

*République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des frères Mentouri
Faculté des sciences de la technologie
Département d'électronique*



ADMINISTRATION DES SERVICES RESEAUX

TRAVAUX PRATIQUES

Préparée par : Dr. Guelthoum Bendiab

Année Universitaire : 2020/2021

*Dr. Guelthoum Bendiab
kelthoum.bendiab@umc.edu.dz*

INTRODUCTION

Les réseaux informatiques ont atteint une importance cruciale dans le fonctionnement de l'entreprise moderne, quel que soit sa taille et son activité. Dans ce contexte, l'administration des réseaux informatiques s'affirme aujourd'hui comme une activité-clé de toute entreprise. En plus d'être constamment en fonction, ces outils d'échange de données et de partage d'information en temps réel doivent être en mesure d'offrir une confidentialité maximale et une sécurité à toute épreuve. En utilisant des logiciels d'administration de réseau, l'administrateur du réseau sera capable de gérer le réseau comme un ensemble et non comme une association de petits réseaux et de n'importe quel point du réseau, tout en préservant la sécurité du réseau.

Ce module a pour objectif de permettre à l'étudiant d'acquérir les connaissances et les compétences nécessaires pour l'exploitation, l'administration, la maintenance et la surveillance des réseaux informatiques. Plus particulièrement, l'étudiant se familiarisera avec des fonctions et des protocoles qui doivent lui permettre de gérer le bon fonctionnement des services réseaux notamment les services annuaires, les services de messagerie électronique et les services d'applications, etc. On y traitera particulièrement de l'administration d'un réseau informatique à gestion centralisée (i.e. Architecture client/serveur) dans le contexte des deux systèmes d'exploitation réseaux les plus répandus : Microsoft Windows et LINUX. Afin d'atteindre ces objectifs, ce module se devise en cinq TP comme suit :

Le premier TP (Environnement d'administration) présente aux étudiants les outils et les compétences nécessaires pour mettre en place un environnement d'administration des réseaux informatiques en utilisant le simulateur réseau graphique GNS3 (Graphical Network Simulator -3) et le logiciel de virtualisation VMware.

Le deuxième TP (Service DHCP) montre l'importance de service DHCP (Dynamic Host Configuration Protocol) dans l'administration des réseaux informatiques. Il focalise sur l'installation et la configuration de ce service sur un system Unix (routeur Cisco), ainsi d'un agent de relais DHCP. La configuration de ce service sur un system d'exploitation Windows (Windows Server 2003) sera effectuée dans le troisième TP (Service DNS).

Le troisième TP (Service DNS) présente aux étudiants les notions de bases d'un service DNS (Domain name Server). À la fin de ce TP, L'étudiant sera capable d'installer et de configurer un servie DNS sous le système d'exploitation Windows (Windows Servers 2003) et le système d'exploitation Linux (Ubuntu) en utilisant le serveur DNS BIND.

Le quatrième TP (Services Web et FTP) présente aux étudiants les deux services les plus rependus sur Internet ; Web et FTP (File Transfer Protocol). Ce TP permet à l'étudiant d'acquérir les compétences et les outils pour mettre en place un serveur Web et un serveur FTP sous un system d'exploitation Windows (Windows Server 2003).

Le cinquième TP (administration à distance) montre l'importance de l'outil webmin dans la gestion et l'administration des différents services réseau à distance. Il focalise sur la configuration graphique du serveur de résolution de nom DNS, SAMBA, le serveur web et le serveur de connexion à distance ssh.

Le sixième TP (Installation d'un contrôleur de domaine Active Directory) montre aux étudiants l'importance de l'administration centralisée des réseaux informatiques en utilisant l'annuaire Active Directory sous Windows. Avec ce TP, l'étudiant sera capable d'installer et de configurer un contrôleur de domaine, tester l'ouverture d'une session dans ce domaine, intégrer des machines au domaine et créer des stratégies de groupe.

Le septième TP (service de messagerie) présente aux étudiants le service de messagerie. Il focalise sur l'installation et la configuration de Postfix en tant que serveur SMTP (Simple Mail Transfer Protocol) pour l'envoi et la transmission des courriers électronique.

OUTILS NECESSAIRES

WIRESHARK

Le logiciel Wireshark est un analyseur de paquets gratuit. Il permet l'analyse de transmissions réseau sur presque toutes les technologies. Wireshark fonctionne sur de nombreux environnements compatible UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows.



Lien de téléchargement : <https://www.wireshark.org/>

FILEZILLA

Filezilla est un client FTP gratuit (licence publique générale GNU), c'est-à-dire un logiciel permettant l'échange de fichiers entre un ordinateur et un serveur ou vice-versa. Il est simple, rapide d'utilisation et vous permettra de vous connecter à n'importe quel serveur FTP, même si vous avez un proxy ou un firewall.



Lien de téléchargement : <https://filezilla-project.org/>

WINSCP

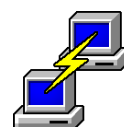
WinSCP (Windows Secure Copy) est un client SFTP graphique pour Windows en utilisant SSH et SCP (Secure Copy Protocol). Le but de ce programme est de permettre la copie sécurisée de fichiers entre un ordinateur local et un ordinateur distant. Il fonctionne avec PuTTY Agent pour un support complet de l'authentification par clé publique.



Lien de téléchargement : <https://winscp.net/eng/download.php>

PuTTY

PuTTY (open source) est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin, et TCP brut. Il comprend un client SFTP en ligne de commande appelé **psftp** et un client SCP en ligne de commande appelé **pscp**. La version en ligne de commande de cet outil est appelée Plink. Il supporte l'authentification par clé publique.



Lien de téléchargement : <https://www.wireshark.org/>

WINPCAP

WinPcap est un programme de filtrage qui permet de capturer des trames IP dans un environnement Windows. La plupart du temps intégré aux applications comme Windump ou Ethereal, WinPcap ne fonctionne pas en standalone. Il s'agit en effet d'un API et ne peut être utilisé qu'au travers d'autres applications.



Lien de téléchargement : <https://www.wireshark.org/>

TABLE DES MATIERS

Introduction.....	2
1. Environnement d'administration.....	7
1.1. But.....	7
1.2. Introduction.....	7
1.3. Graphical Network Simulator-3 (GNS3).....	7
1.4. Création et configuration d'un réseau local simple avec GNS3	8
2. Service DHCP (Dynamic Host Configuration Protocol)	10
2.1. But.....	10
2.2. Introduction.....	10
2.3. service DHCP sur un routeur Cisco	11
3. Service DNS (Domain Name System).....	13
3.1. But.....	13
3.2. Introduction.....	13
3.3. Structure arborescente du DNS.....	13
3.4. Enregistrements DNS.....	14
3.5. Installation et configuration d'un serveur DNS sous Windows.....	15
3.6. Installation et configuration de BIND9, interaction avec DHCP.....	16
4. Services Web (http) et FTP.....	17
4.1. But.....	17
4.2. Introduction.....	17
4.3. Installation et configuration d'un serveur web/FTP.....	18
5. Administration des services réseau avec webmin	20
5.1. But.....	20
5.2. Introduction.....	20
5.3. Administration des services réseaux à partir du webmin.....	21
6. Installation d'un contrôleur de domaine Active Directory.....	23
6.1. But.....	23
6.2. Introduction.....	23
6.3. Contrôleur de domaine Active Directory	24
7. Service de messagerie	27
7.1. But.....	27
7.2. Introduction.....	27
Abréviations.....	27
7.3. Serveur de messagerie avec Postfix	28
8. Préparation de l'environnement d'administration.....	30
8.1. Installation et configuration de GNS3 sous MS Windows.....	30
8.1.1. Installation de GNS3.....	30
8.1.2. Configuration de GNS3	33
8.1.3. Présentation de l'interface graphique de GNS3	35
8.2. Installation et configuration de VMware sous MS Windows	36
8.3. Création d'une machine virtuelle sous VMware Workstation 11.....	40
8.4. Ajout d'une VM au GNS3	42
8.5. ajout d'une image IOS d'un routeur Cisco sous GNS3	43
9. Exercices	49
Références.....	51

FIGURES

Figure 1.1: Topologie de réseau local.....	8
Figure 1.2: Topologie de réseau local.....	9
Figure 2.1: Requête DHCP complète.....	11
Figure 2.2: Schéma du réseau « Serveur-DHCP ».....	12
Figure 3.1: Modèle hiérarchique de nom de domaine.....	14
Figure 3.2: Topologie du réseau DNS	15
Figure 3.3: topologie réseau pour BIND9.....	16
Figure 4.1: Principe de FTP	17
Figure 4.2: Principe de HTTP	18
Figure 4.3: Topologie réseau de TP4	18
Figure 4.4: Page web Default.htm	19
Figure 5.1: Interface web du webmin	20
Figure 5.2: topologie réseau pour webmin.....	21
Figure 6.1: structure d'une forêt	24
Figure 6.2: Topologie réseau du TP6.....	25
Figure 7.1: Structure d'un system de messagerie	28
Figure 7.2: topologie réseau pour le serveur de messagerie	28
Figure 8.1: Site Web pour télégérer GNS3	30
Figure 8.2: Création d'un nouveau compte sur le site GNS3	30
Figure 8.3: fenêtre de téléchargement de GNS3	31
Figure 8.4: Les fonctionnalités associées à GNS3.	31
Figure 8.5: Interface d'installation de WinPcap et de Npcap.	32
Figure 8.6: Fin d'installation de GNS3.....	32
Figure 8.7: Mode d'exécution de GNS3	33
Figure 8.8: Paramètres de serveur local	33
Figure 8.9: Connexion au serveur local	34
Figure 8.10: Fin de la configuration de GNS3.....	34
Figure 8.11: Interface graphique de GNS3.	35
Figure 8.12: Fenêtre d'installation de VMware.....	36
Figure 8.13: Agreement de VMware Workstation.....	37
Figure 8.14: Sélection de type d'installation	37
Figure 8.15: Chemin d'installation de VMware Workstation.	38
Figure 8.16: Processus d'installation de VMware	38
Figure 8.17: Clé d'activation de VMware Workstation 11.	39

Figure 8.18: Interface graphique de VMware.....	39
Figure 8.19: Chemin vers le fichier d'exécution de VMware	40
Figure 8.20: Fenêtre de création d'une nouvelle VM.....	40
Figure 8.21: Clé Windows 7 et location de la VM	41
Figure 8.22: Configuration de disque VMDK	41
Figure 8.23: Démarrage de l'installation de Windows 7 sur la VM.....	42
Figure 8.24: Ajout de la VM Windows 7 au GNS3.....	42
Figure 8.25: Paramètres de la VM Windows 7	43
Figure 8.26: Template de la VM Windows 7.....	43
Figure 8.27: Ajout de l'image iso d'un routeur.....	44
Figure 8.28: Cisco C7200-I/O-2FE/E 800-07114-06 7200 Input/Output	44
Figure 8.29: Image IOS de routeur c7200.....	44

ACRONYMES

ACRONYME	EXPLICATION
BIND	Berkeley Internet Name Domain
CIFS	Common Internet File System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GNS3	Graphical Network Simulator -3
HTTP	HyperText Transfer Protocol
IBM	International Business Machines
IIS	Internet Information Services
IMAP	Internet Message Access Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MTA	Mail Transfer Agents
MUA	Mail User Agent
NS	Name Server
OU	Organizational Unit
PC	Personal Computer
POP3	Post Office Protocol 3
RAM	Random Access Memory
SCP	Secure Copy Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SOA	Start of Authority
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TTL	Time To Live
URL	Uniform Resource Locator
VM	Virtual Machine
VMDK	Virtual Machine Disk

Unité d'enseignement : UEM 1.2
réseaux VHS : 22h30 (TP : 1h30)

Matière : TP Administration des services
Crédits :2, Coefficient : 1

TP 1 : Environnement d'administration

1. ENVIRONNEMENT D'ADMINISTRATION

1.1. BUT

À l'issue de ce TP, l'étudiant aura les outils et les compétences pour mettre en place un environnement d'administration des réseaux. Il sera aussi en mesure de créer et de configurer une topologie réseau avec un outil de simulation.

Objectifs spécifiques:

1. Installation et configuration de simulateur de réseau graphique GNS3 (Graphical Network Simulator -3) et de logiciel de virtualisation VMware.
2. Création et configuration d'un réseau local simple avec GNS3 et ajout d'une VM au réseau.
3. Vérification de la connectivité entre les différents nœuds du réseau grâce aux commandes suivantes : ping , tracepath et telnet.

1.2. INTRODUCTION

Les TP de ce module ne nous seront pas réalisés avec des équipements physiques (i.e. machines clientes, routeurs, switches, câbles RG45, etc.), mais « en dématérialisé » en raison du prix des équipements et de la complexité des configurations mises en jeu dans un réseau d'opérateur de l'Internet ISP (Internet Service Provider). Plus précisément, les TP seront réalisés dans un environnement de simulation ou d'émulation.

Un environnement de simulation peut être réalisé avec un outil, ou logiciel de simulation. Ce dernier est un ensemble de programmes reproduisant le système désiré, avec plus ou moins de simplification [1]. Cependant, un environnement d'émulation est généralement créé par un outil d'émulation. Avec cet outil, le vrai système est implémenté dans un environnement virtualisé, et non pas matériel. L'outil d'émulation que nous allons utiliser dans ces TP est GNS3.

1.3. GRAPHICAL NETWORK SIMULATOR-3 (GNS3)

GNS3¹ est un simulateur de réseau graphique libre (sous licence GPL), qui permet de réaliser des configurations réseau arbitraires tant que le matériel (hardware) des équipements réseau impliqués peut être supporté par GNS3 [1], [2]. Il est utilisé par les professionnels, notamment ISP (Internet Service Provider) pour le design de leurs réseaux . De plus, GNS3 peut être interfacé avec VirtualBox et VMware pour que de vraies machines puissent être incluses dans le réseau. Il peut également être relié à un réseau physique [2].

L'émulation de nœuds terminaux avec GNS3 nécessite l'utilisation de machines virtuelles. Dans ce contexte, il existe plusieurs outils permettant la création de machines virtuelles tels que Virtual box² et VMware³. En effet, l'association de ces outils et de GNS3 permettra la réalisation d'un réseau virtuel qui dispose de toute l'aptitude requise pour en situation de fonctionnement réel.

¹ <https://www.gns3.com/>

² <https://www.virtualbox.org/>

³ <https://www.vmware.com/>

1.4. CREATION ET CONFIGURATION D'UN RESEAU LOCAL SIMPLE AVEC GNS3

Pour prendre en main rapidement GNS3, nous allons créer la topologie réseau présentée dans la Figure 1.1. Le réseau est constitué d'un routeur Cisco (c7200), un commutateur (Ethernet Switch) et de 4 machines clientes (Direction, Secrétariat, Technique1 et Technique2). Ce réseau est connecté à Internet via le routeur.

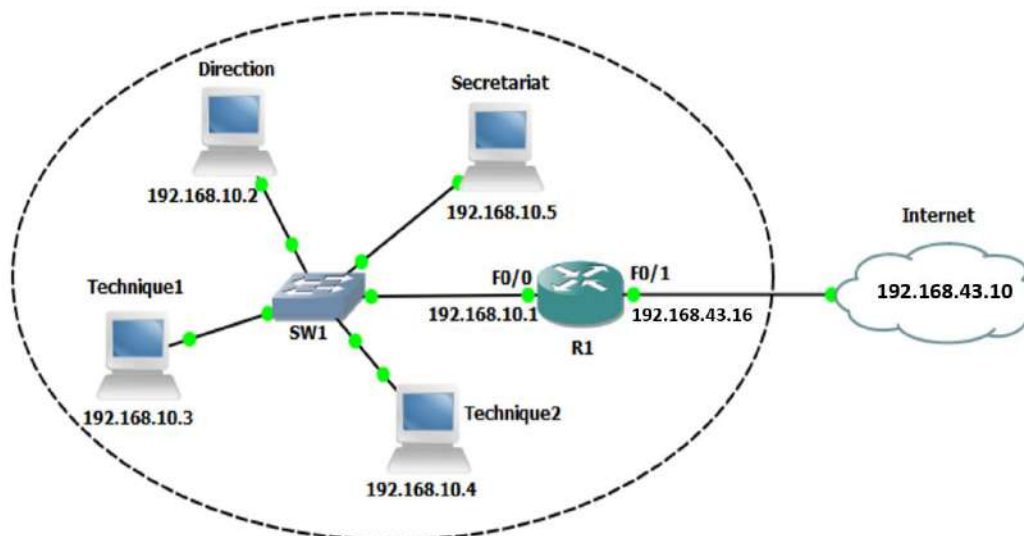


FIGURE 1.1: TOPOLOGIE DE RESEAU LOCAL

Travail demandé

Partie 01 : Création de la topologie de réseau local

1. Lancer GNS3 est réalisé la topologie réseau de la Figure 1.1
2. Renommez chaque équipement comme indiqué sur le schéma.
3. Configurer les cartes réseau des machines en indiquant l'adresse IP de chaque interface réseau et de routeur comme montré sur le schéma.
4. Créer une connexion à Internet via le retour, puis tester la connexion à Internet à partir de la machine « Direction ».
5. Tentez de vous connecter depuis la machine Technique1 vers la machine « Secrétariat » en utilisant la commande « *tracert* ».
6. Tester les connexions entre les différentes machines en utilisant la commande « *Ping* ».

Partie 02 : Utilisation des machines virtuelles dans GNS3

1. Créer une nouvelle machine virtuelle VMware, puis démarrer la machine virtuelle et installer Windows 7 à partir de l'image iso de ce dernier.
2. Ajouter la machine virtuelle à la topologie précédente.
3. Connecter la machine au « SW1 »
4. Configurer une adresse IP fixe (192.168.10.7) à votre machine ainsi qu'un nom de machine (win7).
5. Tester la connexion aux autres nœuds depuis cette machine.

Software nécessaire pour réaliser ce TP : GNS3, VMware Workstation

EXERCICE

Soit la topologie réseau suivante :

1. Proposez un plan d'adressage pour cette topologie
2. Créer la topologie avec GNS3.
3. Tester la connexion entre les différents nœuds du réseau en utilisant les commandes ping, tracepath et telnet

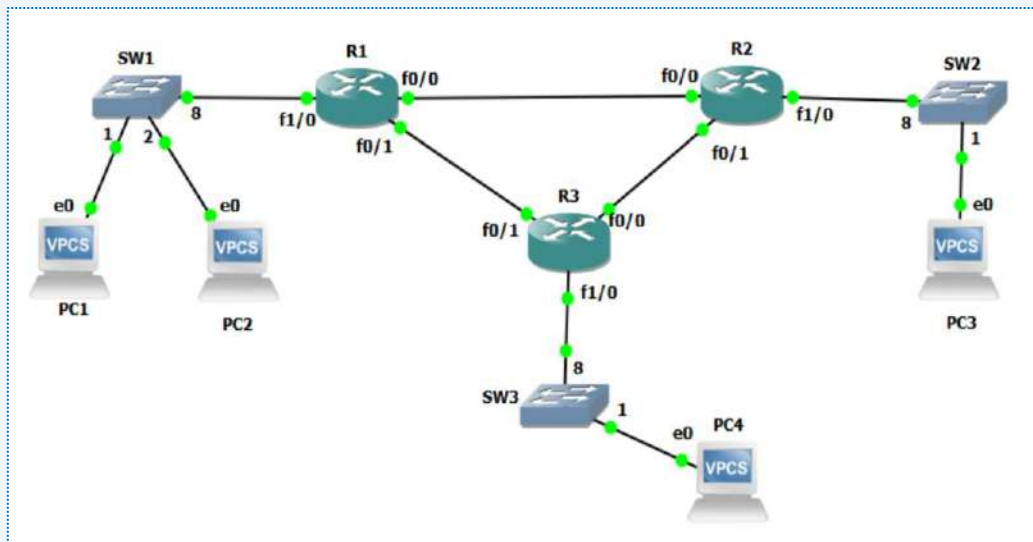


FIGURE 1.2: TOPOLOGIE DE RESEAU LOCAL

REMARQUE : ME RENDRE SUR PAPIER OU ELECTRONIQUE (RAPPORT) LA DEMARCHE DOCUMENTEE DE CE QUE VOUS AVEZ FAIT.

TP 2 : Service DHCP

2. SERVICE DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

2.1. BUT

À l'issue de ce TP, l'étudiant sera capable de mettre en place un service DHCP (Configuration de DHCP, Gestion d'un bail limité en environnement hétérogène, Réservation d'adresses (@mac). Il sera aussi capable de paramétrer un serveur DHCP.

Objectives spécifiques

1. Configuration d'un serveur DHCP sur un routeur Cisco
2. Configuration du relais DHCP

2.2. INTRODUCTION

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole fonctionnant en mode client/serveur. Il permet à un hôte d'obtenir automatiquement une adresse IP lorsqu'il se connecte au réseau. Le serveur DHCP peut fournir principalement une adresse IP, un masque de sous réseau, l'adresse IP de la passerelle par défaut, l'adresse IP du serveur DNS (Domain Name System) et d'autres informations [3]. Le but principal étant la simplification de l'administration d'un réseau.

