الجمهوريةالجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université de 8 Mai 1945 – Guelma -

Faculté des Mathématiques, d'Informatique et des Sciences de la matière

Département d'Informatique

Mémoire de Fin d'études Master

Filière: Informatique

Option: Sciences et Technologies de l'Information et de la Communication

Thème :

Simulation sous GNS3 d'une Solution Réseau Intégrée

Application à l'université 8 Mai 1945, Guelma

Encadré Par :

Berrehouma Nabil

Présenté par :

Belgherbi Zineddine

Octobre 2020

Résumé

Avec l'agrandissement du parc informatique du l'université de 8 Mai 1945, Guelma, Le besoin de la mise en place d'un système intégré pour l'exploitation, la sécurisation et la maintenance est devenue une nécessité absolue. Ces systèmes reposent sur des protocoles réseaux standardisés et répondent à des exigences de performances bien définis. L'objectif de ce projet est de concevoir une architecture réseau qui répond aux besoins de l'université et la configuration des différents protocoles afin d'assurer des services différents tels que les services Web ,Messagerie, DNS. La validation de l'architecture et l'ensemble de protocoles mis en œuvre se fait via simulation sous GNS3.

Mots Clés : Réseaux, Administration , maintenance , sécurité , Simulation , GNS3

With the expansion of the network infrastructure at the University of 8 Mai 1945, Guelma. The need for an integrated system for management , security and troubleshooting has become an absolute necessity. These systems are based on standardized network protocols and meet well-defined performance requirements. The goal of this project is to design a network architecture wich reqponds to the needs of the university and the configuration of the different protocols in order to ensure different services such as Web services, Mail, DNS etc. Architecture validation and protocols implementation are realized under GNS3 simulation.

Dedicace

Toutes les lettres ne sauraient trouver les mots qu'il faut...

Tous les mots ne sauraient exprimer la gratitude,

L'amour, le respect, la reconnaissance...

Aussi, c'est tout simplement que

Je dédie ce mémoire

À mes chers parents ma mère et mon père Pour leur patience, leur amour, leur soutien, et leurs encouragements, Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

À mes adorables enfants, le petit ALI Yasser, Taha Kossaï et Mustapaha Saïf El Islem.

À ma chère femme.

À mes Frères et leurs enfants.

À L'âme de mes chers amis : Titou, Saïf eddine et Hamdi.

À mes amis et mes camarades en particulier Ridha Bousaha, Abd Elmalek, Ahmed et Amar de BAYTEK.

À Tout la famille BELGHERBI et AOUADI.

Sans oublier tous les professeurs que ce soit du primaire, du moyen, du secondaire ou de l'enseignement supérieur.

Remerciements

Il nous est particulièrement agréable avant de présenter notre travail, d'exprimer toute Notre gratitude envers les personnes qui de près ou de loin nous ont apporté leur soutien et sollicitude.

Nous adresserons nos profondes reconnaissances à notre encadreur Mr Berrehouma Nabil, pour sa présence permanent durant la réalisation de ce projet ainsi que son soutient et son aide priseuse.

Nous présentons tous nos respects et nos sincères remerciements aux membres du jury qui ont accepté d'évaluer notre travail.

Nous remercions aussi tous les profs de Master STIC pour leur aide, leur explications pertinentes et conseils précieux qui ont eu un grand impact dans la réussite du projet réalisé.

Enfin Nous voudrions exprimer, également, nos vifs gratitudes et remerciements à Mr le Directeur Opérationnel d'Algérie télécom Guelma Mr BOUMAKH Yacine et le Sous Directeur Technique Mr Chakar Marouane pour leurs soutiens et encouragements ainsi que tous nos responsables et collèges qui nous ont soutenu durant toutes les années universitaires.

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

La politique de numérisation adopté par l'état Algérien dans tous les secteurs et particulièrement dans le secteur de l'enseignement supérieur et de la recherche scientifique impose naturellement la mise en place d'une infrastructure technologique capable non seulement de supporter une charge potentiel de trafic mais aussi une architecture flexible permettant à la fois la facilité de gestion, la maintenance et la protection contre tout acte malintentionné. Pour répondre à ces exigences, plusieurs conditions doivent se réunir. Nous pouvons les résumer dans les points suivants :

1. Un cadre humain qualifié qui veille à la continuité des services.
2. Une pile de logiciels et des systèmes d'information et des des systèmes serveurs (SGBD, Serveurs WEB, Mail,...etc).
3. Un parc des machines dotées des systèmes d'exploitation fiables et peu vulnérables.
4. Un réseau informatique qui fédère toutes les ressources.

Dans ce projet de fin d'étude pour l'obtention du diplôme de Master, nous focalisons sur le dernier point su-cité. Notre mission sera alors la conception d'une architecture réseau pour un parc informatique qui permet à la fois la fluidité du trafic, l'administration, la maintenance et la sécurisation des ressources. Nous projetons notre étude sur notre université de 8 Mai 1945. Le choix de l'université de Guelma était motivé par la présence des problème récurrents concernant la présence du réseaux lui même mais aussi -et qui est plus gênant- la qualité des services qui ne remonte pas à la hauteur de l'université. Dans ce cadre là, nous avons opter pour un stage pratique dans lequel nous avons envisagé de faire une audit qui nous permettra de :

1. Analyser les besoins réels en termes de réseau et des services réseaux.
2. Faire une anatomie du réseau existant.
3. Repérer les points faibles et le point forts.
4. Construire une plate-forme de base pour concevoir la nouvelle architecture.
5. Proposer nos solutions aux insuffisances constatés.

.

Malheureusement, nos démarches de stage ont été été interrompus à cause de la suspension de toutes les activités de l'université suite au confinement générale dictée par la tutelle pour prévenir contre la pandémie de COVID-19. Nous avons décider par conséquence de réorganiser notre plan d'action en remplaçant le stage par des scénarios de simulation standards valables pour toutes les organisations.

Pour bien mener ce travail, nous avons suivie une démarche qui s'articule sur deux axes :

1. Un mémoire auto suffisant (Self-Contained) où le lecteur trouve toutes les connaissances nécessaires dedans.
2. Un contenu purement pratique qui permet aux lecteurs d'acquérir les compétences minimales pour configurer un réseau et ses services.

En tenant compte de ces axes, nous avons organisé notre mémoire en cinq (5) chapitres dont le contenu est brièvement décrit dans les points suivant :

— **chapitre1 :** Consacré aux concepts fondamentaux des réseaux. Vu la limite d'espace et l'étendu du domaine des réseaux, nous nous présenterons durant ce chapitres que quelques protocoles des couches liaison et réseau particulièrement et qui vont nous servir dans les prochains chapitres.

— **chapitre 2 :** Dédié à l'administration des réseaux dans un environnement Linux. En effet, La compréhension de Linux joue un rôle primordial dans la maîtrise des différents services réseaux.

— **chapitre 3 :** Couvre le puissant eco-système GNS3 qui permet de simuler , émuler et même virtualiser une large variété des systèmes d'exploitation. GNS3 se distingue par sa capacité de s'intégrer avec l'analyseur de trafic Wirechark pour analyser tous les protocoles envisageables.

— **chapitre 4 :** Travailler avec des équipements réseaux de type Cisco ne se peut faire sans maîtriser son système d'exploitation réseau appelé IOS. Durant ce chapitre, nous donnerons une introduction aux différentes manipulations nécessaires pour achever les configurations faites à travers les scénarios de simulation dans le dernier chapitre.

— **chapitre 5 :** La concrétisation de tout ce que nous avons abordé dans les chapitres précédents est présenté à travers des scénarios de simulations en considérant toujours des cas qui représente notre université.

CHAPITRE 1

Généralités sur les Réseaux

1.1 Introduction :

Avant de s'approfondir dans l'essentiel du notre projet , il est recommandé de commencer par discuter les fondamentaux des réseaux informatiques. Vu l'étendu du domaine . Nous ne présentons que des définitions assez larges qui couvrent uniquement les points que nous allons aborder dans les prochains chapitres. vu son caractère généraliste et devant les contraintes du temps qui nous ont été imposés. Nous avons complètement inspiré le contenu de ce chapitre des mémoires du master [BOU15], [BOU16] pour qu'on puisse consacrer plus de temps à l'essentiel de notre projet.

1.2 Définition d'un Réseau :

Un réseau connecte un ensemble d'équipements informatiques (ordinateur, périphériques...etc) entre eux via des supports de communication comme le réseau filaire ou le réseau sans fil, qui gérera l'accès à l'Internet, e-mails, aux droits d'accès partagés aux documents et le travail collaboratif. La plupart des réseaux informatiques sont classés en réseaux locaux LAN et WAN.

1.3 Réseaux LAN (Local Area Network) :

Les réseaux locaux, ou LAN (réseaux locaux), correspondent en taille aux réseaux intra société. Ils sont utilisés pour transporter toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.

1.4 Réseaux Wan (Wide Area Network) :

Les réseaux étendus, ou WAN (Wide Area Network), sont destinés à transporter des données numérique sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et dans ce cas il utilise des infrastructures au niveau du au sol, principalement de grands réseaux à fibre optique, soit sans fil, tels que les réseaux Satellite.

1.5 Le modèle OSI :

Le modèle OSI (Open Interconnection Model) [Zim80] est un modèle standard universel des réseau à 7 couches développé par l'organisation ISO (Organisation internationale de normalisation) En 1984, ces différentes couches ont été identifiées sur la base de ces caractéristiques Selon les exigences ISO :

- Définissez précisément les services et les opérations de chaque couche.
- Définit le fonctionnement de chaque couche selon le protocole standardisation. Le modèle OSI comporte sept couches, comme le montre la figure ci-dessous De bas en haut. Ces couches sont parfois divisées en deux groupes.

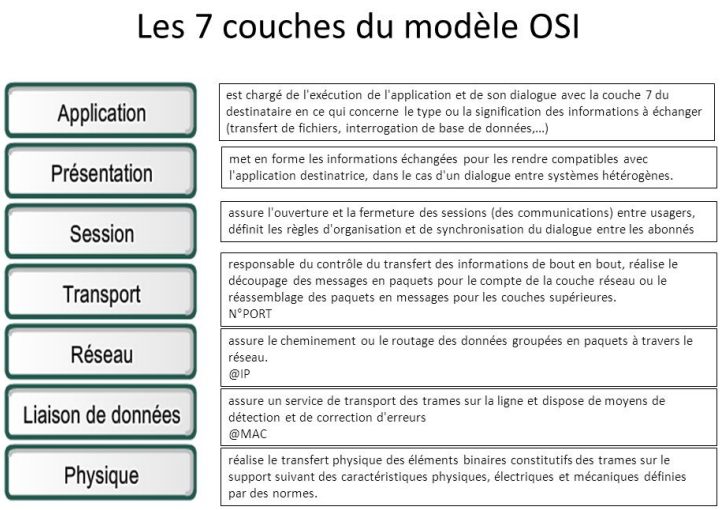

FIGURE 1.1 – Les 7 couches du modèle OSI

1.6 Le modèle TCP /IP :

Le protocole TCP / IP [MS13] a été développé à l'origine par le département américain de la Défense en En 1981, l'évolution du concept qui a été partiellement utilisé dans le réseau historique ARPAnet a été proposée (1972) et est largement utilisé sur Internet. Au-delà de l'apparence L'histoire de TCP / IP est également attribuée à son succès indépendamment de tout constructeur l'informatique. Les deux principaux protocoles définis dans l'architecture TCP / IP sont :

- **IP (Internet Protocol) :**, au niveau du réseau, fournit un service sans connexion.
- **TCP (Transmission Control Protocol)**, niveau de transmission, via lien. Le modèle TCP / IP comporte quatre couches, comme illustré dans la figure ci-dessous.

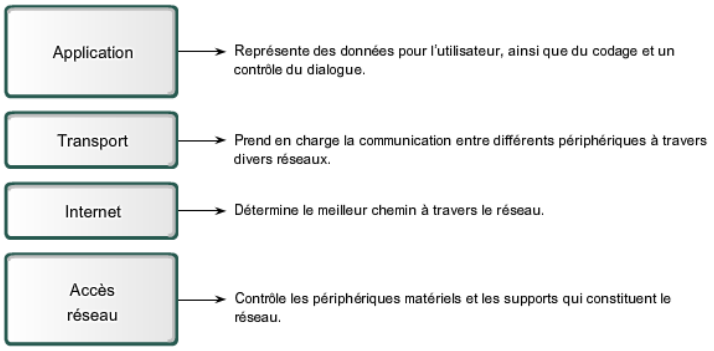

FIGURE 1.2 – Modèle en couche TCP/IP

La couche physique :

La couche réseau intègre les services de la couche physique et de la couche liaison du modèle OSI, et est chargée de communiquer avec l'interface physique afin de transmettre ou de restaurer les paquets de données transmis de la couche supérieure à l'interface. L'interface n'est pas clairement définie car elle dépend du réseau et du nœud utilisés.

La couche Transport :

La couche de transport parvient à diviser et à réassembler les paquets de données dans le flux de données à transmettre. Cette couche gère également le réarrangement ordonné de tous les paquets de données du même message. Les deux principaux protocoles qui peuvent fournir cette couche de service sont :
1. TCP (Transmission Control Protocol) : Un protocole fiable qui garantit une communication sans erreur via un mécanisme de question / réponse / synchronisation.
2. UDP (User Datagram Protocol) : Un protocole peu fiable qui ne peut pas assurer une communication rapide, mais qui utilise le mécanisme de question / réponse peut contenir des erreurs.

La couche Application :

La couche application correspond à différentes applications qui utilisent les services réseau pour communiquer sur le réseau. Un grand nombre de différents protocoles de haut niveau fournissent des services à cette couche :

- **Telnet :** Connexion à distance.
- **FTP (File Transfer Protocol) :** File Transfer Protocol.
- **http (Hypertext Transfer Protocol) :** Hypertext Transfer Protocol.
- **DNS (Domain Name System) :** Domain Name System.

1.7 Les équipements de base d'un réseau informatique :

Les unités hôte :

L'hôte est une unité directement connectée au segment réseau, et on peut les trouver sous la forme d'un ordinateur, serveur, scanner ou imprimante.

Les commutateurs (Switch) :

Un commutateur réseau est un appareil qui connecte plusieurs câbles ou fibres optiques dans un réseau informatique ou un réseau de télécommunications. Avec les commutateurs, vous pouvez créer des circuits virtuels et diriger des informations vers des destinations spécifiques sur le réseau. Contrairement à un concentrateur qui envoie des informations à tous les ordinateurs via un concentrateur, l'utilisation d'un commutateur peut protéger la sécurité des informations transmises sur le réseau, et le commutateur envoie uniquement les données aux destinataires qui ont besoin de recevoir les données. L'échange est un mode de transmission de trames dans les ordinateurs et les réseaux de communication.

Les routeurs :

Le routeur est l'élément intermédiaire reliant les deux réseaux. Il fournit le routage Paquets de données d'une interface à une autre interface. Il fonctionne sur la troisième couche du modèle OSI (couche réseau). La plupart des routeurs peuvent déterminer automatiquement Utilisez l'itinéraire le plus approprié entre le point de départ et le point d'arrivée. Autoriser Organisez le forfait avec le meilleur itinéraire. Pour amorcer les informations, le routeur doit Comprendre le protocole utilisé, qui est la langue utilisée par l'ordinateur Communication, par exemple : TCP / IP, TCP, IP.

1.8 Les protocoles LAN (protocoles de niveau 2) :

Les VLAN : Virtual LAN :

VLAN (Virtual Local Area Network ou Virtual Local Area Network en français Virtual Local Area Network) est Un réseau local regroupe un groupe d'ordinateurs de manière logique et non physique. Le VLAN est un réseau logique de couche 2, et le VLAN a été normalisé selon la spécification IEEE 802.1Q. [BOU15] Cependant, il y a encore des changements d'implémentation d'un fabricant à un autre.

Agrégation de VLAN :

L'agrégation est un lien point à point entre deux périphériques réseau qui transporte plusieurs VLAN vers l'ensemble du réseau. La jonction VLAN n'appartient pas à un VLAN spécifique, mais fournit un conduit pour le VLAN entre le commutateur et le routeur.

VLAN Trunking protocol, VTP :

À mesure que le nombre de commutateurs dans les réseaux des petites et moyennes entreprises augmente, la gestion globale requise pour gérer les réseaux locaux virtuels (VLAN) et les jonctions réseau devient plus difficile. VTP est un protocole propriétaire de Cisco. Il est utilisé pour gérer de manière centralisée les VLAN, de sorte que vous pouvez vous connecter plusieurs fois pour ajouter, modifier ou supprimer des commutateurs de configuration VLAN sans administrateur réseau. Ce protocole définit le concept de domaine VTP, qui regroupe les commutateurs afin qu'ils puissent échanger leur configuration, ainsi que trois modes de fonctionnement que l'appareil peut adopter :

1. Mode serveur, où le commutateur est responsable de la configuration de diffusion Vers le commutateur dans le domaine VTP (créer, supprimer et modifier VLAN).

2. Mode client, où le commutateur sera appliqué par Passez en mode serveur.

3. Mode transparent, dans ce mode, le commutateur ne diffuse et ne le reçoit pas Considérez la configuration du domaine VTP auquel il appartient.

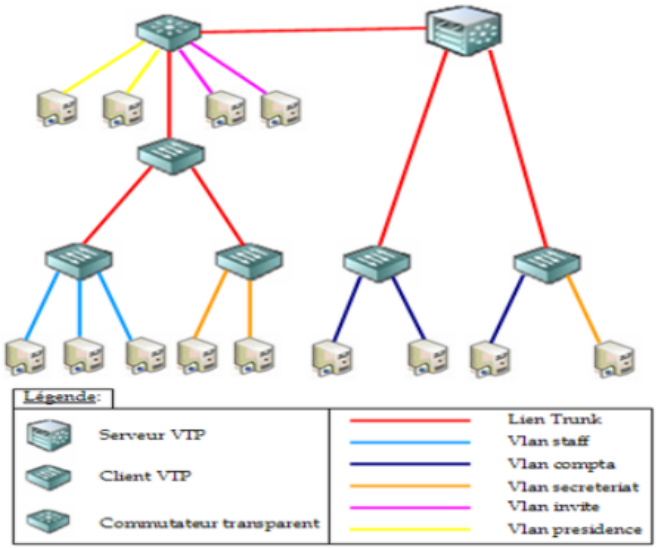

FIGURE 1.3 – VLAN Truncking Protocol.

Si l'une des conditions suivantes n'est pas remplie, le domaine VTP sera invalide et Les informations ne se répandront pas :

- Vous devez attribuer le même nom de domaine VTP à chaque commutateur.
- L'option de relais pour l'interconnexion des commutateurs doit être activée. Le serveur diffuse la liste VLAN. Le paquet publicitaire VTP se compose de Amendement No. Le numéro de révision le plus élevé sera le numéro de version de la base de données modifiée VLAN. Il se propage sur la liaison relais. Le commutateur en mode transparent a sa propre liste. Cette liste n'est pas diffusée sur le réseau, mais les paquets VTP sont diffusés.

Trame VTP :

Si l'une des conditions suivantes n'est pas remplie, le domaine VTP sera invalide et Les informations ne se répandront pas :

- Vous devez attribuer le même nom de domaine VTP à chaque commutateur.
- L'option de relais pour l'interconnexion des commutateurs doit être activée. Le serveur diffuse la liste VLAN. Le paquet publicitaire VTP se compose de Amendement No. Le numéro de révision le plus élevé sera le numéro de version de la base de données modifiée VLAN. Il se propage sur la liaison relais. Le commutateur en mode transparent a sa propre liste. Cette liste n'est pas diffusée sur le réseau, mais les paquets VTP sont diffusés.

