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

Session Juin 2018

Filière : Techniques des Réseaux Informatiques

Epreuve : Théorique

Barème : 40 points

Niveau : Technicien Spécialisé

Durée : 4h

Le CHM « Centre Hospitalier Maroc » est le premier centre hospitalier du genre au Maroc, il s'agit d'un centre de diagnostic, de soins, de traitement, d'hospitalisation, de recherche et de formation.

Etalé sur une superficie de 19 hectares, le CHM est un regroupement de quatre cliniques :

- Clinique G : fournit des services généraux de médecine et de psychiatrie.
- Clinique O : consolide les services d'ophtalmologie, d'ORL et d'orthopédie.
- Clinique M : propose une offre de soins de gynécologie médicale et chirurgicale et médecine de pédiatrie.
- Clinique C : fournit des services des soins d'oncologie et des maladies infectieuses et de l'immuno-allergologie.

Chaque clinique est dotée d'un service de radiologie et d'un laboratoire dédiés.

Un grand immeuble est dédié à l'administration de centre hospitalier et qui intègre tous les services techniques, avec juste à côté un autre immeuble dédié à la formation des médecins et autre personnel de santé.

En fin le CHM propose une dizaine de résidences dédiés aux membres des familles des malades.

L'administration du centre hospitalier est consciente quant à l'importance du système d'information et y investit constamment pour le bien des patients aussi bien que des praticiens hospitaliers.

Les différents sites (cliniques, administration et faculté) sont connectés par un réseau Ethernet à base de fibre optique. Chaque site utilise un réseau IP distinct pour adresser les hôtes des différents VLANs.

Le réseau IP 172.21.0.0 /24 est utilisé pour l'adressage des hôtes du clinique O.

1) ***Remplir le tableau d'adressage fourni en annexe.***

Le protocole OSPF est utilisé pour le routage entre les différents routeurs des sites.

En analysant les résultats de sortie sur le routeur-O (Clinique O), répondre aux questions suivantes :

```
Process ID 10, Router ID 10.0.0.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 9.9.9.9, Interface address **********
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:09
--------------------------------------------------------------------
Affichage tronqué
--------------------------------------------------------------------
```

2) ***Quel est le type de réseau détecté par OSPF ?***
3) ***Expliquer le rôle du routeur d'après cet extrait « state DR » ?***
4) ***Comment se fait le choix du routeur DR pour le protocole OSPF ?***
5) ***Donnez les commandes nécessaires pour configurer le protocole OSPF sur routeur-O pour une zone unique sachant que le réseau 10.20.30.0 /29 est utilisé pour connecter les routeurs des différents sites entre eux.***

Un technicien a opéré un remplacement d'un commutateur en panne du service de radiologie du clinique-M, le commutateur de remplacement possédait une ancienne configuration. Le technicien a commis l'erreur de le connecter sans le réinitialiser ce qui a engendré une série de problèmes.

Le message suivant est affiché systématiquement sur la console de connexion sur le commutateur de remplacement.

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(99), with SW-M5 FastEthernet0/1 (111).
```

6) ***Quelle est la cause de ce problème ? Comment le résoudre ?***

Au bout d'un moment, les utilisateurs signalent des problèmes de connectivité réseau, l'inspection de la configuration VTP du commutateur de remplacement est affichée comme suit :