Le DHCP fonctionne sur un principe de location ou « **bail** ». C'est-à-dire, le serveur attribue une adresse à un client pour une durée prédéterminée en jours, minutes et secondes. Le client doit donc effectuer à nouveau une demande pour voir son bail reconduit [4]. L'attribution de l'adresse IP peut être effectuée selon trois méthodes : automatique, dynamique ou manuelle [4]:

- **Automatique** : l'attribution est effectuée avec un mapping statique (@MAC ↔ @IP). Dans ce cas, la machine préserve la même adresse lors d'une déconnexion / reconnexion (e.g. serveur).
- **Dynamique** : l'attribution est effectuée à la volée. Une IP libre est attribuée à un client en faisant la demande, pour une durée déterminée.
- **Manuelle** : l'attribution est effectuée manuellement par l'administrateur réseau (mappage statique). Le protocole DHCP se charge d'envoyer ces informations au client lors d'une demande.

Comme le montre la Figure 2.1, lorsqu'un client DHCP initialise un accès à un réseau TCP/IP, le processus d'obtention d'une adresse IP est composé de 4 phases [3]. Ces phases sont :

1. **Demande de bail IP** : le client émet une requête de demande de bail IP (DHCPDISCOVER) qui est envoyé sous forme d'une diffusion sur le réseau avec adresse IP source (0.0.0.0), adresse IP destination (255.255.255.255) et adresse MAC.
2. **Proposition de bail IP** : le serveur DHCP répond en proposant une adresse IP avec une durée de bail et l'adresse IP du serveur DHCP (DHCPOFFER).
3. **Sélection de bail IP** : le client sélectionne la première adresse IP (s'il y a plusieurs serveurs DHCP) reçue et envoie une demande d'utilisation de cette adresse au serveur DHCP (DHCPREQUEST). Son message envoyé par diffusion comporte l'identification du serveur sélectionné qui est informé que son offre a été retenue ; tous les autres serveurs DHCP retirent leur offre et les adresses proposées redeviennent disponibles.

4. **Accusé de réception du bail IP** : le serveur DHCP accuse réception de la demande et accorde l'adresse en bail (DHCPACK), les autres serveurs retirent leur proposition.

Enfin le client utilise l'adresse pour se connecter au réseau. Pour les réseaux de petite taille, les services DHCP peuvent être fournis par un petit routeur. Cela concerne de nombreux réseaux domestiques équipés de connexions DSL, par câble ou sans fil.

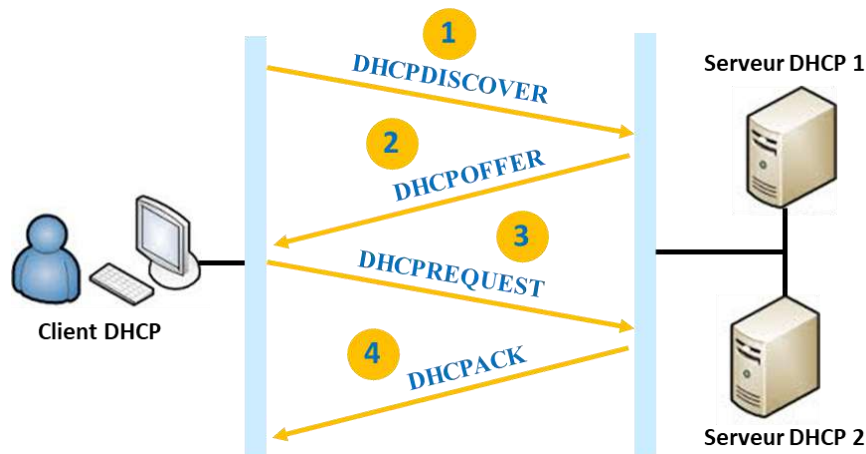


FIGURE 2.1: REQUETE DHCP COMPLETE

Client DHCP : n'importe quel équipement se connecter sur un réseau filaire ou en Wi-Fi. Exemples : ordinateurs, smartphones, tablettes, serveurs, TV connectée, etc.

Serveur DHCP : il existe de nombreuses solutions logicielles pour créer un serveur DHCP. Exemples : le rôle DHCP sous Windows server, sous linux (paquet : isc-dhcp-server-server), à l'aide d'un retour, d'un per-feu, etc.

Étendue DHCP : sur un réseau où l'on trouve plusieurs réseaux différents, que ce soit des réseaux physiques (LANs) ou logiques (VLANs), le serveur DHCP doit gérer les pools d'adresses IP à distribuer pour chaque réseau. C'est ce que l'on appelle étendue.

Réservation : une adresse IP réservée dans un serveur DHCP ne pourra pas être distribuée, sauf à l'équipement pour lequel elle est destinée. Par exemple, une imprimante, un serveur DNS, etc. Cette association se fait grâce à l'adresse **MAC de l'équipement**.

Relais DHCP : les requêtes clientes sont envoyées au serveur DHCP en broadcast. Cela signifie que ces broadcasts ne dépassent pas les routeurs (i.e. un routeur segmentant le réseau arrêtera le broadcast). Il est possible d'éviter ce problème par la configuration de la passerelle du routeur (**ip helper-address**) [3].

```
R1(config)# interface [passerelle]
R1(config-if)# ip helper-address [ip serveur DHCP].
```

Les serveurs DHCP sont généralement gérés par des serveurs d'entreprise (service généralement assuré par l'OS), mais ils peuvent également être configurés sur les routeurs.

2.3. SERVICE DHCP SUR UN ROUTEUR CISCO

Un routeur peut agir comme un serveur DHCP. Il attribue et gère les adresses IP en fonction du ou des pools d'adresses spécifiées par l'administrateur réseau. Un pool DHCP (étendu) est caractérisé par l'identificateur de réseau, le masque de sous réseau, la plage d'adresses IP de réseau, la durée du bail, l'adresse de (passerelle), le nom de l'étendue (pool DHCP) et la plage d'exclusion.

Nous allons donc essayer de configurer un serveur DHCP sur le routeur Cisco c7200 R1 en se base sur la topologie réseau de la Figure 2.2.

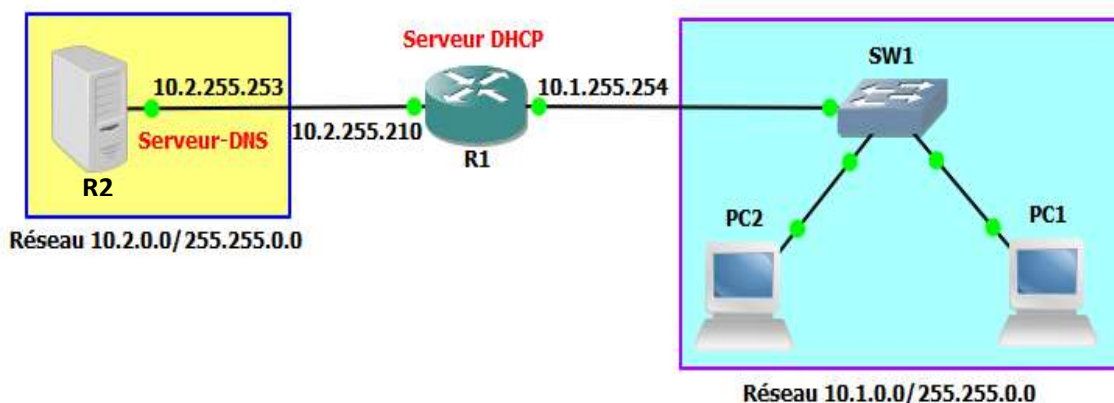


FIGURE 2.2: SCHEMA DU RESEAU « SERVEUR-DHCP ».

Travail Demandé

1. Lancer GNS3 et installez un réseau similaire à celui du schéma 01 «Serveur-DHCP».
2. Avant de configurer le serveur DHCP, il va d'abord être nécessaire de préparer le serveur DNS Maître (ou premier serveur DNS) pour permettre au serveur DHCP de mettre à jour dynamiquement la zone zarzara.com. Configurer la zone DNS zarzara.com sur le routeur « R2 » selon les paramètres suivants :
 - Nom de domaine : *zarzara.com*
 - Nom de serveur DNS : *ns1.zarzara.com*
 - E-mail de l'administrateur : *koko.zarzara.com*
3. Créer un enregistrement pour le serveur DNS ns « ip host zarzara.com ns 10.1.255.253 ». (*L'enregistrement de serveur de noms (Name Server ou NS) annonce les serveurs de noms faisant autorité pour une zone*)
4. Créer des enregistrements pour les autres nœuds du réseau.
5. Configurez le routeur **Cisco c7200** (R1→ serveur-DHCP) selon les paramètres suivants et enregistrez les configurations.
 - Le nom de l'étendue (pool DHCP) : *campus*
 - Le réseau à écouter + masque : *10.1.0.0 /255.255.0.0*
 - La passerelle par défaut : *10.1.255.254*
 - La plage d'exclusion : *adresse de la passerelle et du serveur DNS*
 - La durée du bail : *5 jours*
 - Le nom du domaine : *zarzara.edu*
 - L'adresse de serveur DNS : *10.1.255.253/16*
6. Tester la configuration de serveur DHCP et indiquer l'adresse IP affectée à chaque PC?
7. Créer une réservation (attribuer une adresse IP donnée à l'adresse MAC de PC1)

Remarque : par défaut, le service DHCP est activé sur le routeur. Pour désactiver le service utiliser la commande « *no service dhcp* ».

Unité d'enseignement : UEM 1.2
réseaux VHS : 22h30 (TP : 1h30)

Matière : TP Administration des services
Crédits :2, Coefficient : 1

TP 3 : Service DNS

3. SERVICE DNS (DOMAIN NAME SYSTEM)

3.1. BUT

À l'issue de ce TP, l'étudiant sera capable d'installer et configurer un service DNS (Notions de root-server, TLD, zone, enregistrement, Format des articles et fichiers de configuration, Notion de DNS dynamique, Interaction avec DHCP.

Objectives spécifiques

1. Installation et configuration d'un serveur DNS sous Windows.
2. Installation et configuration d'un serveur DNS BIND9
3. Interaction avec un serveur DHCP.

3.2. INTRODUCTION

Le système DNS (Domain Name System) prend en charge l'établissement de la correspondance entre un nom pleinement qualifié (ou FQDN) et une adresse IP. Il permet à des hôtes du réseau de soumettre des requêtes à un serveur DNS afin d'obtenir l'adresse IP d'un hôte connaissant le nom de cet hôte [5]. Par exemple, `www.google.com` ↔ `209.85.229.99`. Cette traduction des noms aux adresses IP doit toujours être réalisée puisque seule l'adresse IP permet de communiquer sur le réseau.

Le premier mécanisme de résolution de noms mis en place sous Windows est NetBIOS (*NetBIOS Extended User Interface*), un protocole créé par IBM dans les années 80. Cette méthode de résolution de noms a de nombreux inconvénients. C'est pourquoi sous Windows 2000/2003/XP le nouveau système de résolution de noms DNS a été adopté. Il corrige les inconvénients du protocole NetBIOS.

Bind (Berkeley Internet Name Domain) est le serveur DNS le plus utilisé sur Internet, spécialement sur les systèmes du type UNIX. Ce dernier permet d'associer des noms d'hôtes d'un réseau à des adresses numériques et vice-versa [6], [7]. Actuellement, ce logiciel gère la plupart des noms de domaines sur Internet. Il existe des alternatives à BIND, comme DJBdns⁴ ou MaraDNS⁵, qui sont souvent réputés plus sécurisés, mais ils sont encore beaucoup moins utilisés.

3.3. STRUCTURE ARBORESCENTE DU DNS

Comme l'illustre la Figure 3.1, le DNS possède un modèle hiérarchique dont le sommet est appelé **Domaines racines (root)**. On représente ce dernier par un point «.» qui sépare les niveaux hiérarchiques du domaine. Il y a apparemment 13 serveurs racine du DNS dont les noms sont de la forme *lettre.root-servers.net* (A.root-servers.net, ..., M.root-servers.net, ...) [6].

Les domaines se trouvant immédiatement sous la racine sont appelés **domaine de premier niveau (TLD : Top Level Domain)**. Il existe deux catégories de TLD :

1. **Générique** : les domaines génériques, aussi appelés **gTLD** (pour generic TLD), sont des noms de domaines génériques de niveau supérieur proposant une classification selon le secteur d'activité, par exemple «.org», «.edu», «.net», «.gov» où «.com».

⁴ <https://cr.yp.to/djbdns.html>

⁵ <https://maradns.samiam.org/>

2. **Nationaux** : les domaines nationaux, aussi appelés **ccTLD** (pour **country code TLD**), correspondent aux différents pays et leurs noms correspondent aux abréviations des noms de pays définies par la norme **ISO 3166**, par exemple **dz (Algeria)**, **it (Italy)**, **uk (United Kingdom, etc.**

L'extrémité d'une branche est appelée **hôte**, et correspond à une machine ou une entité du réseau (e.g. un ordinateur, une imprimante ou bien encore un routeur). Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine. À titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom **www**.

Nom de domaine : on appelle nom de domaine chaque nœud de l'arbre (voir Figure 3.1). Chaque nœud possède une étiquette (en anglais « label ») d'une longueur maximale de 63 caractères.

FQDN : le nom de domaine pleinement qualifié ou FQDN (Fully Qualified Domain Name) est composé de deux parties : les noms d'hôte et le suffixe DNS. Par exemples, www.admin.uk, mail.admin.uk.

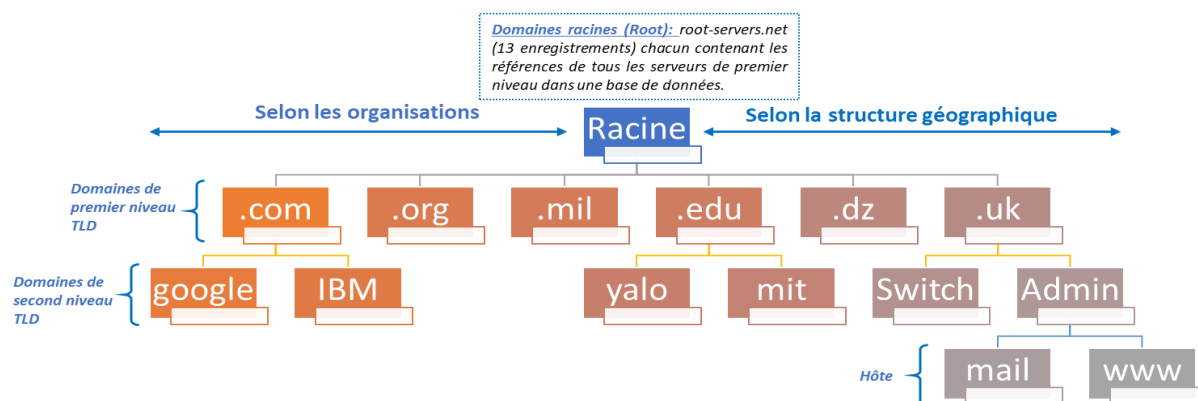


FIGURE 3.1: MODELE HIERARCHIQUE DE NOM DE DOMAINE

Serveur de noms primaire et secondaire : chaque domaine possède un serveur de noms de domaines, appelé serveur de noms primaire (*Primary domain name server*), ainsi qu'un serveur de noms secondaire (*Secondary domain name server*), permettant de prendre le relais du serveur de noms primaire en cas d'indisponibilité [7].

3.4. ENREGISTREMENTS DNS

Enregistrements DNS : est une base de données répartie contenant des enregistrements, appelés RR (Resource Records), concernant les noms de domaines. Seuls les administrateurs de la gestion de domaine peuvent lire les informations de ces enregistrements. En effet, le fonctionnement des serveurs de noms étant totalement transparent pour les utilisateurs. D'une manière générale, un enregistrement DNS comporte les informations suivantes [7]:

- Nom de domaine (FQDN) : exemple, www.admin.uk
- TTL (Time To Live) : 36000 seconds.
- Type : exemple, **SOA**
- Classe : IN
- RData : exemple, 136.5.255.85

Il existe plusieurs types d'enregistrements DNS comme par exemple :

- *SOA (Start Of Authority)* : permet de définir le serveur maître du domaine.
- *NS (Name Server)* : indique quel nom de serveur a autorité sur le domaine.
- *MX (Exchanger Record)* : gère la liste des serveurs de messageries,
- *A (Address)* : gère la liste des adresses IP (IPv4) des hôtes, et AAAA (IPv6)
- *CNAME (canonical name)*: abréviation de canonique. Elle permet de réaliser un alias (un raccourci) d'un hôte vers un autre.

TTL (Time To Live) - En général cette valeur est associée à un nombre, Exemple 86400. Ce dernier est en secondes ce qui fait 24 heures. Au bout de ces 24 heures le cache du serveur sera réinitialisé.

Zone DNS : une zone DNS se réfère à l'espace administratif dans le DNS. C'est un fichier où se trouvent les enregistrements d'un domaine. Les enregistrements sont les liens entre les adresses IP et les noms, cela sert donc à la résolution de nom. **Les fichiers de zone** sont gérés sur des serveurs DNS [7].

Un serveur DNS peut être configuré pour héberger zéro, une ou plusieurs zones. Chaque zone peut faire autorité pour un ou plusieurs domaines DNS, à condition que ces domaines soient contigus dans l'arborescence DNS. Le fonctionnement normal des serveurs DNS fait intervenir trois zones [8]:

- **Zone principale :** contient une version en lecture - écriture du fichier de zone. Toute modification apportée à la zone est consignée dans ce fichier. Elle doit être créée à chaque fois qu'une nouvelle zone est créée.
- **Zone secondaire :** contient une version en lecture seule du fichier de zone. Toute modification apportée à la zone est consignée dans le fichier de zone principale puis dupliquée dans le fichier de zone secondaire. On doit promouvoir une zone principale avant de créer des zones secondaires.
- **Zone de stub :** cette zone ne contient que les enregistrements nécessaires permettant d'identifier les serveurs. Elle contient les enregistrements du type SOA, NS et A. Elle permet de retourner les adresses des serveurs DNS d'une zone DNS lors de recherches du type itératif entre serveurs DNS.

3.5. INSTALLATION ET CONFIGURATION D'UN SERVEUR DNS SOUS WINDOWS

Dans cette partie de TP, nous allons essayer d'installer et configurer un serveur DNS sous Windows. Pour ce faire, nous allons utiliser la topologie réseau suivante:

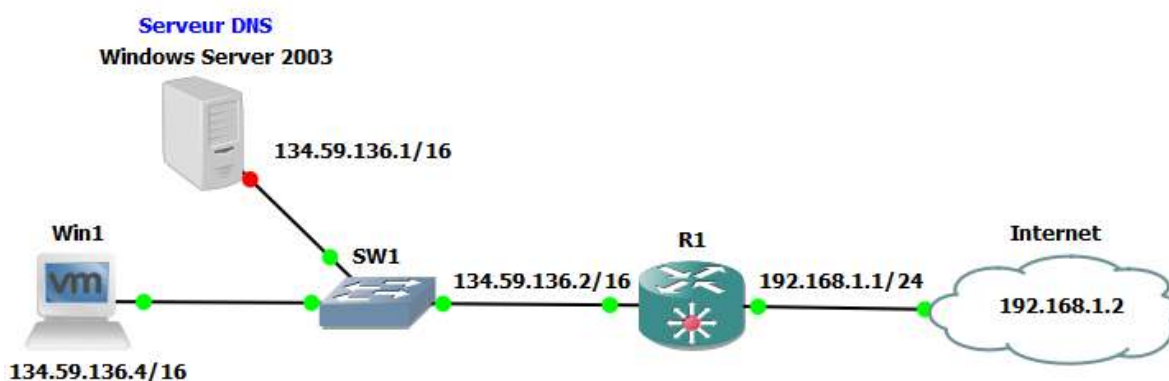


FIGURE 3.2: TOPOLOGIE DU RESEAU DNS

Travail demandé

1. Créer une nouvelle machine virtuelle VMware, puis démarrer la machine virtuelle et installer Windows 2003 server à partir de l'image iso de ce dernier.
2. Créer une autre machine virtuelle VMware, puis démarrer la machine virtuelle et installer Windows 7 à partir de l'image iso de ce dernier.
3. Lancer GNS3 est réalisé la topologie réseau de la Figure 3.2 en ajoutant les deux machines virtuelles précédentes.
4. Configurer une adresse IP fixe à votre serveur ainsi qu'un nom de machine.
 - Serveur DNS : nom → umc, adresse IP → 137.59.136.1/16
 - Machine cliente : nom → win7, adresse IP → 137.59.136.4/16

5. Installer un serveur DNS sur votre serveur, puis vérifier dans le "Server Manager" que le rôle DNS a bien été ajouté.
6. Configurer votre serveur DNS selon les paramètres suivants :
 - Type de serveur : primaire.
 - Nom de domaine : zarzara.edu
 - Nom de fichier de configuration de votre serveur DNS : zarzara.edu.umc
 - Les adresses des DNS public sur lesquels notre serveur ira chercher les noms de site internet sont les célèbres serveurs DNS de google **8.8.8.8** et **8.8.4.4**.
7. Créer une zone primaire sur votre serveur et une zone de recherche inversée.
8. Ajouter manuellement la machine virtuelle win1 a votre zone, puis tester le fonctionnement de votre serveur DNS en utilisant la commande **nslookup**.
9. Ajouter manuellement le routeur « R1 » à votre zone et configurer ce dernier comme client DNS, puis faire un ping sur le nom de serveur (umc.zarzara.edu).