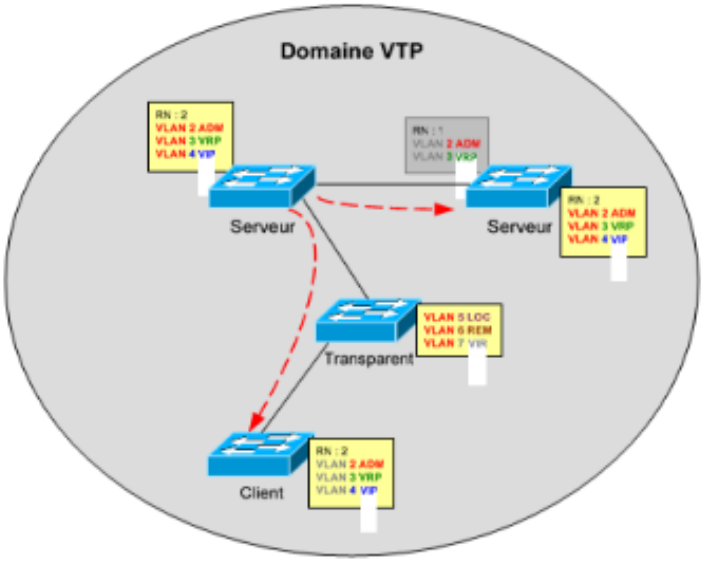

FIGURE 1.4 – Protocole VTP.

Le protocole STP (Spanning-Tree Protocol) :

STP est un protocole de couche 2 adapté aux ponts et commutateurs. La spécification de STP est IEEE 802.1. Le but principal du protocole est de vérifier s'il existe des chemins redondants dans le réseau, car cela est fatal, donc aucune boucle n'est créée.

Principe du STP :

STP utilise l'algorithme Spanning Tree (STA) pour déterminer quels ports de commutateur doivent être configurés comme bloqués pour éviter les boucles sur le réseau [BOU16]. L'algorithme STA désigne un seul commutateur comme pont racine et l'utilise comme point de référence pour calculer tous les chemins. Tous les commutateurs liés au STP échangent des trames BPDU pour identifier le commutateur avec l'identificateur de pont le plus faible (BID) sur le réseau. Le commutateur avec l'identifiant (ID) le plus bas deviendra automatiquement le pont racine utilisé pour calculer l'algorithme STA. BPDU est un télégramme

échangé par le commutateur pour le protocole STP. Chaque trame BPDU contient un identifiant de pont, qui est utilisé pour identifier le commutateur qui envoie la trame BPDU. L'identifiant de pont contient la valeur de priorité, l'adresse MAC du commutateur d'envoi et l'ID système étendu en option. La valeur d'identificateur de pont la plus basse est déterminée par la combinaison de ces trois champs. Après avoir déterminé le pont racine, l'algorithme STA configurera le port du commutateur en tant que rôle de port indépendant. Le rôle de port décrit le lien entre le port et le pont racine du réseau et spécifie s'ils sont autorisés à transporter du trafic.

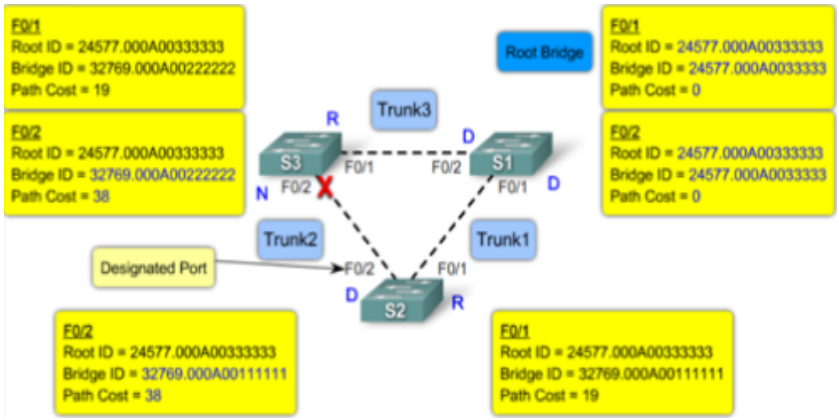

FIGURE 1.5 – Principe du VTP.

1.9 Les protocoles de niveau 3 :

L'adressage IP :

L'adresse IP est un numéro unique utilisé pour identifier chaque ordinateur connecté au réseau. Le numéro est divisé en 4 par 8 chiffres, allant de 0 à 255, séparés par des points. L'adresse IP est divisée en deux parties, la partie réseau et la partie hôte. Le premier identifie le réseau auquel la machine est connectée et le second identifie la machine connectée à ce réseau. Pour identifier ces deux parties, chaque adresse est liée à un masque de sous-réseau qui vous permet de définir le réseau sur lequel elle se trouve. Les adresses IP sont divisées en plusieurs catégories :

- Les adresses IP de classe A : 0 à 127.
- Les adresses IP de classe B : 128 à 191.
- Les adresses IP de classe C : 192 à 223.
- Les adresses IP de classe D : 224 à 239.
- Les adresses IP de classe E : 240 à 255.

Adresse de diffusion :

L'adresse de diffusion est une adresse qui peut spécifier toutes les adresses Connectez l'ordinateur au réseau en définissant tous les bits de la partie machine sur un (1).

Adresse privée :

Pour éviter toute ambiguïté avec les adresses réseau et les adresses de diffusion, " Pour spécifier des ordinateurs sur le réseau, il n'est pas recommandé d'utiliser "zéro" et "tous les uns". Dans chaque type d'adresse, certaines adresses réseau sont réservées aux réseaux privés.

- Classe A : 10.0.0.0 à 10.255.255.255 .
- Classe B : 172.16.0.0 à 172.255.255.255 .
- Classe C : 192.168.0.0 à 192.255.255.255 .

Masque de sous-réseau :

Le masque de sous-réseau est une donnée qui dépasse pas 4 octets, plus l'adresse de sous-réseau, Caractérisez l'adresse IP du sous-réseau. Si tout, le bit du masque de sous-réseau est 1 Adresse IP de sous-réseau, le même bit est le même pour l'adresse IP et le sous-réseau. Par exemple, pour le réseau de classe A 10.0.0.0 avec le masque de sous-réseau 255.0.0.0, les 8 premiers bits de toutes les adresses IP du sous-réseau valent 10. Autre exemple : pour le sous-réseau de classe C 192.54.47.0 et le masque de sous-réseau 255.255.255.0, les 24 premiers bits de toutes les IP du sous-réseau sont 192.54.47. Nous pouvons spécifier le sous-réseau par son adresse et son masque, mais nous pouvons également concevoir le sous-réseau en ne donnant que le nombre de bits du masque. Ensuite nous parlons Les deux premiers exemples utilisant des sous-réseaux 10.0.0.0/8 ou du sous-réseau 192.54.47.0/24.

Le Routage :

Le routage est le processus de sélection du chemin à transmettre dans le réseau Données de l'expéditeur vers un ou plusieurs destinataires, cette fonctionnalité utilise Algorithme de routage et table de routage [SF99]. Le périphérique de routage principal est un routeur, qui utilise une adresse IP pour diriger les paquets de données d'un réseau vers un autre, et doit également maintenir sa table de routage à jour et être conscient des changements qu'il peut apporter via d'autres périphériques. Expédition des paquets. Il existe deux méthodes pour remplir manuellement (routage statique) ou pour remplir et mettre à jour dynamiquement la table de routage.

Types de Routage :

Il existe deux modes de routage très différents lorsque nous allons résoudre les paramètres Protocole de routage, c'est le routage statique et le routage dynamique :

1. Le routage statique : Dans le routage statique, la table est remplie manuellement Administrateur réseau. Il est utilisé pour les petits réseaux ou les réseaux terminaux. RÉ- L'administrateur doit gérer le routage de chaque unité de routage du réseau. Ces routages Statique ne s'adapte pas aux changements de l'environnement réseau, les informations sont Mettez à jour manuellement à chaque changement de topologie dans le réseau.

2. le routage dynamique : Avec le routage dynamique, la table sera automatiquement remplie. Nous configurons un protocole qui sera chargé d'établir la topologie et de remplir la table de routage. Les

protocoles de routage dynamique sont utilisés dans les grands réseaux. Le routage dynamique permet également de modifier automatiquement la table de routage en cas d'interruption de liaison du routeur. Il vous permet également de choisir le meilleur itinéraire disponible d'un réseau à un autre.

Les protocoles de routage :

Le but de tous les protocoles de routage est de maintenir la table de routage des différents routeurs. pour cette fin, le protocole diffuse des informations de routage vers d'autres systèmes du réseau afin que les modifications de la table de routage sont tenu en compte pour la mise à jour des différents table de routage. les protocole de routage sont conçu pour améliorer la vitesse de routage, pas besoin de configurer manuellement toutes les routes, économisant ainsi du temps sur chaque routeur, améliorez la stabilité du réseau en sélectionnant à chaque fois le meilleur itinéraire. Les protocoles de routage peuvent être divisés en deux catégories :

– **Les protocoles à vecteur de distance.**

– **Les protocoles à état de liens.**

1. Les protocoles à vecteur de distance : Le protocole de routage à vecteur de distance utilise un algorithme de routage qui ajoute les distances pour trouver le meilleur itinéraire (Bellman-Ford). Habituellement, chaque routeur envoie sa table de routage entière à ses voisins. Il sont très sensibles aux boucles de routage. Ce type de méthode compte le nombre de sauts entre deux endroits, et en fonction de ce nombre de sauts, il choisira l'itinéraire le plus court. Nous citerons RIP et IGRP.

- **RIP :** Routing Information Protocol, qui est un protocole à vecteur de distance , c'est-à-dire la distance de communication entre chaque routeur et les autres routeurs (le nombre de sauts entre eux). Par conséquent, lorsque le routeur reçoit l'un de ces messages, il augmentera cette distance de un et transmettra le message au routeur directement accessible. Par conséquent, le routeur peut maintenir le meilleur itinéraire du message de cette manière en stockant l'adresse du routeur suivant dans la table de routage, minimisant ainsi le nombre de sauts vers le réseau.
- **IGRP :** (Interior Gatway Routing Protocol) est un protocole propriétaire développé par Cisco Systems, qui est plus robuste et moins restrictif que RIP. EIGRP (Extended Interior Gateway Routing Protocol) est une version avancée de IGRP.

2. Les protocoles à état de liens : Le protocole de routage d'état de liaison utilise un algorithme plus efficace (Dijkstra ou chemin le plus court en premier). Le routeur collecte tous les coûts de liaison de son point de vue et construit une arborescence de tous les chemins. Intégrez ensuite le meilleur itinéraire dans la table de routage. L'avantage de ces algorithmes est qu'ils fournissent une convergence rapide sans boucle ni multiacheminement. Nous citerons OSPF.

- **OSPF :** (Open Shortest Path First),Il est plus efficace que RIP, il le remplace donc progressivement. Contrairement à RIP, ce protocole n'envoie pas le nombre de sauts entre eux, aux routeurs voisins, mais leur envoie l'état de la liaison. De cette manière, chaque routeur peut mapper l'état du réseau, afin de pouvoir choisir à tout moment la route la plus appropriée pour le message. De plus, ce protocole peut empêcher les routeurs intermédiaires d'augmenter le nombre de sauts, réduisant ainsi la génération d'informations, obtenant ainsi une meilleure bande passante disponible que RIP.

1.10 Conclusion

Après cette passage rapide sur les concepts fondamentaux des réseaux nécessaire pour toute personne désirant aborder les sujets des réseaux. Nous commençons a partir du prochain chapitre la discussion des éléments pratiques des réseaux commençant d'abord par la maîtrise de l'environnement Linux.

CHAPITRE 2

Administration Réseaux sous Linux

2.1 Introduction :

Après une brève vol d'horizon des fondamentaux des réseaux dans le chapitre précédent. Nous nous penchons dans ce chapitre sur l'étude des principaux commandes Linux qui nous permet de configurer les machines impliquées dans le réseau. Linux avec son noyaux très stables constitue le systèmes d'exploitation de base de plusieurs équipements réseau allant des routeurs aux switchers ainsi que des pare feu (Firewall) matériels. Il est d'ores et déjà le système d'exploitation de référence pour le déploiement des différents serveurs.

2.2 Configuration d'une station :

Adresses IP et adresse MAC :

Chaque interface de chaque ordinateur sera identifié par
1. son adresse IP : une adresse IP (version 4, protocole IPV4) permet d'identifier un hôte et un sous-réseau. L'adresse IP est codée sur 4 octets. (les adresses IPV6, ou IP next generation seront codées sur 6 octets).
2. L'adresse mac de sa carte réseau (carte ethernet ou carte wifi). Une adresse IP permet d'identifier un hôte. Une passerelle est un ordinateur qui possède plusieurs interfaces et qui transmet les paquets d'une interface à l'autre. La passerelle peut ainsi faire communiquer différents réseaux. Chaque carte réseau possède une adresse MAC unique garantie par le constructeur. Lorsqu'un ordinateur a plusieurs plusieurs interfaces, chacune possède sa propre adresse MAC et son adresse IP. On peut voir sa configuration réseau par la commande ifconfig.

Configurer les interfaces à la main avec ifconfig :

La commande ifconfig permet de connaître la configuration réseaux et de configurer le réseau à la main ou dans un script [Ton05]. Le script suivant montre le résultat de cette commande.

```
root@webserver1:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.2  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::883:b2ff:fea2:b71e  prefixlen 64  scopeid 0x20<link>
        ether 0a:83:b2:a2:b7:1e  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 908 (908.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 508 (508.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 508 (508.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

FIGURE 2.1 – résultat de l'exécution de la commande *ifconfig* sans options

Pour obtenir ce résultat, il faut que la machine soit connectée par un câble ethernet à un routeur (ou un modem-routeur) qui définisse le sous-réseau 192.168.0. On configure alors la station avec ifconfig :

```
  ifconfig eth0 192.168.0.2
```

Pour déconfigurer l'interface eth0

```
  # ifconfig eth0 down
```

FIGURE 2.2 – configurer/ dé-configurer l'interface *eth0* avec *ifconfig*

(vérifier avec ifconfig : l'interface eth0 n'apparaît plus).

Le fichier resolv.conf et la résolution des noms :

Pour accéder à une machine à partir de son nom, notre station doit résoudre l'hôte, c'est à dire qu'elle doit trouver l'adresse IP de l'hôte à partir de son nom. Pour celà, notre station doit accéder à un serveur, appelé serveur de noms ou DNS [SS06]. Ce server connaît les adresses IP correspondant à tous les noms d'hôte. Le fichier /etc/resolv.conf contient les adresses IP d'un ou plusieurs serveurs de noms. Voici un exemple :

```
# cat/etc/hosts
# adresse IP Nom d'hôte
127.0.0.1 localhost
127.0.1.1 portabel
192.168.0.1 router
192.168.0.17 printer
208.77.188.166 example.com
...
```

FIGURE 2.3 – correspondances nom de machine –> adresse IP dans le fichier /etc/hosts

Gérer la configuration dans le fichier interfaces :

La configuration d'une interface avec ifconfig n'est pas enregistrée sur le disque, et en particulier, elle n'est pas conservée en cas de réinitialisation du système (reboot). Pour enregistrer la configuration de manière permanente, if faut créer cette configuration dans un fichier de configuration. La configuration des interfaces utilisée lors de l'initialisation du réseau est contenue dans le fichier /etc/network/interfaces. Pour initialiser le réseau après configuration, il faut faire :

```
# /etc/init.d/networking start ou
# /etc/init.d/networking restart.
```

FIGURE 2.4 – ré-initialisation du réseau après reconfiguration des interfaces

```
#cat /etc/network/interfaces
# This is a sample network config uncomment lines to configure the network
# Static config for eth0
auto eth0
iface eth0 inet static
address 192.168.2.2
netmask 255.255.255.0
gateway 192.168.2.1
up echo nameserver 192.168.2.1 > /etc/resolv.conf

# DHCP config for eth0
 auto eth1
 iface eth1 inet dhcp
```

FIGURE 2.5 – configuration permanente des interfaces dans le fichier /etc/network/interfaces

2.3 Routage :

Le routage permet de faire communiquer plusieurs sous-réseaux. Une passerelle (en anglais gateway) est en communication avec différents sous-réseaux sur différentes interfaces, et assure la communication entre les différents sous-réseaux.

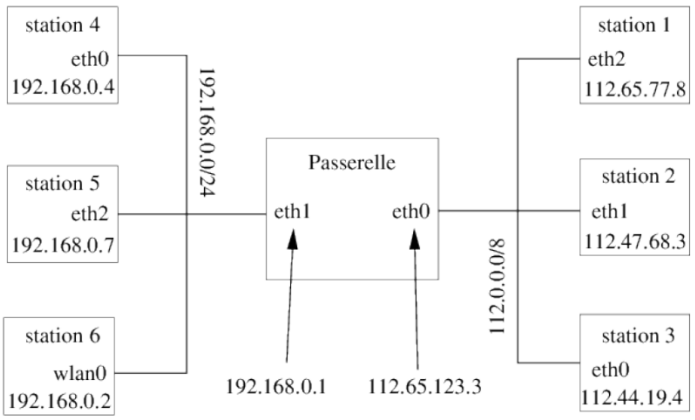

FIGURE 2.6 – Exemple de deux sous réseau reliés par une passerelle

Routes :

Une route définie sur une station est un chemin que doivent prendre les paquets à destination d'un certain sous-réseau. Prenons l'exemple (voir figure précédente) d'une station, appelée station 1, d'adresse IP 112.65.77.8 sur un réseau 112.0.0.0/8. Elle est connectée à une passerelle qui a pour IP dans ce réseau 112.65.123.3 sur son interface eth0. La passerelle est aussi connectée au réseau 192.168.0.0/24 via son interface eth1 qui a pour IP 192.168.0.1. Si la station 1 veut communiquer directement avec la station, appelée station 6, d'adresse IP 192.168.0.2 sur le réseau 192.168.0.0/24, trois condition doivent être réunies.
1. Une route doit être définie sur la station 1 indiquant que les paquets à destination du réseau 192.168.0.0/24 doivent passer par la passerelle 112.65.123.3. Pour celà, on peut utiliser la commande route :

```
# route add -net 192.168.0.0/24 gw 112.65.123.3
```

FIGURE 2.7 – Ajouter une route dans la table de routage du passerelle

2. Une route doit être définie sur la station 6 indiquant que les paquets à destination du réseau 112.0.0.0/8 doivent passer par la passerelle 192.168.0.1 ; Pour celà, on peut utiliser la commande route :

```
# route add -net 112.0.0.0/8 gw 192.168.0.1
```

FIGURE 2.8 – Configuration d'une chemin par défaut d'une station sur la passerelle

3. La passerelle doit être configurée pour transmettre (ou forwarder) les paquets IP d'un réseau à l'autre, ce qui se fait par la commande :

```
# echo1>/proc/sys/net/ipv4/ip_forward
```

FIGURE 2.9 – Permettre le routage sur la passerelle

On peut voir l'état des routes avec la commande route -n. Par exemple, sur la station 1 :

```
nabil@nabil-assus:/media/nabil/segate nabil UUI/outils/linux_os$ route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         192.168.43.1    0.0.0.0         UG    600    0        0 wlp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp1s0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 virbr1
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp1s0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
```

FIGURE 2.10 – Obtention de la table de routage via la commande Route -n

Route par défaut (gateway) :

Quand on a défini un certain nombre de routes sur une station, on peut définir une route spéciale pour les paquets IP à destination des réseaux non prévus dans les autres routes. On appelle une telle route une route par défaut. En général, c'est la route qu'il faut employer pour aller sur internet. On emploie le réseau 0.0.0.0 (masque 255.255.255.255). Pour définir une route par défaut on peu employer route. Par exemple, pour définir la route par défaut via la passerelle 194.56.87.1 :

```
#route add default gw 194.56.87.1
```

Pour supprimer cette même route :

```
#route del default gw 194.56.87.1
```

FIGURE 2.11 – Ajout/ suppression d'un chemin par défaut au passerelle

Protocoles :

Un protocole (IP, TCP, UDP,...) est un mode de communication réseau, c'est à dire une manière d'établir le contact entre machine et de transférer les données. Sous linux, la liste des protocoles reconnus par le système se trouve dans le fichier /etc/protocols.

A chaque protocole est associé un numéro d'identification standard. Le protocle IP est rarement utilisé directement dans une application et on utilise le plus couramment les protocoles TCP et UDP.

