|  |  |
| --- | --- |
| Office de la Formation Professionnelle **et de la Promotion du Travail**  **OFPPT** |  |
|  |  |

**Direction Recherche et Ingénierie de la Formation**

**Examen de Fin de Formation CDJ**

**Session Juin 2018**

# Session Novembre 2004

|  |  |
| --- | --- |
| **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 routeurO, 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*

1. ***Quel est le type de réseau détecté par OSPF ?***

*Réseau à accès multiple avec diffusion*

1. ***Expliquer le rôle du routeur d’après cet extrait « state DR » ?***

*Dans une zone OSPF composée de réseaux de diffusion (*broadcast networks*) ou de réseaux à accès multiples sans diffusion, un «routeur désigné» (DR) doit être élu, il sert de référent pour la base de données topologique représentant le réseau. Tout autre routeur du réseau doit envoyer ses annonces OSPF au DR qui se charge de les retransmettre aux autres routeurs.*

1. ***Comment se fait le choix du routeur DR pour le protocole OSPF ?***
2. ***Le routeur ayant la valeur de priorité de l’interface la plus élevée.***
3. ***La valeur de router-id la plus élevée.***
4. ***L’adresse IP d’une interface de bouclage la plus élevée.***
5. ***L’adresse IP d’une interface physique la plus élevée.***
6. ***Donnez les commandes nécessaires pour configurer le protocole OSPF sur router-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.***

router ospf 1

log-adjacency-changes

network 172.21.0.0 0.0.0.63 area 0

network 172.21.0.64 0.0.0.31 area 0

network 172.21.0.96 0.0.0.31 area 0

network 172.21.0.128 0.0.0.31 area 0

network 172.21.0.160 0.0.0.15 area 0

network 172.21.0.176 0.0.0.7 area 0

network 10.20.30.0 0.0.0.7 area 0

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).

1. ***Quelle est la cause de ce problème ? Comment le résoudre ?***

*L’id de vlan natif configuré sur les deux commutateurs diffère.*

*Reconfigurer l’id de vlan du le commutateur de remplacement.*

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)

1. ***Expliquer la ligne soulignée dans le résultat de la commande.***

*Le numéro de révision de configuration est un nombre de 32 bits qui indique le niveau de la révision pour un paquet VTP. Ces informations sont utilisées afin de déterminer si les informations reçues sont plus récentes que la version actuelle. Chaque fois que a configuration VLAN dans un périphérique VTP est modifiée, le numéro de révision de la configuration est incrémentée de un.*

1. ***Comment expliquer les problèmes de connectivité signalés par les utilisateurs, (noter que le nom de domaine VTP utilisé par les autres commutateurs est : CliniqueM) ?***

*Le commutateur de remplacement n’ayant pas été réinitialisé, il contient une ancienne configuration avec un numéro de révision supérieur ce qui a donné que sa configuration VLAN a été propagée vers les autres commutateurs.*

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.

1. ***Quelle est la différence entre un cloud privé et un cloud public ?***

*Un cloud public est un service de cloud computing qui est hébergé par un fournisseur de services de cloud computing et mis à disposition pour un usage public. Un cloud public peut héberger un locataire unique ou il peut héberger des locataires issus de plusieurs organisations. En tant que tel, la sécurité d'un cloud public n'est pas aussi forte que celle d'un cloud privé, mais l'hébergement dans un cloud public est en général moins coûteux parce que les différents locataires absorbent le coût.  
À l'inverse, les clouds privés représentent une infrastructure de cloud computing dédiée à une organisation unique. Les clouds privés peuvent être hébergés par l'organisation elle-même ou peuvent être hébergés par un fournisseur de services de cloud computing qui garantit que les services de cloud computing ne sont partagés avec aucune autre organisation.*

1. ***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 ?***

*Certains services sont indispensable pour accéder au cloud et par conséquent doivent être déployés localement :*

* *Services d’infrastructures réseaux : DNS, DHCP.*
* *Serveur d’impression.*
* *Les serveurs d’authentification.*
* *Serveurs de déploiement du système d’exploitation et d’applications.*

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.

1. ***Qu’est-ce que le protocole LLMNR et quel est son rôle dans un réseau d’entreprise ?***

*LLMNR (Link-local Multicast Name Resolution) est un protocole normalisé par l'IETF pour la résolution de noms sur un réseau local lorsqu'il n'y a pas d'administrateur système présent et qu'il est donc difficilement envisageable d'utiliser le DNS.*

*Le port utilisé est le port UDP 5355 .*

*L'adresse de multicast est 224.0.0.252 ou son équivalent IPv6 FF02::1:3*

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 )

1. ***Expliquer l’ordre d’application des objets GPO ?***

*L’ordre d’application des stratégies de groupe est :*

* *Local : la GPO d’ordinateur qui est la première crée lorsque l’ordinateur est installé.*
* *Site : une GPO de site.*
* *Domaine : une GPO qui applique des paramètres communs à l’ensemble du domaine.*
* *OU : Unité d’Organisation contenant l’utilisateur ou l’ordinateur*

1. ***Quelle option doit être appliquée pour le paramètre de cet objet GPO afin de s’assurer de la désactivation du protocole LLMNR ?***

*Activé*

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.