3.6. INSTALLATION ET CONFIGURATION DE BIND9, INTERACTION AVEC DHCP

Dans cette partie de TP, nous allons essayer d'installer et de configurer un serveur DNS « Bind » sous linux et les mises à jour dynamiques du DNS par le DHCP. Pour ce faire, nous allons utiliser la topologie réseau suivante :

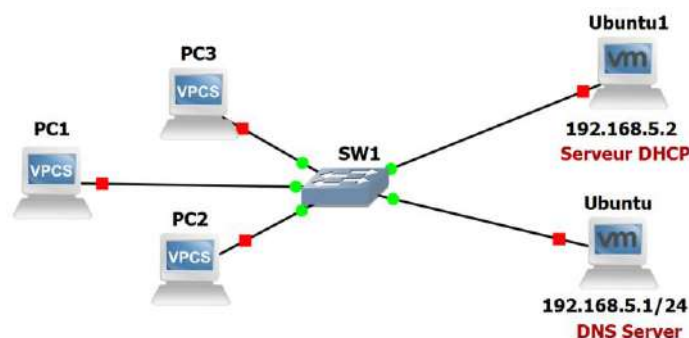


FIGURE 3.3: TOPOLOGIE RESEAU POUR BIND9

1. Créer une machine virtuelle linux (Ubuntu 14.04.5 LTS (Trusty Tahr)), clone la VM, puis créer la topologie de la Figure 3.3 en utilisant GNS3.
2. Utiliser un serveur DHCP pour l'adressage automatique des nœuds du réseau.
3. Installer le serveur DNS Bind9 (apt-get install bind9). Puis, allez dans le dossier de "Bind" et configurer le serveur DNS pour qu'il "écoute" sur toutes les adresses IP (réseau local où Internet).
4. Créer une zone de recherche directe (Elle traduit le nom de domaine en adresses IP).
5. Créer une zone de recherche inverse (Elle traduit les adresses IP en nom de domaine).
6. Vérifier la configuration de base de BIND, en utilisant la commande suivante (named-checkconf -z).
7. Rechargez la configuration de BIND pour sauvegarder les changements de votre serveur DNS (service bind9 reload).
8. Tester le serveur DNS pour être sûr qu'il fonctionne correctement en utilisant la commande **"nslookup"**

REMARQUE : ME RENDRE SUR PAPIER OU ELECTRONIQUE (RAPPORT) LA DEMARCHE DOCUMENTEE DE CE QUE VOUS AVEZ FAIT.

TP 4 : Services Web (http) et FTP

4. SERVICES WEB (HTTP) ET FTP

4.1. BUT

A l'issue de ce TP, l'étudiant aura les outils et les compétences pour mettre en place un serveur Web ou un serveur FTP. Il sera aussi capable d'utiliser et de configurer les outils disponibles pour utiliser les services web et ftp.

Objectives spécifiques

1. Installation et Configuration d'un serveur web et un serveur ftp,
2. Présentation des technologies coté client et coté serveur
3. Mettre à disposition d'une application web et d'une application ftp

4.2. INTRODUCTION

Un serveur FTP utilise le protocole de transfert de fichier FTP (File Transfer Protocol) pour l'échange de fichiers de tous types (texte, images, sons, logiciels, etc.) avec un client FTP situé sur une machine distante au travers les ports 20 (données) et 21 (commandes). La version sécurisée du FTP (FTPS) est accessible au travers du port 990. La numérotation des ports est une pure convention, elle peut varier selon les choix de l'administrateur système [9].

« Filezilla server » est un exemple de serveur FTP open-source. Il est très puissant, pratique et fonctionne à merveille avec un « client Filezilla ». Il y a aussi Cyberduck, Transmit, Cute FTP, LeechFTP, FireFTP, etc.

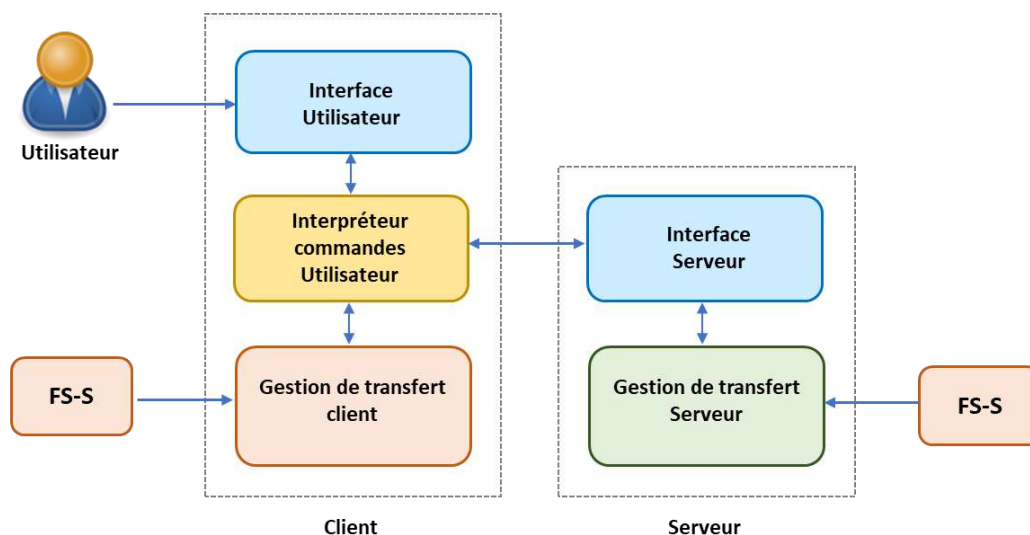


FIGURE 4.1: PRINCIPE DE FTP

Un serveur Web (également appelé « **Serveur http** ») utilise le protocole HTTP (HyperText Transfer Protocol) pour fournir les fichiers qui constituent les pages Web que les utilisateurs ont demandées via des requêtes transmises par les clients HTTP de leurs ordinateurs tels que Internet Explorer, Mozilla, google chrome, etc [8].

IIS (Internet Information Services) est un exemple de serveur web (FTP, SMTP, HTTP etc.) des différents systèmes d'exploitation Windows NT. Il y a aussi Apache HTTP server, Oracle Java System Web Server, Zeus Web Server, etc [8].

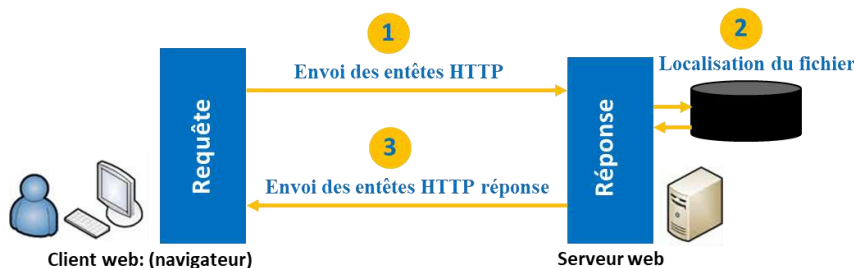


FIGURE 4.2: PRINCIPE DE HTTP

4.3. INSTALLATION ET CONFIGURATION D'UN SERVEUR WEB/FTP

Pour réaliser ce TP, nous allons créer la topologie réseau présentée dans la Figure 4.3. Le réseau est constitué d'un routeur Cisco (c7200), un commutateur (Ethernet Switch) et de deux machines virtuelles, un serveur Windows 2003 qui nous servira de **serveur FTP et Web**, et une machine cliente sous **Windows 7**. Ce réseau est connecté à Internet via le routeur « R1 ».

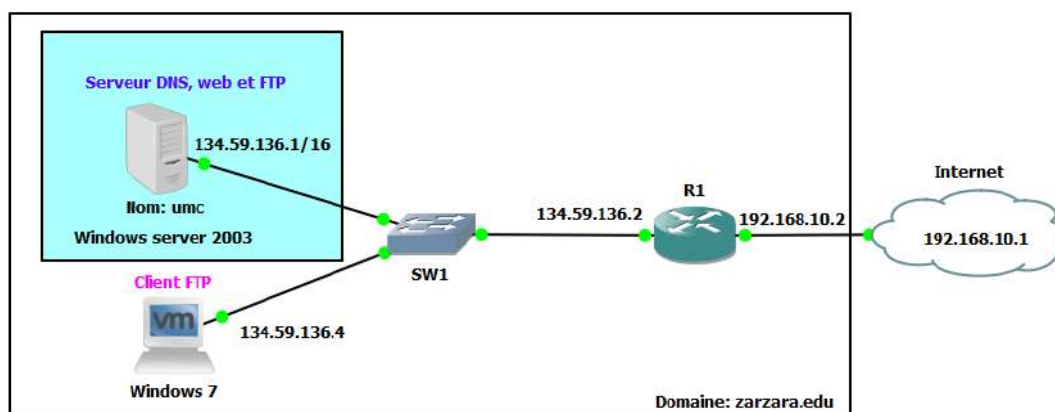


FIGURE 4.3: TOPOLOGIE RESEAU DE TP4

Travail demandé

1. Créer une VM (Windows 7) et une autre VM (Windows server 2003) avec le logiciel de virtualisation VMware.
2. Créer la topologie réseau de la Figure 4.3 en utilisant GNS3.
3. Tester les connexions entre les deux machines et le routeur en utilisant la commande ping

Partie 01 : Serveur Web/FTP sous Windows

1. Installer et configurer le serveur web **IIS** (Internet Information Services) de serveur « Windows Server 2003 » pour fonctionner comme serveur FTP et serveur Web.
2. Créer et configurer un Serveur FTP avec les paramètres suivant :
 - Répertoire de base : *C:\Inetpub\ftproot\Direction*
 - Autorisations : *Lecture et Ecriture*
 - Adresse IP : *134.59.136.1*
 - Port : *21*
 - Sécurité : *Autorisé les connexions anonymes*
3. Tester le serveur FTP localement avec la commande « ftp Localhost », puis, à partir de la machine cliente « Windows 7 », tester une connexion anonyme sur le serveur FTP à l'aide d'Internet Explorer en donnant l'URL correspondant.

4. Crée un nouveau site web avec les paramètres suivants:
 - Répertoire de base : C:\Inetpub\wwwroot\site2
 - Autorisations : *Lecture et Ecriture*
 - Adresse IP : *134.59.136.1*
 - Port : 80
 - Documents par défaut (Page d'index) : Default.htm (Figure 4.4)



FIGURE 4.4: PAGE WEB DEFAULT.HTM

5. Tester la connexion à votre site web à partir du navigateur Web de la VM « Windows 7 ».
6. Créer un répertoire virtuel sur votre site Web avec l'option de partage Web selon les paramètres suivants :
 - Alias du répertoire virtuel : *Mon-virtuel-site*
 - Répertoire de contenu : *Rep-virtuel*
 - Autorisations d'accès : *Lecture et Ecriture*
7. Créer un répertoire virtuel sur votre site FTP selon les paramètres suivants :
 - Alias du répertoire virtuel : *Mon-virtuel-site*
 - Répertoire de contenu : *Rep-virtuel*
 - Autorisations d'accès : *Lecture et Ecriture*
8. Tester la connexion aux répertoires virtuels depuis le navigateur de la machine cliente « Windows 7 » et indiquer les principaux avantages de l'utilisation des répertoires virtuels.

Partie 2 : Serveur FTP avec Filezilla

1. Installer et de configurer un serveur FTP avec Filezilla.
 2. Utiliser un client Filezilla pour connecter au serveur FTP et uploadé certains fichiers.
- Pour réaliser cette partie de TP, utiliser deux VMs (Windows 7).

Dans ce TP, nous allons utiliser comme outils :

- **WinSCP** : Pour faire des transferts de fichiers vers le serveur.
- **Notepad++** : éditeur de textes orienté pour le développement web.
- **Putty** : Un client SSH pour une connexion sécurisée vers le serveur,
- **Filezilla** (*Server et client*)

REMARQUE : ME RENDRE SUR PAPIER OU ELECTRONIQUE (RAPPORT) LA DEMARCHE DOCUMENTEE DE CE QUE VOUS AVEZ FAIT DANS LA PARTIE 2.

Unité d'enseignement : UEM 1.2
réseaux VHS : 22h30 (TP : 1h30)

Matière : TP Administration des services
Crédits :2, Coefficient : 1

TP 5 : Administration à distance

5. ADMINISTRATION DES SERVICES RESEAU AVEC WEBMIN

5.1. BUT

A l'issue de ce TP, l'étudiant sera capable d'utiliser l'interface d'administration **webmin** (SSH, Telnet) pour l'administration des services réseaux à distance. En particulier, les services DNS (BIND9), open SSH, Apach, SQL server et SAMBA.

Objectives spécifiques

1. Installation et configuration de l'outil graphique webmin
2. Administration des services réseaux à partir du webmin
3. Test et évaluation



5.2. INTRODUCTION

Webmin⁶, dont le nom vient de la contraction Web et Admin, est un outil d'administration open source (licence BSD) basé sur une interface Web pour les serveurs Unix/Linux. Il est très puissant, et également très simple à utiliser. A travers une connexion sécurisée, il peut être utilisé pour administrer de façon sûre la plupart des services réseau (e.g. DHCP Apache, Postfix, Sendmail, FTP, MySQL, PostgreSQL, Samba, SSH, DNS (BIND), etc.) depuis n'importe quel poste sur le réseau.

Webmin est disponible pour les différentes distributions linux tels que Redhat, Fedora, CentOS, SuSE, Debian, Ubuntu, Gentoo, etc.

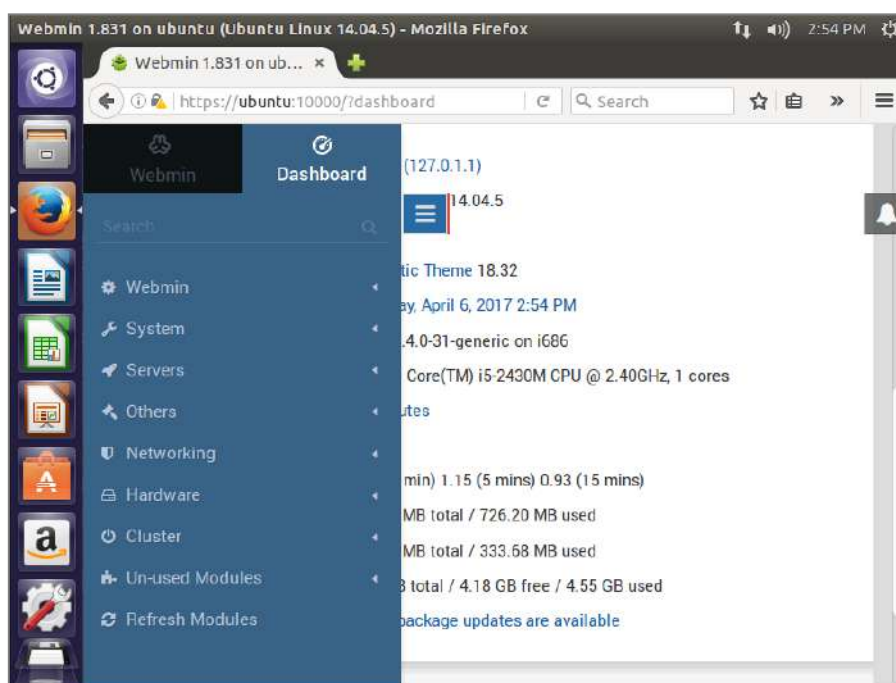


FIGURE 5.1: INTERFACE WEB DU WEBMIN

⁶ <https://www.webmin.com/>

5.3. ADMINISTRATION DES SERVICES RESEAUX A PARTIR DU WEBMIN

Dans ce TP Nous allons intéressés par le service web apache, service de résolution des noms DNS (BIND), Samba et les services de connexion à distance telnet et ssh. Pour réaliser ce TP nous aurons besoin d'utiliser trois machines virtuelles (Figure 5.2). Machine serveur sous Ubuntu 14.04.5-desktop-i386 (Adresse IP : 134.59.136.1), et deux machines cliente, Client 1 sous Ubuntu 14.04 (Adresse IP : 134.59.136.2) et Client 2 sous Windows 7 (Adresse IP : 134.59.136.3).

Webmin utilise le port **10000**.

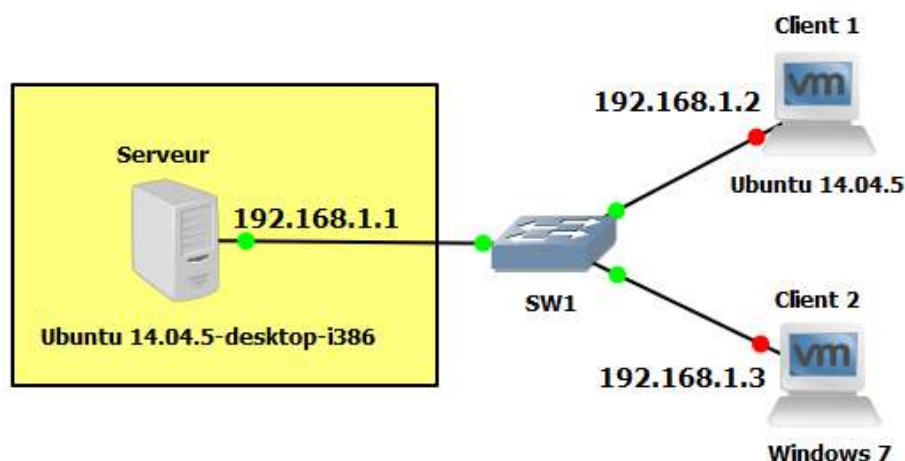


FIGURE 5.2: TOPOLOGIE RESEAU POUR WEBMIN

Travail demandé

1. Créer la topologie réseau de la Figure 5.2 en utilisant GNS3, puis tester les connexions entre les machines virtuelles en utilisant la commande ping.
2. Installer les paquets nécessaires à l'interface d'administration Webmin sur la machine serveur (Ubuntu 14.04.5). Puis tester la connexion à Webmin en utilisant l'URL **<https://ubuntu:10000/>** ou **<https://localhost:10000/>**.
3. Installer les paquets nécessaires de serveur Bind sur la machine serveur (Ubuntu 14.04.5), puis procéder à la configuration de ce dernier en utilisant l'outil Webmin selon les paramètres suivants : (Commande d'installation : **apt-get install bind9**).

1- Zone principale	
Nom de domaine	zarzara.edu
Fichier d'enregistrement	Automatique
Serveur primaire	umc. zarzara.edu
Adresse électronique	admin@ zarzara.edu
Adresse	134.59.136.1
2- Enregistrements Adresse (serveur, client 1 et client2)	
Noms	umc. zarzara.edu (serveur) client-1. zarzara.edu (Client 1) client-2. zarzara.edu (Client 2)
Adresses IP	134.59.136.1 (serveur) 134.59.136.2 (Client 1) 134.59.136.3 (Client 2)
Mettre à jour l'adresse inverse	Oui
3- De la même manière, créer la zone Inverse	

4. Installer les paquets nécessaires au serveur OpenSSH sur la machine serveur (Ubuntu 14.04.5), puis procéder à la configuration de ce dernier en utilisant l'outil Webmin (Commande d'installation : *apt-get install ssh*).

Contrôle d'accès (autorisés)	<i>Serveur et client 1</i>
Contrôle d'accès (Refusé)	<i>Client 2</i>
Port (par défaut)	22
Connexion	Par mot de passe

5. Installer les paquets nécessaires au serveur web (apache) sur la machine serveur (Ubuntu 14.04.5), puis procéder à la configuration de ce dernier en utilisant l'outil Webmin (Commande d'installation : *apt-get install apache2*).

Créer et configurer un "Serveur Virtuel" ou hôte virtuel avec les paramètres suivants :

Document racine	<i>/var/www/</i>
Port	<i>Par défaut</i>
Options du serveur virtuel	
E-mail du responsable	<i>Votre @ Electronique</i>
Nom d'hôte du serveur	<i>Automatique</i>
Page par défaut	<i>index.htm</i>

6. Installer les paquets nécessaires au serveur Telnet sur la machine serveur (Ubuntu 14.04.5), puis procéder à la configuration de ce dernier en utilisant l'outil Webmin.
- Quel est l'intérêt de SSH par rapport à Telnet ?
 - Tester la console avec : Telnet 127.0.0.1.
 - Etablir une connexion Telnet à la machine Client 1.

7. Installer les paquets nécessaires au serveur Samba server sur la machine serveur (Ubuntu 14.04.5), puis procéder à la configuration de ce dernier en utilisant l'outil Webmin.

Partager le dossier **/home** avec les machines clientes avec le nom de partage : **mon-dossier** et avec les permissions : **777**.

8. Installer les paquets nécessaires au serveur MySQL server sur la machine serveur (Ubuntu 14.04.5), puis procéder à la configuration de ce dernier en utilisant l'outil Webmin.

Créer une nouvelle base de données avec les options suivantes :

Nom de la base	<i>fstech</i>
Set caracteres	<i>Utf8 (UTF-8-Unicode)</i>
Table 1	<i>Client 1</i>

Les champs

Field name	Data type	Type width	Key?	Auto-increment?	Allow nulls?	Unsigned?	Default value
num	int		<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	
Designation	char	50	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	
adresse	char	15	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	
			<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Yes	

Remarque : me rendre sur papier ou électronique (Rapport) la démarche documentée de ce que vous avez fait dans les questions 7 et 8.