```
#cat /etc/protocols
# Internet (IP) protocols
# Updated from http://www.iana.org/assignments/protocol-numbers and other sources.
# New protocols will be added on request if they have been officially  assigned
# by IANA and are not historical.
# If you need a huge list of used numbers please install the nmap package.

ip 0 IP # internet protocol, pseudo protocol number
icmp 1 ICMP # internet control message protocol
igmp 2 IGMP # Internet Group Management
ggp 3 GGP # gateway-gateway protocol
tcp 6 TCP # transmission control protocol
ipv6 41 IPv6 # Internet Protocol, version 6
...
eigrp 88 EIGRP # Enhanced Interior Routing Protocol (Cisco)
ospf 89 OSPFIGP # Open Shortest Path First IGP
ax.25 93 AX.25 # AX.25 frames
ipip 94 IPIP # IP-within-IP Encapsulation Protocol
etherip 97 ETHERIP # Ethernet-within-IP Encapsulation [RFC3378]
encap 98 ENCAP # Yet Another IP encapsulation [RFC1241]
....
```

FIGURE 2.12 – IP Protocoles

Services et ports

Il peut y avoir de nombreuses applications réseau qui tournent sur la même machine. Les numéros de port permettent de préciser avec quel programme nous souhaitons dialoguer par le réseau. Chaque application qui souhaite utiliser les services de la couche IP se voit attribuer un numéro de port. Un numéro de port est un entier sur 16 bits (deux octets). Il y a un certain nombre de ports qui sont réservés à des services standards. Pour connaître le numéro de port correspondant à un service tel que ssh, on peut regarder dans le fichier /etc/services.

```
#nabil@nabil-assus$ cat /etc/services
# Network services, Internet style
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux 1/tcp # TCP port service multiplexer
echo 7/tcp
echo 7/udp
discard 9/tcp sink null
discard 9/udp sink null
systat 11/tcp users
daytime 13/tcp
daytime 13/udp
netstat 15/tcp
qotd 17/tcp quote
msp 18/tcp # message send protocol
msp 18/udp
chargen 19/tcp ttytst source
chargen 19/udp ttytst source
ftp-data 20/tcp
ftp 21/tcp
fsp 21/udp     fspd
ssh 22/tcp # SSH Remote Login Protocol
telnet 23/tcp
smtp 25/tcp mail
time 37/tcp timserver
```

FIGURE 2.13 – Services et Ports

2.4 Sécurité du trafic avec les pare-feu (Firewall) IPTABLES

Le pare-feu (en anglais firewall) netfilter, configuré avec la commande iptables, permet de filtrer les paquets réseau entrants, sortants, et transmis, sur une machine. On peut filtrer par interface, par port, par adresse de source ou de destination des paquets. La configuration d'iptables permet aussi de partager une adresse IP (par exemple sur internet) entre plusieurs machines d'un réseau local.

Principe de routage avec IPTABLES

Les politiques :

Lorsqu'un paquet IP rentre ou sort de votre machine, on peut adopter trois politiques différents : ACCEPT, REJECT ou DROP. Avec la politique ACCEPT, le paquet est simplement transmis normalement. Avec la politique REJECT le paquet n'est pas transmis et la machine source est prévenue. Avec la politique DROP, le paquet n'est pas transmis et la machine source n'est pas prévenue.

Les directions de paquets :

Il y a principalement trois directions de paquets (ces directions de paquets sont appelés chaînes) qui circulent sur la machine :

1. INPUT : paquets entrants à destination de la machine et venant d'une autre machine.
2. OUTPUT : paquets sortants venant de la machine et à destination d'un autre machine.
3. FORWARD paquets venant d'un autre machine et à destination d'une troisième machine lors de l'utilisation de la machine comme passerelle pour le routage.

Les rêgles :

La configuration iptables consiste en un ensemble de règles. Une règle est une commande iptables en ligne de commande comprenant :

- -A chaine ou -I chaine : La chaîne INPUT, OUTPUT ou FORWARD ;
- -i interface et/ou -o interface Les interfaces d'entrée et de sortie (optionnel) ;
- -p protocole Le protocole (si besoin) (voir /etc/protocols) ;
- –sport ou –dport ; Les ports de source ou de destination (si besoin) ;
- -s adresse ou -d adresse : L'adresse (ou le sous-réseau) de provenance ou de destination (optionnel). On pet aussi utiliser la négation (avec !) pour exclure une adresse au lieu d'inclure une adresse ;
- La politique ACCEPT, REJECT ou DROP, spécifiée avec l'option -j. L'ordre des règles est important. Si l'on met, par exemple, un politique de rejet systématique d'un certain type de paquets, on peut ensuite mettre une règles qui accepte ce type de paquet à partir d'une certaine machine ou d'un certain sous réseau. C'est la différence entre -A et -I. Le -A rajoute la règle à la fin d'une chaîne et le -I au début. Pour vider toutes les règles :

```
iptables -F chaîne
```

Pour mettre une politique par défaut (qui s'applique à tous les paquets sauf règle contraire) :

```
iptables -P chaîne politique
```

En général, on met toutes les règles dans un script qui va créer toutes les tables. On peut aussi lancer ce script automatiquement au démarage avec

```
update-rc.d
```

FIGURE 2.14 – quelques commandes IPTABLES

```
# On vide toutes les règles
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
# Politique
iptables -P
iptables -P
iptables -P
par défaut (version très sécurisée)
INPUT DROP
OUTPUT DROP
FORWARD DROP
# Autoriser le trafic sur l'interface loopback
iptables -I INPUT -i Io -j  ACCEPT
iptables -I OUTPUT -o Io -j  ACCEPT
# protocole
iptables -A
iptables -A
iptables -A
ICMP (dont ping) dans tous les sens
INPUT -p icmp -j  ACCEPT
OUTPUT -p icmp -j  ACCEPT
FORWARD -P ICMP -J accept
# ssh vers l'etérieur (client ssh) via l'interface eth0
iptable -I INPUT -p tcp -i eth0  -sport ssh -j ACCEPT
iptable -I OUTPUT -p tcp -o eth0 -dport ssh -j ACCEPT
# ssh vers la machine (serveur ssh) via l'interface eeth0
iptable -I INPUT -p tcp -i eth0 -drop ssh -j ACCEPT
iptable -I OUTPUT -p tcp -o eth0 -sport ssh -j ACCEPT
```

FIGURE 2.15 – Exemple de Règle IPTABLES

2.5 Quelques Services Applicatifs :

Service Web avec le Serveur Apache :

Un serveur HTTP permet à un site web de communiquer avec un navigateur en utilisant le protocole HTTP(S) et ses extensions. Apache est probablement le serveur HTTP le plus populaire. Souvent le serveur Apache foncionne conjoitement avec le SGBD Mysql et l'interpreteur PHP.

Service DNS avec Bind :

Sous Linux, DNS est implémenté par le BIND (Berkeley Internet Name Domain). C'est un programme qui repose sur une architecture client/serveur. La partie client du BIND est appelée le resolver. Il génère les demandes qui sont envoyées au serveur. Le serveur DNS répond alors aux requêtes du resolver. La partie serveur du BIND est un démon appelé named.

2.6 Réseaux Virtuels :

Contrairement à un commutateur réel dans un réseau physique qui à un nombre limité des ports Les ponts virtuel (Virtual Bridges) [MVC16], possèdent un nombre illimité de ports virtuels vers lesquels les interfaces des machines virtuelles peuvent s'attacher. Les pont virtuels -sont comme les commutateurs réel - apprennent les adresses MAC à partir des paquets qu'il reçoivent et stocke ces adresses MAC dans la table MAC. Les décisions de transmission de paquets (trames) sont prises en fonction des adresses MAC appris et stocké dans la table MAC. Nous avons mentionné les interfaces attachées aux ports d'un pont. Ces interfaces sont des périphériques réseau spéciaux appelés périphériques TAP. Si vous essayez d'imaginer cela en termes physique, considérez les périphériques TAP comme le câble réseau qui transporte les trames Ethernet entre votre machine virtuelle et le pont. Ces périphériques TAP font partie du modèle TUN /TAP implémenté dans le noyau Linux.

2.7 Conclusion

A travers ce chapitre, nous avons mis la lumière sur les principaux commandes Linux permettant de préparer une machine pour participer à des services réseaux. bien évidemment il est hors de sujet de couvrir tous les aspects de l'administration linux, nous avons retenus que les commandes que nous allons employés dans les prochains chapitres.

CHAPITRE 3

Simulation, Émulation et Virtualisation des Réseaux avec GNS3

3.1 Introduction :

GNS3 est un simulateur réseau graphique multi-plateforme (windows , linux , Mac OS). GNS3 permet de concevoir et de tester des réseaux virtuels sur PC, y compris (mais sans s'y limiter) Cisco IOS, Juniper, MikroTik, Arista et Vyatta net. Il est couramment utilisé par les besoins des expériences pratiques avec le routage et la commutation Cisco IOS en tant compte la difficulté de réaliser ces expériences réellement vu la cherté des équipement et l'étendu des superficies nécessaires pour les réaliser. Dans ce chapitre , nous focalisons notre intérêt sur l'étude approfondie de cet outil ainsi que d'autre outils qui tournent dans son orbite. l'objectif est de sortir avec des connaissance suffisantes pour simuler des scénarios qu'on peut rencontrer dans la pratique et évaluer leurs faisabilités.

3.2 Mise en place de l'Environnement de simulation GNS3 :

Installation :

Nous avons réaliser notre travail sur un PC portable avec un processeur Intel I5 cadencé à 2.4 GHz et une mémoire vive de 6 GO avec un système d'exploitation Linux Ubuntu 18.04. mais d'une manière générale le performances miniums requises pour travailler sont les suivantes :

- processeur 1.5 GHz
- RAM 4GB
- disque dur avec 250MB d'espace libre La meilleurs façon pour installer GNS3 est d'utiliser le console en tapant la ligne de commande :

