

**République Algérienne Démocratique et Populaire**

**Ministère de l'enseignement supérieur et de la recherche scientifique**

**UNIVERSITE KASDI MERBAH OUARGLA**

**Faculté des Nouvelles Technologies de l'Information et de la Communication**

**Département d'Informatique et des Technologies de l'information**



**Pour l'obtention du diplôme de Master en Informatique**

**Domaine : Mathématique et Informatique**

**Filière : Informatique**

**Spécialité : Administration et sécurité des Réseau**

**Thème**

**Monitoring Réseau**

**Encadré Par :**

*Hamioud Sohaib*

**Présenté par :**

*Hammacha Sonia*

**Année Universitaire : 2021/2022**

# Table des matières

Table des matières	- 2 -
Dédicace	- 4 -
Remerciements	- 5 -
Résumé	- 6 -
Liste des figures	- 7 -
Liste des tableaux	- 9 -
Introduction générale	- 1 -
<b>Chapitre 1 : Généralités sur les réseaux</b>	<b>- 2 -</b>
1. Définitions	- 1 -
1.1 Les réseaux	- 1 -
1.2 Réseaux informatiques	- 1 -
2. Types des réseaux	- 1 -
2.1 Réseau personnel	- 1 -
2.2 Réseau local	- 2 -
2.3 Réseau métropolitain	- 2 -
2.4 Réseau étendu	- 3 -
2.5 Réseau de stockage	- 3 -
2.6 Réseau régional	- 4 -
3. Le modèle OSI	- 4 -
3.1 Couche Physique	- 5 -
3.2 Couche Liaison	- 5 -
3.3 Couche Réseau	- 5 -
3.4 Couche Transport	- 5 -
3.5 Couche Session	- 5 -
3.6 Couche Présentation	- 6 -
3.7 Couche Application	- 6 -
4. Le modèle TCP/IP	- 6 -
4.1 La Couche D'application	- 7 -
4.2 La Couche Transport	- 7 -
4.3 La Couche Internet	- 7 -
4.4 La Couche Accès Réseau	- 8 -
5. La différence entre le modèle OSI et le modèle TCP/IP	- 8 -
6. L'adressage IP	- 9 -
6.1 Les types d'adresse IP	- 9 -
6.2 Adressage en classe	- 9 -
6.3 Masque de sous-réseau	- 10 -
6.4 Passerelle par défaut	- 10 -
7. Les supports de transmission	- 10 -
7.1 Le câble coaxial	- 11 -
7.2 La paire torsadée	- 11 -

7.3	La fibre optique	11
8.	<i>Les topologies</i>	11
9.	<i>Les Méthodes d'accès</i>	13
10.	<i>Equipements réseau</i>	14
10.1	Les modems	14
10.2	Les concentrateurs (Hubs)	14
10.3	Les commutateurs (Switch)	15
10.4	Le routeur	15
11.	<i>Sécurité informatique</i>	15
<b>Chapitre 2 : Réseau ENAFOR</b>		<b>17</b>
1.	<i>Historique</i>	18
2.	<i>Direction Technologies de Communication et de l'Information</i>	19
3.	<i>Département Administration Système et Réseau</i>	19
3.1	Administration Réseaux	20
3.2	Administration Systèmes	20
3.3	Administration ERP	21
4.	<i>Schéma du réseau ENAFOR</i>	22
4.1	Connexion entre siège social et chantiers distants	24
4.2	Architecture du siège social	25
5.	<i>Data Center</i>	26
6.	<i>Les chantiers distants</i>	28
<b>Chapitre 3 : Simulation basée-GNS3 du réseau ENAFOR</b>		<b>30</b>
1.	<i>Présentation de GNS3</i>	31
2.	<i>Installation et Configuration de GNS3 :</i>	31
3.	<i>Simulation du réseau informatique ENAFOR</i>	36
<b>Chapitre 4 : Développement et mise en œuvre de l'application Monitoring Réseau</b>		<b>42</b>
1.	<i>La mise en relation de l'administrateur avec GNS3</i>	43
1.1	Le Cloud	43
1.2	La carte de bouclage	43
2.	<i>Développement de l'application de Monitoring Réseau</i>	44
2.1	Langage de programmation	44
2.2	Les fonctionnalités de l'application	45
3.	<i>Les problèmes réseau détectés par l'application</i>	48
3.1	Problème de connectivité	48
3.2	Problème de disponibilité des équipements	49
3.3	Problème de conflit d'adressage	49
<b>Conclusion générale</b>		<b>51</b>
<b>Références</b>		<b>52</b>