Unité d'enseignement : UEM 1.2
réseaux VHS : 22h30 (TP : 1h30)

Matière : TP Administration des services
Crédits :2, Coefficient : 1

TP 6 : Installation d'un contrôleur de domaine Active Directory

6. INSTALLATION D'UN CONTROLEUR DE DOMAINE ACTIVE DIRECTORY

6.1. BUT

A l'issue de ce TP, l'étudiant sera capable d'effectuer les tâches suivantes :

- Installation et configuration du contrôleur de domaine
- Tests d'ouverture de session
- Intégrer des stations au domaine
- Créer des restrictions de groupe
- Configurer les services d'impression
- Créations d'approbations



6.2. INTRODUCTION

Groupe de travail : toutes les machines sous Windows sont par défaut dans un groupe de travail nommé « WORKGROUP ». Ce dernier permet de mettre en relation des machines d'un même groupe de travail, notamment pour le partage de fichiers, mais il n'y a pas de notions d'annuaire, ni de centralisation avec ce mode de fonctionnement (chaque machine contient sa propre base d'utilisateurs indépendante les unes des autres.). Par conséquent, ce modèle devient très vite inadapté dès que le nombre de postes et d'utilisateurs augmente, car cela devient lourd en administration [8].

Domain : un domaine se réfère à un regroupement logique de serveurs et de machines clientes dans un réseau local. Il est géré par un serveur appelé contrôleur de domaine, qui est chargé d'autoriser les machines à rejoindre le domaine et d'autoriser les utilisateurs à accéder aux ressources de l'ensemble du domaine. Les domaines sont principalement utilisés dans le cadre des entreprises, pour gérer de manière centralisée les utilisateurs, les machines, etc. Il permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données (**annuaire**) stockée dans un contrôleur de domaine.



Contrôleur de domaine : le serveur depuis lequel on effectue la création d'un domaine est promu au rôle de contrôleur du domaine créé. Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine. Il permet de [10]:

- Vérifier les identifications des objets (utilisateurs, ordinateurs, groupes, etc.),
- Traiter les demandes d'authentification,
- Veiller à l'application des stratégies de groupe
- Stocker une copie de l'annuaire Active Directory

Arbre : un arbre est un regroupement hiérarchique de plusieurs domaines.

Forêt : une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt. Les domaines d'une forêt fonctionnent de façon indépendante, mais la forêt facilite les communications entre les domaines dans toute l'architecture.

De manière générale, Une forêt est un ensemble d'arbres, qu'un arbre est constitué d'une racine et potentiellement de branches qui sont représentées par des domaines et des sous-domaines. La Figure 6.1 illustre la structure d'une forêt.

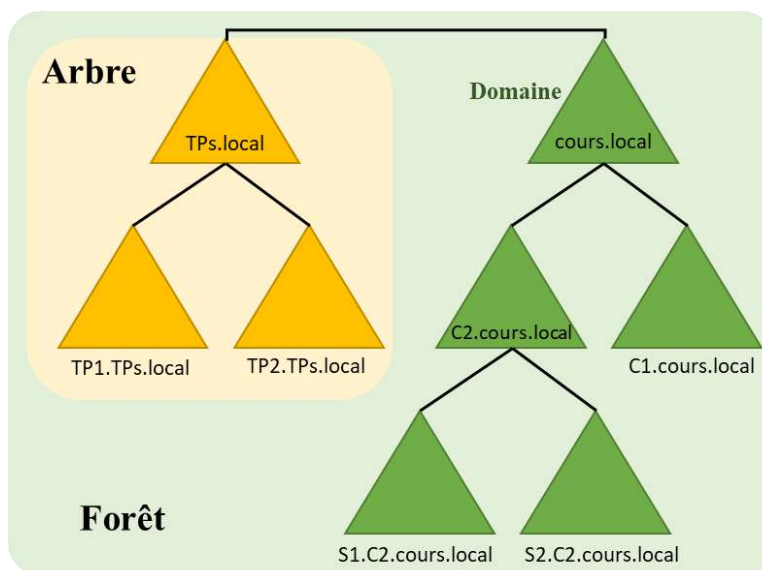


FIGURE 6.1: STRUCTURE D'UNE FORET

Active Directory : l'Active Directory est un annuaire LDAP (*Lightweight Directory Access Protocol*) pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc.), l'objectif étant de centraliser deux fonctionnalités essentielles : l'identification et l'authentification au sein d'un système d'information [8], [10].

Au sein de l'annuaire Active Directory, il y a différents types d'objets, comme par exemple les utilisateurs, les ordinateurs, les serveurs, les unités d'organisation ou encore les groupes. En fait, ces objets correspondent à des classes, c'est-à-dire des objets disposant des mêmes attributs.

La base de données Active Directory est divisée de façon logique en trois partitions de répertoire (appelé « Naming Context »). Ces trois partitions sont [10]:

1. **La partition de schéma** : cette partition contient l'ensemble des définitions des classes et attributs d'objets, qu'il est possible de créer au sein de l'annuaire Active Directory. Elle est unique au sein d'une forêt.
2. **La partition de configuration** : cette partition contient la topologie de la forêt (informations sur les domaines, les liens entre les contrôleurs de domaines, les sites, etc.). Cette partition est aussi unique au sein d'une forêt
3. **La partition de domaine** : cette partition contient les informations de tous les objets d'un domaine (ordinateur, groupe, utilisateur, etc.). Elle est unique au sein d'un domaine, il y aura donc autant de partitions de domaine qu'il y a de domaines.

Active Directory s'appuie donc sur une organisation des machines en domaines **DNS**, dont il assure la bonne intégration ; sur une centralisation des informations des membres du réseau (machines, utilisateurs, ...) dans un annuaire **LDAP** ; sur une sécurisation forte par le protocole d'authentification **Kerberos** ; sur des partages de ressources (dossiers, imprimantes, ...) par le protocole **SMB/CIFS**.

6.3. CONTROLEUR DE DOMAINE ACTIVE DIRECTORY

Dans cette partie de TP, nous allons installer et configurer un contrôleur de domaine Active directory. Pour ce faire, nous aurons besoin d'utiliser trois machines virtuelles, un serveur Windows 2003, et deux machines Windows 7 (version **Professionnel**) selon la topologie réseau suivante (Figure 6.2).

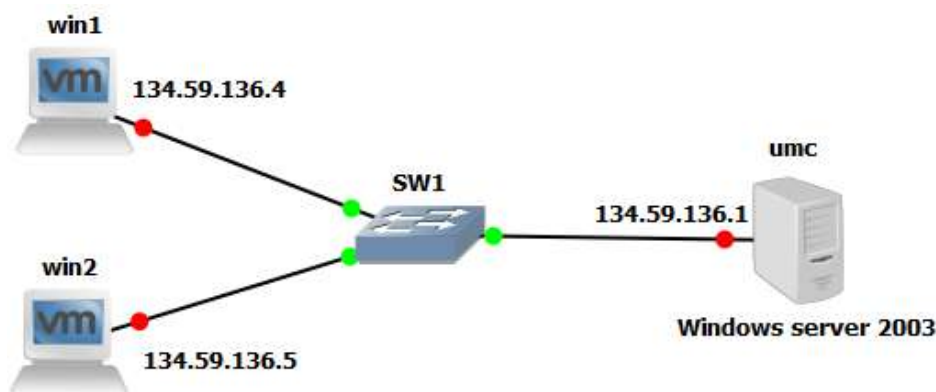


FIGURE 6.2: TOPOLOGIE RESEAU DU TP6

Travail demandé

- Créer la topologie réseau de la Figure 6.2 en utilisant GNS3, puis tester les connexions entre les machines virtuelles en utilisant la commande ping
- Configurer la machine serveur « *Windows server 2003* » en contrôleur de domaine Active Directory et les autres machines virtuelles en membres du domaine.
 - Le nom de domaine : *zarzara.edu*
 - Nom NetBios : *zarzara*
 - Niveau fonctionnel : *Windows 2003*
 - Les autres options seront laissées par défaut.
- Créez les trois unités organisationnelles (U.O) Electronique, Mécanique et G-transport dans le domaine *zarzara.edu*.
 - Dans l'U.O. Electronique, créez le groupe Cours et le groupe TP.
 - Dans l'U.O. Mécanique, créez le groupe accueil et le groupe laboratoires.
 - Dans l'U.O. G-transport, créez le groupe développeurs et le groupe techniciens.
- Déplacer la machine virtuelle « win1 » vers l'U.O. Electronique
- Créez les comptes utilisateurs suivant : AMIRA KOKO, MERIEM MIMI, AHMED RIDA et ANIS FOFO.
 - Ajouter les utilisateurs AMIRA KOKO et MERIEM MIMI au groupe cours de l'U.O. Electronique.
 - Ajouter l' utilisateurs AHMED RIDA au groupe TP de l'U.O. Electronique.
 - Ajouter l' utilisateurs ANIS FOFO au groupe laboratoires de l'U.O. Mécanique et au groupe techniciens de l'U.O. G-transport.
- Faites en sorte que les utilisateurs du groupe cours ne puissent se connecter que de 8^h à 18^h.
- Créer une nouvelle stratégie du groupe pour l'U.O. Electronique avec les paramètres suivants :
 - Désactiver la connexion au domaine depuis un compte **invité**.
 - Renommer le compte administrateur à **admin-electronique**.
 - Désactiver l'exécution de **Windows Messenger**.
 - Interdire aux utilisateurs de partager des fichiers de leur profil.
 - Interdire le menu contextuel (clic droit) dans Internet Explorer.

La console **gpedit.msc** (à lancer depuis Démarrer → Exécuter) permet d'éditer individuellement les stratégies de groupes locales. Cette console existe pour tous les Windows y compris les versions clientes.

EXERCICE

- 1- Créez l'unités organisationnelles (U.O) **Etablissement**, puis ajouter a cette dernière les groupes **enseignants** et **étudiants**, l'ordinateur **win2** et le compte utilisateur **CHEF** qui est un compte administrateur.
- 2- Ajouter au groupe « **enseignants** » les utilisateurs **ens1**, **ens2** (administrateur) et **ens3** (utilisateur). Et au groupe « **étudiants** » les utilisateurs **etu1**, **etu2** et **etu3** (utilisateur).
- 3- Ouvrez une session du domaine sur la machine **win2** avec le compte « **CHEF** ».
- 4- On souhaite imposer à l'unités organisationnelles (U.O) **Etablissement** les règles suivantes:
 - Un étudiant est autorisé à réinitialiser les mots de passe des autres étudiants.
 - Aucun étudiant et aucun enseignant n'a de commande « **Exécuter** » dans son menu « **Démarrer** ».
 - On souhaite partager un dossier nommé « **Cours** » situé à la racine de c:\ sur **win2** de façon que les **enseignants** et le **CHEF** aient les accès en contrôle total au partage Alors que les **étudiants** aient uniquement accès en « lecture /affichage » du contenu du dossier.
 - Empêcher les étudiants d'accéder à internet.
 - Un enseignant ne pouvant ouvrir de session que sur la machine **win2** aux horaires de travail (du Dimanche au Jeudi de 8h à 17h).

Remarque : me rendre sur papier ou version électronique (Rapport) la démarche documentée de ce que vous avez fait.

Unité d'enseignement : UEM 1.2
réseaux VHS : 22h30 (TP : 1h30)

Matière : TP Administration des services
Crédits :2, Coefficient : 1

TP 7 : Service de messagerie

7. SERVICE DE MESSAGERIE

7.1. BUT

A l'issue de ce TP, l'étudiant sera capable d'installer et de configurer Postfix en tant que serveur SMTP (Simple Mail Transfer Protocol) pour l'envoi et la transmission des courriers électronique.

Objectifs spécifiques

1. Comprendre le fonctionnement d'un serveur de messagerie
2. Installation et configuration de Postfix
3. Mise en place de serveurs SMTP
4. Testé les différentes fonctionnalités offertes par un serveur de messagerie

7.2. INTRODUCTION

Electronique mail (e-mail) ou courrier électronique, est un des services les plus utilisés sur Internet. Contrairement au courrier conventionnel ou même du fax (fac-simile), le succès du courrier électronique tient à sa facilité d'utilisation, sa rapidité d'envoi et son coût extrêmement faible.

Le transfert de courrier électronique d'un expéditeur à un destinataire est effectué via un serveur de messagerie. Ce dernier possède deux fonctions principales (envoi / réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs de messagerie. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie, soit un courrielleur web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages [11].

Comme l'illustre la Figure 7.1, l'envoi d'un courrier électronique se déroule généralement via le protocole SMTP, (Simple Mail Transfer Protocol), littéralement « protocole simple de transfert de courrier ». Le client SMTP (i.e. l'expéditeur), télécharge le message électronique sur le serveur SMTP, c'est à dire le serveur d'email sortant du fournisseur de messagerie correspondant (**Etape 1**). Ceci s'effectue via une application Webmail dans le navigateur ou un programme de messagerie (techniquement un « Mail User Agent » abrégé en MUA), comme Windows Live Mail ou bien Mozilla Thunderbird. Après, le serveur SMTP envoie l'email via un ou plusieurs « Mail Transfer Agents » (MTA) au serveur SMTP cible (**Etape 2**). L'opération de transfert est effectuée selon le protocole SMTP. Le serveur SMTP de destination (cible) stocke temporairement l'email dans le stockage temporaire d'emails, puis, le destinataire MUA télécharge l'email via IMAP ou POP3 (**Etapes 3 et 4**).

ABRÉVIATIONS

- **MUA (Mail User Agent)** : agent de gestion du courrier comme Kmail, Eudora, Outlook, etc.
- **MTA (Mail Transfer Agents)** : agent de transport du courrier (protocole SMTP) comme sendmail, exim, postfix ...etc.
- **SMTP (Simple Mail Transfer Protocol)** : ce protocole est utilisé pour poster vos messages.
- **POP3 (Post Office Protocol 3)** : Protocole de gestion du courrier le plus utilisé sur internet pour récupérer vos messages.
- **IMAP (Internet Message Access Protocol)** : Protocole de gestion du courrier plus performant que pop2 ou pop3, pour récupérer vos messages.

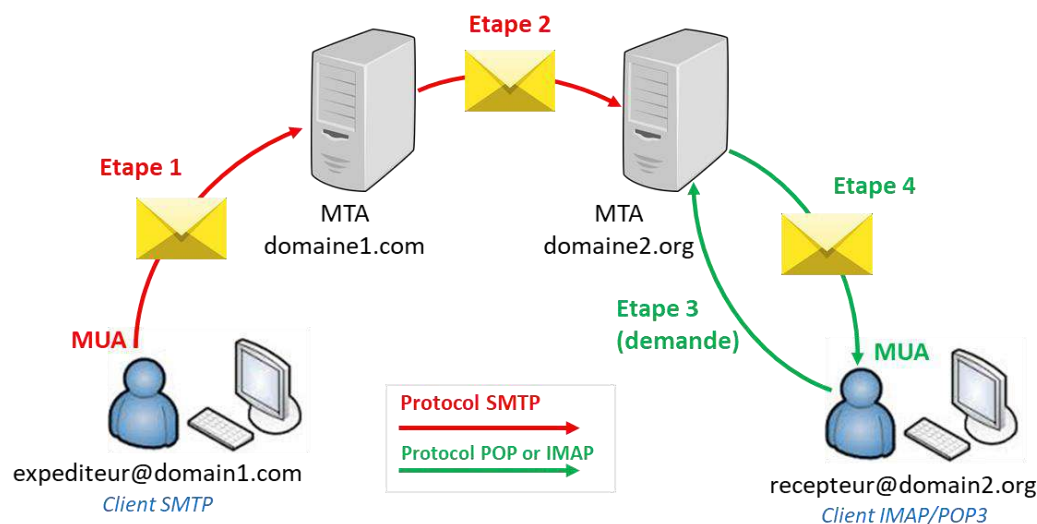


FIGURE 7.1: STRUCTURE D'UN SYSTEM DE MESSAGERIE

Postfix⁷ (MTA) est un serveur libre de messagerie électronique développé à l'origine comme une alternative, plus simple et plus sécurisée, à **sendmail**⁸. Il peut fonctionner sur PC, sur mac ou sur toute autre plateforme compatible avec Unix/Linux, mais, Il n'existe pas de version Windows [12].

Postfix permet de mettre en place un serveur de courrier électronique qui permet d'envoyer et de recevoir du courrier au sein d'une organisation. Il peut communiquer directement avec d'autres serveurs de courrier sur l'Internet à travers le protocole SMTP (Simple Mail Transfer Protocol). L'utilisateur peut accéder à sa messagerie électronique et récupérer son courrier en utilisant le protocole POP3 (Post Office Protocol) ou le protocole IMAP (Internet Message Access Protocol). Postfix présente bien des avantages sur Sendmail au niveau de sécurité et ne comporte qu'un seul fichier de configuration à modifier pour être opérationnel [12].

Documentation de postfix en français : <http://x.guimard.free.fr/postfix>

7.3. SERVEUR DE MESSAGERIE AVEC POSTFIX

Dans ce TP nous allons installer et configurer Postfix en tant que serveur SMTP pour l'envoi et la transmission des courriers électronique. Pour ce faire, nous aurons besoin d'utiliser deux machines virtuelles avec le system d'exploitation Ubuntu 18.04 selon la topologie réseau Figure 7.2 (une architecture client/serveur).

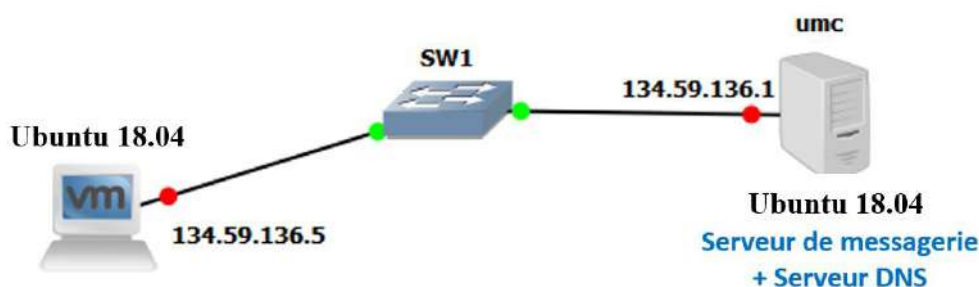


FIGURE 7.2: TOPOLOGIE RESEAU POUR LE SERVEUR DE MESSAGERIE

⁷ <http://www.postfix.org/>

⁸ <http://www.postfix.org/mailq.1.html>

Travail demandé

1. Créer la topologie réseau de la Figure 7.2 en utilisant GNS3, puis tester les connexions entre les machines virtuelles en utilisant la commande ping.
2. Configurer une adresse IP fixe à votre serveur ainsi qu'un nom de machine.
 - Serveur DNS : nom →umc, adresse IP→137.59.136.1/16
 - Machine cliente : nom →client, adresse IP→137.59.136.5/16
3. Installer et configurer un serveur DNS sur votre serveur, selon les mêmes paramètres proposés dans le TP 2 (Service DNS), puis tester le fonctionnement de votre serveur DNS en utilisant la commande **nslookup**. Le serveur DNS doit être utilisé sur le réseau local par toutes les machines clientes.
4. Installez le paquetage **postfix** et ses dépendances sur votre serveur. Choisir "Site Internet" lors de l'installation et valider les options par défaut, puis tester le fonctionnement de Postfix (démarrage du service Postfix avec la commande **service postfix start**).
5. Identifiez le fichier de configuration du service Postfix, la commande pour afficher les options de configuration et le script de démarrage.
6. Expliquez les variables :
 - mydestination,
 - mynetworks,
 - inet_interfaces
 - relayhost.
7. Pour tester le serveur SMTP, ajouter un nouvel utilisateur et changer son mot de passe avec la commande **Passwd**.
8. Installer l'outil **Dovecot** pour pouvoir consulter la messagerie à distance.
9. Installe le Webmail **Thunderbird** et créer un nouveau compte de messagerie.
10. Envoyer un message au récepteur et vérifier que le nouveau message est bien reçu.

8. PREPARATION DE L'ENVIRONNEMENT D'ADMINISTRATION

8.1. INSTALLATION ET CONFIGURATION DE GNS3 SOUS MS WINDOWS

8.1.1. INSTALLATION DE GNS3

Les étapes suivantes montrent comment installer GNS3 sous MS Windows. Premièrement, vous devez télécharger l'installateur Windows depuis le site (<https://www.gns3.com/>) (Figure 8.1). Afin de pouvoir télécharger le fichier d'installation PC vous devrez créer un compte sur le site de GNS3 (Figure 8.2).



FIGURE 8.1: SITE WEB POUR TELEGERER GNS3

FIGURE 8.2: CREATION D'UN NOUVEAU COMPTE SUR LE SITE GNS3



FIGURE 8.3: FENETRE DE TELECHARGEMENT DE GNS3

Une fois que le téléchargement de GNS3 terminé, lancez l'exécution de l'installateur. Lorsque la fenêtre de bienvenue s'affiche, appuyez sur « **Next** », puis, acceptez les termes de la licence sur la suivante. Aussi, ne modifiez pas le répertoire du menu démarrer au travers duquel GNS3 est accessible sur la fenêtre suivante. Pour les fonctionnalités (Figure 8.4), il y en a plusieurs comme par exemple wireshark⁹, putty¹⁰ (client Telnet et SSH) et WinPcap¹¹ (capturer des trames IP dans un environnement Windows). Dans cette fenêtre, laissez les paramètres par défaut afin d'avoir ces outils à disposition pour la suite.