```
SW-M2#show vtp status
VTP Version : 2
Configuration Revision : 35
Maximum VLANs supported locally : 255
Number of existing VLANs : 40
VTP Operating Mode : Server
VTP Domain Name : CliniqueM
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xCA 0x1F 0xE4 0x23 0x04 0x2A 0x74 0xEB
Configuration last modified by 0.0.0.0 at 3-1-93 00:03:29
Local updater ID is 0.0.0.0 (no valid interface found)
```

7) ***Expliquer la ligne soulignée dans le résultat de la commande.***
8) ***Comment expliquer les problèmes de connectivité signalés par les utilisateurs, (noter que le nom de domaine VTP utilisé par les autres commutateurs est : CliniqueM) ?***

Un seul domaine Active Directory « chm.ma.loc » est utilisé pour tout le centre CHM.

Pour fournir différents services réseaux et applicatifs à ces utilisateurs, l'administration a optée pour une solution de cloud privé tout en gardant des serveurs locaux.

9) ***Quelle est la différence entre un cloud privé et un cloud public ?***
10) ***Quelles sont les raisons qui poussent une société à utiliser des serveurs en local tout en exploitant une technologie de cloud ? donnez quelques exemples de services à déployer en local ?***

Un technicien réseau devait intervenir sur la machine « ORDI-D19 » du service réception du clinique M et qui tourne sous Windows7 pour résoudre un problème de connexion, l'exploitation d'un logiciel de capture de trames sur cette machine a révélée qu'un trafic énorme est lié au protocole LLMNR.

11) ***Qu'est-ce que le protocole LLMNR et quel est son rôle dans un réseau d'entreprise ?***

D'après les recherches menées par le technicien sur le protocole et en consensus avec l'administrateur, ils ont conclu qu'il serait préférable de désactiver le protocole LLMNR pour des raisons de performances et aussi pour réduire les risques de sécurité.

Pour désactiver LLMNR, l'administrateur a prévu l'utilisation d'un objet GPO. (voir annexe2)

12) ***Expliquer l'ordre d'application des objets GPO ?***
13) ***Quelle option doit être appliquée pour le paramètre de cet objet GPO afin de s'assurer de la désactivation du protocole LLMNR ?***

L'objet GPO est créé et est lié au domaine « chm.ma.loc » (voir annexe), après déploiement et redémarrage des machines, l'administrateur constate que le protocole est toujours activé sur les ordinateurs du clinique O.

14) ***Quelle est la cause la plus probable pour ce dysfonctionnement ?***

15) Que doit faire l'administrateur pour s'assurer de la désactivation du protocole LLMNR pour les hôtes du clinique O ?

Vous venez de déployer un nouveau serveur virtuel en local fonctionnant sous Windows server 2008 R2 en installation core. Vous devez dans un premier temps configurer cette machine avec les informations suivantes :

Adresse IP :	**172.21.5.200**
Masque de sous-réseau :	**255.255.255.240**
Passerelle :	**172.21.5.193**

16) Donnez l'instruction en ligne de commande nécessaire pour configurer cette machine avec les informations ci-dessus :

On désire installer les services de domaine Active directory et déployer un nouveau contrôleur de domaine pour le domaine « chm.ma.loc », l'administrateur a conçu un fichier de réponse d'installation du contrôleur de domaine.

```
1.  [DCInstall]
2.  UserName=Th3Admin
3.  UserDomain=chm.ma.loc
4.  Password=Th3P@55w0rd

5.  ReplicaOrNewDomain=Replica

6.  InstallDNS=Yes
7.  ConfirmGc=Yes

8.  DatabasePath= »C:\Windows\NTDS »
9.  LogPath= »C:\Windows\NTDS »
10. SYSVOLPath= »C:\Windows\SYSVOL »

11. SafeModeAdminPassword=L0cP@55w0rd

12. RebootOnCompletion=Yes
```

17) Expliquer les lignes 5,6 et 7 pour décrire l'installation prévue pour ce contrôleur de domaine.

La figure en annexe 3 correspond à une capture de trame réalisée sur la machine « ORDI-D19 ».

En utilisant les descriptifs de structures de trames Ethernet, de paquet IP et de datagramme UDP :

18) Quelles sont l'adresse Mac source et de destination ?
19) Quelle est l'adresse IP source et l'adresse IP de destination ?
20) Quel est le code du protocole de couche 4 utilisé ?
21) Quels sont les numéros de port source et de destination ?

Un administrateur système Linux a développé un script shell (présenté ci-dessous) pour automatiser la sauvegarde des dossiers utilisateurs dans le dossier /users et de bases de données mysql.