1. ***Quelle est la cause la plus probable pour ce dysfonctionnement ?***

*L’option « bloquer l’héritage » est configuré au niveau de l’unité d’organisation « Clinique-O ».*

1. ***Que doit faire l’administrateur pour s’assurer de la désactivation du protocole LLMNR pour les hôtes du clinique O ?***

*Enlever l’option « bloquer l’héritage » ou activer l’option « appliqué » sur le lien.*

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**

1. ***Donnez l’instruction en ligne de commande nécessaire pour configurer cette machine avec les informations ci-dessus :***

*netsh interface ip set address "connexion au réseau local" static 172.21.5.200 255.255.255.240 172.21.5.193*

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*
13. ***Expliquer les lignes 5,6 et 7 pour décrire l’installation prévue pour ce contrôleur de domaine.***

*Installation d’un contrôleur de domaine supplémentaire sur lequel le service DNS sera installé et qui jouera le rôle de serveur de catalogue global.*

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 :

1. ***Quel est le code du protocole de couche 4 utilisé ?***

*17 (UDP)*

1. ***Quelle est l’adresse IP source et l’adresse IP de destination ?***

*IP SRC = 192.168.0.100**IP DST = 224.0.0.252*

1. ***Quels sont les numéros de port source et de destination ?***

*Port SRC = 60554**Port DST = 5355*

1. ***Quelles sont l’adresse Mac source et de destination ?***

*Mac SRC = 08:3e:8e:ca:d7:b7**Mac DST = 01:00:5e:00:00:fc*

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 du SGBD 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

1. ***Expliquer la ligne 3 en relation avec la ligne 1 et 2 ?***

*Création d’un dossier dans le dossier /ExternalDSK, le nom du dossier sera composé du mot backup auquel est ajouté la date.*

1. ***Ajouter la ligne 4 permettant de sauvegarder le dossier /users avec l’option d’archivage et de compression.***

*Les commande tar,cpio,dar ou pax peuvent être utilisées.*

1. ***Comment s’assurer de l’exécution périodique du script backup.sh chaque samedi à 20h30 ? donnez l’instruction à ajouter ?***

*Programmer l’exécution du script, utiliser cron, l’instruction à ajouter est :*

*30 20 \* \* 6 backup.sh*

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.*

1. ***Qu’est qu’un ransomware ? expliquez le principe de fonctionnement des ransomwares récents ?***

*Un ransomware, ou rançongiciel en français, est un logiciel informatique malveillant. Le ransomware chiffre les données contenues sur le disque dur et demande une rançon en échange d'une clé permettant de les déchiffrer.*

*Bien souvent, le ransomware s'infiltre sous la forme d'un ver informatique, à travers un fichier téléchargé ou reçu par email et chiffre les données et fichiers de la victime. La finalité est d‘extorquer une somme d'argent à payer le plus souvent par monnaie virtuelle pour éviter toute trace.*

*Il existe deux types principaux de ransomware :*

* *Locker ransomware, qui verrouille l'ordinateur ou l'appareil.*
* *Crypto ransomware, qui empêche l'accès aux fichiers ou aux données, généralement par cryptage.*

*Le ransomware crypte les données en utilisant un cryptage symétrique ou asymétrique, cette clé est récupérée depuis le serveur « Commande et contrôle » ou générée localement puis enregistrée après sur le serveur de « Commande et contrôle ».*

1. ***Citer quelques mécanismes permettant d’éviter de telles attaques et/ou diminuer leurs impacts ?***

* *Mise à jour du système d’exploitation.*
* *Former les utilisateurs.*
* *Sauvegarder les données.*
* *Contrôler le trafic entrant et les règles de pare-feu.*
* *S’assurer que les antivirus et logiciels anti-malware sont à jour.*
* *…*

1. ***Décrire le protocole de cryptage utilisé par ce ransomware ?***

* *Chiffrement asymétrique.*
* *Utilisation d’une paire de clés (publique / privée)*
* *Longueur de clé : 4096 bits.*

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.