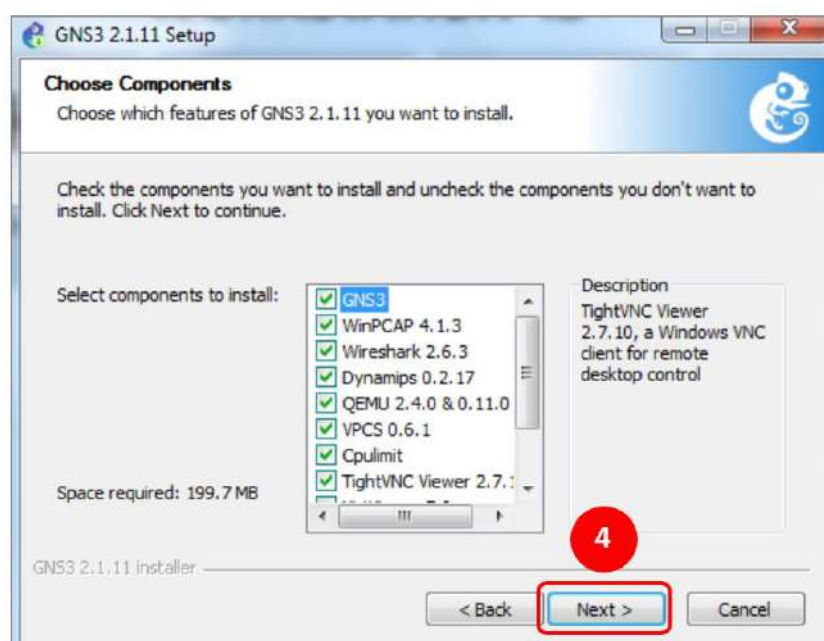


FIGURE 8.4: LES FONCTIONNALITES ASSOCIEES A GNS3.

⁹ <https://www.wireshark.org/>

¹⁰ <https://www.putty.org/>

¹¹ <https://www.winpcap.org/>

A l'apparition de l'écran de bienvenue de WinPcap, appuyez sur « next ». Acceptez les termes de la licence. Autorisez le module WinPcap à s'exécuter au démarrage. Lorsque l'installation se termine, cliquez sur « Finish ». Même chose pour Npcap et Wireshark.

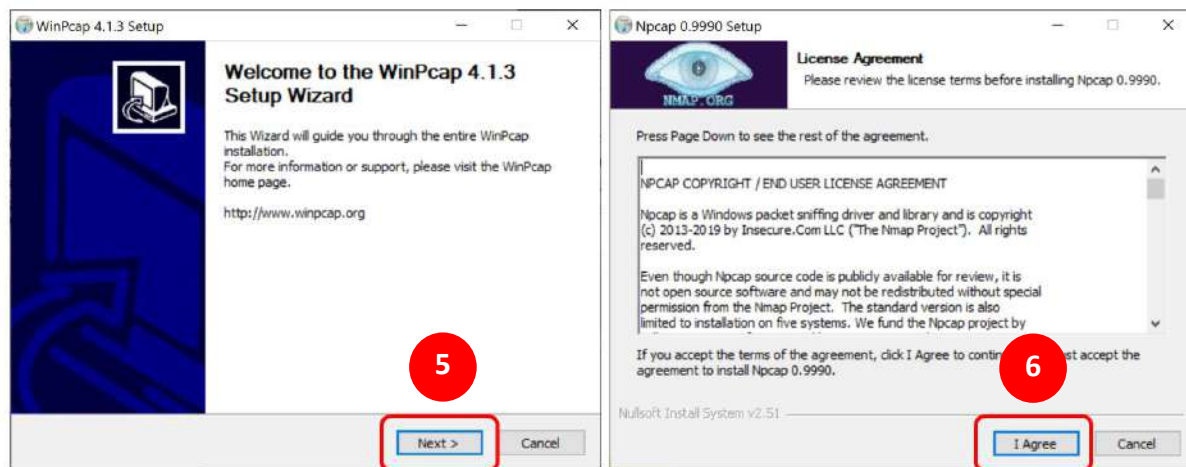


FIGURE 8.5: INTERFACE D'INSTALLATION DE WINPCAP ET DE NPCAP.

Après l'installation de Wireshark, cliquez sur « next » puis sur « finish » dans la fenêtre suivante. Après l'installation de GNS3, cliquez sur « Next ». A la demande d'inscription à la mailing-list de GNS3, cliquez sur « next » puis sur « Yes » à la fenêtre demandant de confirmer. Décochez « Start GNS3 » et cliquez sur « Finish » (Figure 8.6). L'installation est terminée.

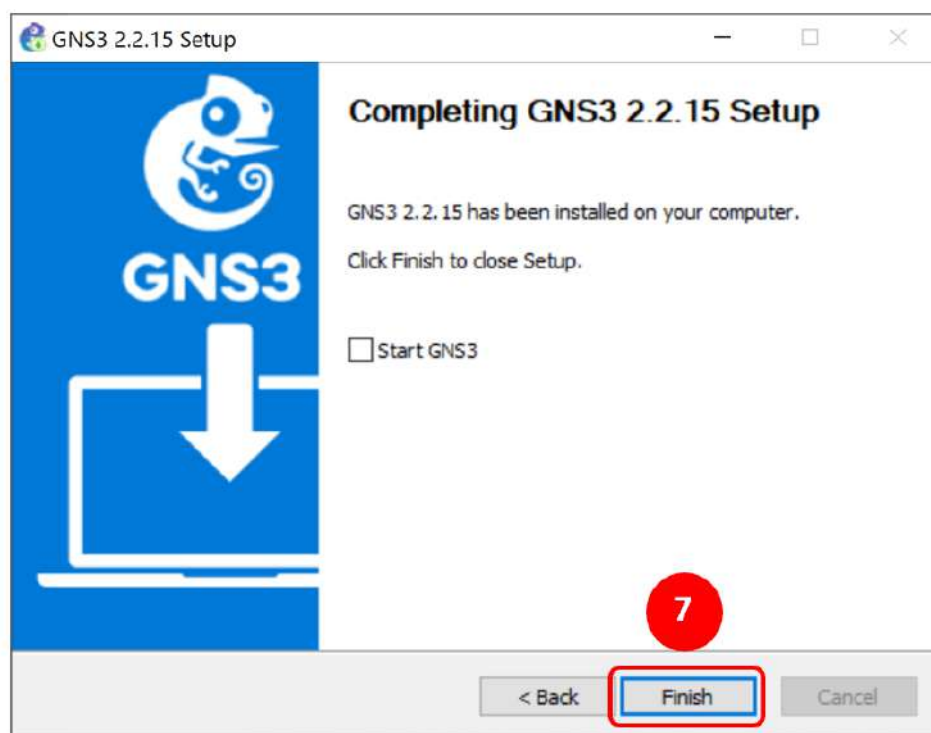


FIGURE 8.6: FIN D'INSTALLATION DE GNS3.

Remarque : GNS3 nécessite pour fonctionner les droits d'administrateur, il est donc recommandé de l'exécuter à partir d'un compte administrateur.

8.1.2. CONFIGURATION DE GNS3

GNS3 intègre à la fois un **client** et un **serveur**. Le client est l'interface graphique et sera évidemment lancé depuis votre PC. Pour le serveur vous avez trois modes d'exécution:

- **Local Server** : Le serveur est directement exécuté sur votre PC.
- **VM-Server** : Le serveur est installé sur une VM Ubuntu, qui est exécuté depuis votre PC. GNS3 fournit des images disques pour VMware et Virtual Box. Cela nécessite donc d'avoir un des deux logiciels de virtualisation.
- **Remote-Server** : Identique à la seconde solution mais la virtualisation se fait sur une autre machine distante.

Au premier démarrage de GNS3, vous devez sélectionner le mode d'exécution de ce dernier. Pour notre TP, nous choisissons le deuxième mode (i.e. exécution sur la machine physique locale) (Figure 8.7).

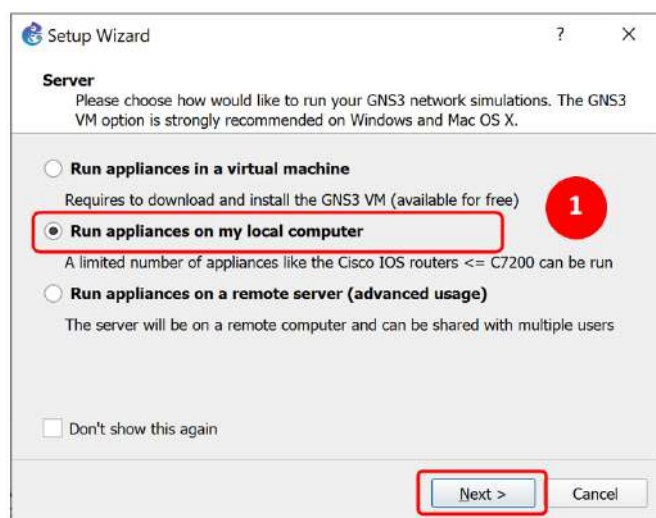


FIGURE 8.7: MODE D'EXECUTION DE GNS3

Dans cette étape de configuration, sélectionnez l'adresse IP et le port du serveur local. Il est recommandé de sélectionner l'adresse IP 127.0.0.1 (localhost). Veuillez vérifier si le port par défaut (3080) est occupé par d'autres programmes. S'il est occupé, remplacez le port ou quittez le programme occupant le port.

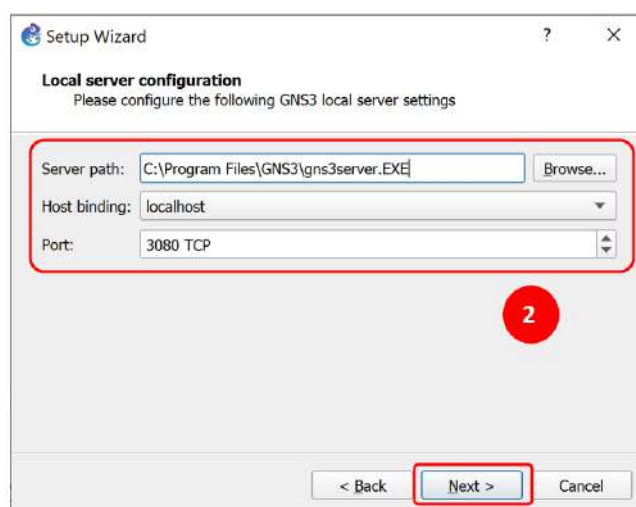


FIGURE 8.8: PARAMETRES DE SERVEUR LOCAL

Après avoir cliqué sur « Next », GNS3 vérifie la connexion au serveur local. Si la connexion au serveur local est réussie, passez à l'étape suivante, sinon, vérifiez les étapes précédentes (Figure 8.9).

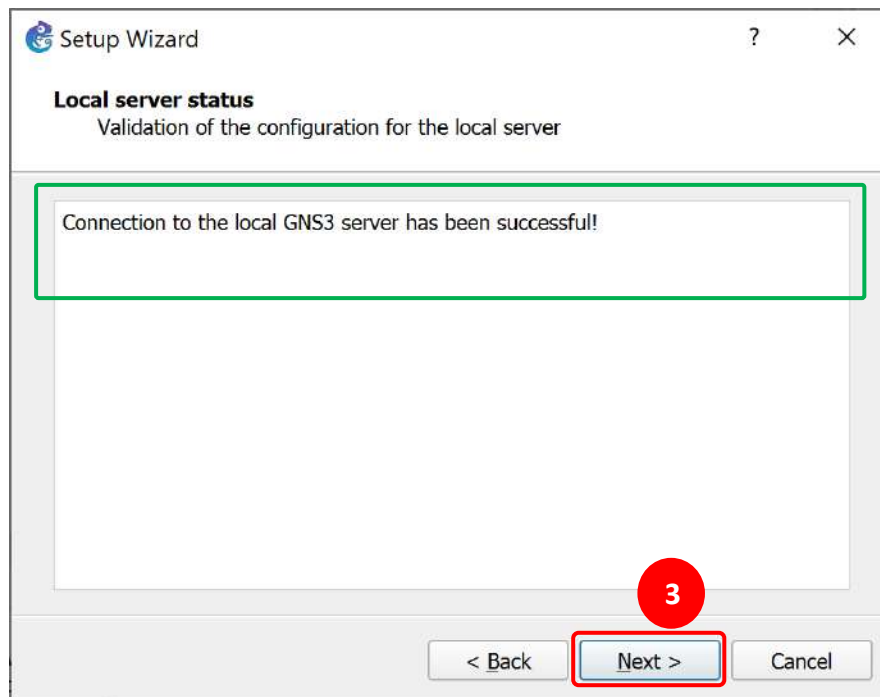


FIGURE 8.9: CONNEXION AU SERVEUR LOCAL

Si la configuration est terminée avec succès, cliquez sur « Finish » (Figure 8.10)

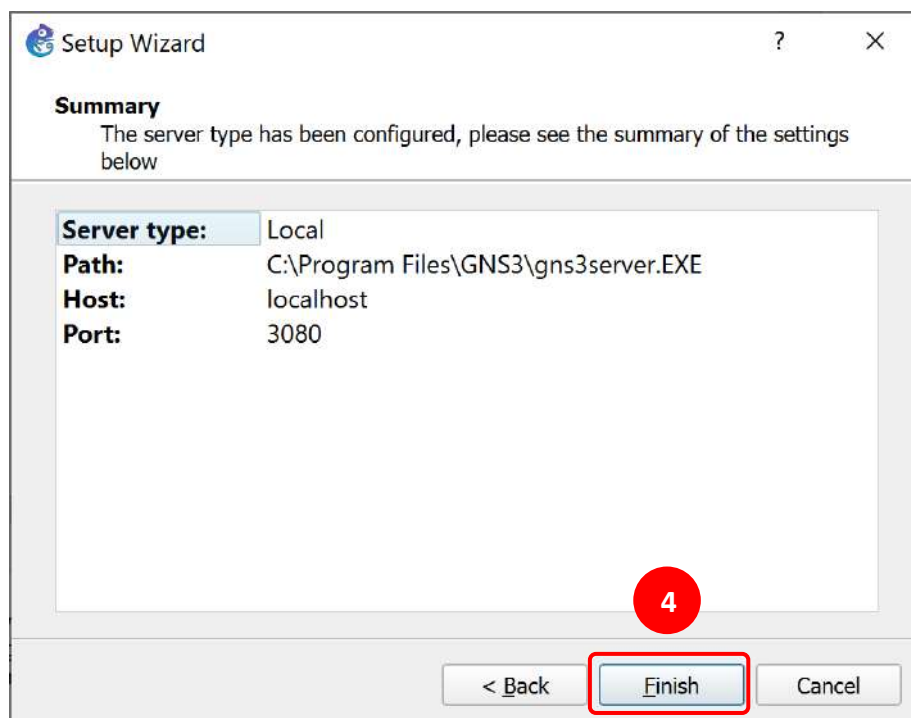


FIGURE 8.10: FIN DE LA CONFIGURATION DE GNS3

8.1.3. PRESENTATION DE L'INTERFACE GRAPHIQUE DE GNS3

GNS3 fonctionne en utilisant la notion de projet. Chaque projet correspond à une configuration de réseau dans laquelle on conserve les équipements utilisés (e.g. hôtes, routeurs, switches, etc.), comment ces équipements sont connectés les uns aux autres (i.e. la topologie), ainsi que la configuration de chaque équipement. Comme le montre la Figure 8.11, l'interface graphique de GNS 3 est composée des éléments suivants :

1. Gestion de projets (Créer un nouveau projet, Recharger un projet existant, Sauvegarder un projet,
2. Gestion de l'émulation des équipements
3. Edition de la topologie (Annotations, formes, etc.)
4. Gestion des nœuds (routeurs, switches, PC, équipements de sécurité, etc.)
5. Console log et messages d'erreurs
6. Etat de ou des services
7. Etat de ou des équipements.
8. Feuille GNS3

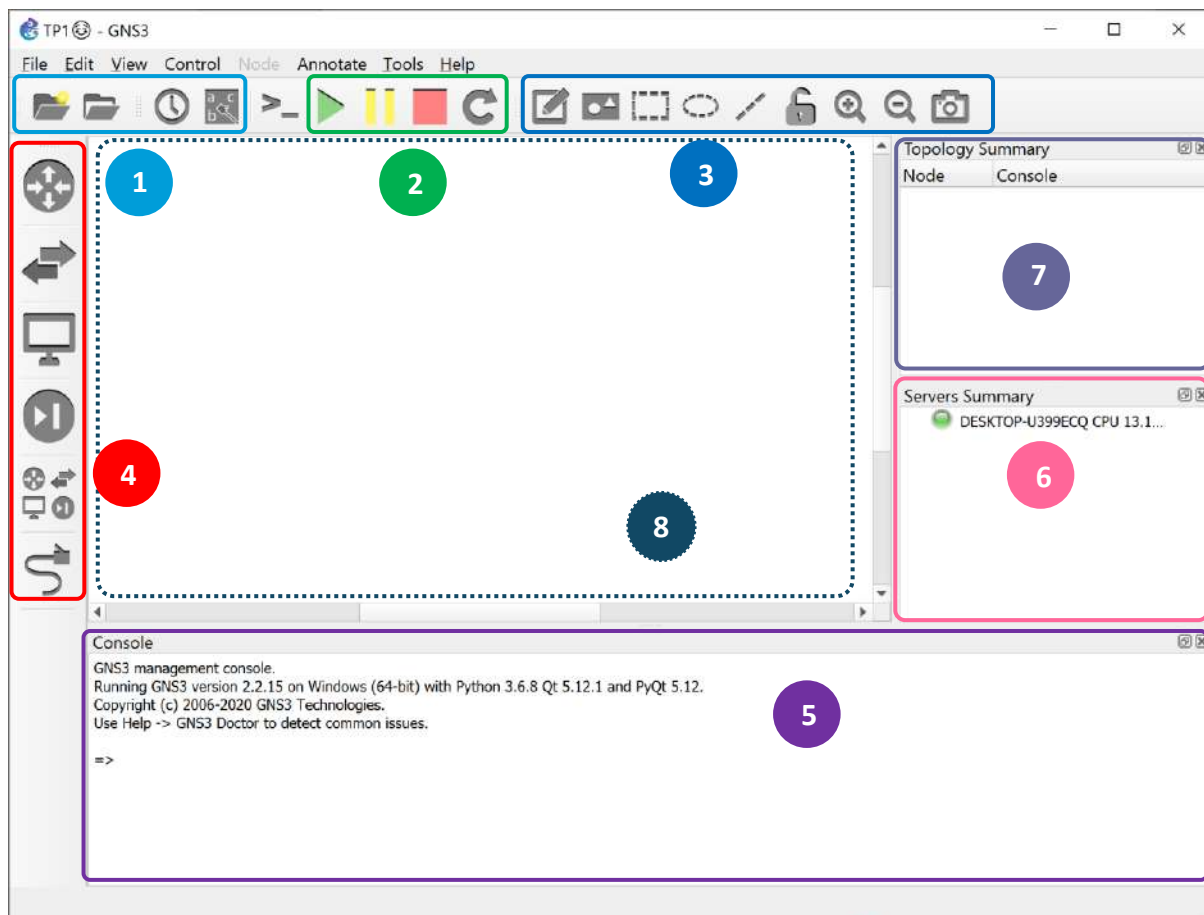


FIGURE 8.11: INTERFACE GRAPHIQUE DE GNS3.

8.2. INSTALLATION ET CONFIGURATION DE VMWARE SOUS MS WINDOWS

VMware Workstation est logiciel de virtualisation qui permet d'exécuter plusieurs machines virtuelles sur une même machine physique. Les différentes machines virtuelles se partagent les ressources du serveur physique, telles que le networking et la RAM, mais chacune d'entre elles peut tourner sur un système d'exploitation différent [13].

Le couple GN3 et VMware permettra alors la réalisation d'un réseau virtuel qui dispose de toute l'aptitude requise pour en situation de fonctionnement réel. En particulier, il permet d'utiliser des terminaux virtuel et physique, connecter un réseau virtuel avec un réseau physique, etc. Il permet également une connexion à différentes interfaces réseau utilisé par le système d'exploitation de la machine physique.

Pour pouvoir installer VMware, il faut que votre ordinateur ait certaines spécificités en termes de processeur, quantité de mémoire vive (RAM), écran et espace de disque dur. Ces informations sont disponibles dans le site de téléchargement VMware , pour chaque version de VMware Workstation.

Vous pouvez le télécharger à l'adresse suivante :

<https://www.youwindowsworld.com/en/downloads/virtualization/vmware/vmware-workstation-11>

Téléchargez la version la plus récente et cliquez sur le lien d'installation (Figure 8.12).

