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 2014

Filière : Techniques des Réseaux Informatiques

Epreuve : Théorique

Barème : 40 points

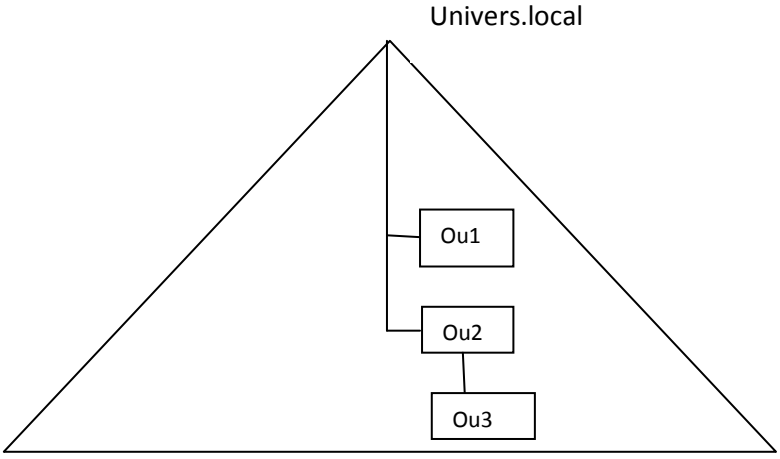
Niveau : Technicien Spécialisé

Durée : 4h30

Partie I : Administration et sécurité des réseaux informatiques

Vous êtes l'administrateur de la société « univers ».Vous êtes chargé au niveau de l'entreprise d'installer et de configurer des serveurs. Vous avez décidé d'implémenter le service active directory pour mieux gérer le réseau informatique de cette entreprise. Vous avez adopté le schéma suivant :

Le nom de domaine active directory est « univers.local » et trois unité d'organisation OU1,OU2 et OU3.



1) Quels sont les rôles de maîtres d'opération qu'un contrôleur de domaine peut jouer ?

Au niveau de la foret : maître du schéma, maître d'attribution de nom de domaine

Au niveau du domaine : maitre RID, maitre d'infrastructure, maitre PDC

2) En utilisant les commandes, créer le compte ordinateur « poste 3 »dans l'unité d'organisation OU3.

Dsadd computer « cn=poste3,ou=OU3,ou=OU2,dc=univers,dc=local »

3) En utilisant la ligne de commande, créer le compte utilisateur « said hilmi » dans l'unité d'organisation OU1

Dsadd user « cn=said hilmi,ou=OU1,dc=univers,dc=local »

4) L' utilisateur said souhaite utiliser un espace disque important alors qu' il ne possède que 40Go sur son poste local. Comment vous pouvez lui attribuer de l'espace disque à partir du contrôleur de domaine.

On peut lui configurer un dossier de base

5) En utilisant les commandes, supprimer le compte ordinateur « poste3 »

Dsrm « cn=poste3,ou=OU3,ou=OU2,dc=univers,dc=local »

Vous avez configuré des stratégies de groupes pour gérer les utilisateurs et les ordinateurs à distance .

6) Vous avez paramétré deux stratégies de groupe (GPO1et GPO2) :
   - ✓ GPO1 : Désactiver l'accès au panneau de configuration
   - ✓ GPO2 :Retirer le solitaire

   Appliquer les GPO et « bloquer l'héritage » sur l'objet convenable pour atteindre les résultats suivants :
   - Désactiver l'accès au panneau de configuration pour les utilisateurs du domaine et du OU2 et OU3
   - Retirer le solitaire pour les utilisateurs de l'unité d'organisation OU1

   Appliquer GPO1 sur le domaine et GPO2 sur OU1 et bloquer l'héritage sur OU1

7) Vous avez paramétré deux stratégies de groupe (GPOA et GPOB) :
   - ✓ GPOA :installe Microsoft Office
   - ✓ GPOB :installe l'application de sauvegarde

   Appliquer chaque GPO et blocage d'héritage sur le bon endroit pour atteindre les résultats suivant :