```
#!/bin/bash
1- backupdate=$(date +%Y-%m-%d)
2- dirbackup=/ExternalDSK/backup-$backupdate
3- mkdir $dirbackup
4- ……
5- /usr/bin/mysqldump --user=xxxx --password=xxxx --all-databases |
/usr/bin/gzip > $dirbackup/mysqldump-$backupdate.sql.gz
```

22) Expliquer la ligne 3 en relation avec la ligne 1 et 2 ?

23) Ajouter la ligne 4 permettant de sauvegarder le dossier /users avec l'option d'archivage et de compression.

24) Comment s'assurer de l'exécution périodique du script backup.sh chaque samedi à 20h30 ? donnez l'instruction à ajouter ?

A cause d'une faille sur le protocole SMB, certains ordinateurs connectés à Internet ont subi une attaque de ransomware.

Un serveur de fichiers fonctionnant sous Windows 2008 R2 et contenant les dossiers de base des utilisateurs et des dossiers partagés a été parmi les touchés, et les données qu'il contienne ont été chiffrés.

Le message suivant est un extrait du texte affiché sur les machines clientes infectées.

Tous vos fichiers ont été chiffrés avec l'algorithme RSA-4096.

25) Qu'est qu'un ransomware ? expliquez le principe de fonctionnement des ransomwares récents ?

26) Citer quelques mécanismes permettant d'éviter de telles attaques et/ou diminuer leurs impacts ?

27) Décrire le protocole de cryptage utilisé par ce ransomware ?

Les techniciens ayant isolé et désinfecté les machines touchées, leur prochaine tâche consiste à récupérer les données des utilisateurs, ils comptent exploiter les clichés instantanés des données du serveur créés sur un volume séparé non touché par le ransomware.