```
sudo apt-get install gns3
```

Lorsque vous y êtes invité, entrez votre mot de passe. La sortie de cette commande affiche une liste des packages qui seront installés et indique la quantité de disque l'espace sera utilisé par l'installation. Le programme d'installation vous invite à confirmer que tout va bien avant de continuer. Une fois confirmés, les packages sont installés et GNS3 est prêt à fonctionner. Vous pouvez démarrer GNS3 à partir du console en entrant gns3 ou en lançant à partir du menu d'application de votre gestionnaire d'affichage.

Une machine GNS3 :

une alternative à l'installation de GNS3 sur votre PC consiste à utiliser un machine GNS3. Une machine GNS3 est simplement une machine virtuelle qui vient avec GNS3 déjà installé. Les machine GNS3 sont extrêmement flexibles car ils fonctionnent à l'aide d'une application telle que VirtualBox. VirtualBox est gratuit et fonctionne sur la plupart des systèmes d'exploitation (y compris Windows, OS X, Linux et FreeBSD).

Configuration :

l'installation de GNS3 n'est que la première étape vers la création de projets. La deuxième étape est la configuration. Heureusement, GNS3 a n'a jamais été aussi simple à configurer et ne vous devez qu'effectuez quelques tâches qu'on va traiter dans cette section .

Acquisition d'une image IOS :

Sous GNS3 les routeurs Cisco sont émulé avec un émulateur qui s'appelle Dynamips. Comme un disque dur de PC fraîchement formaté, Dynamips à besoin d'une image d'un système d'exploitation pour routeur Cisco (appellé IOS) pour qu'ils puissent faire un peu des choses utiles.
Donc, avant de pouvoir démarrer un routeur, il faut l'installer et le configurer sur au moins un fichier image Cisco IOS dans GNS3.
Les images des systèmes d'exploitation Cisco sont la propriété de la firme Cisco est qui sont destinées à s'installer et s'exécuter exclusivement sur ses équipements et non pas pour des finalités de simulation avec des outils open source comme GNS3. Néanmoins, plusieurs sites et forum sur internet offrent des images IOS réduites pour certains routeurs Cisco qui sont largement suffisantes pour réaliser ce projet de fin d'étude.

Configuration du premier routeur :

Une fois que vous avez une image IOS, vous devez effectuer quelques opérations avant de pouvoir commencez à utiliser vos routeurs virtuels.

- Tout d'abord, vérifiez le chemin vers Dynamips. Ensuite, copiez vos images IOS dans un dossier,
- puis ajoutez le images vers GNS3.
- Enfin, définissez une valeur Idle-PC pour chaque image IOS que vous avez ajouté à GNS3.

Configuration de Dynamips :

Sous GNS3, accédez à Edit–>Preferences, sélectionnez Dynamips et cliquez sur le onglet Paramètres, comme illustré à la Figure suivante . vérifiez que le champ Path to Dynamips pointe vers / usr / bin / dynamips. Si vous avez installé l'application Dynamips dans un autre répertoire, définissez le chemin vers ce répertoire à la place.

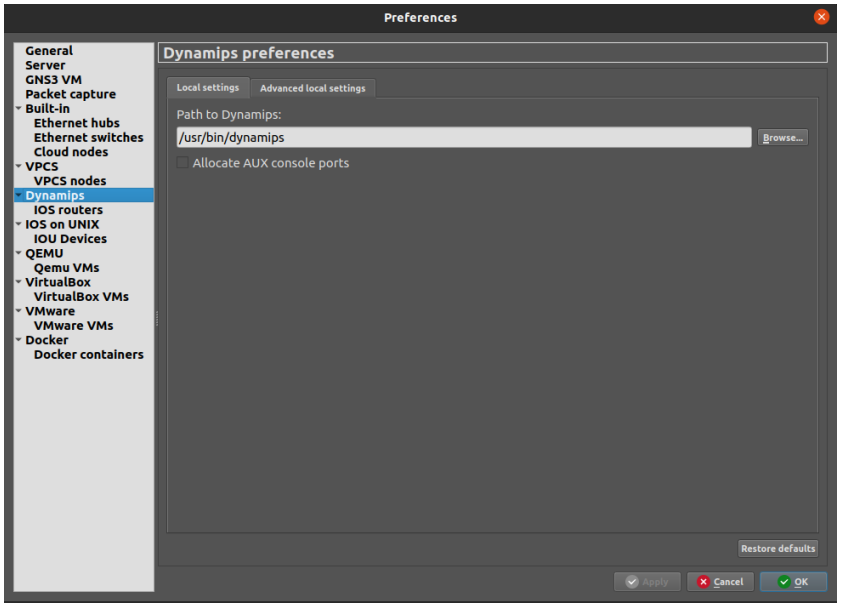

FIGURE 3.1 – Configuration Dynamips

Ensuite, cliquez sur l'onglet Paramètres avancés pour afficher les paramètres de la Figure suivante :

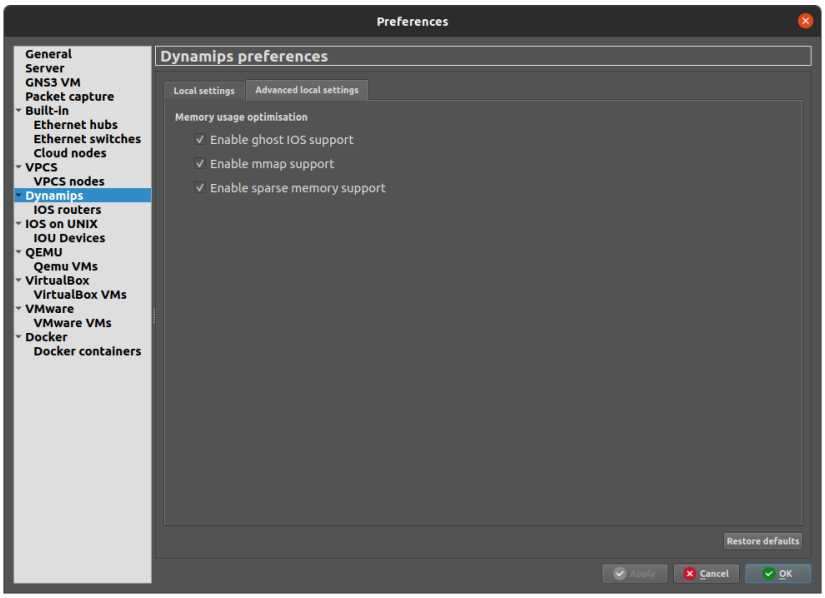

FIGURE 3.2 – Paramères avancés Dynamips

Les options de paramètres avancés du Dynamips concernent principalement la stabilité de dynamips et son utilisation de la mémoire. En règle générale, vous ne devriez pas les changer. Les paramètres d'optimisation de l'utilisation de la mémoire visent à conserver l'espace mémoire utilsé. Moins Dynamips utilise de mémoire par routeur, plus de routeurs que vous pouvez ajouter au projet.

- L'option « Activer la prise en charge de Ghost IOS » réduit la consommation de mémoire de votre PC

en allouant une région partagée de mémoire que plusieurs routeurs peuvent utiliser, tant qu'ils exécutent le même image IOS. C'est une bonne raison d'utiliser le même modèle de routeur plusieurs fois dans un projet ; en utilisant plusieurs modèles différents, avec différents versions, consommeront plus de mémoire .

• L'option « Enable mmap » permet d'écrire le contenu de la mémoire du routeur dans un fichier sur votre disque dur, similaire à un cache ou à un fichier d'échange.

• L'option « Enable sparse memory support » réduit la quantité de mémoire virtuelle utilisée par vos routeurs afin vous pouvez exécuter plus d'instances de routeur par processus Dynamips.

Ajouter une image IOS :

Avant de commencer à créer des projets contenant de routeurs IOS, ajoutez au moins une image IOS à GNS3. Pour ajouter une image IOS, sélectionnez Edit–>Preferences , développez Dynamips depuis le volet de gauche et cliquez sur Routeurs IOS, comme illustré à la Figure suivante :

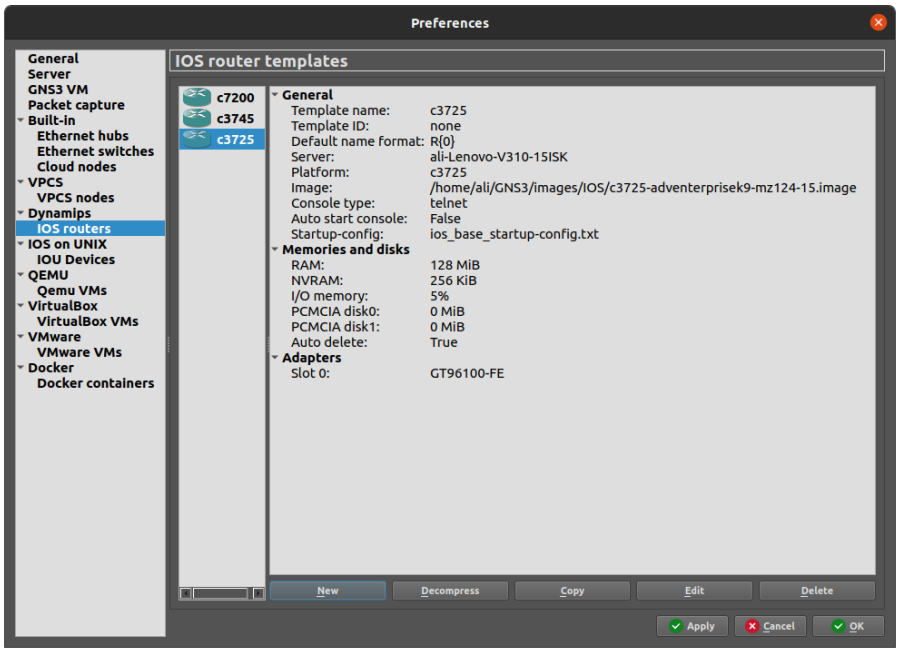

FIGURE 3.3 – Ajouter une nouvelle image IOS

Cliquez sur Nouveau pour démarrer l'assistant, puis sur le bouton Parcourir pour localiser votre fichier image. Après avoir sélectionné votre fichier image, il vous sera demandé si vous souhaite décompresser l'image IOS, comme le montre la figure sivante :

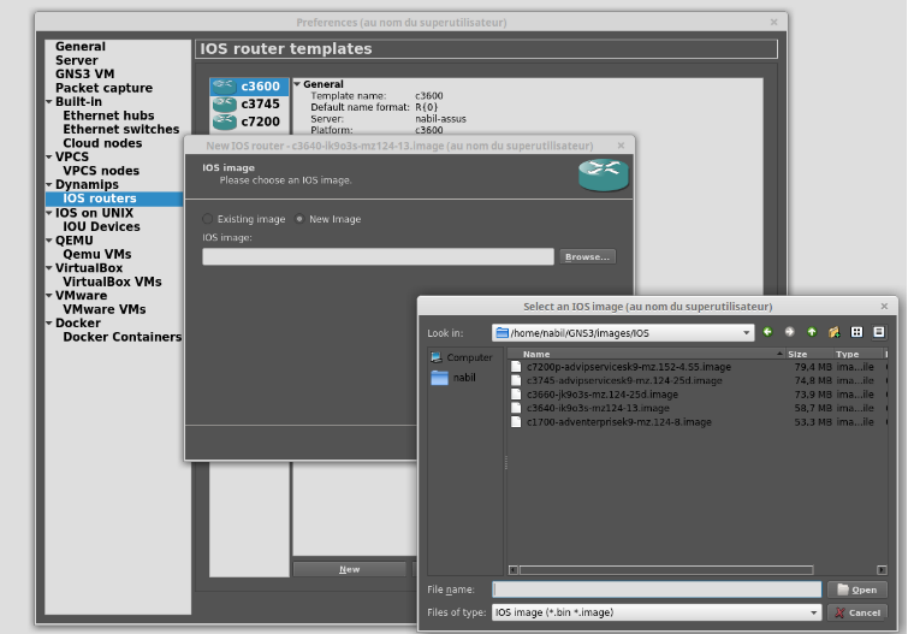

FIGURE 3.4 – Etape d'ajoue d'une Image IOS

C'est une bonne idée de laisser GNS3 décompresser les fichiers image ; autrement, dynamips devra décompresser les images chaque fois qu'un routeur se charge. La décompression des images à l'avance fera que les routeurs démarreront beaucoup plus rapide. Après avoir décompressé une image, cliquez sur Suivant et GNS3 tentera pour reconnaître la plate-forme de routeur à laquelle appartient l'IOS, comme indiqué dans Figure suivante :

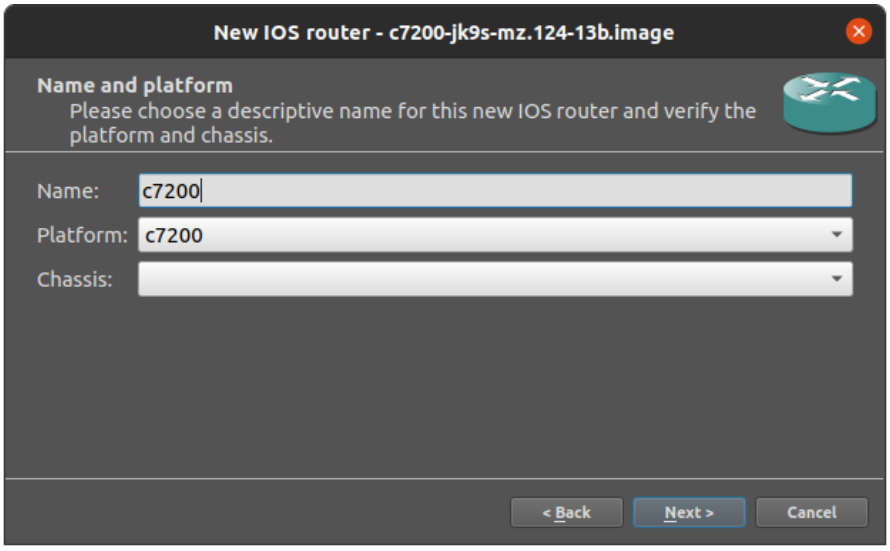

FIGURE 3.5 – Configuration du plateforme du routeur

GNS3 a déterminé que le fichier image appartient à une plate-forme de routeur c7200 et l'a automatiquement nommé c7200. Si nous pensons que c'est incorrect, on peut utiliser le menu déroulant Plateforme pour choisir une autre plateforme. Comme on peut changer le nom de routeur en en entrant un nom dans le champ Nom. En général, à partir de ce moment , nous pouvons simplement choisir sur toute la

configuration par défauts pour configurer un modèle de routeur de base, mais l'assistant offre l'opportunité pour personnaliser la mémoire du routeur et d'autres fonctionnalités pendant cette processus.

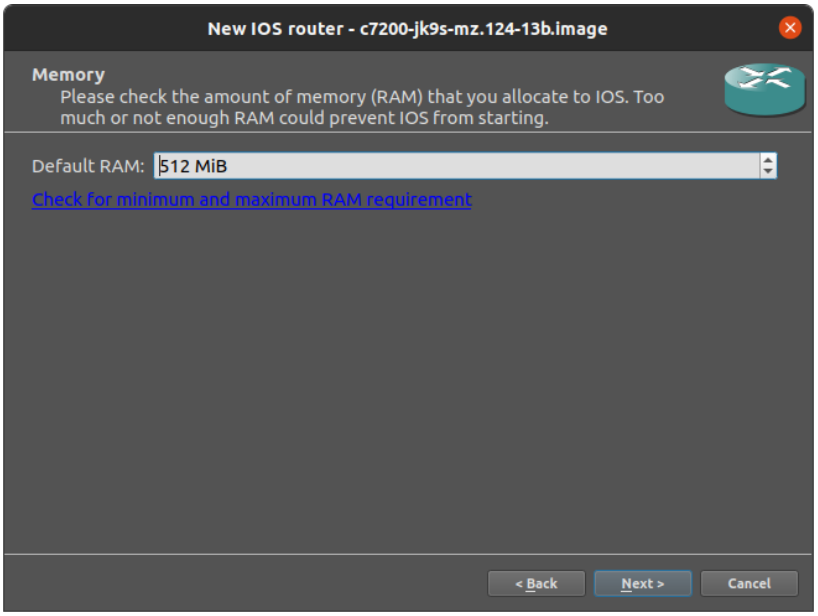

FIGURE 3.6 – configuration du plateforme du routeur (2)

Cliquer sur next pour obtenir la fenêtre suivante qui permet de configurer les différentes slot du chasis du routeur.

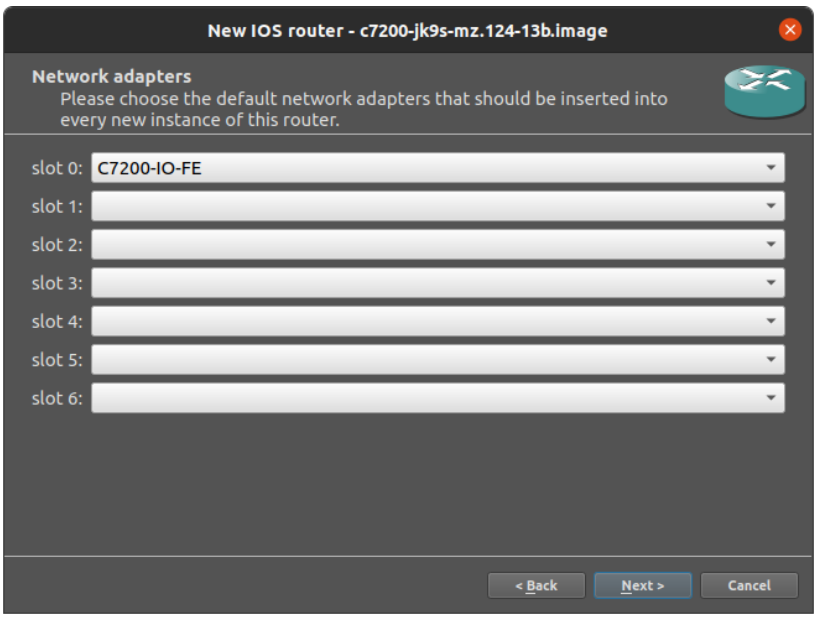

FIGURE 3.7 – Configuration du plateforme du routeur(3)

puis cliquer sur next pour régler la valeur Idle-pc.

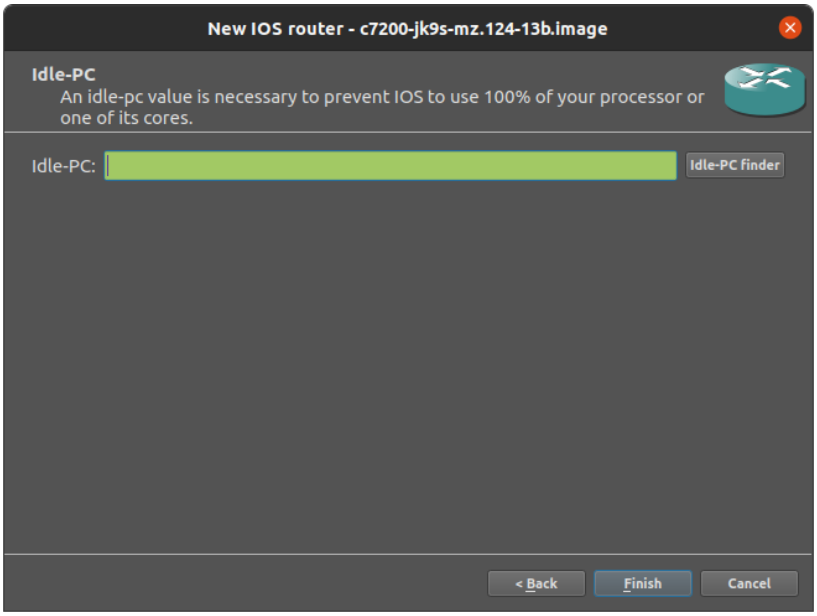

FIGURE 3.8 – Configuration du plateforme du routeur idle-pc

Si on démarre un routeur dans GNS3 sans paramètre Idle-PC, Le taux d'utilisation du processeur atteint rapidement 100% et y restera. Ceci se produit parce que Dynamips ne sait pas les besoins en terme des ressource du routeur virtuel, donc il lui donne toutes les ressources possibles. GNS3 fonctionnera lentement jusqu'à ce que corrigée, et si l'utilisation du processeur est laissée à 100% pendant une longue période, il risque de se surchauffer). On peut facilement résoudre ce problème en demandant à GNS3 de rechercher des emplacements dans le programme IOS où une boucle inactive existe (les boucles inactives provoquent un pic de CPU). le résultat de ce calcul est appelé une valeur Idle-PC. Quand le bon La valeur Idle-PC est appliquée, Dynamips devrait périodiquement mettre le routeur en veille lorsque ces boucles inactives sont exécutées, ce qui réduit considérablement l'utilisation du processeur. Pour que GNS3 trouve automatiquement une valeur, cliquez sur le buton « Idle-PC Finder » . GNS3 tentera de rechercher une valeur. Si GNS3 trouve un valeur, alors vous avez terminé ; cliquez sur Terminer. En cas d'échec, quittez le champ vide et cliquez sur Suivant pour enregistrer le routeur sans configuration Idle-PC. Si GNS3 ne parvient pas à trouver automatiquement une valeur Idle-PC, vous devrez trouver un manuellement. Vous devez calculer une valeur Idle-PC une seule fois par IOS image. GNS3 applique ce paramètre à tous les routeurs virtuels utilisant ce fichier image. Fermez la fenêtre Préférences et faites glisser un routeur depuis la barre d'outils Périphériques à votre espace de travail GNS3, comme illustré à la Figure suivante :

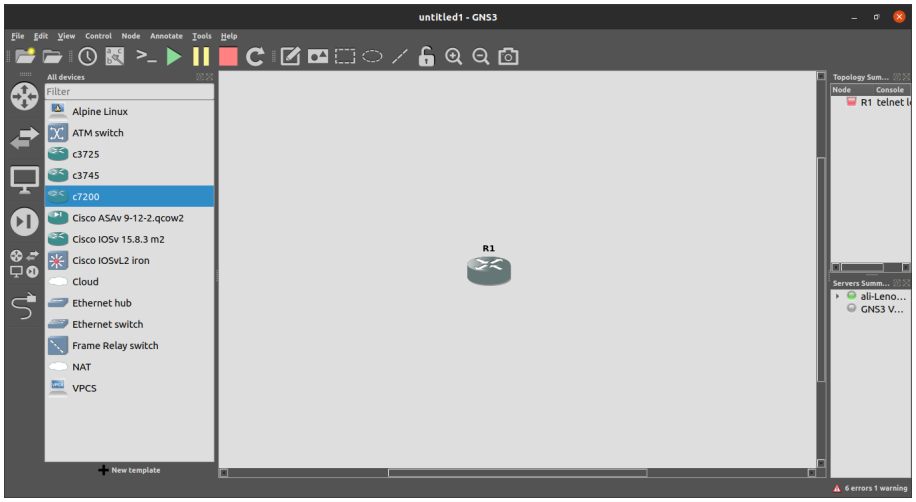

FIGURE 3.9 – Espace de travail GNS3 (01)

Ensuite, démarrez le routeur en cliquant avec le bouton droit sur l'icône du routeur et en sélectionnant Début ; puis vérifiez que l'IOS se charge correctement en cliquant immédiatement avec le bouton droit de la souris le routeur et en sélectionnant Console. Une fenêtre de console Cisco doit s'ouvrir et afficher les messages de démarrage du routeur. Si le routeur démarre correctement, vous êtes prêt à commencer le calcul Idle-PC ; sinon, assurez-vous que le le modèle et les paramètres de RAM par défaut attribués au routeur sont corrects, ou essayez une image IOS différente.

3.3 Création et Gestion des projets :

La principale caractéristique de GNS3 est la gestion de projet. Un nombre illimité de conceptions de réseaux peuvent être créer et enregistrer et même partager chaque fois que on en a besoin. Cela signifie que vous n'aurez jamais à perdre de temps à démonter un projet existant pour en créer un nouveau, ce qui arrive souvent lorsque s'agit d'un équipement physique. l'autre atout du GNS3 et que non seulement gérer enregistrer plusieurs projets simultanément mais également enregistrer plusieurs snapshot (captures instantanés) d'une configuration d'un projet . Un snapshot préserve l'état du projet (la disposition du réseau et l'état de toutes les configurations de votre routeur à un moment dans le temps). Vous pouvez restaurer un snapshot à chaque fois que vous souhaitez lancer votre tout le projet à l'état dans lequel il se trouvait lorsque l'instantané a été pris.

Un premier projet :

Lorsque vous lancez GNS3, une fenêtre « Nouveau projet » apparaît, comme indiqué dans Figure suivante. À partir de là, vous pouvez soit ouvrir un projet existant, soit créer un nouveau.

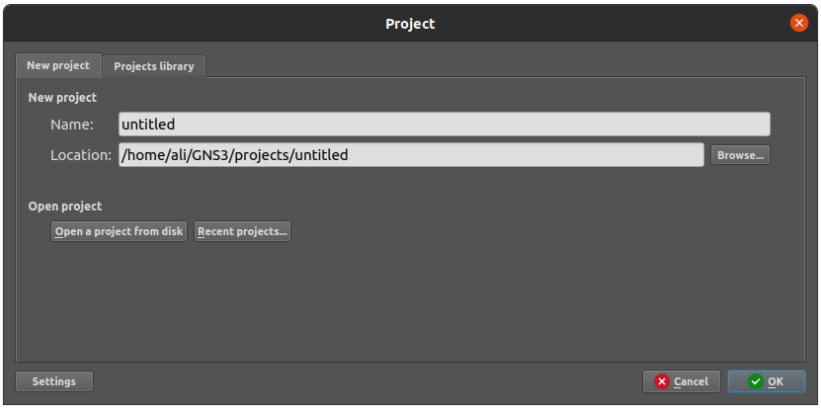

FIGURE 3.10 – Espace de travail GNS3 (création nouveau projet)

Après la création d'un nouveau projet ,il est temps de créer une topologie, en commençant par certains routeurs Dynamips.

Manipulation des routeurs :

Commençant par l'insertion de (02) deux routeurs Cisco 3660 qui s'appelle R1 et R2 comme montrée dans la figure suivante :

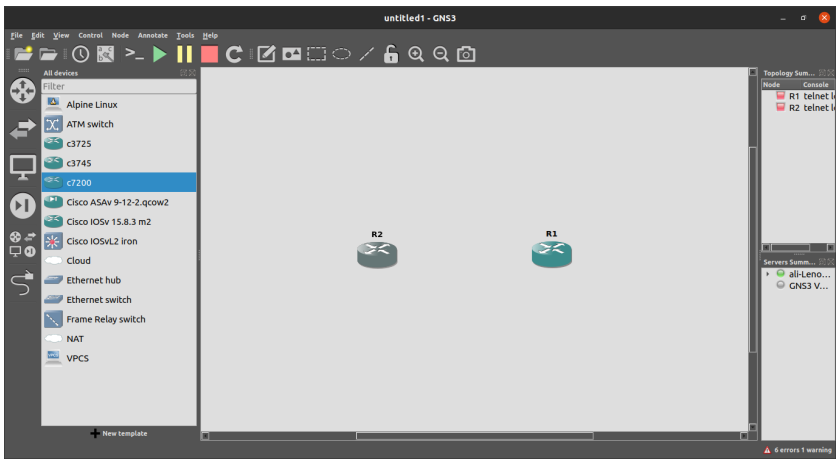

FIGURE 3.11 – Espace de travail GNS3 (02)

il est possible d'éditer le nom ainsi que plusieurs autres paramètres du routeur en cliquant avec le boutons droit du souris sur le symbole du routeur. Les routeurs tirent leur nom de la commande nom d'hôte %h trouvé dans le fichier «ios_base_startup-config.txt». Ce fichier contient tous les paramètres par défaut appliqués à tous les routeurs et attribués à un appareil lorsqu'il est configuré avec un fichier image IOS.

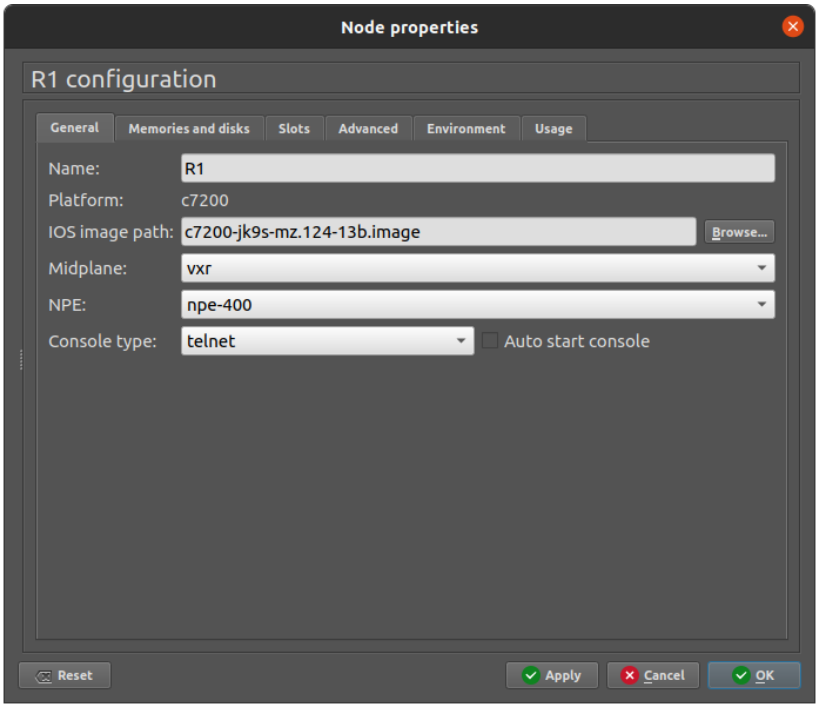

FIGURE 3.12 – ios_base_startup-config

Une fois que les routeurs sont placés dans l'espace de travail, il faut ajouter des liens entre eux pour créer un réseau entièrement fonctionnel. Pour ce propos il faut choisit les bon interface disponibles (cercle vert) sur chaque routeur comme indiqué dans la figures suivante :

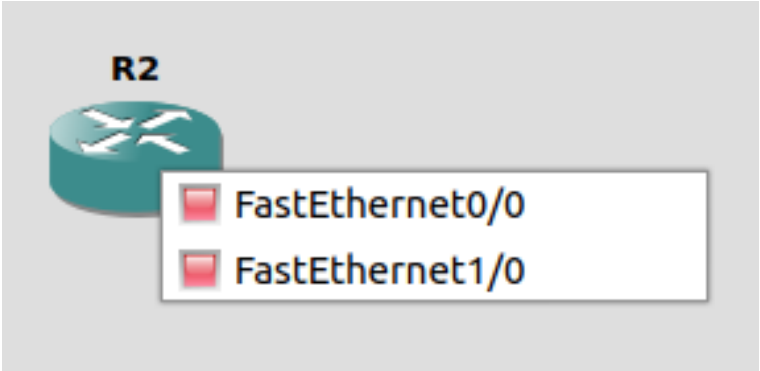

FIGURE 3.13 – Interface d'un router

A ce stade , on peut lancer , arrêter et même suspendre notre routeur un des simple cliq sur le bouton droit et le choix du commande souhaitée.

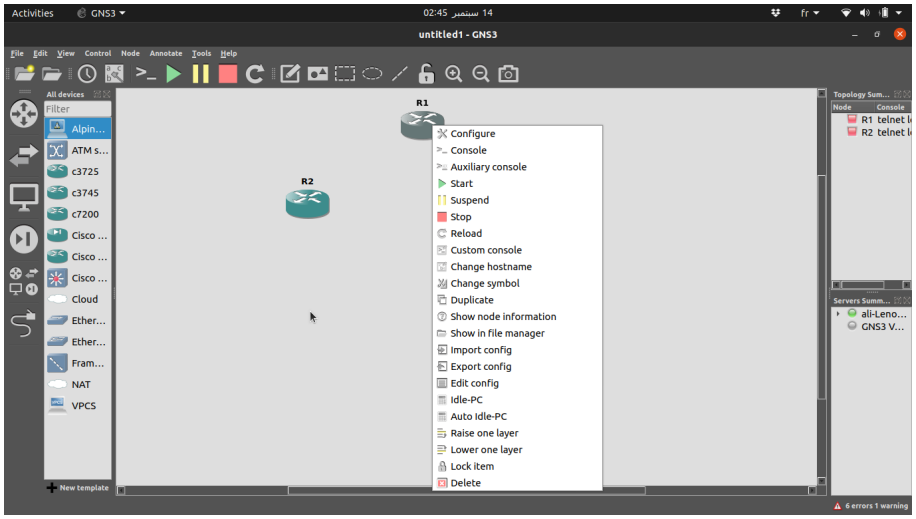

FIGURE 3.14 – Menu contextuel d'router dans GNS3

3.4 Analyse d'un routeur Cisco :

Composants internes :

Schématiquement, les composants internes qui nous intéressent principalement sont les différentes mémoires utilisées :

1. RAM : C'est la mémoire principale de travail du routeur. Elle contient entre autres le système d'exploitation une fois chargé, le fichier de configuration active, la ou les tables de routage, ainsi que les mémoires tampon utilisées par les interfaces et la pile utilisée par les processus logiciels. Sa taille varie en fonction du modèle de routeur (64 ou 96 Mo sur un 2620XM). Le contenu de cette mémoire est effacé lors de la mise hors tension ou du redémarrage.

2. NVRAM (Non-Volatile RAM) : Cette mémoire est non volatile, c'est-à-dire que son contenu n'est pas effacé lorsque l'alimentation est coupée. Sa très petite capacité de stockage (32 Ko sur un 2620XM) ne lui permet pas de stocker autre chose que le registre de configuration et le fichier de configuration de sauvegarde.

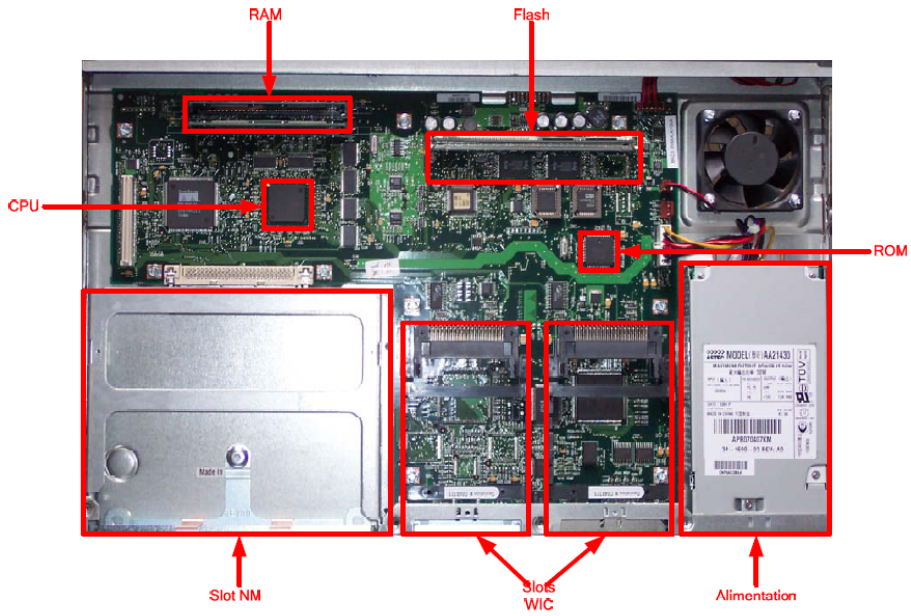

FIGURE 3.15 – Vue interne d'un routeur cisco 2620 XM

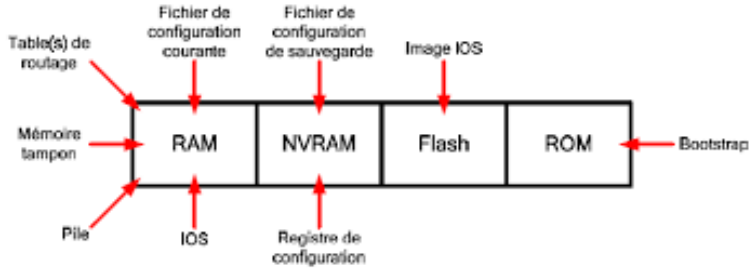

FIGURE 3.16 – Shema des mémoires d'un routeur cisco

3. Flash : C'est la mémoire de stockage principale du routeur. Elle contient l'image du système d'exploitation Cisco IOS (32 Mo sur un 2620XM). Son contenu est conservé lors de la mise hors tension et du redémarrage.

4. ROM : Elle contient le bootstrap ainsi que la séquence d'amorçage du routeur. Celle-ci est donc uniquement utilisée au démarrage du routeur.

Composants externes :

Un routeur Cisco peut offrir plusieurs types de connectiques parmi les suivantes :

- Port console : Accès de base pour configuration.
- Port auxiliaire : Accès pour configuration au travers d'une ligne analogique et modems interposés.
- Interface(s) LAN.
- Interface(s) WAN.
- Slot(s) NM (Network Module).
- Slot(s) WIC (WAN Interface Card).

FIGURE 3.17 – Vue arrére d'un routeur cisco

3.5 Branchements :

Interfaces LAN et WAN :

Les interfaces réseaux fournies par un routeur Cisco peuvent être de divers types et sont classifiées en fonction du type de réseau à connecter (LAN ou WAN). Elles peuvent être fixées au châssis ou livrées sous la forme de cartes (WIC ou NM) pour les routeurs modulaires. Ces interfaces seront utilisées par les protocoles de couche 3 du modèle OSI pour le routage.

FIGURE 3.18 – Cisco HWIC-2T 2-Port Serial WAN Interface Card

Accès pour configuration :

La configuration d'un routeur se fait en mode ligne de commande . Un routeur peut être configuré à partir des sources externes suivantes :

1. Ligne console : Accès primaire, à utiliser si aucun autre accès de configuration n'est disponible.
2. Ligne auxiliaire : Accès à distance via une liaison RTC et modems interposés.
3. Ligne(s) VTY : Accès via un client Telnet (5 ou 16 lignes disponibles par routeur en fonction du modèle).
4. Explorateur Web : Accès utilisant le serveur HTTP interne du routeur.
5. Serveur TFTP : Import/export de fichiers de configuration.
6. Serveur FTP : Import/export de fichiers de configuration.

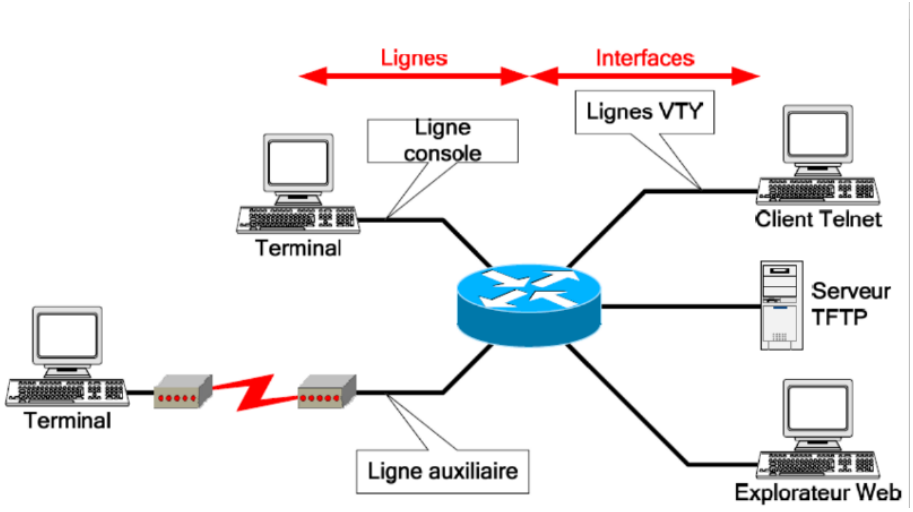

FIGURE 3.19 – Moyens d'accès pour configuration

3.6 Les Commutateur (Switchers) Ethernet :

Le nœud de commutateur Ethernet est un commutateur virtuel émulé qui permet de créer des accès VLAN (nous reviendrons aux réseaux VLAN dans le chapitre prochain) . Pour utiliser un nœud de commutateur Ethernet, faites glisser le nœud vers l'espace de travail. un nœud de commutateur Ethernet démarre automatiquement et n'a pas besoin d'être lancé manuellement. Pour configurer le commutateur, cliquez avec le bouton droit sur l'icône du nœud de commutateur Ethernet et sélectionnez Configurer comme illustrée à la figure suivante :

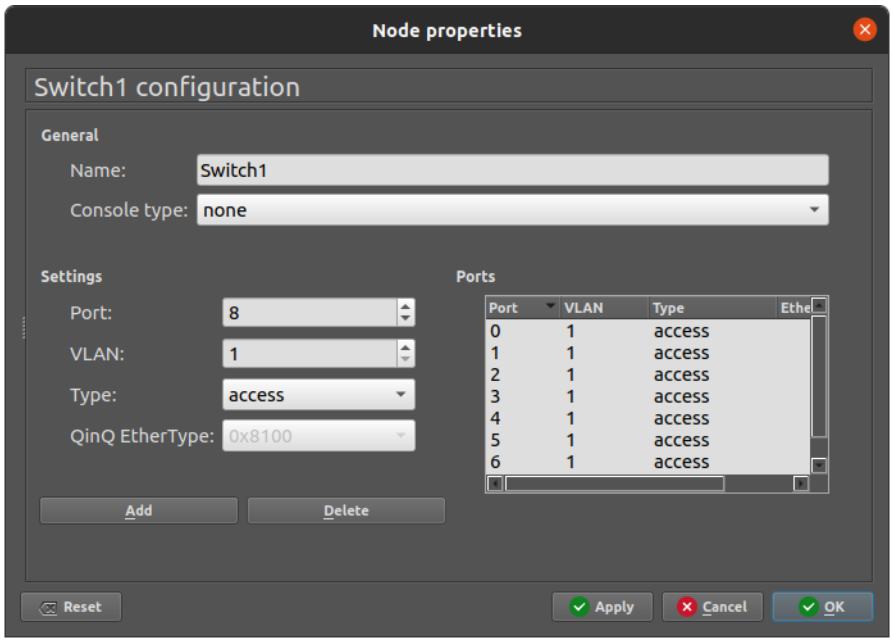

FIGURE 3.20 – Switch Configuration GNS3

cliquez sur le nom du commutateur (switch1, par exemple) pour modifier les ports de commutateur par défaut ou ajoutez de nouveaux ports. Par défaut, huit ports (08) d'accès sont affectés au VLAN 1. Pour