   - ➢ Les utilisateurs du domaine et de OU1 et OU3 nécessitent Microsoft Office.
   - ➢ Les utilisateurs dans l'unité d'organisation OU2 et OU3 doivent disposer de l'application de sauvegarde

   Appliquer GPOA sur le domaine ET SUR OU3 et GPOB sur OU2 et bloquer l'héritage sur OU 2

8) Vous avez paramétré trois stratégies de groupe (GPOA , GPOB et GPOC) :
   - GPOA : applique un script de fermeture de session
   - GPOB : garantit l'affichage de l'option « exécuter » dans le menu démarrer et retire l'option rechercher de ce menu
   - GPOC : garantit l'affichage de l'option « rechercher» dans le menu démarrer

   Appliquer les stratégies de groupes sur l'emplacement approprié afin d'obtenir les résultats suivants :

   - ➢ Le script de fermeture de session s'applique à tous les utilisateurs du domaine et des OU

- **Exécuter** affichée uniquement pour les utilisateurs dans les OU2 et OU3
- Afficher l'option **Rechercher** uniquement pour les utilisateurs dans l'unité d'organisation OU3

Appliquer GPOA sur le domaine et GPOB sur OU2 et GPOC sur OU 3

9) Pour implémenter le service DNS sous linux, vous devez déclarer la zone principale directe « univers.local » et inversée dans le fichier named.conf sachant que l'adresse réseau de cette entreprise est 192.168.23.0/24

   a) Ajouter la zone principale directe et inversée dans le fichier named.conf

Zone « univers.local.» IN {
Type master ;
File « univers.local.zone » ;
};
Zone « 32.168.192.in-addr.arpa. » IN {
Type master ;
File « univers.local.zone.rev » ;
};

   b) Quel utilitaire permet de tester un serveur DNS

Nslookup, dig ou host

10) Pour tolérer les pannes vous voulez mettre en œuvre un serveur dns secondaire. Faites les modifications convenable au niveau du fichier named.conf du serveur secondaire. L'adresse IP du serveur DNS principale est 192.168.23.1/24

Zone « univers.local.» IN {
Type slave ;
File « univers.local.zone » ;
Masters {192.168.23.1 ;} ;
}
Zone « 32.168.192.in-addr.arpa. » IN {
Type slave ;
File « univers.local.zone.rev » ;
Masters {192.168.23.1 ;} ;
}

Pour assurer une bonne communication entre les employés de cette entreprise vous avez implémenté un serveur de messagerie exchange 2007

11) Que devez vous vérifiez avant d'installer le serveur Exchange 2007 server ?
    - **Vérifier les pré requis matériels**
    - **Vérifiez qu'Active Directory et le serveur DNS sont installés et configurés.**
    - **Vérifiez que vous avez les autorisations Active Directory appropriées pour exécuter l'installation**
    - **Vérifiez que tous les ordinateurs qui exécutent Exchange dans la même organisation Exchange sont dans la même forêt Active Directory**
12) Quel est l'enregistrement qu' il faut ajouter au niveau du serveur DNS pour publier les serveur de messagerie ?

L'enregistrement MX

13) Quel est le rôle des agents SMTP

- **MUA : Mail User Agent, c'est le client de messagerie (KMail, Evolution, etc.).**
- **MTA : Mail Transfert Agent, c'est l'agent qui va transférer votre mail vers le serveur chargé de la gestion des emails de votre destinataire. Dans la pratique, le courrier peut transiter par plusieurs MTA.**
- **MDA : Mail Delivery Agent est le service de remise du courrier dans les boîtes aux lettres des destinataires.**

Pour sécuriser le réseau de cette entreprise, un pare feu est installé pour contrôler les accès qui arrivent sur les différentes interfaces. Ce pare feu est doté également d'une fonction de translation d'adresse.

14) Expliquer en quoi la translation d'adresses est intéressante pour la sécurité de l'entreprise?