1. ***Qu’est-ce qu’un cliché instantané d’un dossier partagé ?***

*La fonction Clichés instantanés de dossiers partagés permet d’obtenir des copies ponctuelles de fichiers qui se trouvent sur des ressources partagées, comme par exemple un serveur de fichiers. Grâce aux clichés instantanés de dossiers partagés, les utilisateurs peuvent afficher le contenu des fichiers et des dossiers partagés à différents moments. Il s’avère utile d’accéder à des versions précédentes, ou clichés instantanés, des fichiers car les utilisateurs peuvent :*

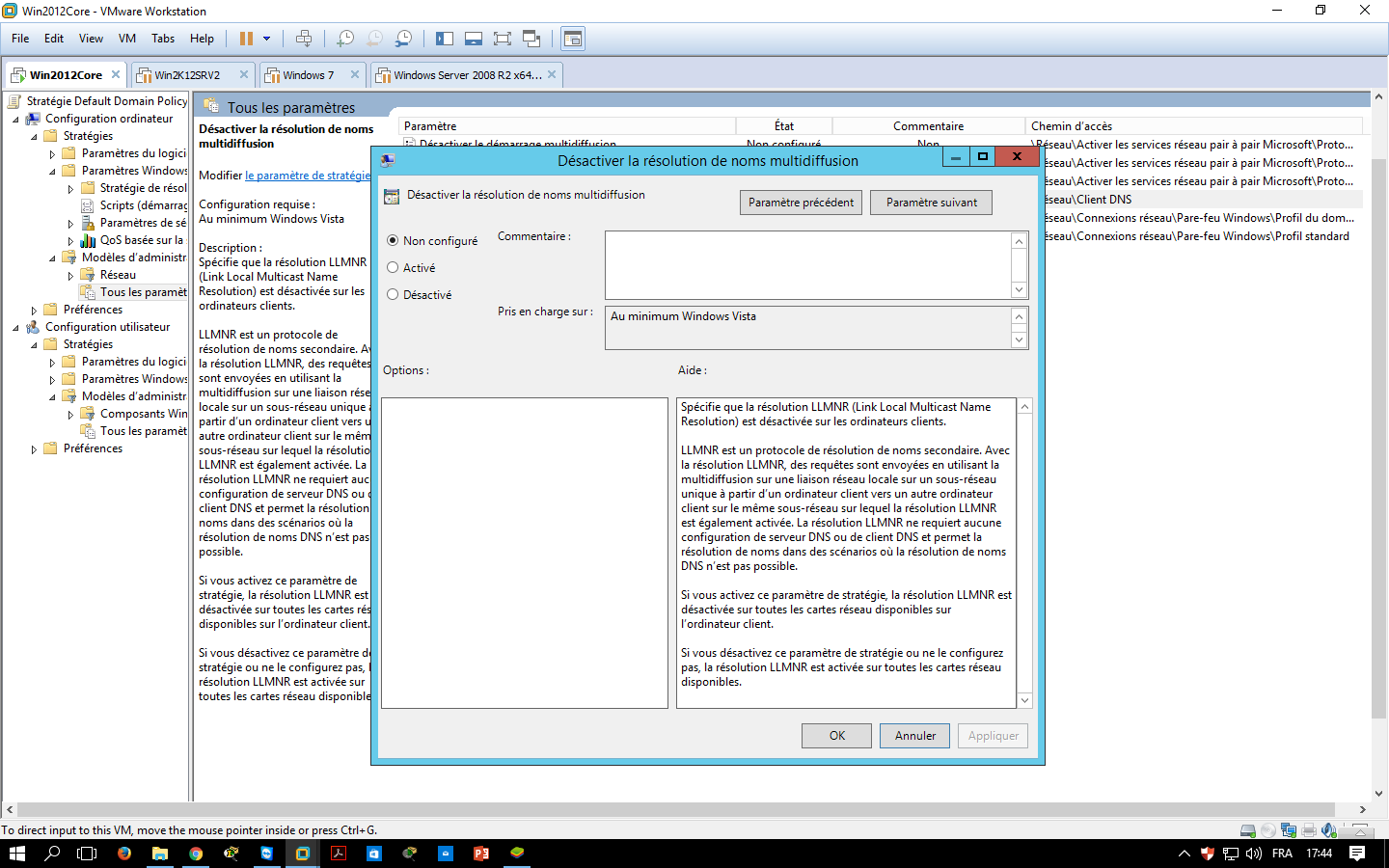
* *Récupérer des fichiers qui ont été accidentellement supprimés.*
* *Récupérer des fichiers qui ont été accidentellement écrasés.*
* *Comparer différentes versions d’un fichier en cours de travail.*