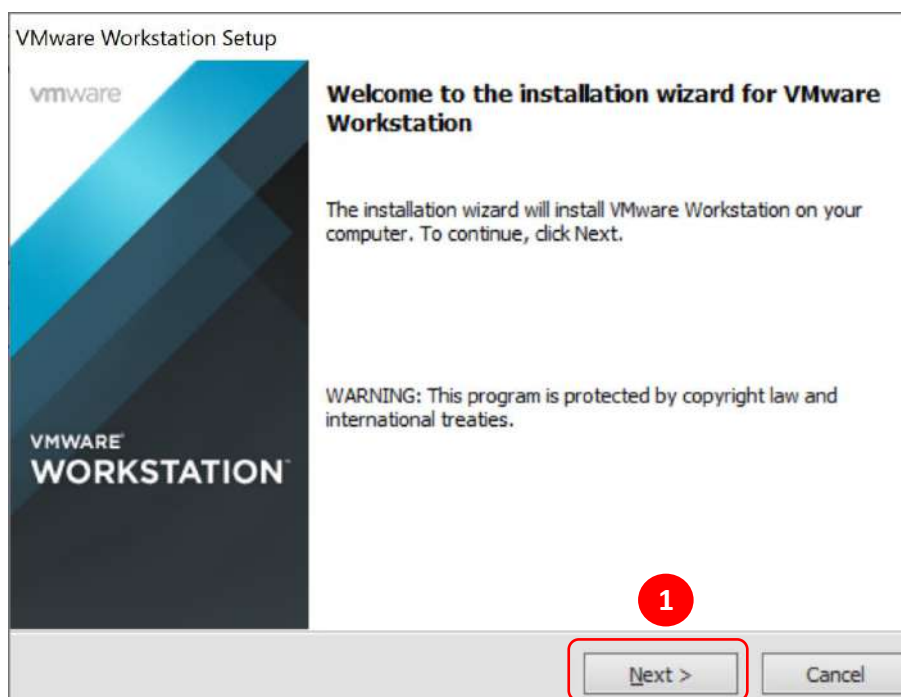


FIGURE 8.12: FENETRE D'INSTALLATION DE VMWARE

Comme pour tout programme, vous devez lire et approuver les conditions d'utilisation de VMware Workstation avant de commencer l'installation.

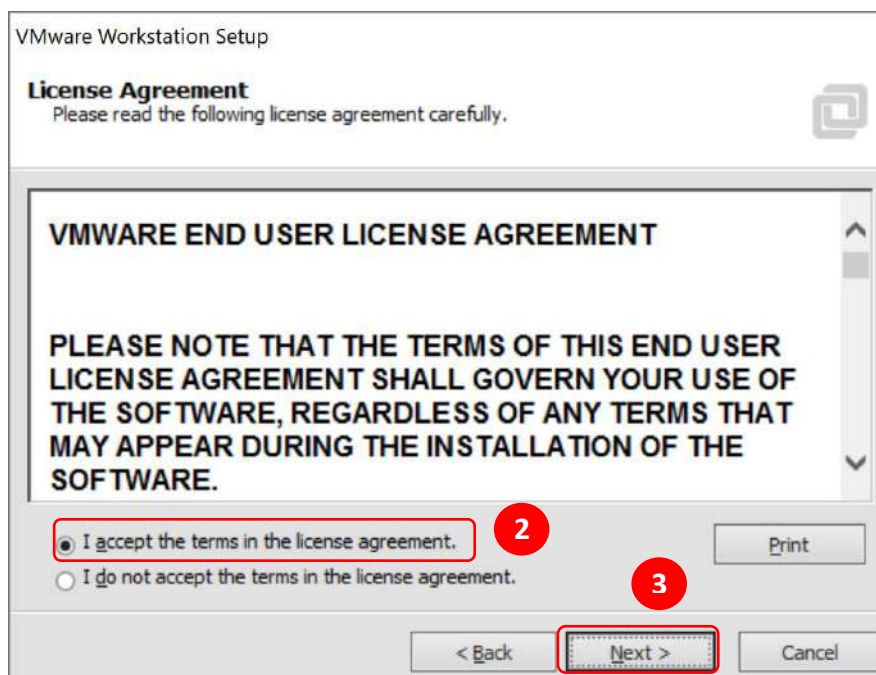


FIGURE 8.13: AGREEMENT DE VMWARE WORKSTATION

Sélectionnez le type d'installation standard (**Typical**).

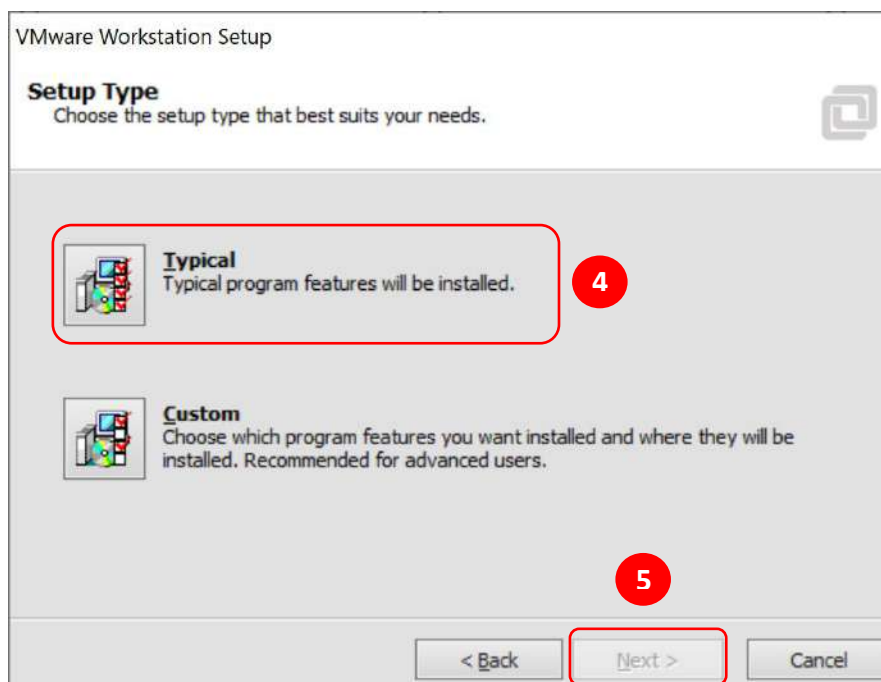


FIGURE 8.14: SELECTION DE TYPE D'INSTALLATION

Ne modifiez pas le répertoire dans lequel VMware Workstation sera installer.

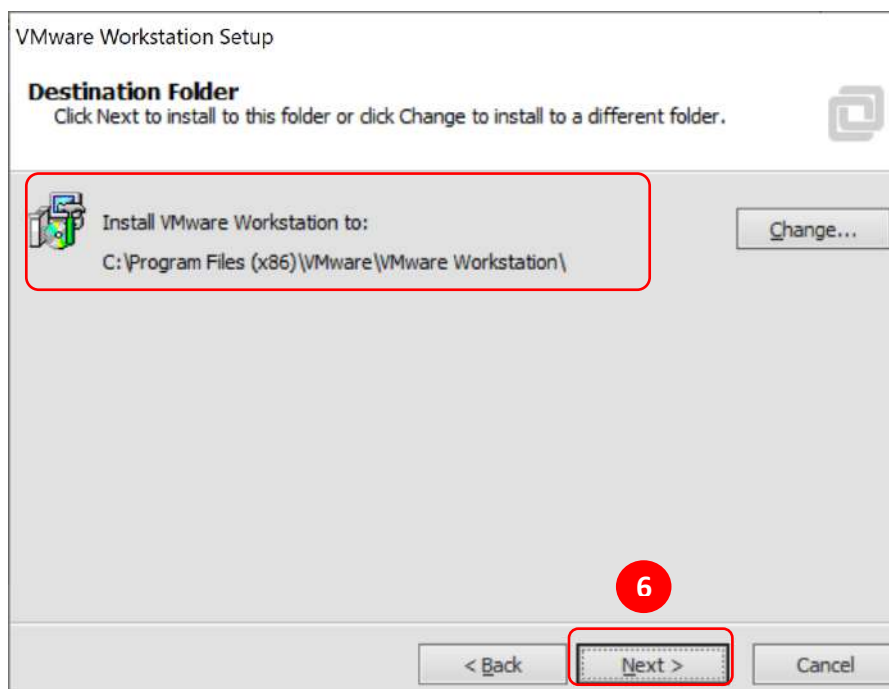


FIGURE 8.15: CHEMIN D'INSTALLATION DE VMWARE WORKSTATION.

Dans la fenêtre suivante cocher les cases permettant de créer un raccourci au programme VMware sur le bureau et dans le menu démarrer, puis cliquez sur le bouton « **Next** ». Cliquez sur le bouton « **continue** » dans la fenêtre suivante pour lancer le processus d'installation (Figure 8.16).

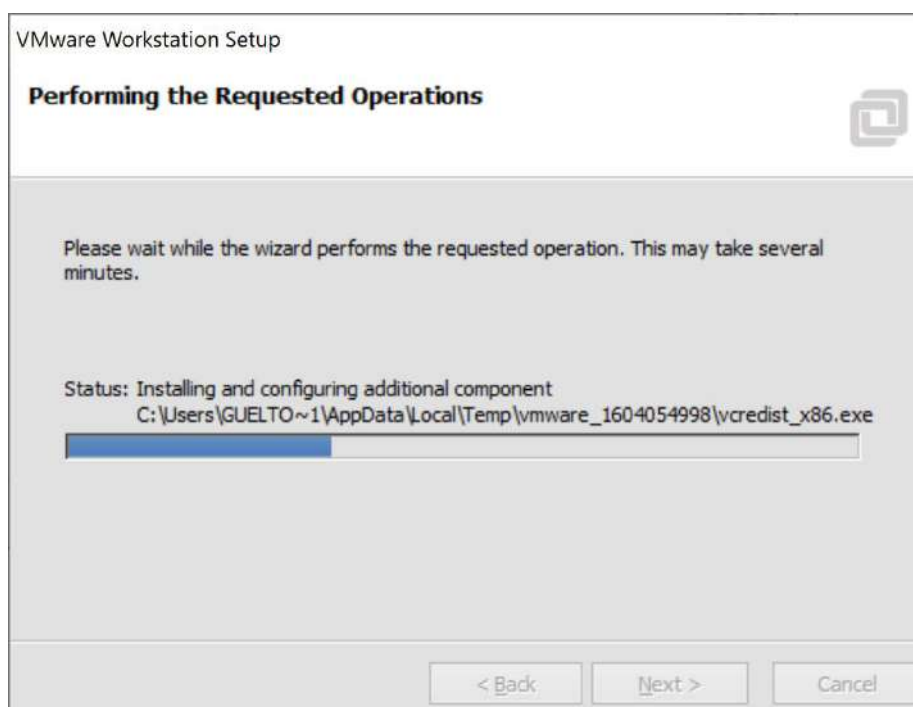


FIGURE 8.16: PROCESSUS D'INSTALLATION DE VMWARE

En fin d'installation, on vous demandera d'entrer la clé du produit. En effet, avec Windows et les autres systèmes d'exploitation sous licence, vous devrez entrer votre clé de produit.

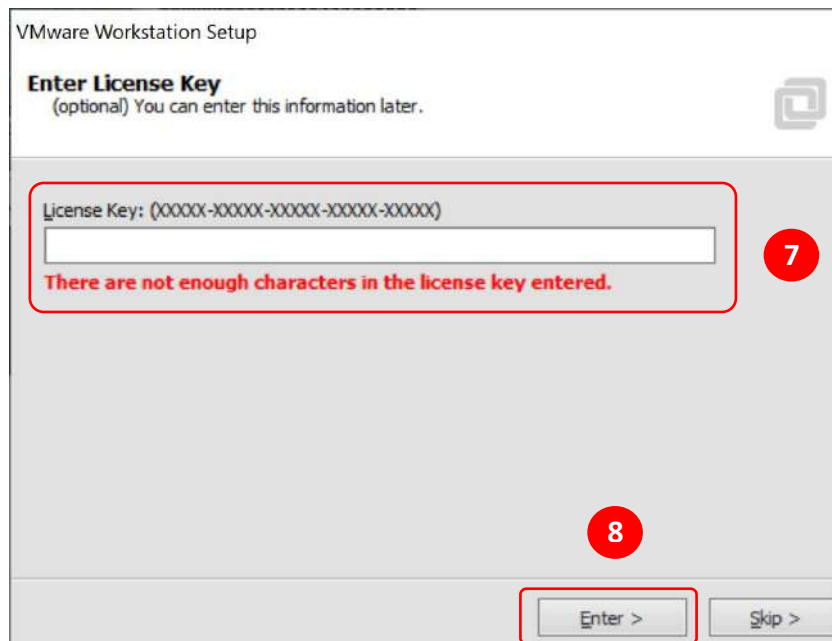


FIGURE 8.17: CLE D'ACTIVATION DE VMWARE WORKSTATION 11.

Après l'introduction de la clé d'activation, cliquez sur « finish dans la fenêtre suivante pour terminer l'installation. Puis, redémarrez l'ordinateur.

La Figure 8.18 présente l'interface graphique du programme VMware Workstation 11.

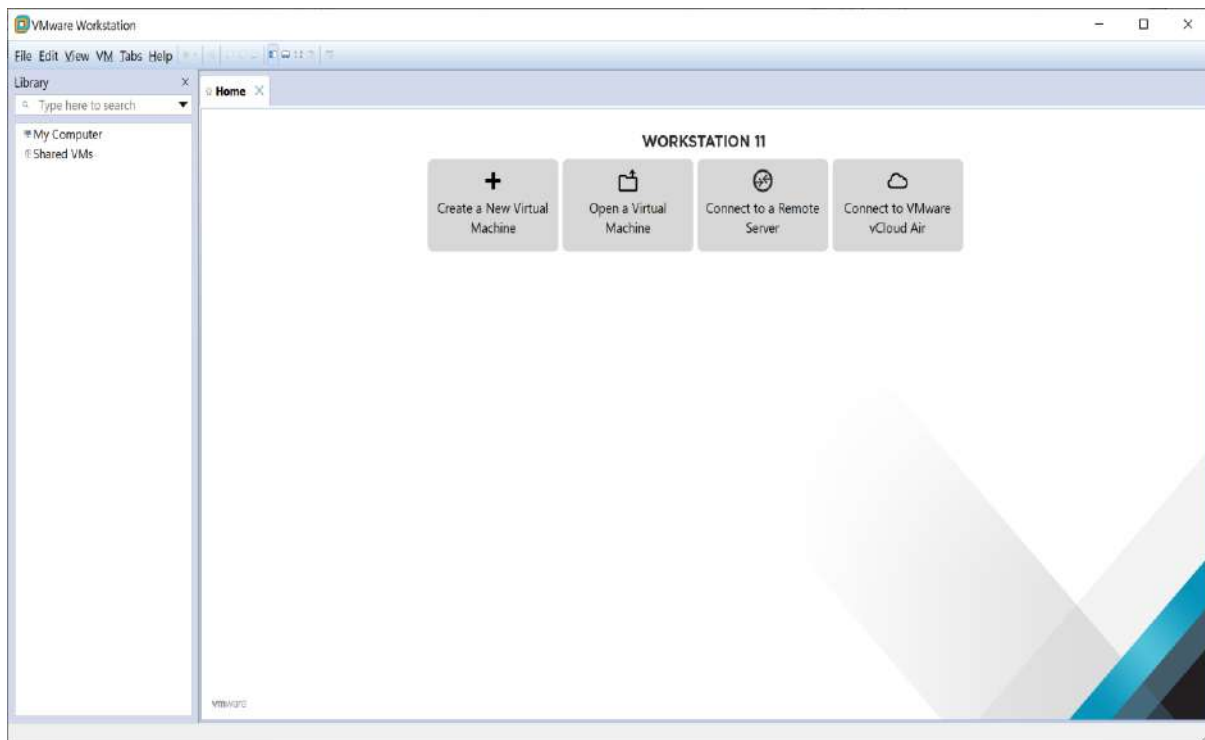


FIGURE 8.18: INTERFACE GRAPHIQUE DE VMWARE

Remarque : Vérifier que le logiciel VMware est associé au GNS3. Pour ce faire, allez vers « Edit / Preferences / VMware »).

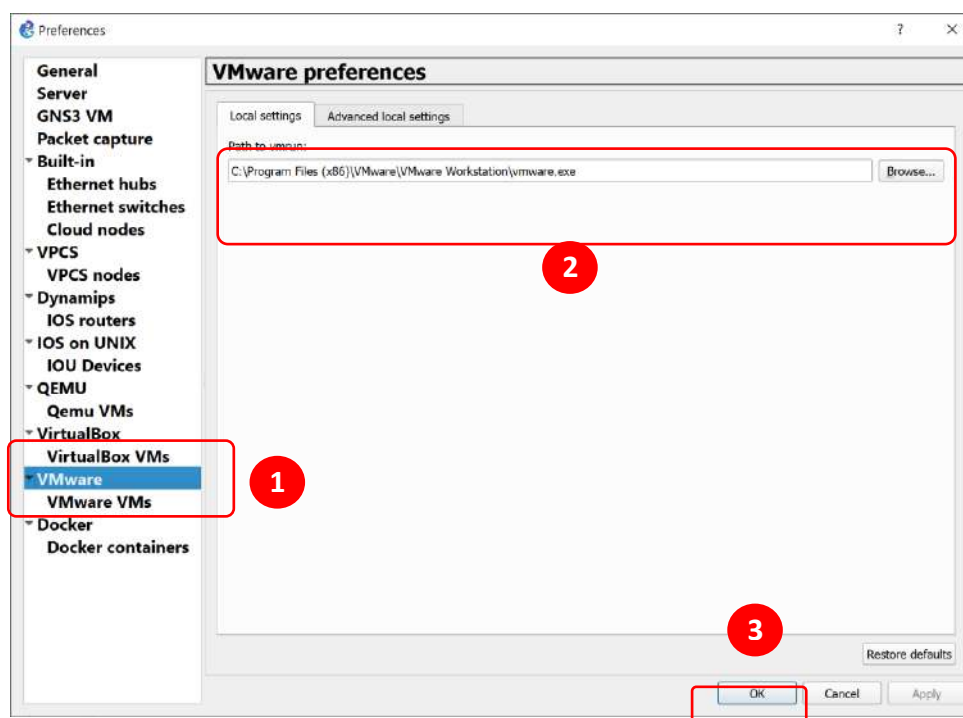


FIGURE 8.19: CHEMIN VERS LE FICHIER D'EXECUTION DE VMWARE

8.3. CREATION D'UNE MACHINE VIRTUELLE SOU VMWARE WORKSTATION 11

Pour commencer la création de la machine virtuelle, allez dans "File", "New Virtual Machine". Dans la fenêtre qui s'affiche, sélectionnez l'installation en mode recommandé (Typical). Vous pouvez aussi sélectionner le mode "Custom (Advanced)", pour pouvoir configurer la VM selon votre besoin. Dans la fenêtre suivant sélectionner l'image ISO du system d'exploitation qui va être installé sur la VM (Windows 7).

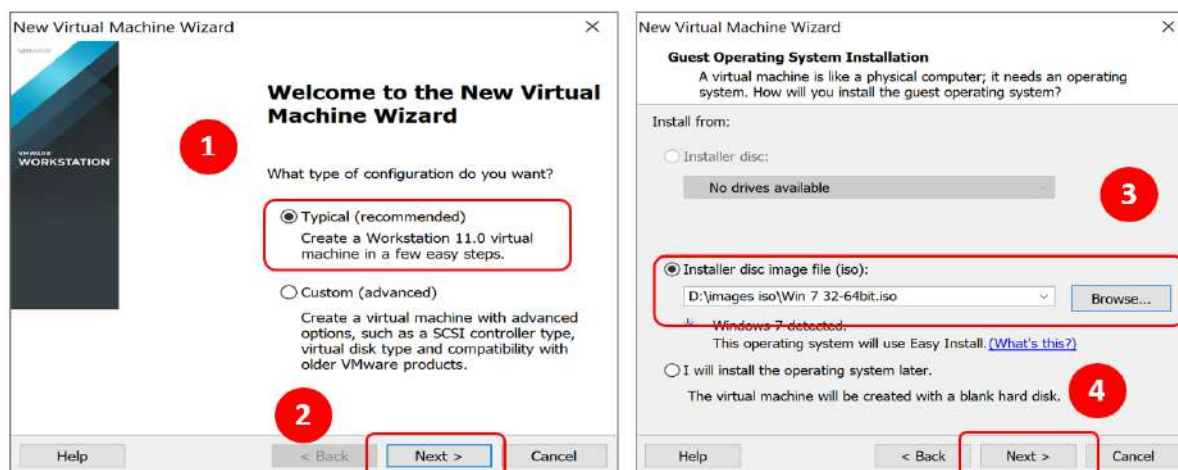


FIGURE 8.20: FENETRE DE CREATION D'UNE NOUVELLE VM

Sur la première fenêtre, introduire la clé d'activation du system Windows 7, ainsi que le nom d'utilisateur et le mot de passe. Cette étape est optionnelle. Dans la fenêtre suivante, changer le nom de votre VM et sélectionnez le dossier dans lequel la VM sera stockée. Le dossier par défaut est (Documents/Virtual Machines).