Le mécanisme de translation d'adresses permet de sécuriser le réseau interne étant donné qu'il camoufle complètement l'adressage interne. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de la même adresse IP.

15) Expliquez les deux types de translation ?

- ✓ **Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.**
- ✓ **Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (PAT - Port Address Translation)**
- ✓ **Le PAT**

Réseaux Informatiques :

Etude de cas :

Le réseau d'une société nommée ITTech est illustré sur le schéma de l'annexe. On veut réaliser un plan d'adressage pour l'ensemble des réseaux locaux et étendus de la société.

Sachant que l'adresse réseau initiale de la société est : 172.16.0.0/22

1) En utilisant la technique **VLSM**, reproduire et remplir le tableau de l'annexe 2 dans la feuille de rédaction.
Réponse : proposition de correction qui n'est pas unique (les masques sous réseau sont spécifiés sur le tableau)

2) Toutes les images IOS ainsi que les fichiers de configuration sont stockés au niveau du serveur FTP/TFTP du SIEGE, donner la procédure permettant de mettre à jour l'image IOS du routeur SIEGE avec la méthode **TFTPDNLD** ?
rommon 1 > IP_ADDRESS=x.x.x.x
rommon 2 > IP_SUBNET_MASK=y.y.y.y

rommon 3 > DEFAULT_GATEWAY=z.z.z.z
rommon 4 > TFTP_SERVER=w.w.w.w
rommon 5 > TFTP_FILE=nom-image
Note : Une fois cette étape réalisée il est possible de vérifier si les variables ont été prises en compte avec la commande SET.
rommon 6 > tftpdnld

Les renseignements qui suivent s'affichent alors à l'écran :

IP_ADDRESS: x.x.x.x
IP_SUBNET_MASK: y.y.y.y
DEFAULT_GATEWAY: z.z.z.z
TFTP_SERVER: w.w.w.w
TFTP_FILE: nom-image

Répondre Yes à la question qui suit:

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y

(Le téléchargement de l'image commence)

Receiving c1700-sv3y-mz.122-13.bin from 172.26.1.2!!!!!!!!!!!!!!!
!!!
!!!

File reception completed.
Copying file nom_image.bin to flash.

3) En se basant sur l'extrait du résultat de la commande **show version** présenté dans la figure ci-dessous, donnez les valeurs des paramètres suivants :

Valeur du registre de configuration : 0x2102
Nombre d'interfaces FastEthernet : 2
Nombre d'interfaces Serial :3
Capacité de la NVRAM :32K
Capacité de la mémoire Flash :63488K
Série du routeur :C2600

```
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"

Cisco 2621 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memor
y
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
3 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

4) En se basant sur votre plan d'adressage, donner la table de routage complète du routeur SIEGE :

Adresse réseau De destination	**Masque sous Réseau**	**Interface de sortie**	**Passerelle**	**Nombre de sauts**
VLAN100	/26	Fa0/0.100	*	0
VLAN200	/26	Fa0/0.100	*	0
LANSRV	/28	Fa0/1	*	0
200.0.0.0	/28	S0/0	*	0
SRV-A1	/28	S0/0	200.0.0.2	1
VLAN10	/28	S0/0	200.0.0.2	1
VLAN20	/27 ou /26	S0/0	200.0.0.2	1
LAN-A3	/25	S0/0	200.0.0.3	1
WLAN-A2	/26	S0/0	200.0.0.3	1
LAN-A2	/27	S0/0	200.0.0.4	1
LAN-A4	/26	S0/0	200.0.0.3	2

5) L'administrateur a décidé de mettre en place le routage dynamique au lieu du routage statique. Quels sont les points forts du routage dynamique, et ceux du routage statique ? dans quel cas il est utile d'utiliser les deux ?

Réponses :

Routage statique :

- Facilite la maintenance de tables de routages dans les petits réseaux stables
- Effectue le routage depuis et vers des réseaux d'extremité
- Utilise une seule route par défaut
- Traitement processeur minimal
- Facile à comprendre par l'administrateur
- Facile à configurer

Routage dynamique :

- maintenance et config simplifiée lors de l'ajout/supresion de réseau
- Réagit automatiquemetn aux modifs topologiques

- Configuration avec moins de risques d'erreurs
- plus évolutif

6) L'administrateur a configuré les routeurs pour utiliser RIP, les réseaux directement connectés aux routeurs A2 et A4 n'arrivent pas à communiquer, la commande « debug ip rip » a été exécutée, un extrait de son résultat est donné dans la figure ci-dessous :