**Annexe 1 : Tableau d’adressage du clinique O :**

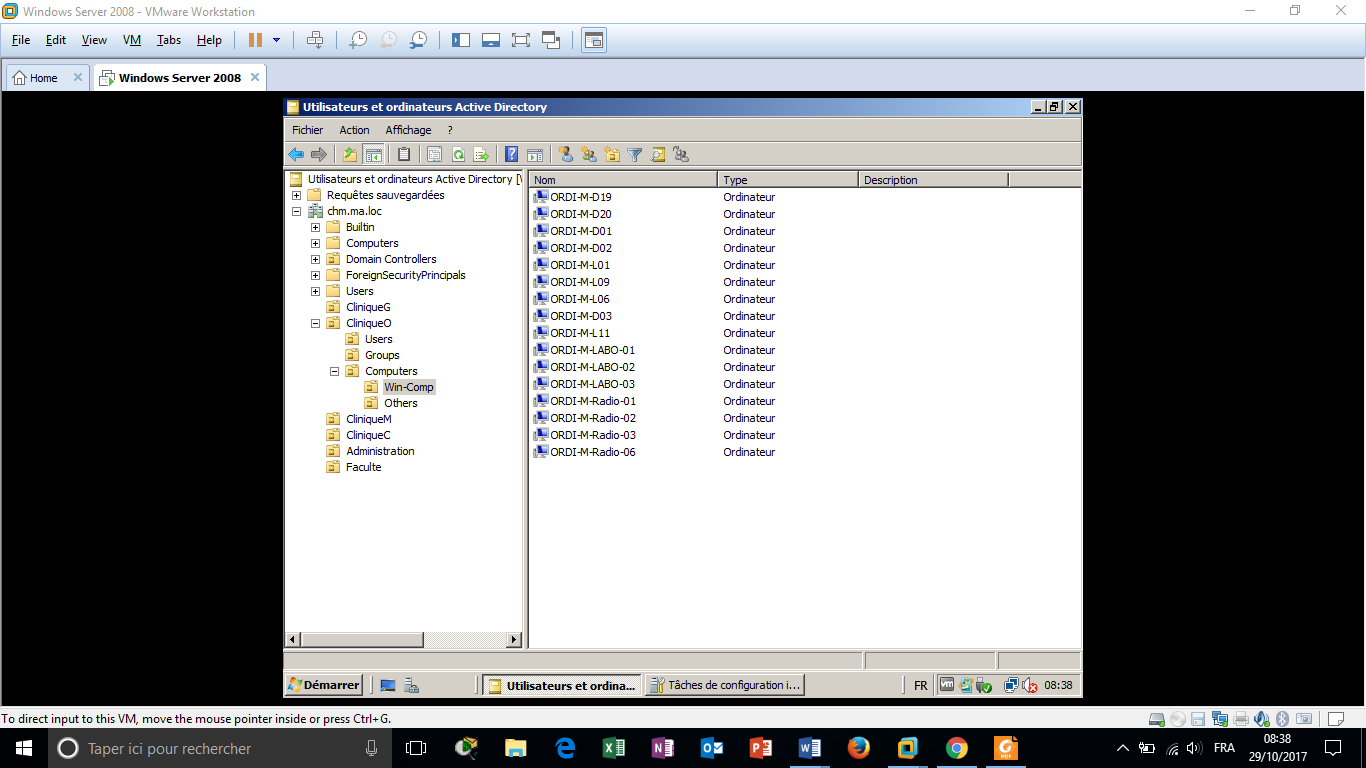
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Réseau** | **ID du VLAN** | **Adresses IP en besoin** | **Adresse réseau /longueur de préfixe** | **Première adresse utilisable** | **Dernière adresse utilisable** |
| Service Radiologie | VLAN10 | 22 | 172.21.0.64 /27 | 172.21.0.65 | 172.21.0.94 |
| Laboratoire | VLAN20 | 18 | 172.21.0.96 /27 | 172.21.0.97 | 172.21.0.126 |
| Administration  du clinique | VLAN30 | 15 | 172.21.0.128 /27 | 172.21.0.129 | 172.21.0.158 |
| Affaires médicales | VLAN40 | 38 | 172.21.0.0 /26 | 172.21.0.1 | 172.21.0.62 |
| Affaires financières | VLAN50 | 7 | 172.21.0.160 /28 | 172.21.0.161 | 172.21.0.174 |
| Logistique et maintenance | VLAN60 | 5 | 172.21.0.176 /29 | 172.21.0.177 | 172.21.0.182 |