# Dédicace

A ma mère, qui m'a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et présence dans ma vie, reçois à travers ce travail aussi modeste, soit-il l'expression de mes sentiments et d'éternelle gratitude.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse dieu faire en sorte que ce travail porte son fruit, merci pour les valeurs nobles, l'éducation et le soutien permanent venus de vous.

Mes frères qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité.

Mes chères copines Halima et Djihad et Inass, vous êtes les personnes qui m'ont toujours encouragé et soutenu moralement

# Remerciements

Avant toute personne, nous tenons à remercier ALLAH le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

Nous tenons à exprimer notre sincère gratitude à notre encadreur Mr.Hamioud Sohaib pour ses conseils et ses encouragements tout au long de ce projet.

Nous tenons à exprimer toute notre gratitude à tous les membres de jury, pour avoir bien voulu juger notre travail.

Nous voulons aussi adresser nos sincères remerciements à tous les enseignants de département de l'informatique qui ont contribué à notre formation.

Aussi nos parents qui nous ont toujours soutenus et encouragés au cours de ce mémoire.

A ma famille pour son soutien tout au long de mon stage de fin d'étude. Je tiens à exprimer toute ma reconnaissance au super viseur de stage Mr. Boulifa Ismail .je le remercie de m'avoir encadré, orienté, aidé Et conseillé.

A Monsieur le directeur des Technologies de l'information et au secrétaire pour m'avoir accueilli

A Monsieur le chef du département Système et Réseau pour m'avoir intégré dans son équipe

Aux administrateurs Réseaux pour avoir élargi mes connaissances

Aux administrateurs SAP pour leur générosité

A toute la cellule informatique d'ENAFOR pour son accueil chaleureux

Et à tout le personnel d'ENAFOR Merci pour cette expérience passée à vos coté.

# Résumé

Les réseaux informatiques sont essentiels pour fournir des services dans tous les domaines et assurer la transmission des données entre les sites éloignés d'un établissement ou d'une entreprise. Les erreurs et les pannes qui peuvent toucher les réseaux informatiques présentent des risques indéniables au bon fonctionnement de l'entreprise et sa performance. La présence d'un administrateur qui gère les éventuelles erreurs du réseau d'entreprise demeure indispensable. Pour faciliter son travail, un système d'administration réseau en temps réel est généralement utilisé.

Les systèmes d'administration existants sont payants et limités en termes de fonctionnalités. En Algérie, plusieurs entreprises ne disposent pas d'un système d'administration réseau (e.g., ENTP) ou utilisent un système d'administration limité (e.g., ENAFOR).

Ce projet a été réalisé dans le cadre de la mise en place d'un système d'administration réseau de l'Entreprise Nationale du Forage (ENAFOR). L'objectif du système est de superviser le fonctionnement du réseau en temps réel et, en cas de panne, informe l'administrateur du réseau immédiatement par une notification (par email).

Nous avons développé une application de monitoring et de gestion du réseau informatique ENAFOR. Pour valider notre travail et tester cette application, nous avons simulé ce réseau et exécuté des scénarios de panne possibles.