```
RIP: build update entries
      172.16.0.0/16 via 0.0.0.0, metric 1, tag 0
RIP: ignored v1 packet from 200.0.0.66 (illegal version)
```

Quelle est la cause probable de ce disfonctionnement ?

Réponse :

Les versions de RIP ne sont pas les mêmes.

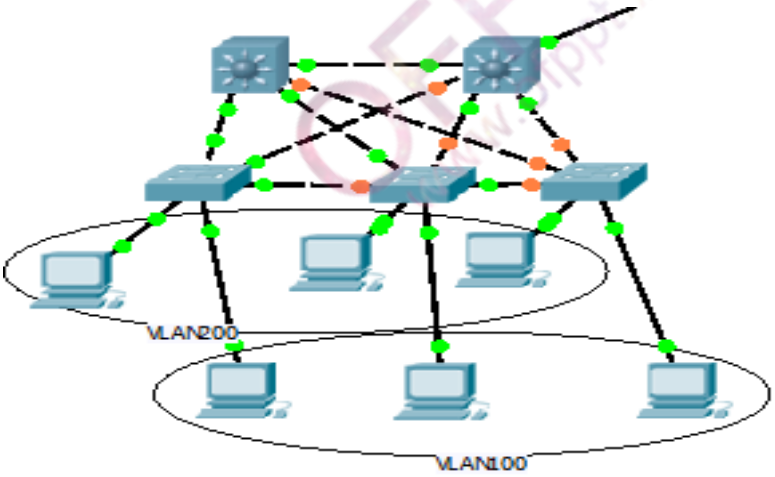
7) Le réseau local du routeur SIEGE, est basé sur une architecture multicouches, répondre aux questions suivantes :

a- Donner des exemples d'équipement :.

Réponses : Routeurs, commutateurs multicouches

b- Pour une tolérance aux pannes, l'administrateur veut mettre en place de la redondance des équipements et des liaisons, proposer un schéma avec des chemins et équipements redondants.

Proposition :



c- Spanning tree

8) Les switchs du réseau local du SIEGE exécutent le protocole VTP, la commande « show vtp status » a été exécutée au niveau du switch multicouche et a donné le résultat suivant :