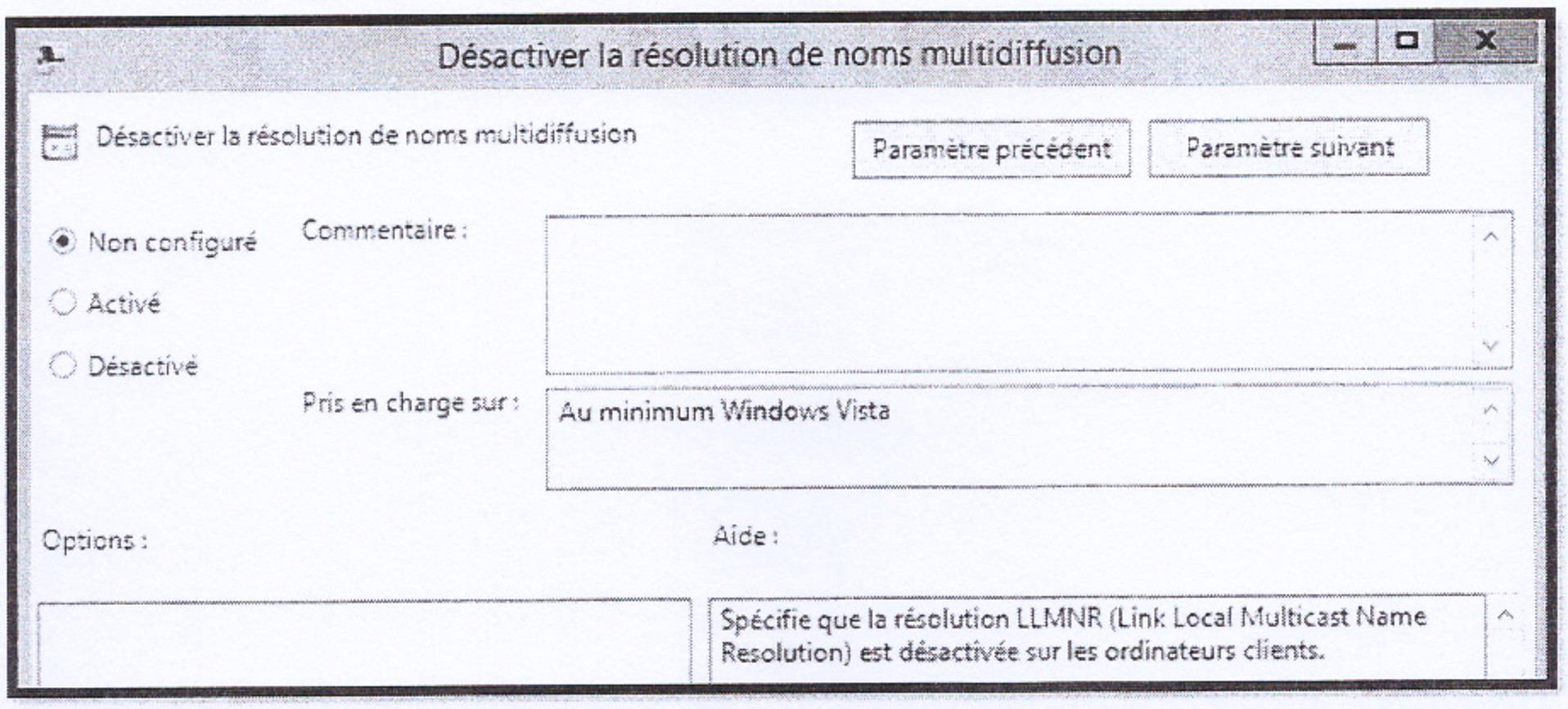
28) Qu'est-ce qu'un cliché instantané d'un dossier partagé ?

Annexe 1 : Tableau d'adressage du clinique O :

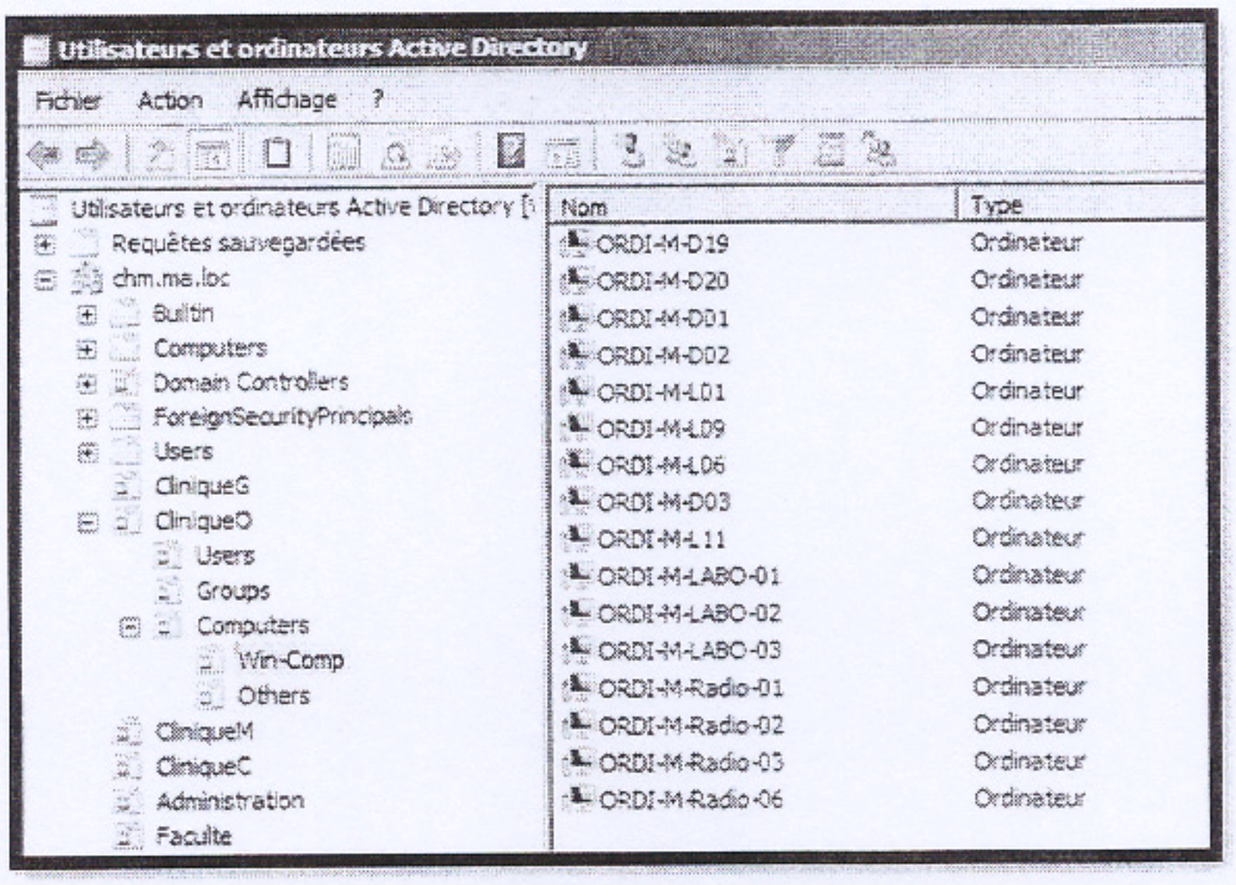
Réseau	ID du VLAN	Adresses IP en besoin	Adresse réseau /longueur de préfixe	Première adresse utilisable	Dernière adresse utilisable
Service Radiologie	VLAN10	22			
Laboratoire	VLAN20	18			
Administration de la clinique	VLAN30	15			
Affaires médicales	VLAN40	38			
Affaires financières	VLAN50	7			
Logistique et maintenance	VLAN60	5			

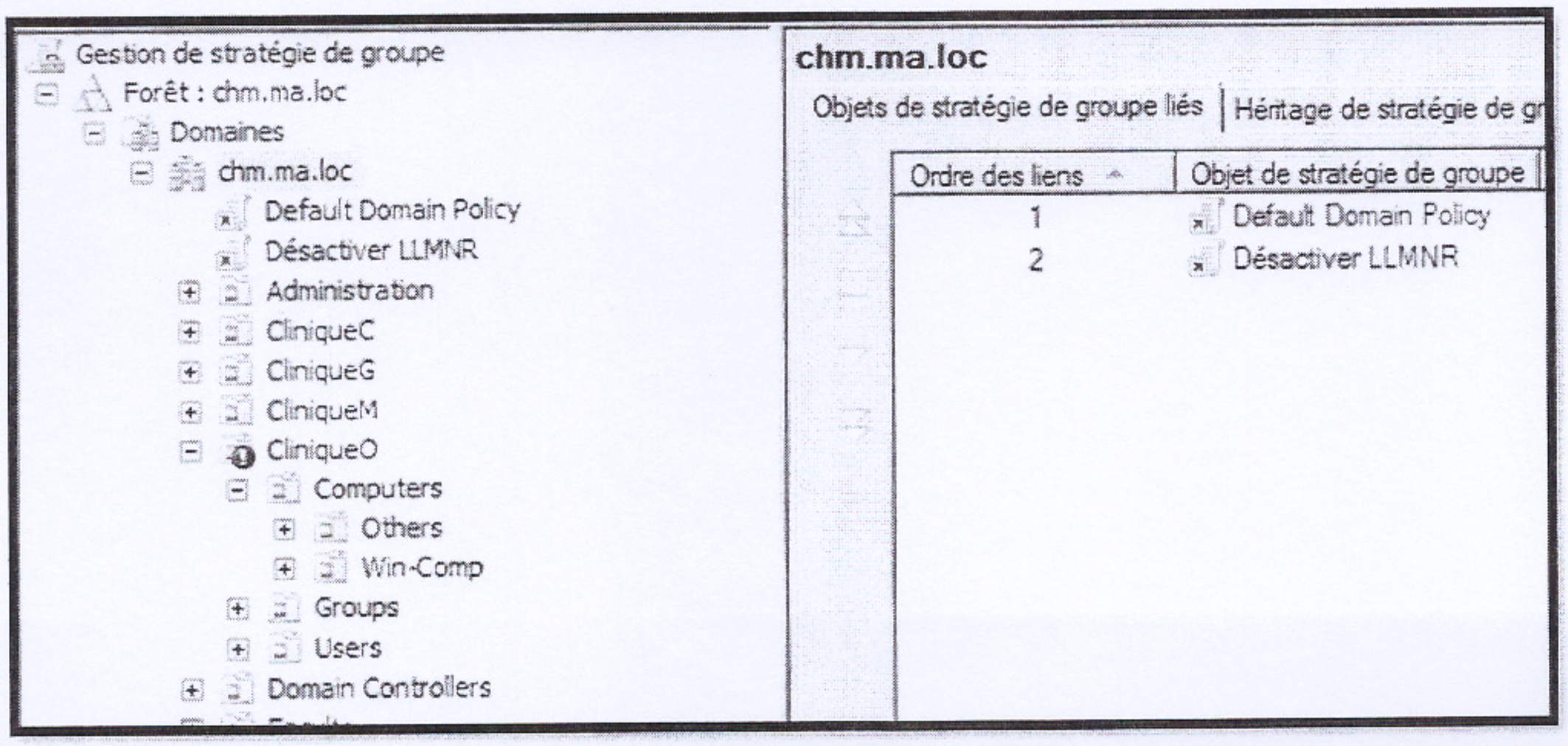
Annexe 2 :

Paramètre GPO désactiver LLMNR



Organisation des objets AD et objets GPO





Annexe 3 :

Capture Wireshark d'une trame LLMNR :