Mots clés : Réseaux Informatiques, Monitoring, Simulation, Détection de pannes

# Liste des figures

FIGURE 1: RESEAU PAN.....	- 1 -
FIGURE 2: RESEAU LAN .....	2
FIGURE 3: RESEAU MAN .....	2
FIGURE 4: RESEAU WAN .....	3
FIGURE 5: RESEAU DE STOCKAGE .....	3
FIGURE 6: ARCHITECTURE DE MODELE (OSI) .....	4
FIGURE 7: ARCHITECTURE DE MODELE (TCP/IP) .....	6
FIGURE 8: ARCHITECTURE DE MODELE (OSI-TCP/IP).....	8
FIGURE 9: LES CLASSES DE RESEAU .....	9
FIGURE 10: CABLE COAXIAL .....	11
FIGURE 11: PAIRE TORSADEE.....	11
FIGURE 12: FIBRE OPTIQUE.....	11
FIGURE 13: TOPOLOGIE EN ANNEAU.....	12
FIGURE 14: TOPOLOGIE EN ANNEAU.....	12
FIGURE 15: TOPOLOGIE DE RESEAU EN ETOILE .....	12
FIGURE 16: TOPOLOGIE DE RESEAU MAILLE .....	13
FIGURE 17: MODEM .....	14
FIGURE 18: HUB .....	14
FIGURE 19: COMMUTATEUR .....	15
FIGURE 20: ROUTEUR .....	15
FIGURE 21: SECURITE DE L'INFORMATION.....	16
FIGURE 22: ORGANIGRAMME DE LA DIRECTION TECHNOLOGIE DE COMMUNICATION ET DE L'INFORMATION .....	19
FIGURE 23: ORGANIGRAMME DEPARTEMENT ADMINISTRATION SYSTEMES ET RESEAUX.....	20
FIGURE 24: SCHEMA DU RESEAU ENAFOR.....	22
FIGURE 25: LA LIAISON ENTRE LE SIEGE WORKOVER ET LA BASE LOGISTIQUE .....	23
FIGURE 26 : COMMENT RELIER LA BASE MAINTENANCE & LE BASE TRANSPORT AVEC UN RESEAU WIRELESS .....	23
FIGURE 27: L'ARCHITECTURE GENERALE .....	24
FIGURE 28: CONNEXION ENTRE SIEGE SOCIAL ET CHANTIERS DISTANTS .....	24
FIGURE 29: CONNEXION ENTRE LES SITES.....	25
FIGURE 30: RECEPTION ET EMISSION COTE CHANTIERS DISTANT.....	29
FIGURE 31: LANCEMENT GNS3 .....	31
FIGURE 32 : INSTALLATION .....	32
FIGURE 33.....	33
FIGURE 34.....	33
FIGURE 35.....	33
FIGURE 36.....	33
FIGURE 37-34-35-36 : INSTALLATION WINPCAP .....	33
FIGURE 38 : TERMINER L'INSTALLATION DE GNS3 .....	33
FIGURE 39 : LANCEMENT DE SIMULATEUR CISCO (GNS3).....	34
FIGURE 40: EXEMPLE D'UN ROUTEUR CISCO IOS TELECHARGE .....	34
FIGURE 41 : CHARGEMENT MANUEL IOS IMAGE .....	35
FIGURE 42: IMPORTER ET DECOMPRESSER DES IMAGES .....	35
FIGURE 43 : CREATION D'UN PROJET SOUS GNS3 .....	36
FIGURE 44 : AJOUT DES ROUTEURS SOUS GNS3.....	36
FIGURE 45: LES CINQ ROUTEURS REPRESENTANT LES CINQ SITES ENAFOR.....	37
FIGURE 46: CONNEXION DU ROUTEUR SIEGE AUX DIFFERENTS SITES (ROUTEURS).....	37
FIGURE 47: CONNEXION DES EQUIPEMENTS PAR UN CABLE FASTETHERNET .....	38
FIGURE 48: CONSOLE DU ROUTEUR SIEGE .....	38
FIGURE 49 : RESUME DE TOPOLOGIE .....	39
FIGURE 50: LE RESEAU ENAFOR .....	39