```
s1#
s1#show vtp st
s1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : examen
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
```

a) Donner les valeurs des champs suivants : mode, domaine, numéro de révision ?

Réponse : mode : Server, domaine : examen, numéro de révision : 0

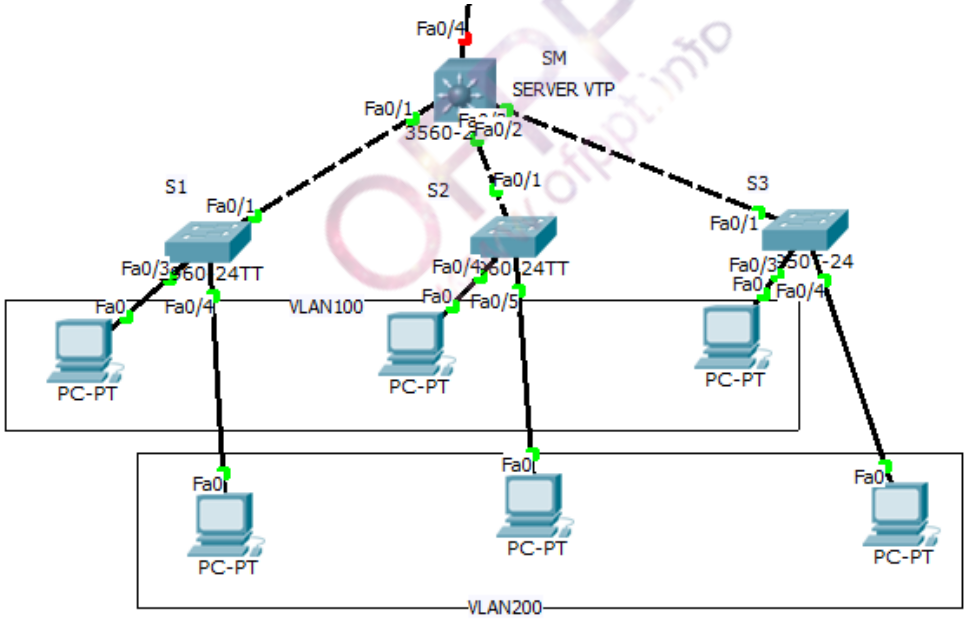
b) Justifier la valeur du numéro de révision ?

Réponse : il n y a eu aucune mise à jour VTP.

c) Quelle est l'utilité de du numéro de révision dans une annonce VTP ?

Réponse : Le n°de révision commence à 0 à l'allumage du switch et s'incrémente par pas de 1 lors de chaque changement de la configuration jusqu'à ce qu'il atteigne 4294927295, point au quel il recommence à 0.

9) L'administrateur a procédé à la création des vlan, sachant qu'il veut mettre en place le protocole VTP pour simplifier la création et la mise à jour de la base de données VLAN, donner toutes les étapes de la création et de l'affectation des ports aux vlan adéquats, ainsi que les ports agrégés (il n'est pas nécessaire de donner les commandes de configuration)



Réponse :

Création du Serveur VTP

Configuration du nom de domaine

Création des trunk

Configuration des clients VTP

Création des Vlan au niveau du serveur VTP

Affectation des ports aux vlan

10) La commande show ip route a été exécutée au niveau du routeur A1, la figure ci-dessous montre son résultat

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C       172.16.0.32/28 is directly connected, FastEthernet0/0.30
C       172.16.0.64/26 is directly connected, FastEthernet0/0.20
C       172.16.0.128/25 is directly connected, FastEthernet0/0.10
```

Répondre aux questions suivantes :

a) Donner les étapes de configuration du routage InterVlan.

Réponse :

Création des sous interfaces.

Configurer l'encapsulation dot1Q et spécifier le numéro de vlan

Affecter l'adresse IP à la sous interface

Exemple :

