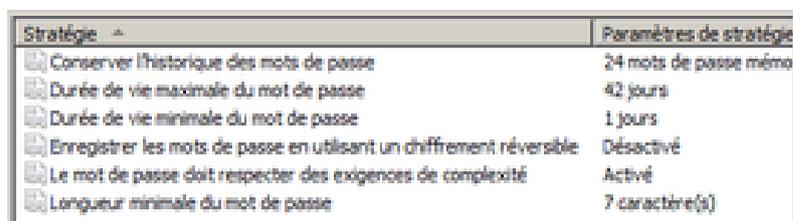
Vous devez intervenir sur les contrôleurs de domaine selon différentes situations professionnelles rencontrées.

Etant donné que les utilisateurs n'utilisent pas toujours les mêmes machines pour se connecter au réseau, l'administrateur a décidé de configurer le stockage des données sur un serveur, les employés de la société d'accéder à leurs dossiers spéciaux (Documents, Téléchargements...) quel que soit la machine utilisée.

23) Proposer une solution permettant aux employés d'accéder à leurs dossiers spéciaux de manière transparente sur le serveur.

Configurer une GPO et l'appliquer à une unité d'organisation qui regroupe les employés concernés. Cette GPO doit permettre de rediriger les données enregistrés en local dans les dossiers spéciaux vers un serveur.

Une stratégie de sécurité concernant les paramètres de mot de passe et de verrouillage des mots de passe est appliquée au domaine.



Stratégie	Paramètres de stratégie
<input checked="" type="checkbox"/> Conserver l'historique des mots de passe	24 mots de passe mémo
<input checked="" type="checkbox"/> Durée de vie maximale du mot de passe	42 jours
<input checked="" type="checkbox"/> Durée de vie minimale du mot de passe	1 jours
<input checked="" type="checkbox"/> Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
<input checked="" type="checkbox"/> Le mot de passe doit respecter des exigences de complexité	Activé
<input checked="" type="checkbox"/> Longueur minimale du mot de passe	7 caractère(s)

L'administrateur a décidé d'affiner ces paramètres pour le groupe d'informaticiens de la façon suivante :

Longueur minimale du mot de passe : 8 caractères.

24) Citer les opérations à réaliser pour aboutir à cette fin.

Utiliser l'éditeur ADSI edit pour créer un objet PSO, modifier les attributs concernés puis appliquer l'objet PSO à un groupe de sécurité regroupant les informaticiens.

Un administrateur doit déployer une application métier sur les postes des responsables de vente, une GPO de distribution de logiciels été créée et est liée à l'unité d'organisation regroupant les ordinateurs des responsables de ventes, en effet l'application nécessite que l'ordinateur possède un minimum de 2Go de RAM.

25) Que faut-il paramétrer pour la GPO afin de s'assurer que l'application ne sera déployée que sur les ordinateurs respectant la contrainte de la mémoire RAM ?

Appliquer une requête WMI

La société reçoit des stagiaires en permanence, un fichier contenant les informations sur ces stagiaires envoyé par la direction à l'administrateur, ce dernier modifie le fichier en y ajoutant des données complémentaires et se retrouve avec un fichier au format csv(Common-separated Values)

26) Quel utilitaire doit-on utiliser pour faciliter la création de comptes pour ces nouveaux stagiaires ? Donnez la commande à appliquer pour importer le fichier stagiaires.csv ?

csvde -i -f stagiaires.csv

Un des assistants de l'administrateur a supprimé par mégarde une unité d'organisation, il tente de restaurer une sauvegarde effectuée avant la suppression mais une fois la restauration terminée et la répllication entre DC1 et DC2 effectuée, on ne retrouve pas l'unité d'organisation supprimée.

27) Comment expliquer le fait que la restauration n'as pas permis de récupérer l'unité d'organisation supprimée ?

28) Que doit faire l'administrateur pour régler le problème ?

Réaliser une restauration de Active directory et marquer l'unité d'organisation comme faisant autorité.

Le contrôleur de domaine DC2 assurait le rôle de maître RID dans le domaine, ce contrôleur de domaine est tombé en panne et il n'est plus récupérable. L'administrateur doit assurer le transfert du rôle vers DC1.

29) Quels sont les différents rôles de maîtres d'opérations uniques ? Organiser-les par domaine/forêt.

Par forêt

Le maître de schéma

Le maître d'attribution de noms de domaine

Par domaine :

Le maître RID

Le maître d'infrastructure

Émulateur PDC

30) Quel est le rôle du maître RID et quel est l'effet de l'absence de DC2 sur le bon fonctionnement du réseau ?