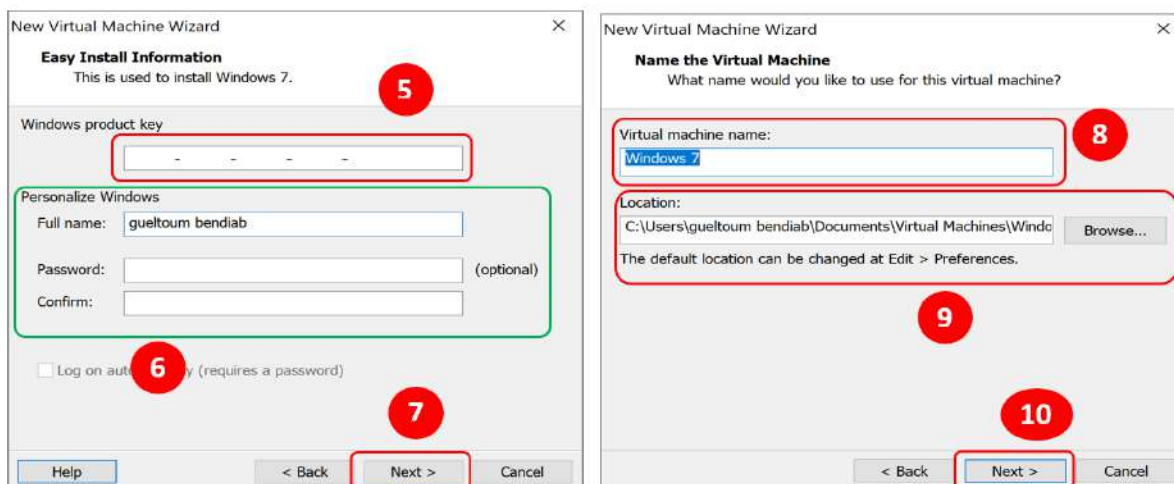


FIGURE 8.21: CLE WINDOWS 7 ET LOCATION DE LA VM

Au-dessous, il est possible d'allouer tout l'espace disque du VMDK (Virtual Machine Disk) à la création et de diviser votre fichier en plusieurs fichiers de 2 Go maximum. Si vous décidez d'allouer tout l'espace disque du VMDK à la création, votre disque virtuel aura une taille fixe qui n'évoluera pas (par exemple 100 Go). Vos fichiers VMDK seront donc plus volumineux, mais vous gagnerez en performance.

Quant à la division du VMDK en plusieurs fichiers de 2 Go, cela permet de déplacer plus facilement la VM sur un autre serveur, mais réduit les performances de la machine.

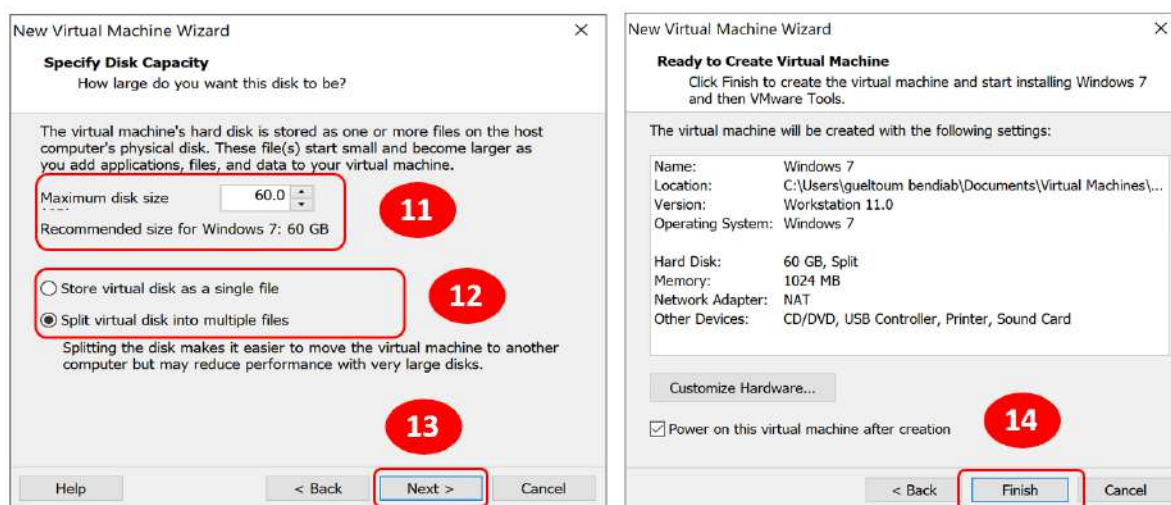


FIGURE 8.22: CONFIGURATION DE DISQUE VMDK

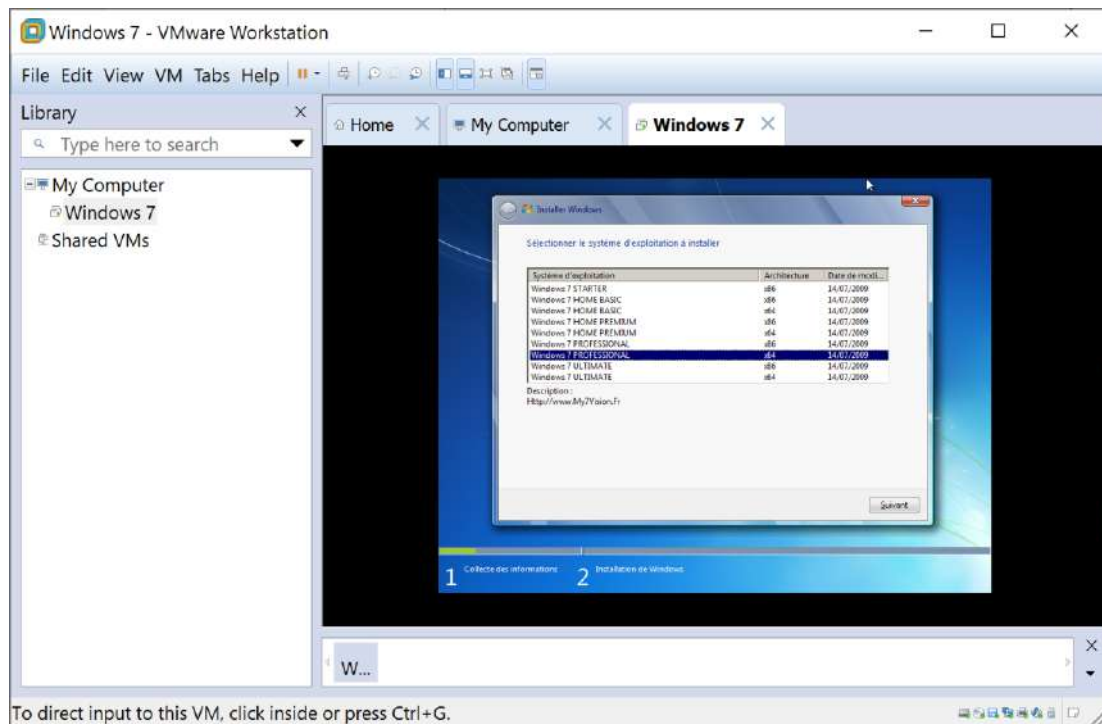


FIGURE 8.23: DEMARRAGE DE L'INSTALLATION DE WINDOWS 7 SUR LA VM

8.4. AJOUT D'UNE VM AU GNS3

Pour ajouter la template de la VM Windows 7 a la liste des équipements de GNS3, aller vers le menu « Edit/Preference », puis sélectionner « VMware VMs/New ». Dans la fenêtre suivante, sélectionner la VM Windows 7 et clique sur le bouton « finish », puis « ok » pour terminer l'importation de la VM.

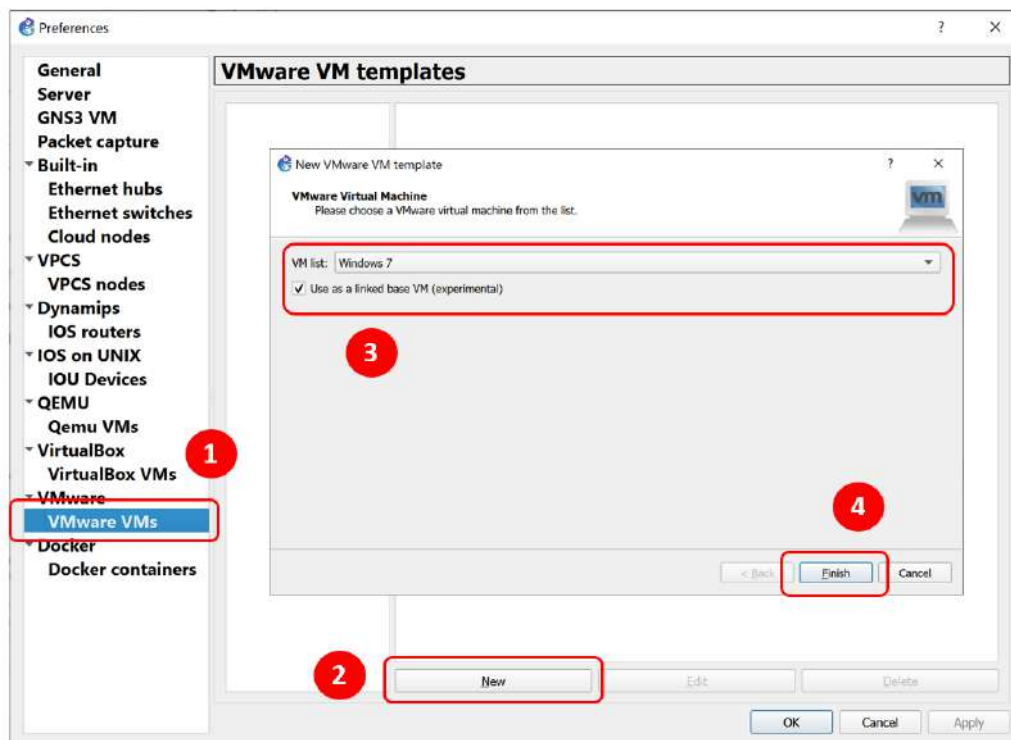


FIGURE 8.24: AJOUT DE LA VM WINDOWS 7 AU GNS3

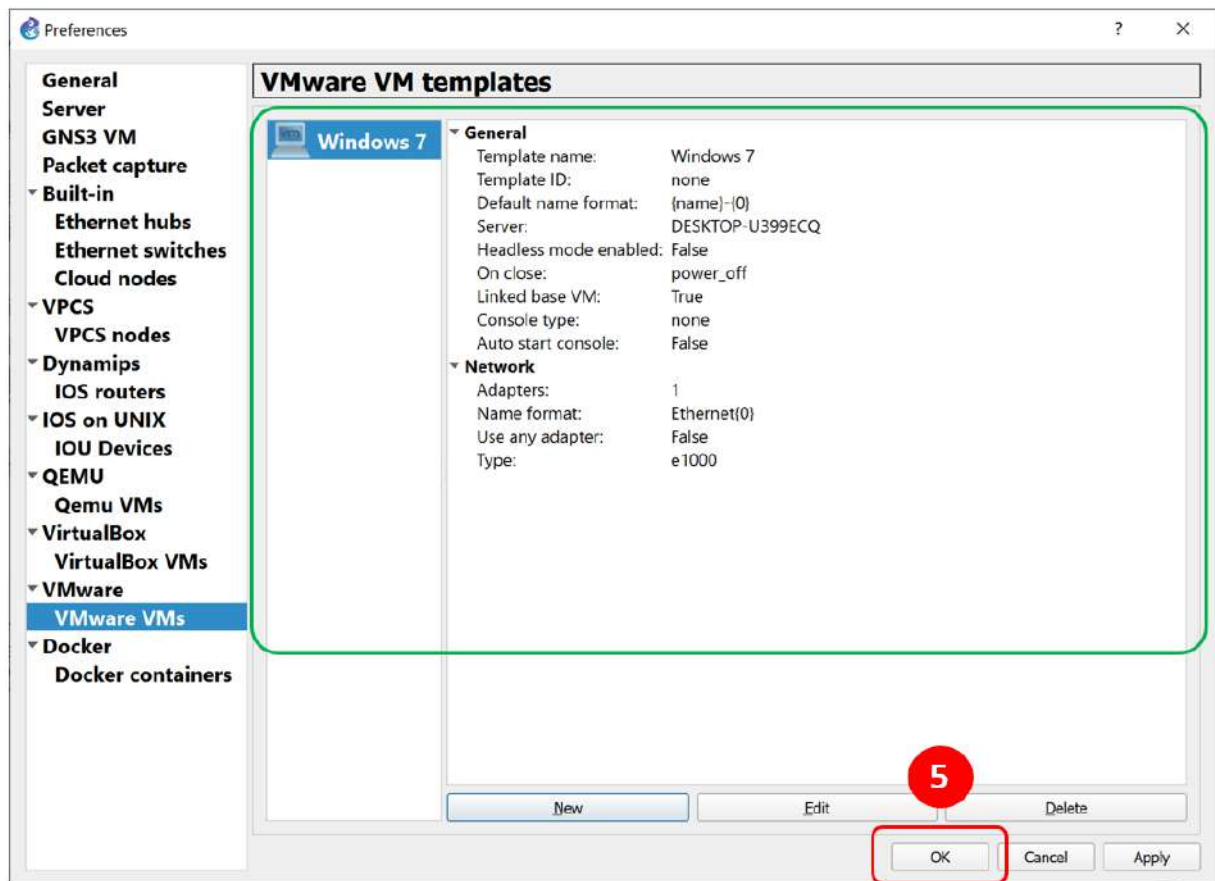


FIGURE 8.25: PARAMETRES DE LA VM WINDOWS 7

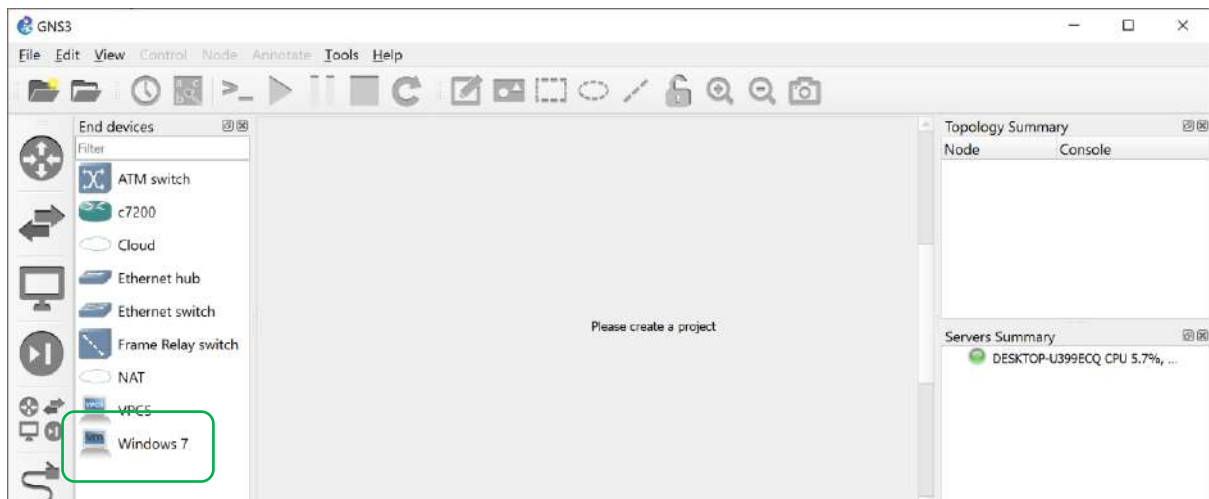


FIGURE 8.26: TEMPLATE DE LA VM WINDOWS 7

8.5. AJOUT D'UNE IMAGE IOS D'UN ROUTEUR CISCO SOUS GNS3

Pour ajouter une image IOS Cisco d'un routeur sous GNS3, aller dans « **Edit / Preferences / IOS routers / New** », puis, sélectionnez l'IOS image de routeur. Dans ce TP nous allons ajouter le retour « **Cisco c7200** ». Cliquez sur le bouton "**Apply**". Puis faites glisser l'icône de routeur sur la droite.

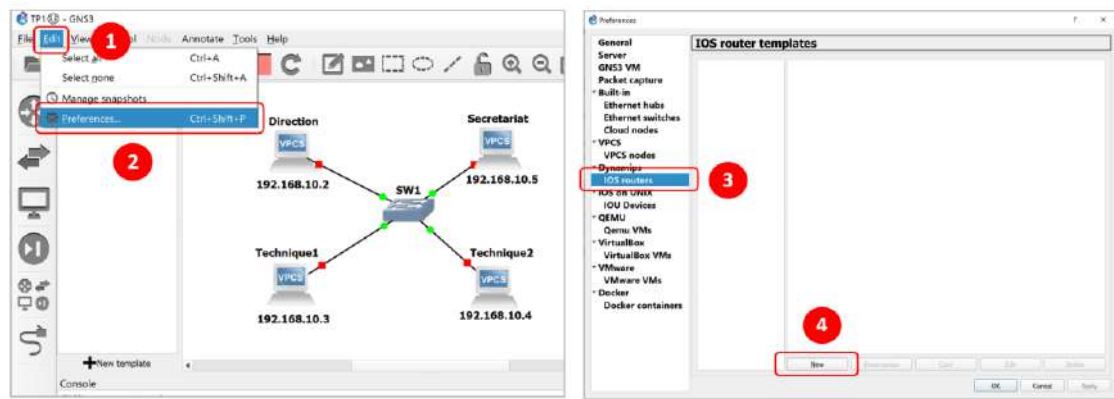


FIGURE 8.27: AJOUT DE L'IMAGE ISO D'UN ROUTEUR

Pour configurer les Connecteurs du routeur. Bouton droit de la souris sur le routeur "R1". Cliquez sur le bouton "**Configurer**". Cliquez sur l'onglet "Slots". Le champ "slot 0:" est associé à "c7200-IO-2FE" c'est-à-dire deux connecteurs fast Ethernet. Sélectionnez, pour le champ "slot 1:", la ligne "PA-1FE-TX". Sélectionnez, pour le champ "slot 2:", la ligne "PA-1-FE-TX".

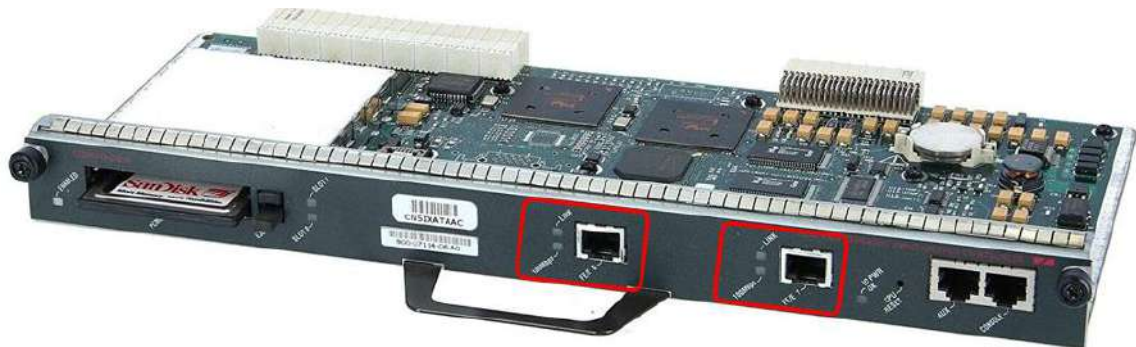


FIGURE 8.28: CISCO C7200-I/O-2FE/E 800-07114-06 7200 INPUT/OUTPUT

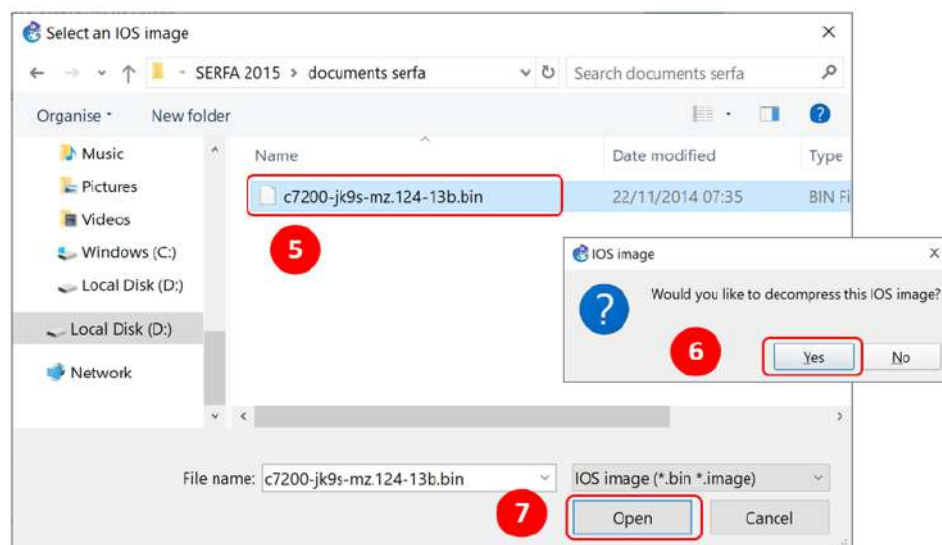


FIGURE 8.29: IMAGE IOS DE ROUTEUR c7200

New IOS router template

IOS image
Please choose an IOS image.

IOS image:

< Back **Next >** Cancel

New IOS router - c7200-jk9s-mz.124-13b.image

Name and platform
Please choose a descriptive name for this new IOS router and verify the platform and chassis.