interface FastEthernet0/0.10

encapsulation dot1Q 10

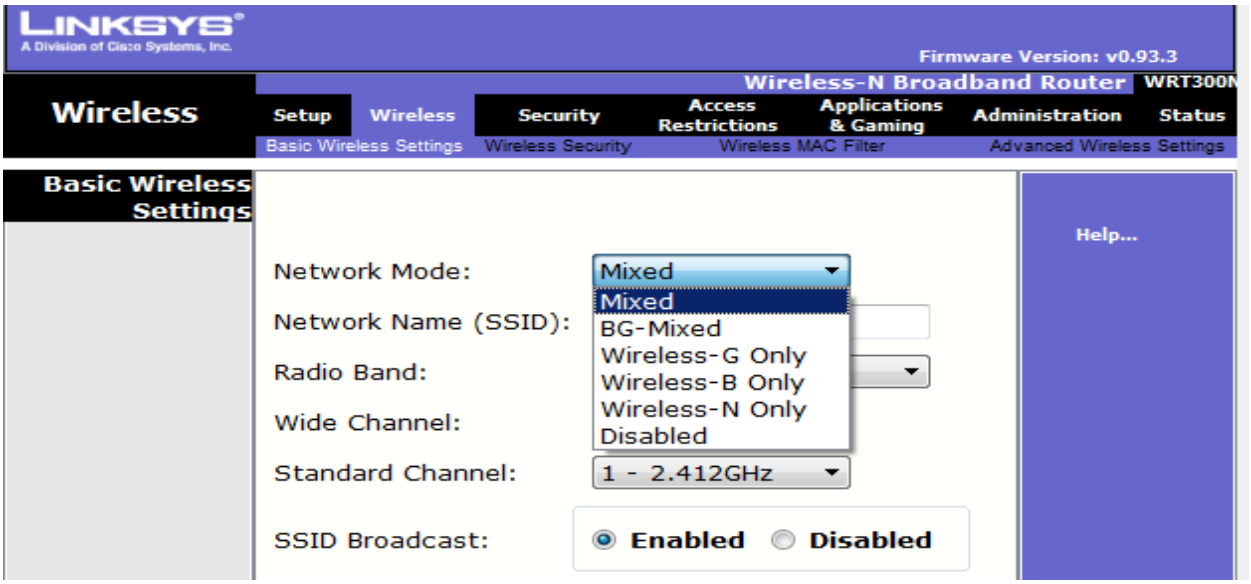
ip address 172.16.0.129 255.255.255.128

b) quelle est la signification de la lettre C qui précède les lignes du résultat de la commande **show ip route ?**
Réponse : réseaux directement connectés.

c) Que signifie "172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks" .
Réponse : Le réseau 172.16.0.0/16 est subdivisé avec VLSM en trois sous réseaux trois masques

d) L'administrateur a testé la connectivité entre les serveurs en envoyant un ping, le test ping n'a pas réussi, le ping à partir des serveurs vers le routeur ne réussit pas non plus, quelles sont les causes probables de l'échec du ping ?
Réponse : Erreur de ports agrégés et d'affectaion de ports aux Vlan.

11)



a) Quel est l'effet de cocher « SSID Broadcast» Enabled ?

Réponse : Le point d'accès sera lisible par tous les clients wifi

SSID Broadcast - Lorsque les clients sans fil recherchent sur le réseau local les réseaux sans fil auxquels s'associer, ils détectent la diffusion du SSID par le point d'accès. Pour diffuser le SSID, conservez le paramètre par défaut, Enabled. Si vous ne voulez pas diffuser le SSID, sélectionnez Disabled. Après avoir apporté les modifications à cet écran, cliquez sur le bouton Save Settings ou sur le bouton Cancel Changes pour annuler vos modifications. Pour plus d'informations, cliquez sur Help.

b) Quel paramètre faut-t-il tenir en compte lors de l'installation de points d'accès sur des zones qui interfèrent ?

Réponse : Le numéro de Canal.

12)

a) Quelle différence entre WPA2 Personal et WPA2 Entreprise ?

Réponse :

- WPA personnel (*WPA-Personal*) : connu également sous le nom de mode à secret partagé ou WPA-PSK (Pre-shared key), WPA personnel est conçu pour les réseaux personnels ou de petites entreprises, car il n'y a pas besoin d'utiliser un serveur d'authentification. Chaque équipement du réseau sans fil s'authentifie auprès du point d'accès en utilisant la même clé sur 256 bits.
- WPA entreprise (WPA-Enterprise) : connu également sous le nom de mode WPA-802.1X ou WPA-EAP, WPA entreprise est conçu pour les réseaux d'entreprise et demande à ce que l'on installe un serveur d'authentification RADIUS. C'est plus compliqué à mettre en place, mais offre plus de sécurité, car cette méthode ne repose pas sur des phrases secrètes, vulnérables auxattaques par dictionnaire. Le protocole EAP (Extensible Authentication Protocol) est utilisé pour l'authentification. EAP existe en plusieurs variantes, dont EAP-TLS, EAP-TTLS et EAP-SIM.

b) Quel mode de sécurité (WEP ou WPA) préférerez-vous utiliser et pour quelle raison ?