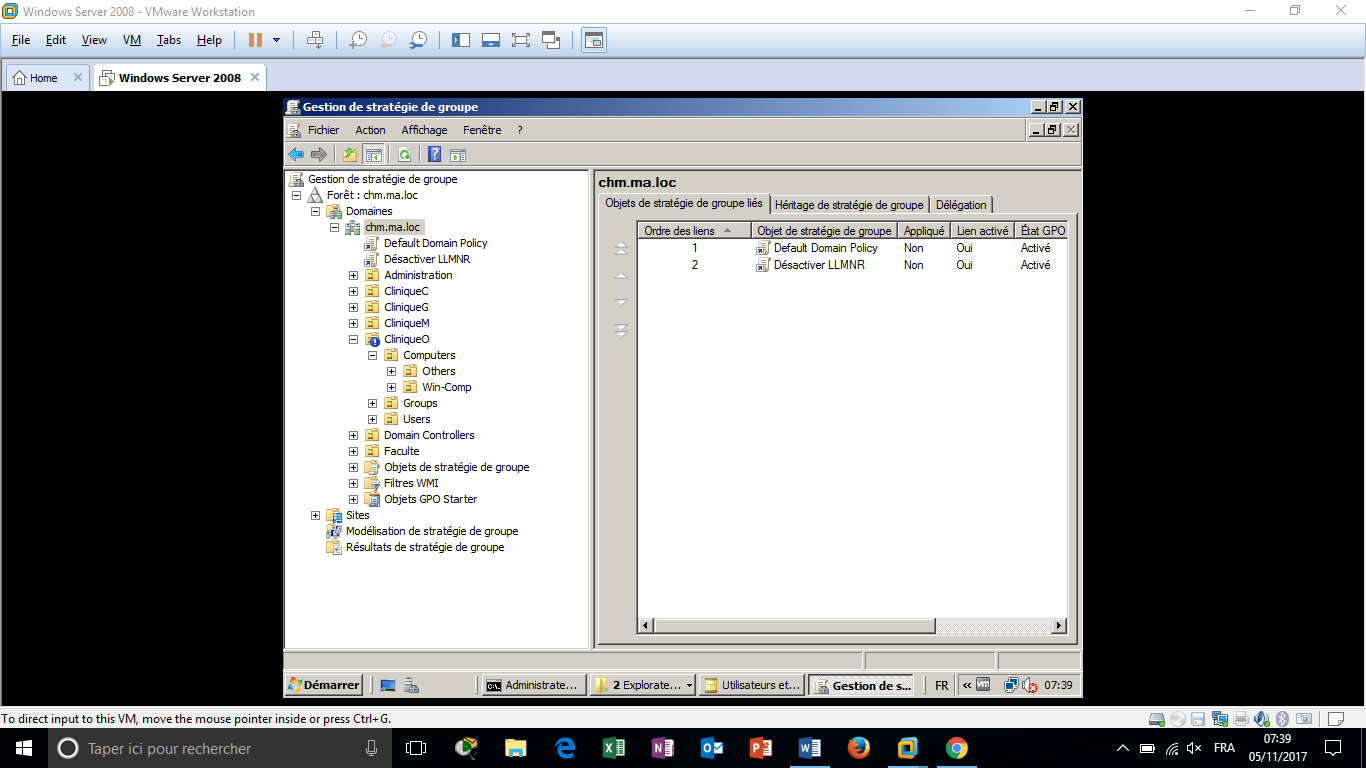
**Annexe 2 :**

**Paramètre GPO désactiver LLMNR**