Le maître RID (*Relative IDentifier*) qui alloue un identificateur relatif à l'intérieur d'un domaine (pour un utilisateur, un groupe ou tout autre objet géré par Active Directory). L'association de ce RID avec l'identificateur du domaine forme le SID (l'identificateur de sécurité). Le maître RID gère aussi le déplacement d'un objet d'un domaine à un autre, à l'intérieur de la forêt.

À un instant donné, il ne peut y avoir qu'un seul maître RID dans un domaine.

31) Que faut-il faire pour régler ce problème ?

Forcer le transfert de rôle

La société possède deux sites publics présents sur le même serveur accessibles comme suit :

Nom du site web	Adresse IP interne	Adresse IP externe
www.neem.ma	172.41.1.197	105.155.186.250
m.neem.ma	172.41.1.198	105.155.186.251

La figure suivante correspond au fichier de ressources de la zone « neem.ma » hébergé sur le serveur DNS public.

```

@           IN      SOA      pubns1.neem.ma. admin.neem.ma.
              (
              2015120402    ;serial
              86400         ;refresh
              21600         ;retry
              604800        ;expire
              3600          ;negative          ttl)
pubns1      IN      NS       pubns1.neem.ma.
pubns1      IN      A        172.41.1.196
www         IN      A        105.155.186.250
m           IN      A        105.155.186.251
  
```

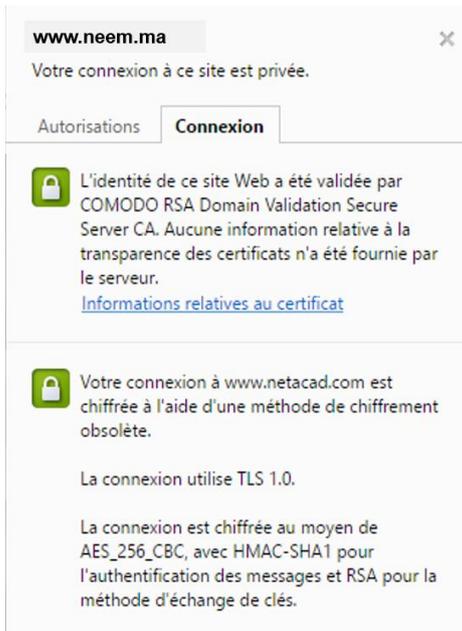
32) Les deux sites web étant hébergés sur la même machine, quelle méthode de mise en œuvre de sites virtuels a été utilisée ? justifier votre réponse.

Le multihosting peut être basé sur l'adresse IP supplémentaire, le numéro de port et l'entête http.

Chaque site possède sa propre adresse IP, donc la méthode utilisée est celle d'adresse IP supplémentaires.

Sécurité informatique :

L'accès aux sites www.neem.ma et m.neem.ma se fait à l'aide du protocole https. La figure suivante est acquise d'après une connexion au site www.neem.ma sur un navigateur.



33) Quel protocole de cryptage asymétrique est utilisé ?

RSA

34) Quel protocole de cryptage symétrique est utilisé ?

AES

35) Quel protocole de hachage est utilisé pour vérifier l'intégrité des données ?

SHA1

36) Qu'est-ce qu'une autorité de certification ? et quelles sont ses fonctions ?

une **Autorité de Certification** (AC ou CA pour Certificate Authority en anglais) est un tiers de confiance permettant d'authentifier l'identité des correspondants. Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fourni.

37) Expliquer le principe de sécurité dans le protocole https en justifiant sur l'utilisation de cryptage symétrique et asymétrique dans cette communication ?