WEP : Authentification non efficace

Clés statiques, cassables

Non évolutif

WPA :

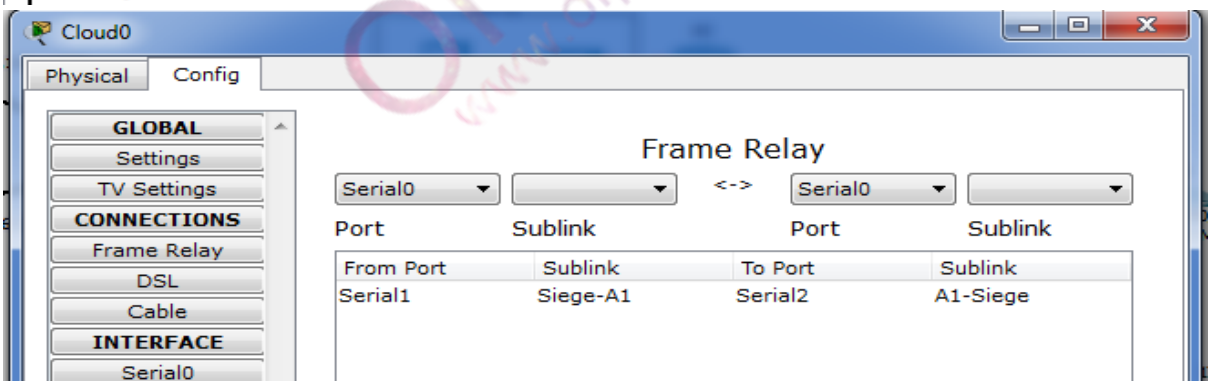
Standardisé

Chiffrement amélioré

Authentification utilisateur efficace (p.ex., LEAP, PEAP, EAP-FAST)

13) L'administrateur désire mettre en place un réseau frame relay de type **Mutipoint** tout en utilisant les sous-interfaces, les figures montrent un échantillon de la configuration.

```
Router#sh frame-relay map
Serial0/0.102 (up): point-to-point dlci, dlci 102, broadcast, status defined, ac
tive
Router#
```



a) La configuration contient une erreur, laquelle ?

Réponse :

Point à point alors que la configuration demandée est multipoint.

b) Donner la configuration à faire pour un réseau frame relay multipoint utilisant l'adresse 200.0.0.0/28, la topologie est montrée sur le schéma :

Réponse :