modifier un port, cliquez sur le numéro de port et modifiez les paramètres selon vos besoins. Quand vous avez terminé, cliquez sur Appliquer et OK. Pour ajouter un nouveau port, définissez les paramètres du ports et cliquez sur le bouton Ajouter, puis Appliquer.

Une alternative au nœud de commutateur Ethernet consiste à configurer un routeur Dynamips avec un module de commutation réseau. L'avantage d'utiliser un module de commutation est qu'il prend en charge plus de fonctionnalités (telles que le protocole Spanning Tree) ; l'inconvénient est que l'utilisation d'un module de commutation réseau utilise plus de ressources PC. Si on n'a besoin que a des fonctions d'un simple interrupteur, il est préférable de rester avec le nœud de commutation Ethernet. Si'il y a un besoin d'une capacité de commutation IOS complète, alors utilser un routeur avec un module de commutation installé comme le routeur EtherSwitch, ou utilisez une image de commutateur IOU L2.

3.7 Ajouter des machine hôtes :

Virtual PC Simulator (VPCS) :

VPCS est une petite application qui simule jusqu'à neuf PC de type DOS. Les hôtes VPCS ont un ensemble limité de mais sont bien adaptées pour tester la connectivité de bout en bout sur des réseaux GNS3. VPCS utilise très peu de ressources PC, ce qui permet d'ajouter de nombreux hôtes à des projets sans embourber le PC. Pour utiliser VPCS, faites glisser un nœud d'hôte VPCS dans l'espace de travail. Avant de pouvoir démarrer un hôte VPCS, il doit être connecté à un autre appareil dans projet. Après avoir démarré un hôte VPCS et en ouvrant une console, une fenêtre similaire à celle de la figure suivante s'affiche.

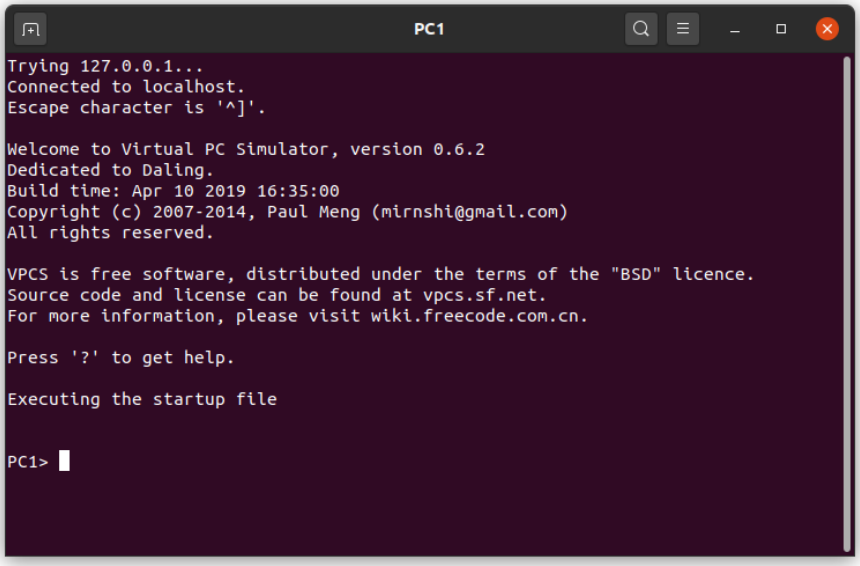

FIGURE 3.21 – Switch Configuration GNS3

Pour avoir une liste de commande (qui sont très simple) tapez ?. Le tableau suivant résume l'essentiel de ces commandes :

Commande	Description (en anglais comme donnée par la commande « ? »)
arp	Shortcut for : show arp. Show arp table
clear ARG	Clear IPv4/IPv6, arp/neighbor cache, command history
dhcp [OPTION]	Shortcut for : ip dhcp. Get IPv4 address via DHCP
disconnect	Exit the telnet session (daemon mode)
echo TEXT	Display TEXT in output. See also set echo ?
help	Print help
history	Shortcut for : show history. List the command history
ip ARG ... [OPTION]	Configure the current VPC's IP settings. See ip ?
load [FILENAME]	Load the configuration/script from the file FILENAME
ping HOST [OPTION ...]	Ping HOST with ICMP (default) or TCP/UDP. See ping ?
quit	Quit program
relay ARG ...	Configure packet relay between UDP ports. See relay ?
rlogin [ip] port	Telnet to port on host at ip (relative to host PC)
set ARG ...	Set VPC name and other options. Try set ?
show [ARG ...]	Print the information of VPCs (default). See show ?
sleep [seconds] [TEXT]	Print TEXT and pause running script for seconds
trace HOST [OPTION ...]	Print the path packets take to network HOST
Version	Version information
save [FILENAME]	Save the configuration to the file FILENAME

TABLE 3.1 – Les commandes VPCS

Virtual Box :

VPCS est un excellent outil pour ajouter des hôtes simples à GNS3 et tester la connexion , mais parfois vous avez besoin d'un hôte qui exécute un vrai système d'exploitation plutôt qu'une simulation. C'est là que VirtualBox entre en jeu. VirtualBox peut exécuter la plupart des systèmes d'exploitation basés sur PC, y compris Windows, Linux, FreeBSD et autres. Il est également utile pour exécuter des systèmes d'exploitation réseau tels que Arista vEOS, Juniper Firefly et NX-OSv. L'avantage de VirtualBox est qu'il vous fournit des hôtes avec des systèmes d'exploitation réels ; l'inconvénient est que ces systèmes d'exploitatio nécessitent des ressources substantielles de votre PC. Si tout ce que vous avez à faire est de tester connectivité, alors restez avec VPCS, mais si vous avez besoin d'un hôte qui fournit un ensemble robuste d'utilitaires réseau (pour tester la sécurité de votre réseau GNS3, pour exemple) ou pour exécuter un autre routeur ou commutateur OS, alors vous voudrez peut-être utilisez VirtualBox.

Wireshark :

Wireshark est l'un des outils d'analyse de paquets gratuit les plus robustes disponibles. Wireshark est un logiciel qui permet de capturer les paquets IP lorsqu'ils traversent un réseau. Vous pouvez ensuite ouvrir les paquets pour révéler et analyser leur Contenu. Les analyseurs de paquets comme Wireshark sont utilisés pour dépanner les protocoles réseau , contrecarrer les pirates et même identifier les virus, utilisez GNS3 et

Wireshark ensemble sont un excellent moyen d'apprendre les tenants et les aboutissants réseau et comment fonctionnent les protocoles réseau. Pour commencer à capturer des paquets dans une simulation GNS3, cliquez avec le bouton droit sur un lien entre deux périphériques et sélectionnez Démarrer la capture, comme illustré à la Figure suivante. (Pour arrêter une capture, faites un clic droit le même lien et sélectionnez Arrêter la capture.)

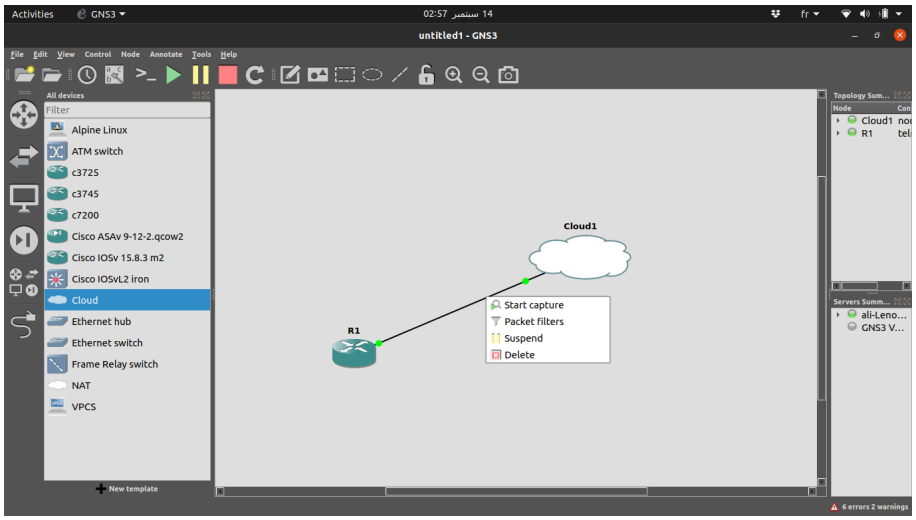

FIGURE 3.22 – Capture de trafics gns3

Après avoir fait une sélection et cliqué sur OK, GNS3 ouvrira Wireshark et commencez à capturer les paquets, comme le montre la figure siuvante. Notez que le La fenêtre Wireshark est divisée en trois volets distincts.

3.8 Conclusion :

Dans ce chapitre. Notre objectif se résume à une présentation d'outil GNS3 et ses accessoires permettant la mise en œuvre de nos conceptions des réseaux qu'on va aborder dans les prochains chapitres. Nous avons pu montrer que GNS3 et non seulement un outil de simulation mais il s'agit d'un puissant environnement fédérateur qui regroupe la virtualisation , la simulation ainsi que l'analyse du trafic réseau.

CHAPITRE 4

Routeurs Cisco et Systèmes Réseaux IOS

4.1 Introduction

Cisco et la firme qui détient la part de lion dans le marché mondial des équipement réseaux. La maîtrise de ses systèmes permet systématiquement d'avoir une très bonne expérience en matière de l'administration réseau. Dans ce chapitre nous nous consacrons à l'étude des routeurs Cisco ainsi que leurs systèmes d'exploitation appelé IOS (Internet Operating System).

4.2 Système d'exploitation Cisco IOS :

Principes et spécifications :

IOS (Internetwork Operating System) est le système d'exploitation propriétaire Cisco utilisé sur la plupart des dispositifs Cisco. Ce système d'exploitation offre une CLI (Command Line Interface). Le programme d'exécution des commandes, ou EXEC, est l'un des composants de la plateforme logicielle Cisco IOS. EXEC reçoit et exécute les commandes entrées dans la CLI.

Modes de commandes :

Il existe une multitude de modes différents accessibles en CLI sur un routeur Cisco :

1. **Mode utilisateur :** Mode lecture qui permet à l'utilisateur de consulter des informations sur le routeur, mais ne lui permet pas d'effectuer des modifications. Dans ce mode, on ne dispose que de commandes de visualisation d'état sur le fonctionnement du routeur. C'est dans ce mode que l'on arrive lorsque l'on se connecte au routeur.
2. **Mode privilégié :** Mode lecture avec pouvoir. On dispose d'une panoplie complète de commandes pour visualiser l'état de fonctionnement du routeur, ainsi que pour importer/exporter et sauvegarder des fichiers de configurations et des images d'IOS.
3. **Mode de configuration globale :** Ce mode permet d'utiliser toutes les commandes de configuration ayant une portée globale à tout le routeur.
4. **Modes de configuration spécifiques :** On ne dispose que dans chaque mode spécifique des commandes ayant une portée localisée au composant du routeur spécifié par ce mode.
5. **Mode SETUP :** Mode affichant un dialogue interactif, grâce auquel l'utilisateur néophyte peut créer une configuration élémentaire initiale.

6. Mode RXBoot : Mode de maintenance permettant notamment de récupérer des mots de passe perdus. On peut facilement identifier le mode dans lequel on est en repérant l'invite de commande que nous fournit l'interpréteur de commandes EXEC :

Mode	**Invite de commande**
Utilisateur	Router>
Privilégié	Router#
Configuration Globale du Router	(config)#
Interface Router	(config-if)#
Ligne Router	(config-line)#
Routage Router	(config-router)#

TABLE 4.1 – Les Modes de Commande IOS

Nous allons maintenant voir les commandes et les combinaisons de touches permettant de naviguer dans ces différents modes d'IOS :

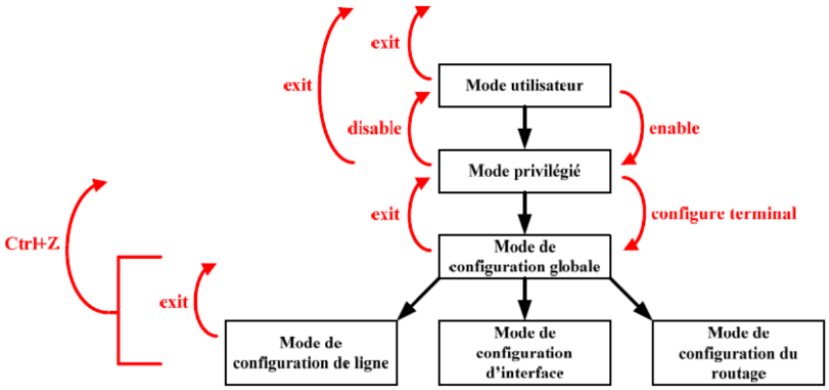

FIGURE 4.1 – Commandes et Combinaisons Modes IOS.

Les commandes à utiliser pour passer dans un mode de configuration spécifique sont les suivantes :

1. line type numéro :

a. Mode de configuration globale.

b. Permet de passer dans le mode de configuration d'une ligne.

2. interface type numéro :

a. Mode de configuration globale.

b. Permet de passer dans le mode de configuration d'interface.

3. router protocole [option] :

a. Mode de configuration globale.

b. Permet de passer dans le mode de configuration du routeur. Pour les lignes et les interfaces, la numérotation commence à 0.

4.3 Fichiers de configuration :

a.show running-config : Affiche la configuration courante.

b.show startup-config : Affiche la configuration de sauvegarde.

c.copy running-config startup-config : Sauvegarde la configuration courante dans la NVRAM.

d.copy running-config tftp : Exporte la configuration courante vers un serveur TFTP.

e.copy tftp running-config : Importe une configuration dans la RAM depuis un serveur TFTP.

f.copy startup-config tftp : Exporte la configuration de sauvegarde vers un serveur TFTP.

g.copy tftp startup-config : Importe une configuration dans la NVRAM depuis un serveur TFTP.

h.erase startup-config : Supprime le fichier de configuration de sauvegarde.

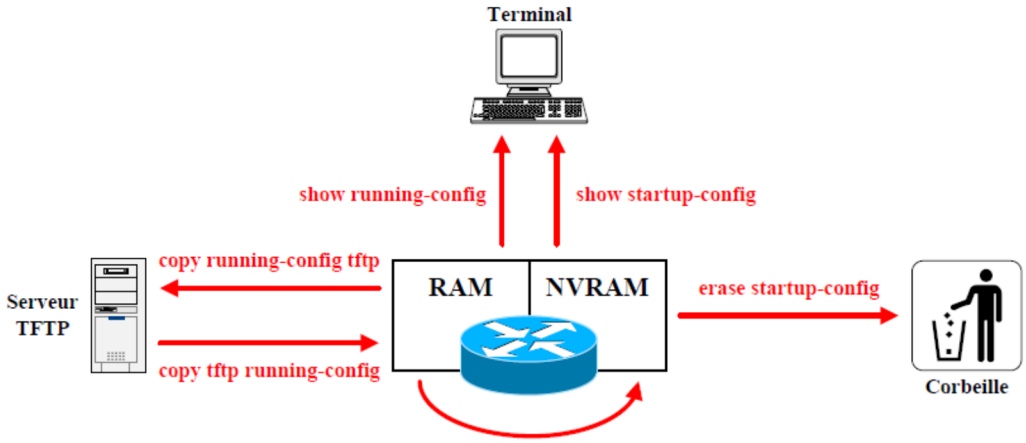

FIGURE 4.2 – Copy running-config startup-config.

4.4 Configuration de base d'un routeur :

Commandes de visualisation d'état :

Les commandes permettant la visualisation de l'état commencent toutes par le mot clé show.

- **show running-config :** Affiche le fichier de la configuration active.
- **show startup-config :** Affiche le fichier de la configuration de sauvegarde.
- **show version :** Affiche la configuration matérielle système, la version d'IOS, le nom et la source de l'image IOS d'amorçage, ainsi que la valeur du registre de configuration.
- **show processes :** Affiche des informations sur les processus actifs.
- **show memory :** Affiche des statistiques sur la mémoire du routeur, y compris sur la mémoire disponible.
- **show stacks :** Contrôle l'utilisation de la pile par les processus et les routines.
- **show buffers :** Fournit des statistiques sur les mémoires tampon des interfaces du routeur.
- **show arp :** Affiche les entrées ARP connues.
- **clear arp :** Vide les entrées dynamiques de la table ARP.
- **show hosts :** Affiche la table de résolution de noms.
- **show flash :** Affiche des informations sur la mémoire Flash, telles que la quantité d'espace libre et le nom des fichiers présents dans cette mémoire.

- **show interfaces [type numéro] :** Affiche les informations de configuration ainsi que des statistiques de trafic pour chaque interface configurée sur le routeur (couches 2 et 3).
- **show controllers [type numéro] :** Affiche les informations de couche 1 des interfaces.
- **show ip interface [type numéro] [brief] :** Affiche les informations IP pour les interfaces.
- **clear counters [type numéro] :** Permet de mettre à zéro toutes les statistiques des interfaces du routeur.
- **show ip route :** Affiche la table de routage IP.
- **show protocols :** Affiche le nom et l'état de tous les protocoles configurés de couche 3.
- **show ip protocols :** Affiche les valeurs des compteurs de routage et les informations de réseau associées à l'ensemble du routeur. Cette commande nous indique les différents réseaux avec lesquels le protocole de routage est configuré pour communiquer, ainsi que la distance administrative de ce dernier.
- **show sessions :** Affiche la liste des sessions en cours.
- **show users :** Affiche la liste des utilisateurs actuellement connectés au routeur.
- **show clock :** Affiche la date et l'heure actuelle.
- **show history :** Affiche la liste des commandes en mémoire.

Date et heure :

- **show clock :** Affiche la date et l'heure du système. **clock set hh :mm :ss jour mois année**.
- **Mode privilégié :** Permet de configurer l'heure sur le routeur.
- **hh :mm :ss** correspond à l'heure (de 0 à 23), aux minutes et aux secondes.
- **jour** est un nombre (de 1 à 31).
- **mois** est le nom du mois.
- **année** est l'année avec 4 chiffres.

Nom d'hôte et résolution de noms :

Il est possible de configurer :

- Le nom d'hôte du routeur.
- La résolution de noms statique.
- La résolution de noms dynamique grâce au protocole DNS Les commandes à utiliser sont les suivantes :

a. hostname nom :

a. Mode de configuration globale.

b. Attribution du nom d'hôte du routeur.

c. Ce nom est affiché par l'invite de commandes.

d. La valeur par défaut est "Router".

b. ip host nom [tcp_port_number] IP1 [IP2...] :

a. Mode de configuration globale.

b. Création d'une entrée statique de résolution de noms dans la table d'hôtes.

c. tcp_port_number permet de spécifier le port TCP à utiliser avec cet hôte pour un accès Telnet.

d. il est possible de spécifier plusieurs adresses IP pour un seul hôte. Dans ce cas, seule la commande telnet

utilisera les adresses autres que la première si les précédentes ne répondent pas.

c. [no] ip domain-lookup :

a. Mode de configuration globale.

b. Active/désactive la résolution dynamique de noms (DNS).

d. ip name-server DNS1 [DNS2...] :

a. Mode de configuration globale.

b. Permet de spécifier le ou les serveurs DNS avec lesquels nous effectuerons les résolutions d'adresses.

c. On peut préciser jusqu'à 6 serveurs DNS différents.

4.5 Configuration des interfaces :

Les interfaces peuvent être de différents types. Dans ce cours, nous étudierons uniquement les interfaces suivantes :

- Loopback.
- Ethernet.
- Serial. La commande **show interfaces** permet l'affichage de l'état des interfaces du routeur. On peut déterminer :

1. L'adresse IP et le masque de sous-réseau.
2. L'adresse de couche 2.
3. L'encapsulation utilisée.
4. Les statistiques sur le trafic transitant au travers de chaque interface.

Interfaces Loopback :

Les interfaces Loopback sont généralement utilisées pour simuler des interfaces réelles. Pour leur configuration, on dispose des commandes suivantes :

- **interface loopback numéro**

o Mode de configuration globale.

o Permet de passer dans le mode de configuration d'interface.

- **ip address IP masque [secondary]**

o Mode de configuration d'interface.

o Permet d'attribuer une adresse IP à cette interface.

o Le paramètre **econdary** précise qu'il s'agit d'une adresse IP secondaire.

Interfaces Ethernet/IEEE 802.3 :

Les interfaces de type Ethernet/IEEE 802.3 peuvent être de type :

- Ethernet (IEEE 802.3).
- Fast Ethernet (IEEE 802.3u).
- Gigabit Ethernet (IEEE 802.3ab ou IEEE 802.3z)
- 10-Gigabit Ethernet (IEEE 802.3ae)

Les interfaces Gigabit ou 10-Gigabit ne seront pas étudiées dans ce cours.

La configuration basique de ces interfaces est très simple, et se résume à ces commandes :

1. interface Ethernet | FastEthernet numéro | slot/numéro :

- Mode de configuration globale
- Permet de passer dans le mode de configuration d'interface

2. ip address IP masque [secondary] :

- Mode de configuration d'interface.
- Permet d'attribuer une adresse IP à cette interface.
- Le paramètre secondary précise qu'il s'agit d'une adresse IP secondaire.

3. [no] keepalive :

- Mode de configuration d'interface
- Active/désactive les "keep alive" sur l'interface
- Utile pour rendre une interface opérationnelle sans avoir à brancher un média.

4. [no] shutdown : Mode de configuration d'interface. Active/désactive administrativement l'interface.

4.6 Configuration d'une route par défaut :

La passerelle par défaut dans l'exemple suivant est : 192.168.3.1 .