****

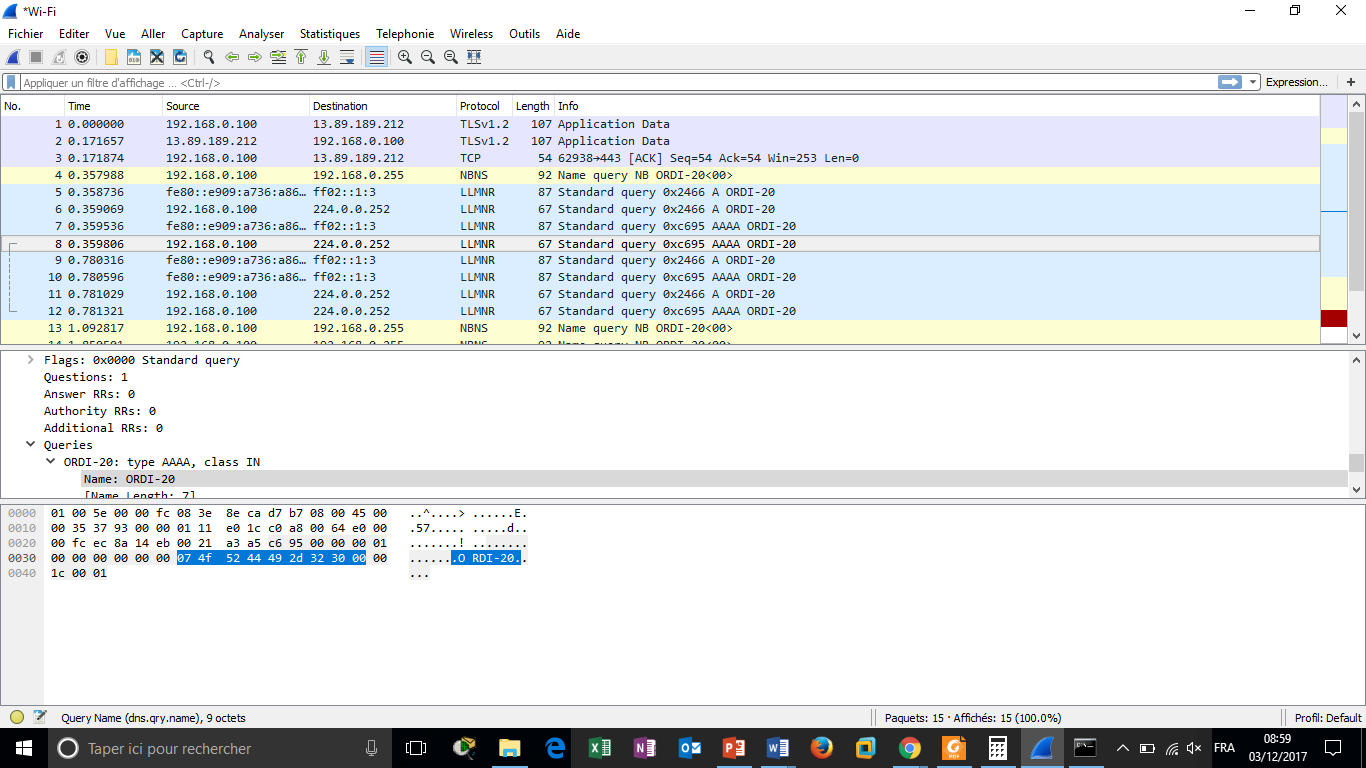
**Organisation des objets AD et objets GPO**