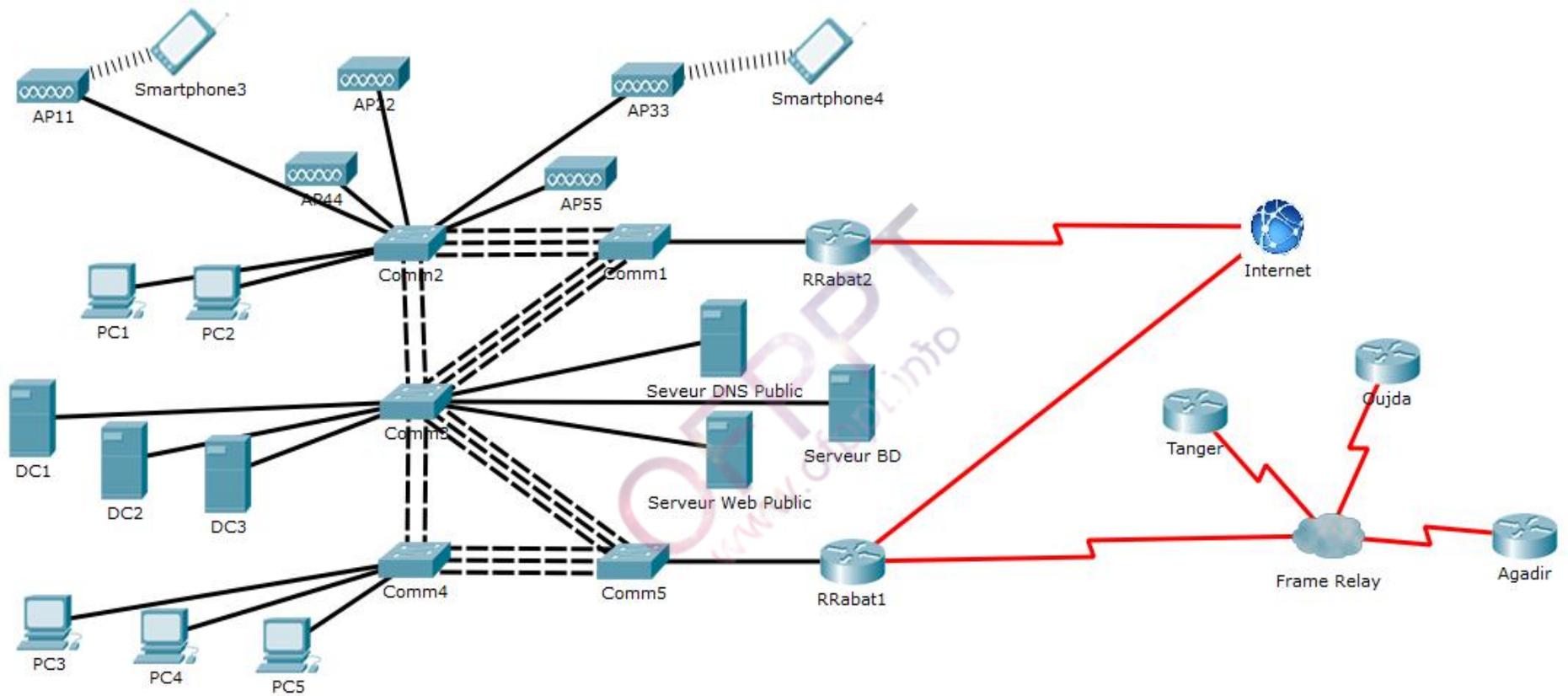
1 - le navigateur fait une demande de transaction sécurisée au serveur en envoyant sa requête HTTPS://, il demande donc le certificat garantissant la clé publique du serveur.

2 - le serveur lui envoie son certificat d'authentification délivré par une autorité de certification (normalement organisme officiel). Ce certificat comporte une clé publique.

3 - Le navigateur s'assure tout d'abord que le certificat délivré est valide puis il envoie au serveur une clé secrète codée issue de la clé publique (de 56 ou 128 bits). Seul le serveur sera donc capable de décoder cette clé secrète car il détient la clé privée. Cette clé secrète ainsi créée sera utilisée pour encoder les messages (cryptographie symétrique). L'algorithme à clé secrète utilisé (ex : DES, RC4) est négocié entre le serveur et le client.

4 - Le serveur et le client possèdent maintenant une clé secrète partagée (la clé de session) et les échanges sont faits par l'intermédiaire de cette clé. Pour assurer l'intégrité des données, on utilise un algorithme de hash (ex : MD5, SHA). S'il y a déconnexion, une nouvelle clé de session sera négociée.

Schéma logique de la topologie réseau :



Réseau	Nombre d'hôtes en besoin	Adresse réseau /préfixe réseau	Première adresse hôte	Dernière adresse hôte	Adresse de diffusion
Service informatique	18	172.41.1.0 /27			
Chargés de produits	88	172.41.0.0 /25			
Responsables de ventes	54	172.41.0.128 /26			
Comptables	20	172.41.0.224 /27			
Direction	24	172.41.0.192 /27			
Serveurs internes	7	172.41.1.32 /28			
Serveurs publics	3	172.41.1.48 /29			

Barème de notation :

Réseaux informatiques :

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Total / 22
2	0,5	0,5	1	0,5	0,5	1	0,5	1	1	1	1	1	1	1	1	1	1	1	1,5	1,5	1,5	22

Systemes serveurs

Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Total / 14
1	2	1	2	0,5	1	2	1,5	1	2	14

Sécurité informatique :

Q33	Q34	Q35	Q36	Q37	Total / 4
0,5	0,5	0,5	1	1,5	4