```
R(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

4.7 Suppression de la route par défaut :

```
R(config)#no ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

4.8 Configuration d'une route statique :

Dans la commande suivante, le réseau à atteindre est le réseau 192.168.2.0/24 et l'interface utilisée pour joindre le réseau est ethernet 1/0. On peut aussi utiliser l'adresse IP du prochain routeur.

```
R(config)#ip route 192.168.2.0 255.255.255.0 ethernet 1/0
```

Autre possibilité :

```
R(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

4.9 Suppression de la route statique :

```
Rconfig)#no ip route 192.168.2.0 255.255.255.0 ethernet 1/0
```

4.10 Affichage de la table de routage :

```
R#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.3.1 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.0.0.0 is directly connected, Ethernet1/0
S 192.168.2.0/24 [1/0] via 10.0.0.2
C 192.168.3.0/24 is directly connected, FastEthernet2/0
S* 0.0.0.0/0 [1/0] via 192.168.3.1
R#
```

On remarque sur cette sortie de commande les réseaux directement connectés (C), les routes statiques (s) et la route par défaut.

4.11 Exemple de configuration :

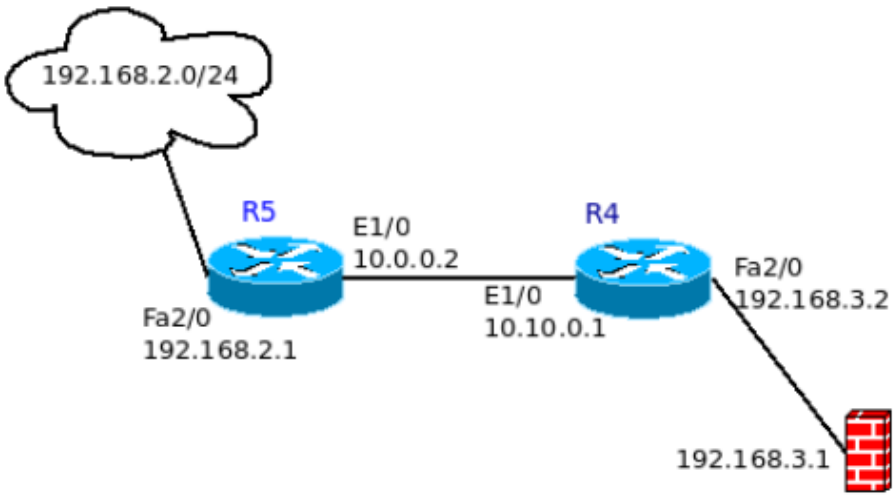

FIGURE 4.3 – Exemple de configuration.