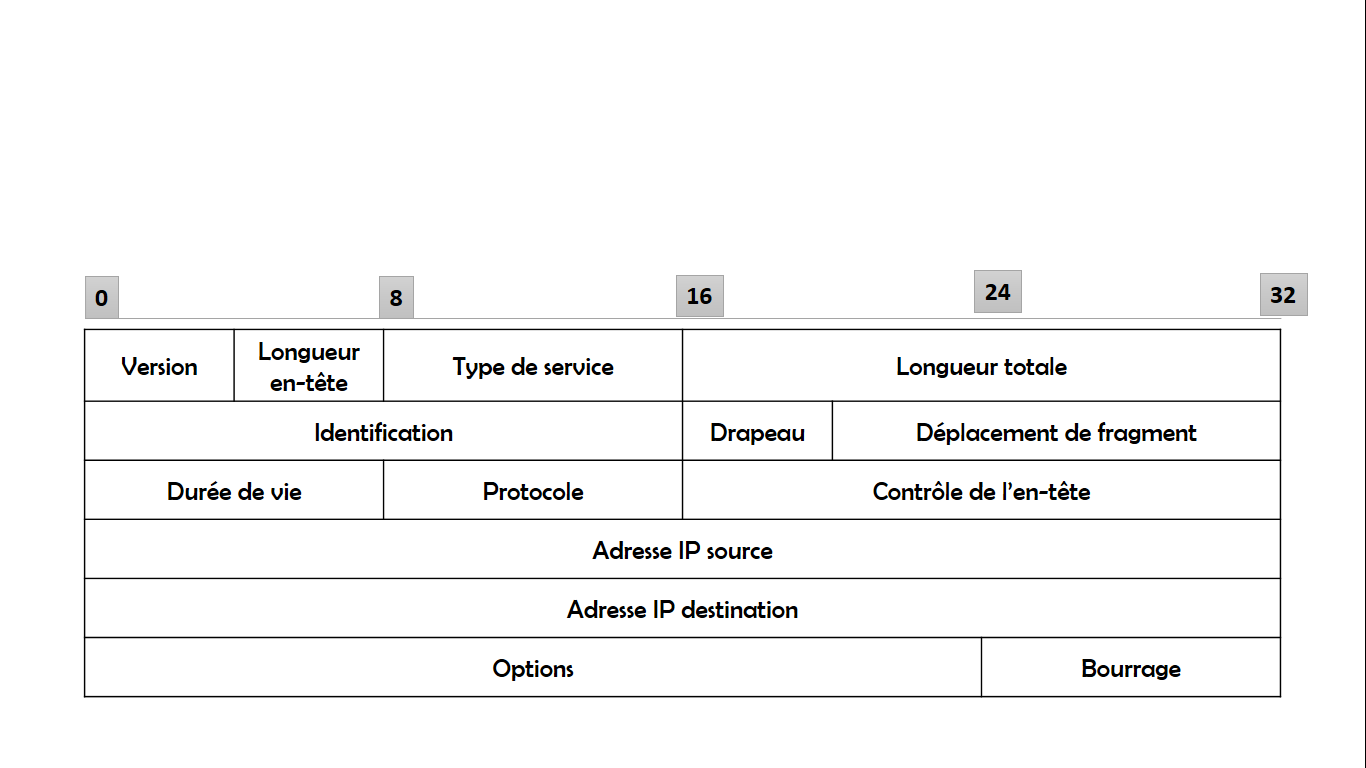


**Annexe 3 :**

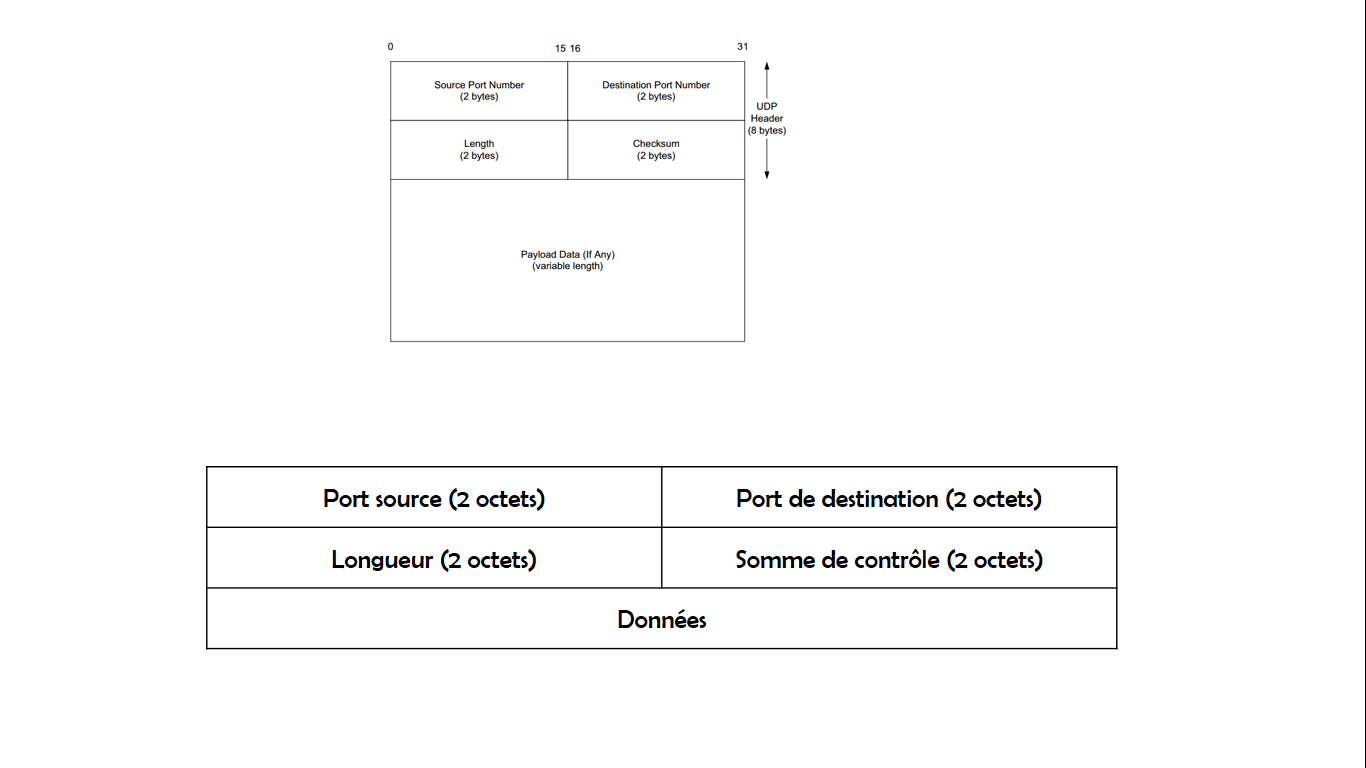
**Capture Wireshark d’une trame LLMNR :**