Interface S0/0

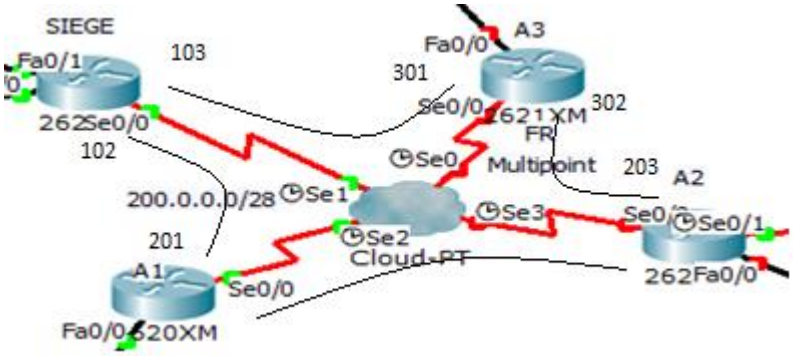
Encapsulation frame-relay

Interface S0/0.100 multipoint

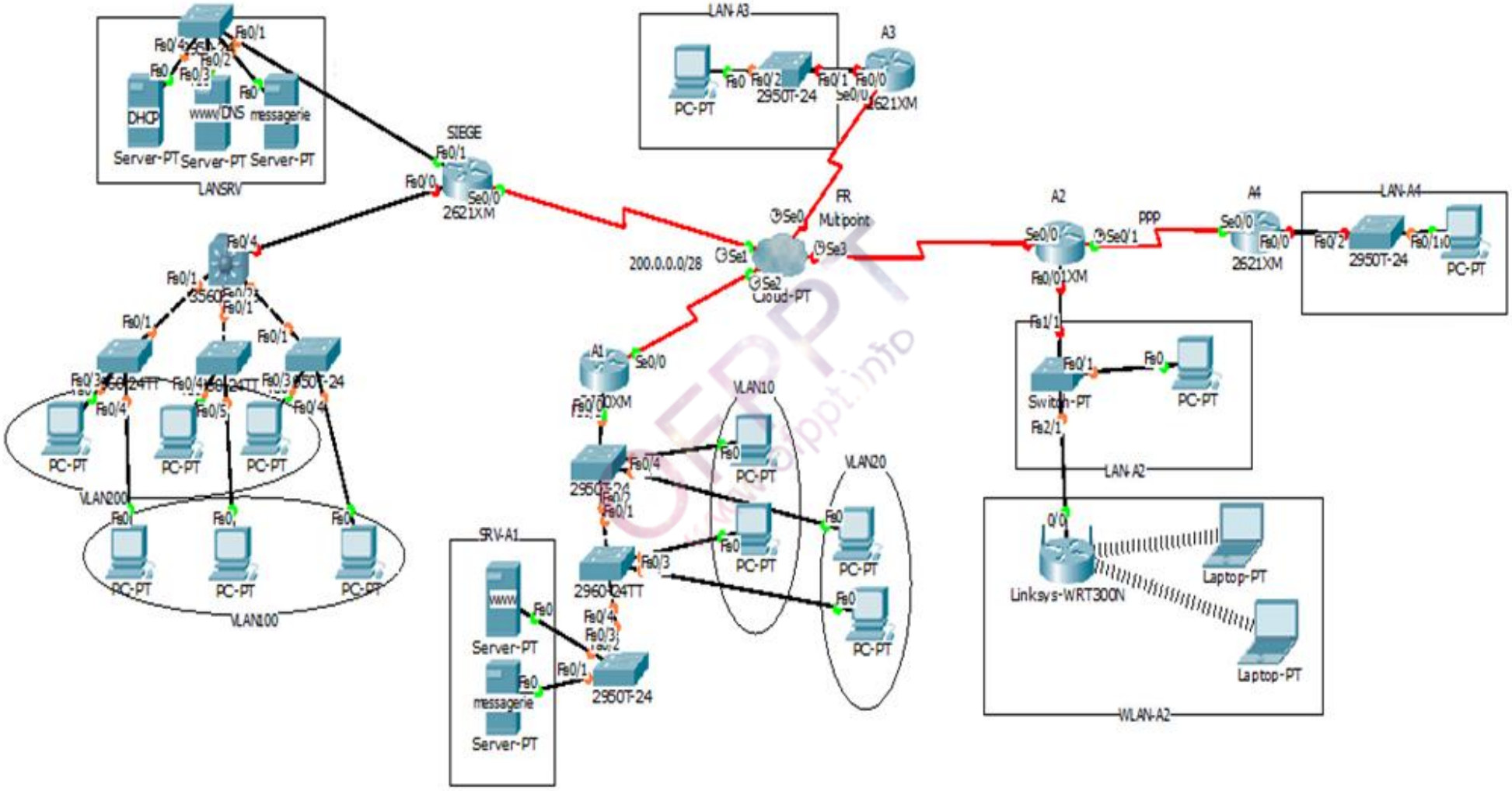
Ip address 200.0.0.1 255.255.255.240

Frame-relay interface-dlci 102

Frame-relay interface-dlci 103



Annexe1 :



Annexe 2 :

Réseau	@Réseau	Masque sous réseau	@Diffusion	1ère adresse	Dernière adresse
VLAN100	45	/26			
VLAN200	50	/26			
LANSRV	12	/28			
SRV-A1	10	/28			
VLAN10	30	/28			
VLAN20	60	/27 ou /26			
LAN-A3	78	/25			
WLAN-A2	40	/26			
LAN-A2	16	/27			
LAN-A4	35	/26			

Barème :