Extrait du fichier de configuration de R4 et R5.

```
R4#sh run
Building configuration...
interface Ethernet1/0
ip address 10.0.0.1 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 192.168.3.2 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 192.168.3.1
ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

```
R5#sh run
Building configuration...
interface Ethernet1/0
ip address 10.0.0.2 255.255.255.0
duplex half
interface FastEthernet2/0
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

Affichage des tables de routage.

```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.3.1 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.0.0.0 is directly connected, Ethernet1/0
S 192.168.2.0/24 [1/0] via 10.0.0.2
C 192.168.3.0/24 is directly connected, FastEthernet2/0
S* 0.0.0.0/0 [1/0] via 192.168.3.1
R4#
R5(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.0.1 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.0.0.0 is directly connected, Ethernet1/0
C 192.168.2.0/24 is directly connected, FastEthernet2/0
S* 0.0.0.0/0 [1/0] via 10.0.0.1
R5(config)#
```

4.12 Conclusion

Le système IOS est un système d'exploitation orienté réseau qui rend les routeurs Cisco des machines avec des puissances incomparables en ce qui concerne le support des différents protocoles réseaux et la prestation des services réseaux variés. nous ne pouvant couvrir toutes la puissance de ce système dans ce petit chapitre. Nous orientons les lecteurs au livre de références des commandes IOS [Hea10].

CHAPITRE 5

Mise en Oeuvre et Expérimentation

5.1 Introduction :

La mise en place d'un réseau pour un parc informatique géant à l'instar de celui de notre université 8 Mai 1945, Guelma, nécessite la conception d'une bonne architecture permettant par la suite la l'évolution ce réseau pour s'adapter aux différents besoins de en terme de fluidité de trafic, la mise en place des nouvelles service et systèmes d'information distribués mais aussi avec des garanties de sécurités pour éviter toutes comportement malintentionnée que ce soit de l'intérieur du réseau ou bien de l'extérieur. Durant ce chapitre, nous allons employées toutes les connaissances acquisses dans les chapitres précédents pour la mise en place des solutions répondant aux exigences su-citées.

5.2 Une Architecture Réseau pour l'Université 8 Mai 1945 :

Pour assurer une haute disponibilité du réseau et une meilleur gestion des ses ressources, nous proposons une architecture en trois couche respectant la norme Cisco :

1. **Core Layer** : se compose des routeurs les plus gros, les plus rapides et les plus chers avec les numéros de modèle les plus élevés. la Core Layer est considéré comme l'épine dorsale des réseaux. Les routeurs Core Layer sont utilisés pour fusionner des réseaux séparés géographiquement. Les routeurs Core Layer déplacent les informations sur le réseau aussi rapidement que possible. Les commutateurs fonctionnant au niveau de la couche centrale commutent les paquets aussi rapidement que possible.
2. **Distribution Layer** : La couche de distribution est située entre les couches d'accès et centrale. Le but de cette couche est de fournir une définition des limites en implémentant des listes d'accès et d'autres filtres. Par conséquent, la couche de distribution définit la politique du réseau. La couche de distribution comprend des commutateurs de couche 3 haut de gamme. La couche de distribution garantit que les paquets sont correctement acheminés entre les sous-réseaux et les VLAN de l'Université.
3. **Access Layer** : La couche d'accès comprend des commutateurs d'accès qui sont connectés aux périphériques terminaux (ordinateurs, imprimantes, serveurs, etc.). Les commutateurs de couche d'accès garantissent que les paquets sont livrés aux périphériques finaux.

La figure 5.1 donne un aperçu de cette architecture. il est important de signaler que les switchers de niveau 3 sont localisé au niveaux des faculté, tandis que les routeurs sont placé chacun dans un campus.

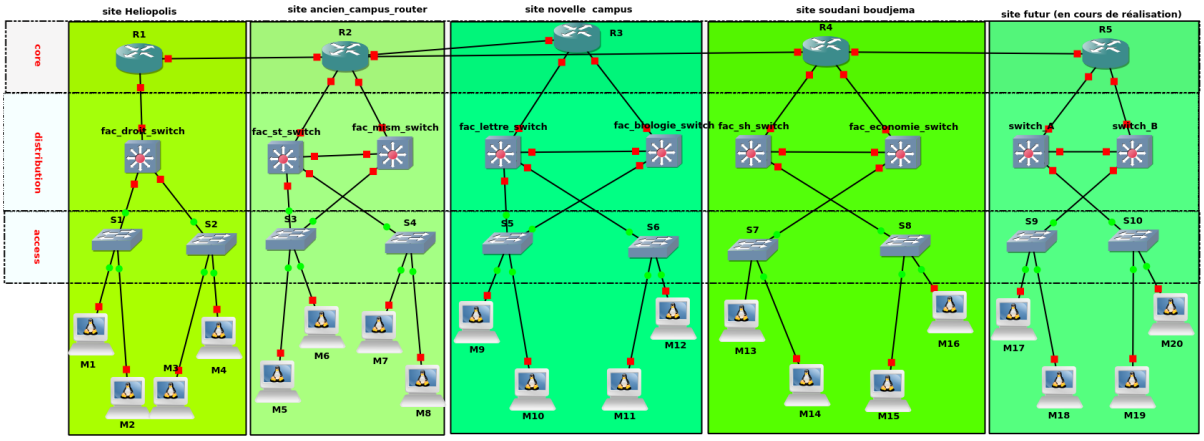

FIGURE 5.1 – Architecture en 3 couches pour l'université de 8 Mai 1945, Guelma.

sur le plan géographique, la figure suivante présente le placement des différents routeurs.

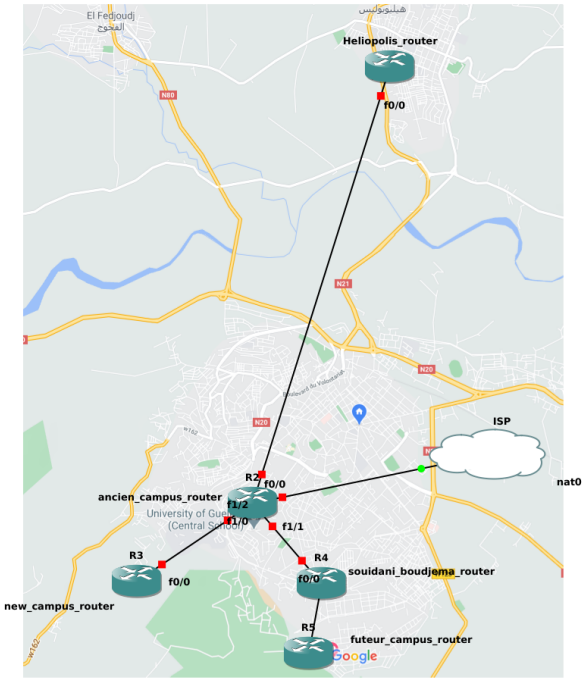

FIGURE 5.2 – distribution géographiques des routeurs.

5.3 Démarche Adoptée :

Pour bien présenter nos solution nous allons suivre une démarche progressive et commençant par les protocoles des couche basse et remontant vers le haut.

— la couche Liaison : solutions de switching avec VLAN ,VTP et STP.

— la couche réseau : : solutions de routage statique et dynamique avec OSPF ainsi que le routage multicast.

— la couche application : solution DHCP , DNS, NAT et Firewall.

Pour chaque solution, nous présentons :

1. le scénario de réalisation et les objectifs visés.
2. la topologie proposée.
3. les scripts de configuration des différents équipements utilisés.
4. les captures de trafic pour des finalité d'analyse et de validation.

5.4 Équipement et Systèmes Utilisés :

Durant les scénarios de simulation que nous allons proposé, nous utilisons une gamme d'équipement variées ainsi que des des systèmes logiciel virtuel divers. Dans GNS3, on utilise le terme *Appareil* (Appliance ne Anglais) pour refléter un équipement ou un système software. Nous décrivons les appareils utilisé dans nos scénarios dans les poins suivants :

Equipement	**Niveau**	**Description**
R c3640	L3	Routeur Cisco série c3640 (virtuel)
R c7200	L3	Routeur Cisco série série c7200 (virtuel)
R IOSv 15.8	L3	Routeur Cisco IOSv 15.8 (3)
S IOSvL2	L2	Routeur Cisco IOSv
Machine VPCS	Application	Machine Virtuelle
Mchine Linux	Application	Machine Virtuelle Apline Linux 3.10
Mchine Micro Core Linux	Application	Machine Virtuelle Micro Core Linux 6.4
NAT Cloud	Application	Network address translation Cloud
NAT	Application	Network address translation
Machine ToolBox	Application	Machine ToolBox
Machine IpTerm	Application	IP Terminal
DNS Machine	Application	Domain Name System

TABLE 5.1 – Équipement et Systèmes Utilisés

5.5 Routage statique et dynamique :

Routage Statique :

Scénario :

En tant que Ingénieur du réseau dans l'université de 8 Mai 1945. et sachant que le lien dédié pour connecter les deux sites de l'université ancien campus et Héliopolis est payant . Nous ne somme pas autorisé à utiliser les protocoles de routage, car ils paient pour chaque bit envoyé sur ce liens. Nous devons par conséquence utiliser le routage statique pour faire le travail en minimisant les dépenses.

Objectifs :

1. Toutes les adresses IP sont à configurer comme indiqué dans l'image de topologie 5.3.
2. Il existe une interface Loopback0 sur le routeur 'ancien campus' : Adresse IP 2.2.2.2/30.
3. Il existe une interface Loopback0 sur le routeur Heliopolis : Adresse IP 1.1.1.1/30.
4. Heliopolis : créez une route statique pointant vers le réseau Loopback0 sur 'ancien campus', le trafic doit passer le réseau 192.168.1.0.
5. 'ancien campus' : créez une route par défaut pointant vers le réseau Loopback0 à Heliopolis, le trafic doit passer le réseau 192.168.2.0. Dans la table de routage, vous devriez voir une entrée 0.0.0.0.
6. Heliopolis : créez une route statique de sauvegarde pointant vers le réseau Loopback0 à ancien campus, la distance administrative doit être de 100.
7. ancien campus : changez la route par défaut pour qu'elle reste dans la table de routage même lorsque l'interface tombe en panne.

Topologie :

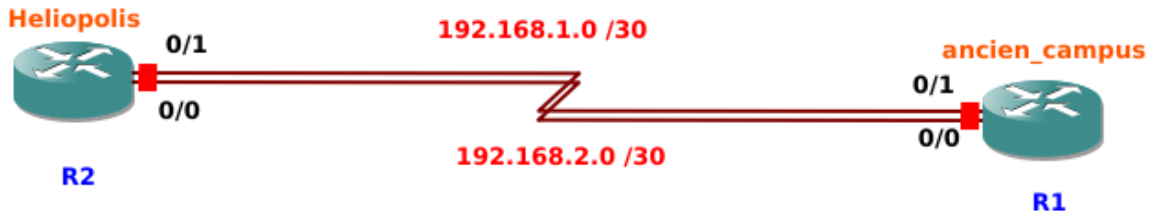

FIGURE 5.3 – Topologie Scénario Routage Static.

Configuration et Scripts :

Nous donnons dans ce qui suit les configurations pour les deux routeurs pour la mise en place de cette topologie.

```
hostname Ancien_Campus
interface Loopback0
ip address 1.1.1.1 255.255.255.252
interface Serial0/0
 ip address 192.168.1.1 255.255.255.0
 serial restart-delay 0
interface Serial0/1
 ip address 192.168.2.1 255.255.255.0
 serial restart-delay 0
interface Serial0/2
no ip address
shutdown
serial restart-delay 0
interface Serial0/3
no ip address
shutdown
serial restart-delay 0
ip http server
no ip http secure-server
ip route 2.2.2.0 255.255.255.0 192.168.1.2
ip route 2.2.2.0 255.255.255.0 192.168.2.2 100
control-plane
line con 0
line aux 0
line vty 0 4
end
```

FIGURE 5.4 – Script Routeur Heliopolis.

```
hostname Helipolis
interface Loopback0
ip address 2.2.2.2 255.255.255.252
interface Serial0/0
ip address 192.168.1.2 255.255.255.0
serial restart-delay 0
interface Serial0/1
ip address 192.168.2.2 255.255.255.0
serial restart-delay 0
interface Serial0/2
no ip address
shutdown
serial restart-delay 0
interface Serial0/3
no ip address
shutdown
serial restart-delay 0
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.2.1 permanent
control-plane
line con 0
line aux 0
line vty 0 4
end
```

FIGURE 5.5 – Script Routeur Ancien Campus.

Routage Dynamique avec OSPF

Scénario

Pour les liens non alloués (propriété de l'université) nous avons estimé que que le protocole OSPF serait un candidat approprié pour le routage dynamique. Étant donné que le réseau en ce moment est encore petit, nous avons décidé qu'une seule zone OSPF devrait suffire.

Objectifs

1. Toutes les adresses IP sont à configurer.
2. Les interfaces de bouclage suivantes sont à configurer : ancien-campus : 1.1.1.1 / 24 nouveau-campus : 2.2.2.2 / 24 soudani-boudjema : 3.3.3.3 / 24

3. ancien-campus : Configurez OSPF (process-id 1) et publiez tous les réseaux en utilisant une seule instruction de réseau. Utiliser area0
4. nouveau-campus : Configurez OSPF (process-id 1) et publiez tous les réseaux en utilisant 2 instructions de réseau, area0.
5. soudani-boudjema : Configurez OSPF (process-id 1) et annoncez tous les réseaux en utilisant 3 instructions de réseau, area0.
6. Facultatif : les interfaces de bouclage apparaissent en tant que / 32 dans la table de routage, assurez-vous qu'elles apparaissent en tant que / 24 telles que vous les avez configurées.
7. nouveau-campus : changez le router-id en 22.22.22.22, assurez-vous de voir ce changement de soudani-boudjema en utilisant les commandes show.
8. Le trafic de soudani-boudjema à ancien-campus devrait utiliser la liaison nouveau-campus-soudani-boudjema, utilisez la commande de coût pour y parvenir.
9. Supprimez la modification précédente avec la commande cost, atteignez le même objectif en utilisant la commande bandwidth.
10. Activez l'authentification en texte clair entre nouveau-campus et ancien-campus. Utilisez «vault» comme mot de passe.
11. Activez l'authentification MD5 entre soudani-boudjema et ancien-campus. Utilisez «Safe» comme mot de passe.
12. Changez les minuteries OSPF sur la liaison entre nouveau-campus et soudani-boudjema pour que les paquets soient envoyés toutes les 5 secondes.
13. Le routeur de ancien-campus aura accès à Internet à l'avenir, vous devez annoncer une route par défaut dans OSPF afin que nouveau-campus et soudani-boudjema envoient du trafic pour les réseaux inconnus à ancien-campus.

Topologie

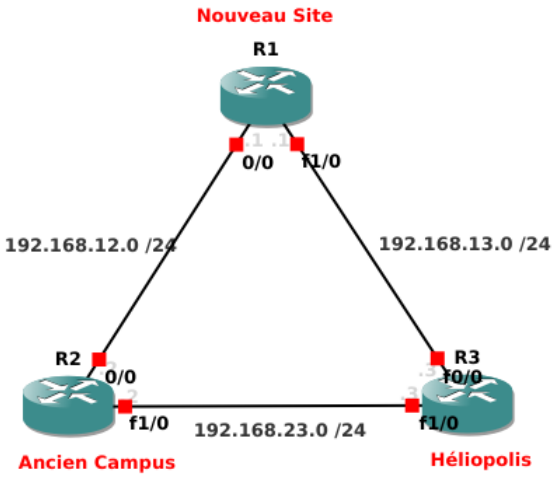

FIGURE 5.6 – Topologie pour un Scénario de Routage dynamique avec OSPF.

Configuration et Scripts

```
hostname Ancien_Campus
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
 ip ospf network point-to-point
!
interface gigabitEthernet 0/0
 no shutdown
 ip address 192.168.12.1 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key vault
 duplex auto
 speed auto
!
interface gigabitEthernet 0/1
 no shutdown
 ip address 192.168.23.1 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Safe
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate always
!
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
 login
```

FIGURE 5.7 – Script de configuration du routeur Ancien-Campus

```
hostname Nouveau_Campus
interface Loopback0
 ip address 2.2.2.2 255.255.255.0
 ip ospf network point-to-point
!
interface gigabitEthernet 0/0
 no shutdown
 ip address 192.168.12.2 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key vault
 duplex auto
 speed auto
!
interface gigabitEthernet 0/1
 no shutdown
 ip address 192.168.13.1 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Safe
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate always
!
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
 login
```