```
0000   01 00 5e 00 00 fc 08 3e  8e ca d7 b7 08 00 45 00   ..^....> ......E.
0010   00 35 37 93 00 00 01 11  e0 1c c0 a8 00 64 e0 00   .57..... .....d..
0020   00 fc ec 8a 14 eb 00 21  a3 a5 c6 95 00 00 00 01   .......! ........
0030   00 00 00 00 00 00 07 4f  52 44 49 2d 32 30 00 00   .......O RDI-20..
0040   1c 00 01                                          ...
```

Structure d'un paquet IPv4 (20 Octets)

0	8	16	24	32
Version	Longueur en-tête	Type de service	Longueur totale	
Identification		Drapeau	Déplacement de fragment	
Durée de vie	Protocole	Contrôle de l'en-tête		
Adresse IP source				
Adresse IP destination				
Options				Bourrage

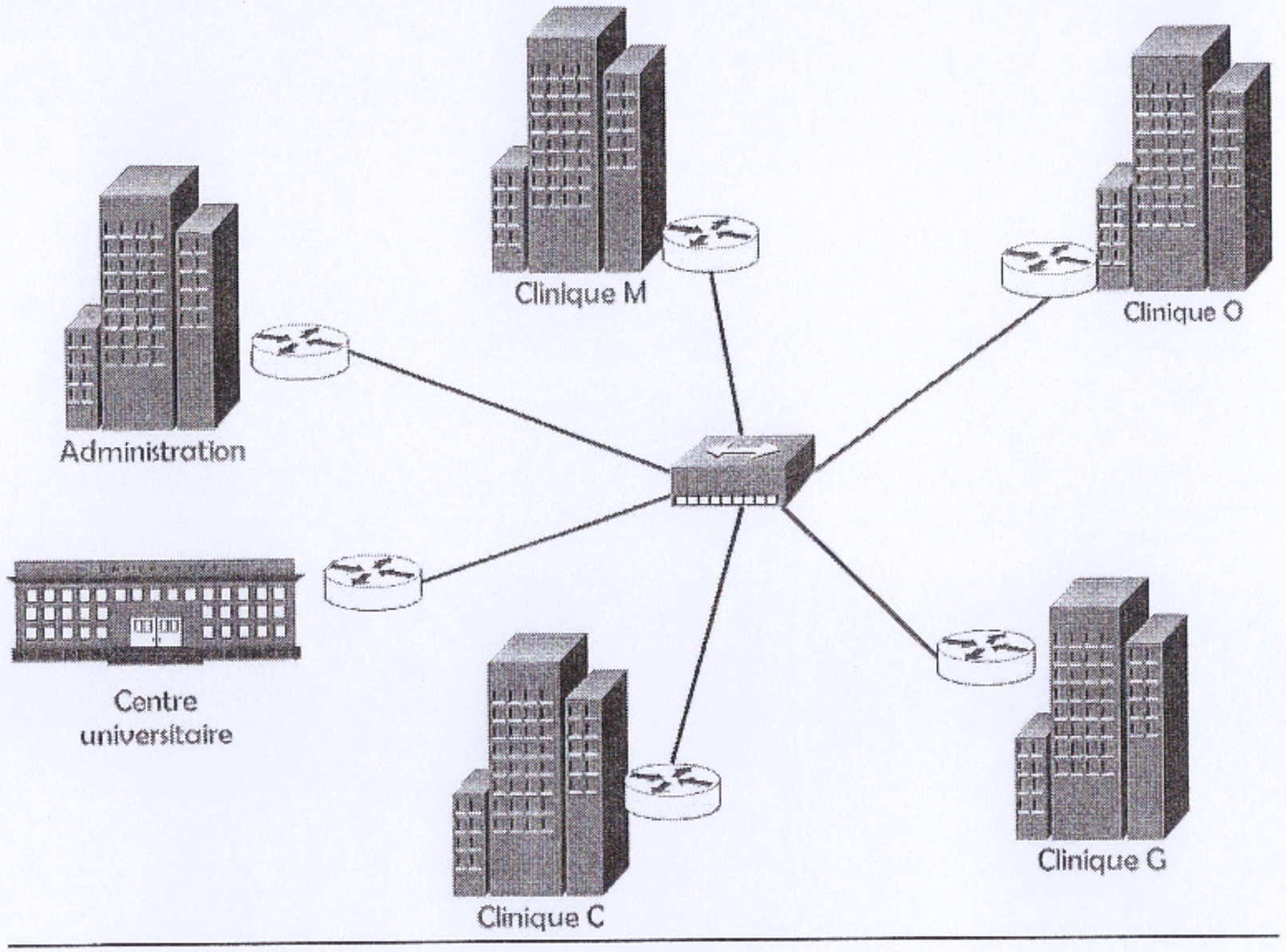
Structure d'un datagramme UDP

Port source (2 octets)	Port de destination (2 octets)
Longueur (2 octets)	Somme de contrôle (2 octets)
Données	

Structure d'une trame Ethernet

Adresse de destination	Adresse source	Type / Longueur (2 octets)	Données	FCS (4 octets)

Topologie du réseau du CHM :



Barème de notation

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
2	*1*	*1,5*	*2*	*2*	*1,5*	*1*	*1,5*	*1,5*	*1,5*	*1,5*	*1*	*1*	*1*

Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28
1	*2*	*2*	*1*	*1*	*1*	*1*	*1,5*	*2*	*1,5*	*1,5*	*1,5*	*1,5*	*1,5*