Name:

Platform:

Chassis:

< Back **Next >** Cancel

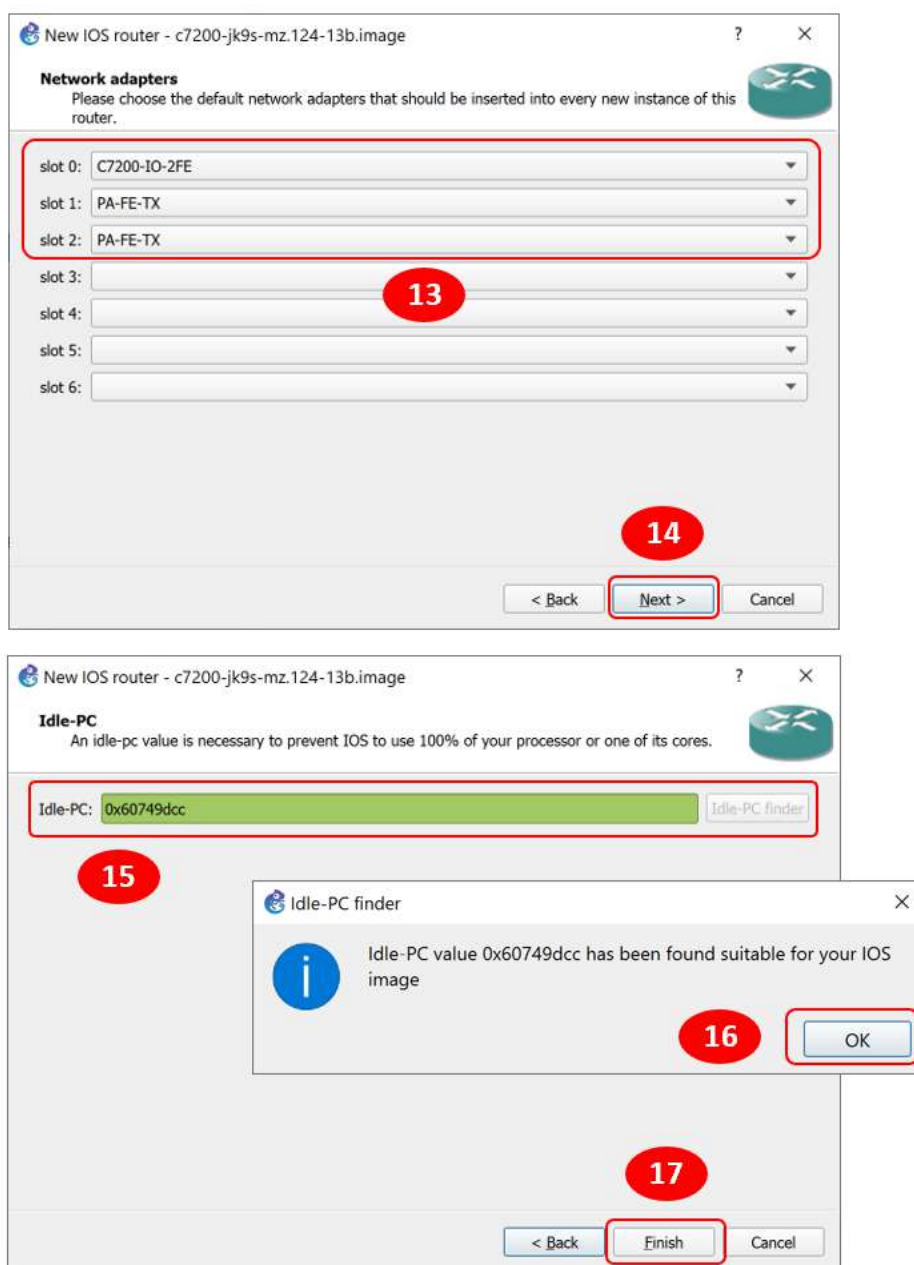
New IOS router - c7200-jk9s-mz.124-13b.image

Memory
Please check the amount of memory (RAM) that you allocate to IOS. Too much or not enough RAM could prevent IOS from starting.

Default RAM:

[Check for minimum and maximum RAM requirement](#)

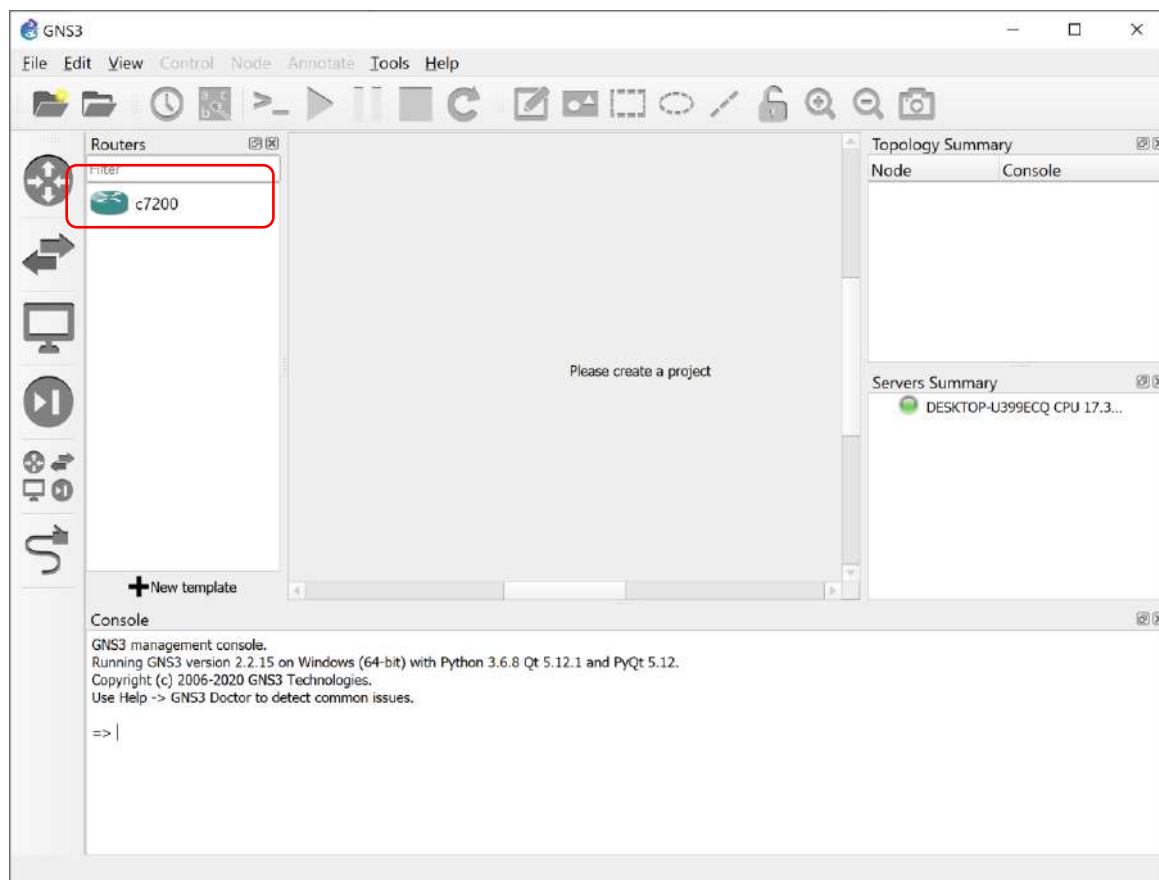
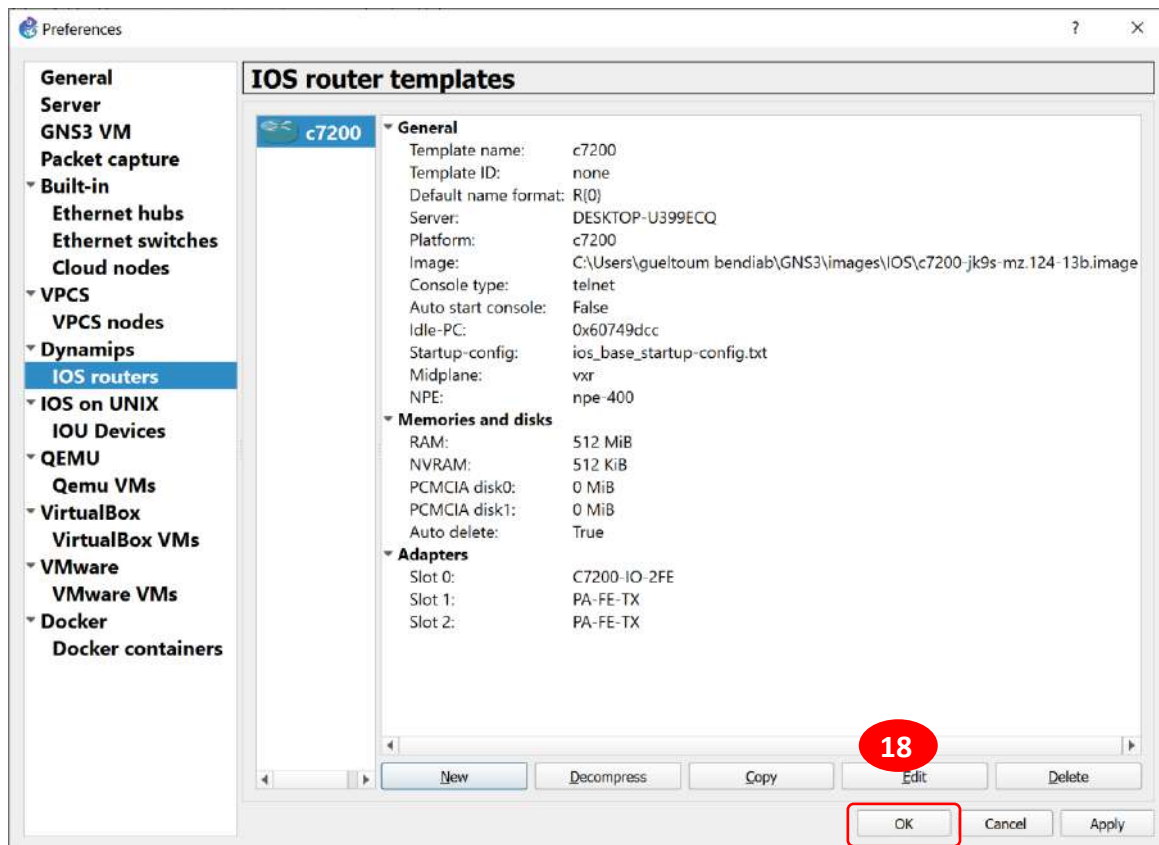
< Back **Next >** Cancel



Le champ "**IDLE-PC**" est une particularité de GNS3. En effet, les utilisateurs de GNS3 rencontrent souvent des difficultés concernant l'utilisation **des ressources CPU par GNS3**, le champ "**IDLE-PC**" est alors utilisé pour répondre à cette problématique. Le problème est que, contrairement à Packet Tracer, GNS3 émule un véritable routeur et l'exécution des instructions est donc faite différemment. **IDLE PC** va en effet, pour chaque image, calculer une valeur qui va permettre l'optimisation et l'économie des ressources pour qu'un réseau virtuel puisse être correctement exécuté sans besoin de ressource considérable.

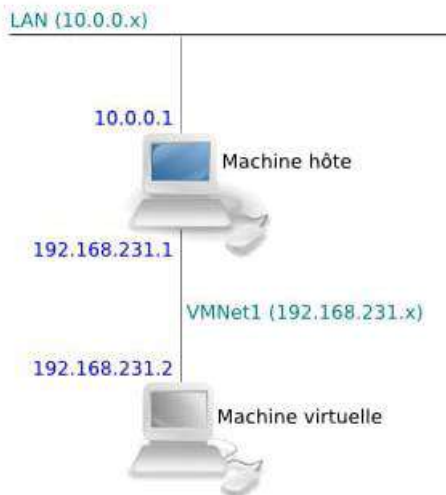
Sur la version actuelle de GNS3 Windows, GNS3 est capable de calculer lui-même cette valeur, ce qui n'est pas forcément le cas dans d'autres versions. Après avoir ajouté l'image, il faut donc simplement cliquer sur le bouton "**Idle-Finder**" (Etape 15).

Après identification de Idle-PC, cliquer sur finish (Etape 17) pour terminer l'importation de l'image IOS du routeur Cisco c7200. La fenêtre suivante montre les informations de configuration du routeur.



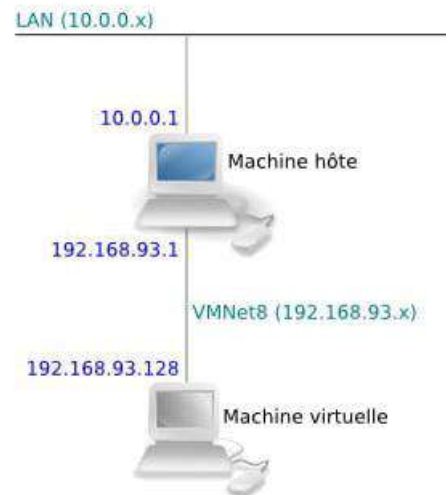
Les types de réseaux VMWare : Quand on crée une machine virtuelle dans VMWare, nous avons le choix entre 3 types de connectivité : Host-only, NAT (Network Address Translation) ou Bridged. Le schéma suivant vous explique la différence entre ces 3 modes [14]:

Machine virtuelle		
	Accès au LAN	Adresse IP de LAN
Host-only	NON	NON
NAT	OUI	NON
Bridged	OUI	OUI



Host-only

La machine virtuelle a accès uniquement à la machine hôte sur un réseau privé virtuel (VMNetX).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine hôte fait office de serveur DHCP pour le réseau VMNet1.



NAT

La machine virtuelle a accès au LAN à travers la machine hôte par un routage de type NAT (Network Address Translation).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine virtuelle envoie ses requêtes sur le LAN en utilisant l'adresse IP de la machine hôte.
Nécessite un LAN opérationnel et connecté.
La machine hôte fait office de serveur DHCP pour le réseau VMNet8.

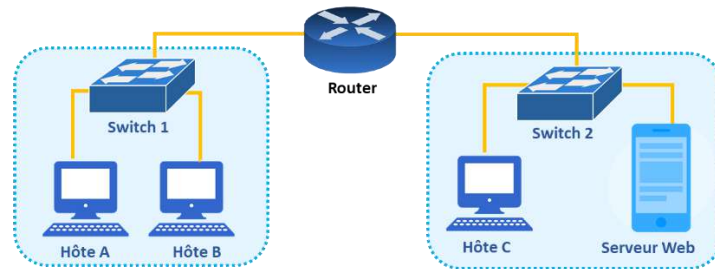


Bridged

La machine virtuelle a accès direct au LAN.
Vu du LAN, il y a une nouvelle machine avec sa propre adresse IP.
Nécessite un LAN opérationnel et connecté.
La machine virtuelle utilise le serveur DHCP du LAN (si présent).

9. EXERCICES

Exercice 1 : Soit la topologie réseau suivante. Quelles sont les configurations requises sur le poste « client A » pour qu'il puisse communiquer avec le serveur Web.



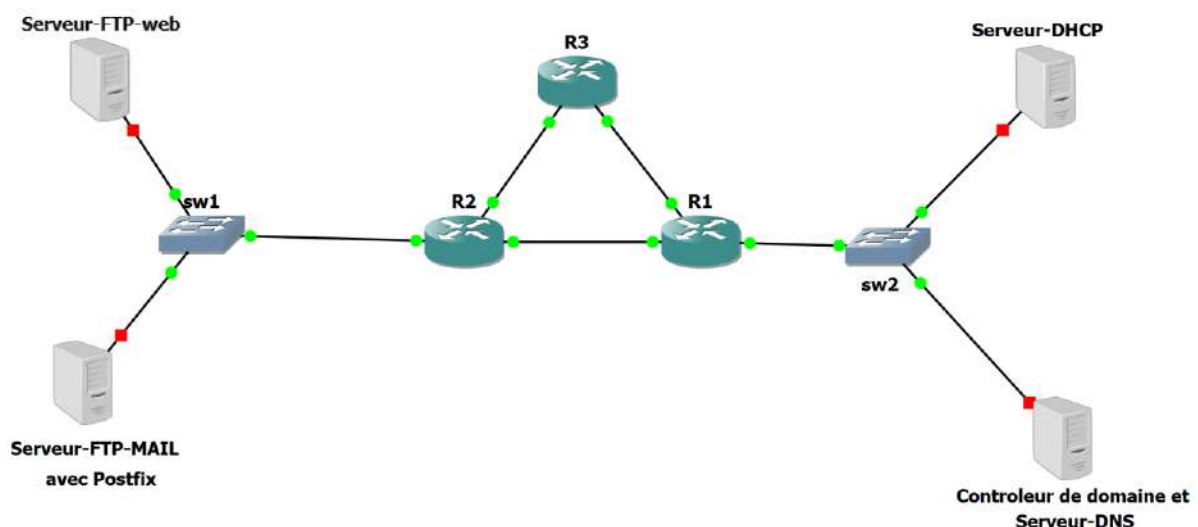
Exercice 2 : Soit un réseau composé d'un un serveur Windows 2003 et 20 postes clients sous Windows 7. Le réseau consiste en un domaine Active Directory nommé « zarzara.edu.dz ». Tous les postes clients doivent avoir des mots de passe complexes. Explique la procédure pour déployer et mettre à jour cette règle de sécurité.

Exercice 3 : Soit un réseau composé de 6 Windows servers , 20 postes clients sous Windows et 30 post clients sous UNIX. L'administrateur du réseau désire mettre en place un serveur DHCP qui pourra fournir une configuration IP aux 2 types de clients et aux serveurs. Les serveurs ne changent pas d'IP. Quelle est la solution IP idéal pour les serveurs ?

- Assigner une adresse IP statique à chaque serveur,
- Créer une réservation client DHCP pour chaque serveur,
- Créer un bail DHCP pour les deux serveurs de six mois,
- Configurer le serveur DHCP de sorte qu'il assigne une adresse IP statique à chaque serveur.

Dans cette situation, quelles sont les avantages de la solution IP sélectionnée et les inconvénients des autres solutions ?

Exercice 4 : (Mini projet) : Créer la topologie réseau suivante en utilisant GNS3, puis proposez un plan d'adressage et tester les connexions entre les hôtes en utilisant la commande ping. Installer et configurer les services DHCP, DNS, FTP/WEB et Mail en utilisant Postfix. Configurer le serveur DNS en tant que contrôleurs de domaine.



QCM à choix multiple : Choisissez la bonne réponse aux questions suivants (Les questions peuvent avoir plusieurs réponses).

- 1) Un fichier de zone dans un serveur DNS contient:
 - A. Enregistrement « NS » (i.e. Serveur de noms)
 - B. Enregistrement « A » de l'hôte
 - C. Alias de nom de l'hôte.
- 2) Si un serveur ne sait pas où trouver l'adresse d'un nom d'hôte, alors ?
 - A. Il demande à son serveur racine.
 - B. Il demande à un serveur adjacent.
 - C. Requête n'est pas traitée.
- 3) La commande « nslookup » permet de :
 - A. Obtenir l'adresse MAC à partir de l'adresse IP
 - B. Attribuer dynamiquement des adresses IP
 - C. Définir le nom du domaine DNS
 - D. Interroger le serveur DNS pour obtenir une adresse IP ou un nom machine.
- 4) Le fichier de configuration principal pour le serveur de noms BIND est :
 - A. /var/named/bind.conf
 - B. /etc/bind.conf
 - C. /etc/named.conf
 - D. /etc/bind/db.local
- 5) Quelle est l'URL correcte pour accéder au fichier « index.html » situé dans le répertoire « /home/user1/ » de la machine « WebServer » ?
 - A. http://WebServer/home/user1/index.html
 - B. http://www.WebServer /home/user1/index.html
 - C. ftp://WebServer/home/user1/index.html
 - D. ssh://WebServer/home/user1/index.html
- 6) Un contrôleur de domaine Active Directory est :
 - A. Un regroupement d'une ou plusieurs arborescences de domaine,
 - B. Un regroupement hiérarchique de plusieurs domaines.
 - C. Un regroupement logique de serveurs et de machines clientes dans un réseau local.
 - D. Le serveur sur lequel l'annuaire Active Directory est hébergé
- 7) Sur quelle couche de modèle TCP/IP fonctionne le protocole DHCP ?
 - A. Internet
 - B. Session
 - C. Application
 - D. Transport
- 8) FTP obéit à un modèle
 - A. Peer-to-Peer (P2P)
 - B. Proactive Provider Participation (P4P)
 - C. Client/serveur
 - D. Tout ce qui précède
- 9) Dans le nom de domaine zarzara.edu.dz, le domaine de premier niveau (en anglais : top-Level Domain, ou TLD) est :
 - A. dz
 - B. zarzara
 - C. Edu
 - D. Aucune de ces réponses

REFERENCES

- [1] “The Book of GNS3,” *Netw. Secur.*, 2015, doi: 10.1016/s1353-4858(15)30067-2.
- [2] R. C. Welsh, *GNS3 Network Simulation Guide*. 2013.
- [3] Geek-university.com, “What is DHCP?,” *geek-university*, 2019. .
- [4] W. Goralski, “Dynamic Host Configuration Protocol,” in *The Illustrated Network*, 2017.
- [5] J. Klensin, “Role of the Domain Name System (DNS),” *Network Working Group*. 2003.
- [6] P. Mockapetris, “Domain Names - Concepts and Facilities,” *Request for Comments*, 1987. .
- [7] P. A. Cricket Liu, *DNS et BIND*, 5th ed. O’Reilly, 2006.
- [8] *Windows Server 2003 Networking Recipes*. 2006.
- [9] M. Gien, “A File Transfer Protocol (FTP),” *Comput. Networks*, 1978, doi: 10.1016/0376-5075(78)90009-0.
- [10] H. Schwichtenberg and H. Schwichtenberg, “Active Directory,” in *Windows PowerShell 5 und PowerShell 7*, 2020.
- [11] K. D. D, *Postfix: The Definitive Guide*, 1st ed. O’Reilly Media, 2003.
- [12] K. Dent, *Postfix : La Référence*, 1st ed. O’Reilly, 2004.
- [13] VMware, “Using VMware Workstation Pro,” *VMWare Inc.*, 2018.
- [14] Yoan, “VMWare et VirtualBox - Les différents types de réseau,” *Comment Ça Marche*, 2010. shorturl.at/gAKQR (accessed May 30, 2021).