FIGURE 5.8 – Script de configuration du routeur Nouveau-Campus.

```
 hostname Soudani-Boudjema
interface Loopback0
 ip address 3.3.3.3 255.255.255.0
 ip ospf network point-to-point
!
interface gigabitEthernet 0/0
 no shutdown
 ip address 192.168.13.2 255.255.255.0
 ip ospf authentication
 ip ospf authentication-key vault
 duplex auto
 speed auto
!
interface gigabitEthernet 0/1
 no shutdown
 ip address 192.168.23.2 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Safe
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate always
!
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

FIGURE 5.9 – Script de configuration du routeur Soudani-Boudjema.

Analyse du trafic :

5.6 Configuration d'un VLAN et du Protocole VTP :

Scénario :

L'université de guelma a une conception de réseau plate et utilise uniquement des commutateurs de couche 2. Il n'y a qu'un seul VLAN et il y a eu des problèmes avec les applications qui génèrent trop de trafic de diffusion. C'est à nous de segmenter le réseau et d'implémenter certains VLAN.

Objectifs :

1. Créez les VLAN suivants et configurez les noms corrects :
   - VLAN 10 : nom Techniques
   - VLAN 20 : nom Staff
   - VLAN 30 : nom Recherche
   - VLAN 40 : nom Students
   - VLAN 50 : gestion des noms.
2. Configurez fa0 / 1 sur SW1 comme interface d'accès dans VLAN 10.
3. Configurez fa0 / 2 sur SW2 comme interface d'accès dans VLAN 20.
4. L'un des liens entre SW1 et SW2 doit utiliser l'encapsulation ISL.
5. L'un des liens entre SW2 et SW3 n'est pas autorisé à négocier dynamiquement un VTP.

6. L'un des liens entre SW1 et SW3 ne doit jamais envoyer de messages PAO.
7. Seuls les VLAN 1,10 et VLAN 20 sont autorisés entre SW1 et SW2.
8. Seuls les VLAN 1,10,20,40 et 50 sont autorisés entre SW2 et SW3.
9. Le VLAN natif entre SW1 et SW3 doit être le VLAN 50 sur les deux liaisons.

Topologie :

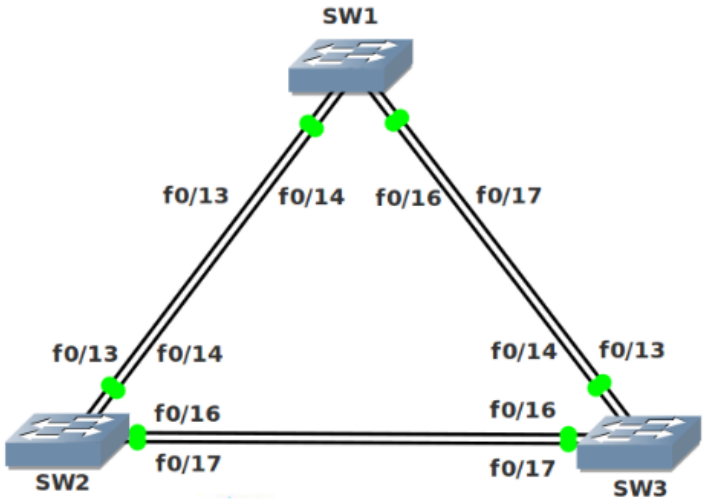

FIGURE 5.10 – Topologie du scénario VLAN et VTP.

Configuration et Scripts :

5.7 Configuration d'un service DHCP :

Scénario :

DHCP (DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer dynamiquement des adresses IP aux hôtes. DHCP fonctionne sur un modèle client-serveur, où le serveur DHCP envoie des informations de configuration aux clients DHCP suite à leur demande. La figure suivante montre la séquance des message echangé entre un serveur DHCP et un client afin de lui attribuer une addrese IP.

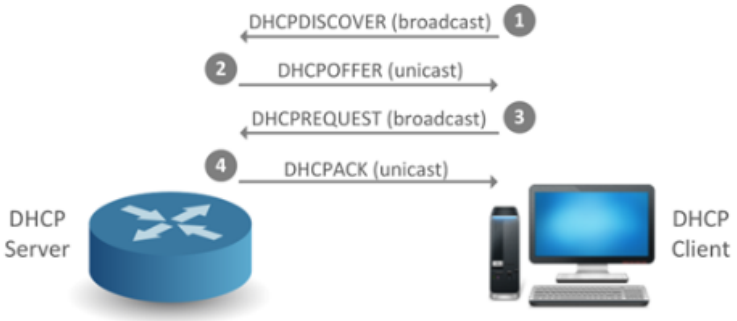

FIGURE 5.11 – Séquence d'échange des messages dans le protocole DHCP.

Les étapes illustrées dans le graphique sont expliquées ci-dessous :

1. Le système d'exploitation de l'hôte est configuré pour obtenir la configuration du réseau via DHCP, de sorte que l'hôte, agissant en tant que client DHCP, envoie un message de diffusion DHCPDISCOVER pour localiser un serveur DHCP.
2. Un serveur DHCP sur le sous-réseau local offre des paramètres de configuration, y compris une adresse IP, au client dans un message de unicast DHCPOFFER.
3. Le client DHCP renvoie une demande formelle pour l'adresse IP proposée au serveur dans un message de diffusion DHCPREQUEST.
4. Le serveur DHCP confirme que l'adresse IP a été effectivement allouée pour être utilisée par le client en renvoyant le message de monodiffusion DHCPACK final.

L'interaction précédente est valable lorsque le client et le serveur sont les deux sur le même sous-réseau . Si ce n'est pas le cas, un agent de liaison (DHCP Relay) est nécessaire, en plus du client et du serveur. Un DHCP ralay est tout hôte qui transmet les paquets DHCP entre les clients DHCP et les serveurs DHCP. L' IOS Cisco comprend à la fois le serveur DHCP et l'agent de liaison. Nous allons couvrir la configuration des deux fonctionnalités à travers la mise en place de la topologie suivante .

Topologie :

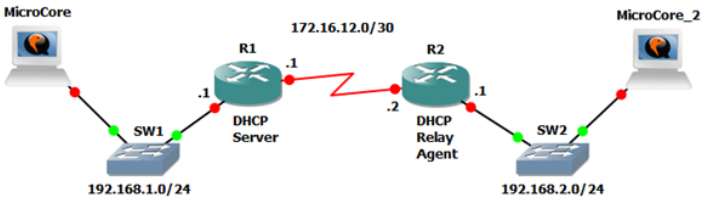

FIGURE 5.12 – Topologie d'un scénario DHCP.

Configuration et Scripts :

```
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1 192.168.1.50
ip dhcp excluded-address 192.168.2.1 192.168.2.50

ip dhcp pool Pool_R1
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1

   dns-server 192.168.1.1
   domain-name mydomian.dz
   lease 0 23 59
!
ip dhcp pool Pool_R2
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.1    dns-server 192.168.2.1
   domain-name mydomain.dz
   lease 0 23 59

no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3

ip tcp synwait-time 5

interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 172.16.12.1 255.255.255.252
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000

end
```

FIGURE 5.13 – Script du routeur R1

```
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 172.16.12.1
 duplex auto
 speed auto

interface Serial0/0
 ip address 172.16.12.2 255.255.255.252
 clock rate 2000000
end
```

FIGURE 5.14 – Script du routeur R2.

5.8 Configuration d'un Serveur de noms avec DNS

Scénario

Dans une établissement académique qui se respecte à l'échelle de notre université de 08 Mai 1945 Guelma . Une des choses que devons assurer est que les recherches DNS soient effectuées rapidement sans trop compter sur des serveurs DNS externes. dans cet optique, noua allons utiliser l'un de nos routeurs pour ce travail.

Objectifs

1. Toutes les adresses IP sont a configurées convenablement selon la topologie donnée.
2. OSPF a été préconfiguré pour une connectivité complète.
3. Configurez le routeur PRIMARY comme serveur DNS principal pour le domaine «Guelma.dz». Ce routeur doit utiliser le nom d'hôte ns1.Guelma.dz.
4. Configurez le routeur SECONDARY en tant que serveur DNS secondaire pour le domaine «Guelma.dz». Ce routeur doit utiliser le nom d'hôte ns2.Guelma.dz.
5. Le routeur CLIENT1 doit être capable de résoudre les noms d'hôte des serveurs DNS.
6. Le routeur CLIENT1 doit utiliser les deux serveurs DNS en utilisant la répétition alternée.
7. Le routeur CLIENT2 doit effectuer des recherches DNS à l'aide de CLIENT1.
8. Configurez une interface loopback0 sur le routeur CLIENT1 avec l'adresse IP 3.3.3.3 / 24.
9. Configurez le réseau afin que CLIENT1 réponde avec l'adresse IP 3.3.3.3 comme réponse DNS lorsque les serveurs DNS sont inaccessibles.

Topologie

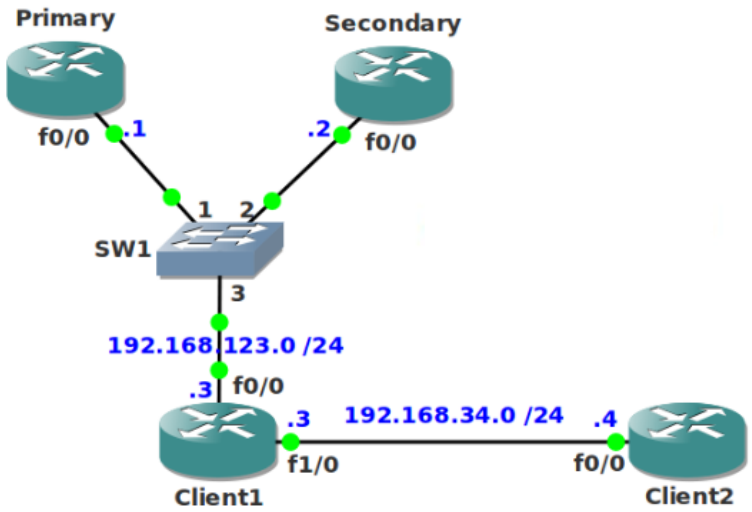

FIGURE 5.15 – Topologie du scénario DNS

Configuration et Scripts

```
hostname Primary
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip domain lookup
ip host Guelma.dz ns 192.168.123.1
ip host Guelma.dz ns 192.168.123.2
ip host ns1 192.168.123.1
ip host ns2 192.168.123.2
!
interface FastEthernet0/0
 ip address 192.168.123.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
no ip http server
no ip http secure-server
!
!
ip dns server
ip dns primary Guelma.dz soa ns1.Guelma.dz rene.Guelma.dz 21600 900 7776000 86400
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
end
```

FIGURE 5.16 – Script de configuration du routeur Primary

5.9 Réalisation d'un DMZ avec IPTables

Scénario

Un des problèmes les plus aigus pour la mise en ouvre de notre réseau et le problème de sécurité. Un DMZ (Demilitraized Zone ou zone démilitarisée) est une partie du réseau de l'université qui héberge les services les plus crucial de l'université tels que les serveurs Web , DNS , Mail etc qui sont exposés à l'extérieur et par conséquences assujettis à des menaces cyber-criminels. Nous avons décidé de réaliser notre DMZ grace à une machine Linux disposant 3 interfaces Ethernet et0, et1 et eth2 comme indiqué dans la topologie suivante.

Objectifs

1. l'interface eth0 est connecté au routeur avec un masque 255.255.255.2 et adresse 192.168.1.2
2. l'interface eth1 est connecté au DMZ avec une adresse 192.168.2.1 et un masque 255.255.255.0
3. l'interface eth2 est connecté au réseau interne de l'université avec une adresse 192.168.3.1et un masque 255.255.255.0
4. les requêtes vers certains ports de l'interface eth0 sont redirigé vers eth1 (DMZ)
5. le trafic provenant de eth0 vers eth1 passe sans aucun problème
6. le trafic provenant de eth2 vers eth1 passe sans aucun problème
7. le trafic passant de eth1 à eth0 est autorisé uniquement s'il s'agit à des réponses aux requêtes faites aux serveurs de la zone DMZ
8. le trafic passant de eth1 à eth2 est autorisé uniquement s'il s'agit à des réponses aux requêtes faites aux serveurs de la zone DMZ

Topologie

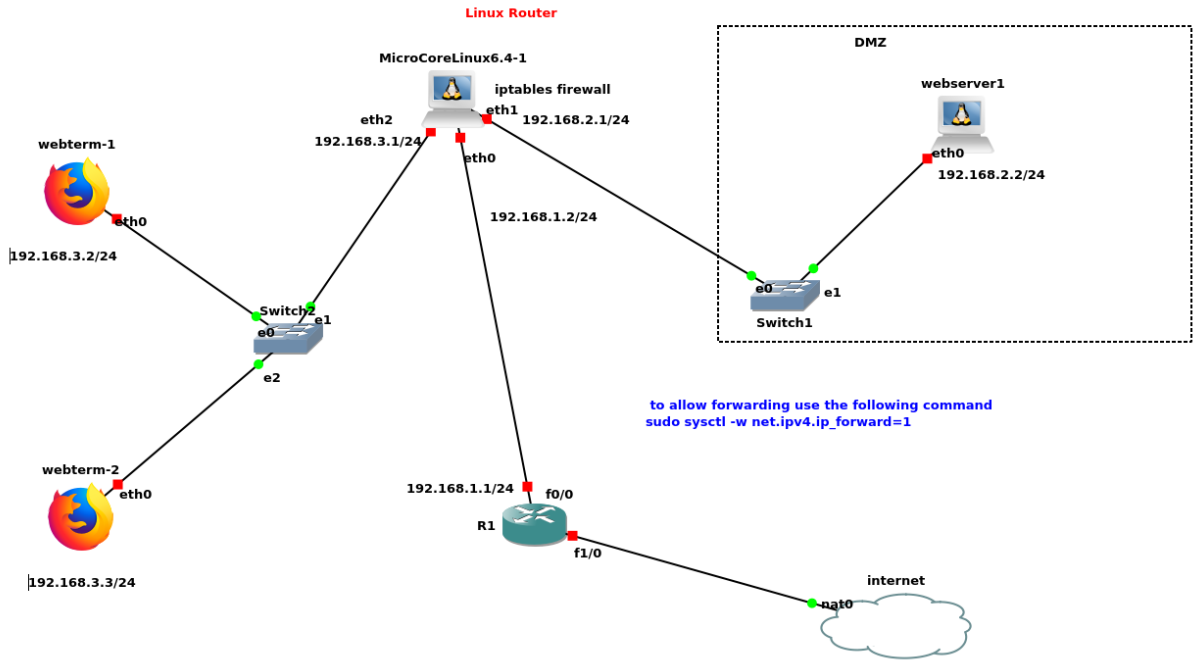

FIGURE 5.17 – Topologie pour le Scénario DMZ

Configuration et Scripts

La réalisation de la solution pour ce scénario passe par la configuration du IPTables au niveau de la machine Linux avec le script suivant :

```
#BASIC RULES
sudo iptables -F
sudo iptables  -t nat -F
sudo iptables -A INPUT -j DROP
sudo iptables -A OUTPUT -j DROP
sudo iptables -A FORWOARD -j DROP
#FORWORD RULES
#allow trafic goes from eth0 to eth1
sudo iptables -A FORWARD -i eth0 -o eth1 -s state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# allow trafic goes from eth1 to eth0 only for response for requests
sudo iptables -A FORWARD -i eth1 -o eth0 -s state --state ESTABLISHED,RELATED -j ACCEPT
#allow trafic goes from eth2 to eth1
sudo iptables -A FORWARD -i eth2 -o eth1 -s state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# allow trafic goes from eth1 to eth2 only for response for requests
sudo iptables -A FORWARD -i eth1 -o eth2 -s state --state ESTABLISHED,RELATED -j ACCEPT
#REDIRECTION from the outside to DMZ
sudo iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 53 -j DNAT --to 192.168.2.4:53
sudo iptables -t nat -A PREROUTING -p udp -i eth0 --dport 53 -j DNAT --to 192.168.2.4:53
sudo iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 -j DNAT --to 192.168.2.2:80
```

FIGURE 5.18 – configuration de la machine linux agissant en tant qu'un firewall pour la mise en place d'un DMZ

5.10 Conclusion :

Couvrir tous les protocoles et tous les services disponibles est impossible. Nous avons essayé de couvrir les plus importants notamment ceux des couches liaison et réseau sur lesquels s'appuient les autres protocoles/services des couches supérieurs. La mise en oeuvre des solutions sous formes des scénarios qui reflétèrent des cas potentiels pour notre université représente un point fort de notre travail. Nous pouvons facilement par la suite interpréter les même topologie sur le réseau physique.

Conclusion Générale

A tout début une fin. Nous arrivons à terme de ce rapport où nous avons veillé sans relâche qu'il soit un manuel pratique pour tout lecteur désirant se pencher sur la configuration et l'administration des parcs et réseaux informatiques.

Nous avons commencé par survoler les généralités des réseaux afin de préparer le terrain aux démonstrations abordés durant tous les autres chapitres.

Commençons par discuter l'administration sous un environnement Linux et puis IOS, ceci représente une pierre angulaire dans tout système réseau, avant de basculer à la simulation/ émulation et virtualisation des réseaux. Ce sujet représente une intérêt particulier parce que ne nous pouvons pas valider nos conceptions qu'à travers ces outils, vu l'absence d'un environnement d'expérimentation physique. Finalement, nous avons pris une démarche progressive pour présenter nos architectures et conception des différentes solutions réseaux proposées. Nous avons démarré avec la gestion des machines virtuelles, puis nous avons intéressé par des problèmes de routage statique et dynamique avec le protocole OSPF avant de se pencher à d'autres problèmes de switching tels que les VLAN et VTP . Nous avons aussi proposé quelques services réseaux comme la gestion dynamique des adresses IP via DHCP ainsi que la gestion des noms de domaines avec DNS.

Nous n'avons pas oublié les problèmes récurrents liés à la sécurisation des serveurs et des machines ainsi que tout le réseau et nous avons proposé. Dans ce cadre là, des architectures réseaux incluant des pare-feu déployé dans des passerelle faisant alors ce que est appelé des DMZ (des Zones Démilitarisés) ont été présenté , le pare-faux est implémenté avec l'outil de référence IPTables qui permet aussi de configurer le protocoles de translation des adresse NAT qui un protocole indispensable pour les fournisseurs des services internet ISP .

Malgré toutes les solutions proposées et validées à travers la simulation GNS3 et les outils qui tournent dans son orbite. Nous considérons que notre travail mérite d'être enrichie par la mise en oeuvre réel sur un réseau physique où nous allons rencontrer d'autres problème de natures différentes liés essentiellement à des besoins non fonctionnelles (d'ordres ergonomiques par exemple).

Nous rappelons aussi que la plupart des nos architectures sont concentrées dans les deux couches Réseaux et Liaison du modèles OSI. Or, des configurations au niveau transport et au niveau applicatifs sont indispensables. Nous envisageons de continuer notre travail dans ce sens par l'intégration des politiques de qualité de service, des systèmes de monitoring ainsi que d'autre services applicatifs à l'instar des serveurs mail, annuaire et bien d'autre en relation avec l'automatisation des processus métier des organisations.

Bibliographie

[BOU15] BOURNANE Fazia, K. Y. « Etude et configuration d'un réseau de campus (SONATRACH Béjaïa) ». Mém. de mast. Bejaia : UNIVERSITE ABDERRAHMANE MIRA, 2015.

[BOU16] BOUBEKRI Sara, M. R. « La haute disponibilité des réseaux campus. Cas d'étude : Sonatrach ». Mém. de mast. Bejaia : UNIVERSITE ABDERRAHMANE MIRA, 2016.

[Boy16] Boyce, G. *Linux Networking Cookbook*. Packt Publishing Ltd, 2016.

[Hea10] Headquarters, C. *Cisco IOS Configuration Fundamentals Command Reference*. 2010. URL : https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.pdf.

[LaC15] LaCroix, J. *Mastering Linux Network Administration*. Packt Publishing Ltd, 2015.

[Low03] Lowe, D. *Networking for dummies*. John Wiley & Sons, 2003.

[Mol20] Molenaar, R. *Cisco R & S Labs*. 2020 (accessed September 10, 2020). URL : https://gns3vault.com/.

[Mon04] Montagnier, J.-L. *Réseaux d'entreprise par la pratique*. Editions Eyrolles, 2004.

[MS13] Meinel, C. et Sack, H. « The Foundation of the Internet : TCP/IP Reference Model ». In : *Internetworking*. Springer. 2013, p. 29-61.

[MVC16] Mukhedkar, P., Vettathu, A. et Chirammal, H. D. *Mastering KVM Virtualization*. Packt Publishing, Limited, 2016.

[Neu15] Neumann, J. C. *The book of GNS3 : build virtual network labs using Cisco, Juniper, and more*. No Starch Press, 2015.

[Pur04] Purdy, G. N. *Linux iptables Pocket Reference : Firewalls, NAT & Accounting*. " O'Reilly Media, Inc.", 2004.

[SF99] Sportack, M. A. et Fairweather, J. *IP routing fundamentals*. Cisco Press, 1999.

[SS06] Stanfield, V. et Smith, R. W. *Linux System Administration : Craig Hunt Linux Library*. John Wiley & Sons, 2006.

[TB11] Tafa, F. et Browning, P. *101 Labs for the Cisco CCNP Exams*. Reality Press Ltd, 2011.

[Ton05] Tony Bautts, T. D. *Linux network administrator's guide, Third Edition*. " O'Reilly Media, Inc.", 2005.

[Zim80] Zimmermann, H. « OSI reference model-the ISO model of architecture for open systems interconnection ». In : *IEEE Transactions on communications* t. 28, n° 4 (1980), p. 425-432.