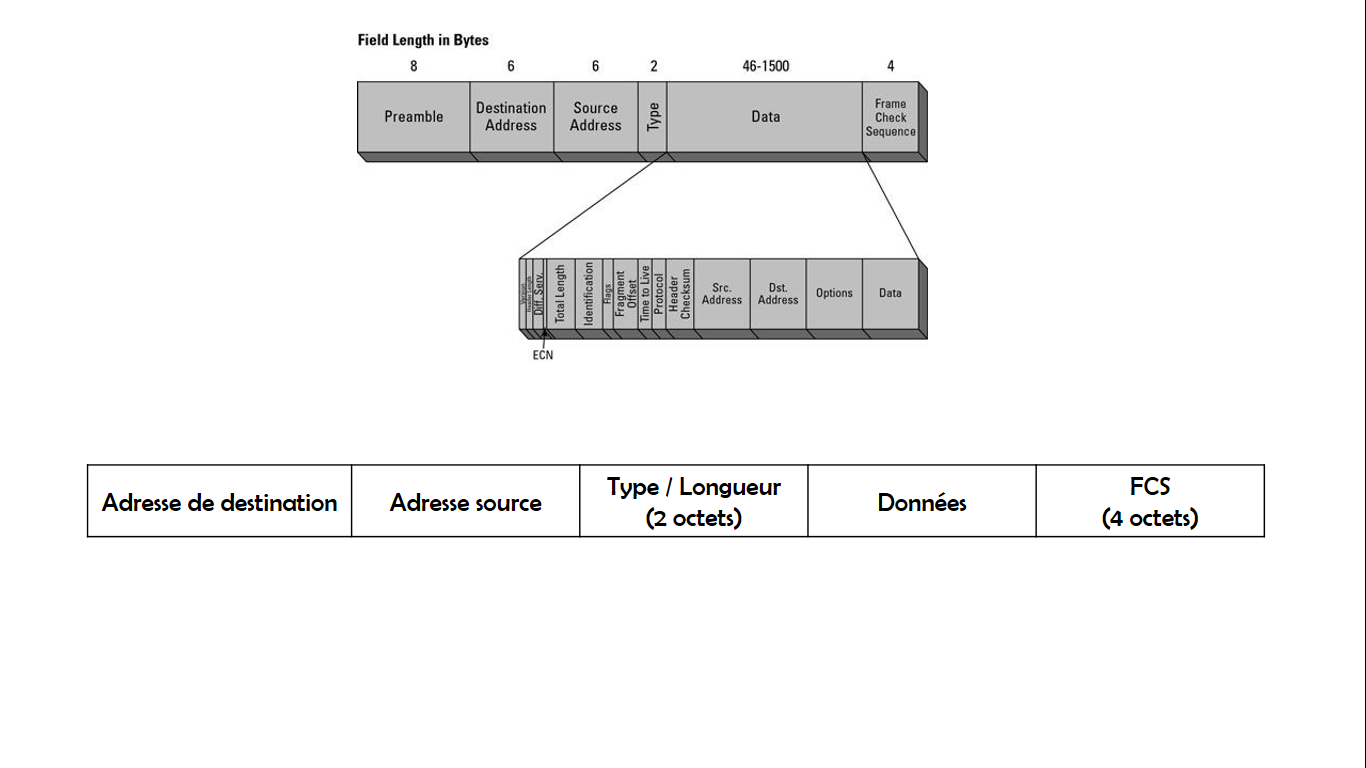
**Structure d’un paquet IPv4**



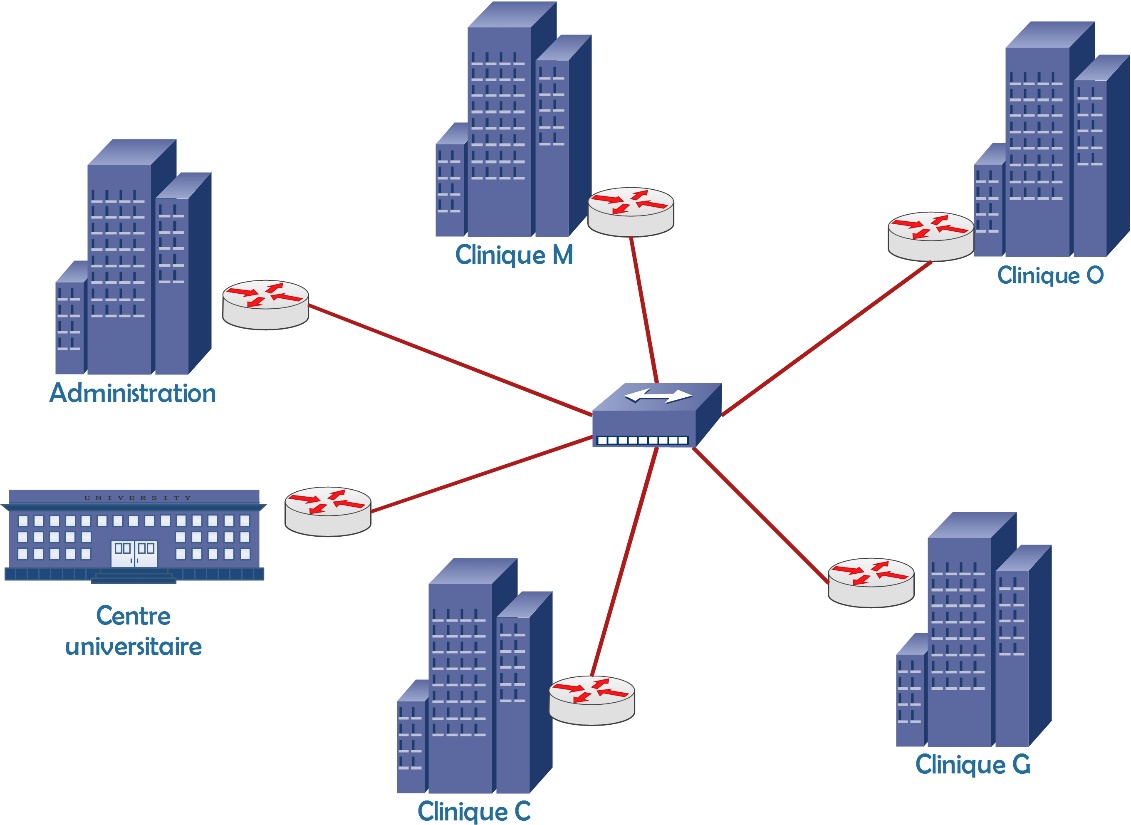
**Structure d’un datagramme UDP**



**Structure d’une trame Ethernet**



**Topologie du réseau du CHM :**

****

**Barème de notation**

****