FIGURE 51: CREATION CLOUD .....	43
FIGURE 52: CONFIGURATION DE LA CARTE RESEAU.....	43
FIGURE 53: CONFIGURATION DU CLOUD .....	44
FIGURE 54: CONNEXION DU CLOUD AVEC LE RESEAU ENAFOR .....	44
FIGURE 55: LA PLATEFORME DE PROGRAMMATION VISUAL STUDIO 2019 .....	45
FIGURE 56: L'INTERFACE DE L'APPLICATION MONITORING RESEAU.....	45
FIGURE 57: LANCEMENT DE GNS3 .....	46
FIGURE 58: AJOUT D'UN EQUIPEMENT A L'APPLICATION.....	47
FIGURE 59: LE SCHEMA FINAL DU RESEAU AVEC LE MONITEUR RESEAU .....	47
FIGURE 60: PROBLEME DE CABLAGE .....	48
FIGURE 61: NOTIFICATION PAR EMAIL D'UN PROBLEME DE CABLAGE .....	48
FIGURE 62: ARRET DU ROUTEUR TRANSPORT .....	49
FIGURE 63: NOTIFICATION PAR EMAIL .....	49
FIGURE 64 : DETECTION D'UN CONFLIT D'ADRESSES .....	50
FIGURE 65: NOTIFICATION PAR EMAIL D'UN PROBLEME DE CONFLIT D'ADRESSAGE.....	50



# Liste des tableaux

TABLEAU 1: LES CLASSES DE RESEAU .....	9
TABLEAU 2: CLASSES ET MASQUES RESEAU .....	10
TABLEAU 3: ARMOIRE DES SWITCH & ROUTEURS .....	26
TABLEAU 4: ARMOIRE DES SERVEURS ERP .....	27
TABLEAU 5: ARMOIRE DES SERVEURS MESSAGERIES & ANTIVIRUS .....	28
TABLEAU 6 : COMMANDES POUR CONFIGURER UN ROUTEUR .....	40
TABLEAU 7 : CONFIGURATION DU PROTOCOL DE ROUTAGE RIP .....	40
TABLEAU 8: ADRESSE IP UTILISES POUR CHAQUE ROUTEUR D'UN SITE .....	41

# Introduction générale

Un réseau informatique en entreprise est aussi important que le système nerveux chez l'être humain. Garantir sa disponibilité et son bon fonctionnement demeure primordiale. Le nombre de nœuds interconnectés au sein d'un réseau ne cesse d'augmenter. Le nombre important des équipements réseau ainsi que les sites géographiquement éloignés pose plusieurs problèmes de disponibilité et de maintenance. Les pannes éventuelles doivent être détectées immédiatement et réglées le plus tôt possible

Pour s'assurer que les services rendus par les réseaux soient disponibles et convenables, il est nécessaire de surveiller et d'agir quand une erreur se produit. Pour se faire, il faut obtenir les données de gestion des équipements des réseaux et, si nécessaire, contrôler ces équipements en utilisant des outils de supervision et d'administration des réseaux.

Il existe déjà un grand nombre d'outils et de plateformes conçus pour l'administration de grands réseaux locaux et distants. Ils sont prévus pour gérer un grand nombre d'équipements et supportent le protocole standard d'administration réseau SNMP (Simple Network Management Protocol). Cependant la majorité des outils d'administration existants sont des systèmes propriétaires, limités en termes de fonctionnalités, et leurs coûts est très élevés.

En Algérie, plusieurs entreprises ne disposent pas d'un système d'administration réseau (e.g., ENTP) ou utilisent un système de supervision et d'administration limité (e.g., ENAFOR). Alors que ENAFOR utilise un système d'administration pour gérer son réseau informatique, ses fonctionnalités sont limités. Par exemple, si un équipement du réseau tombe en panne, le problème est signalé à l'administrateur manuellement.

Pour répondre à ces problèmes, nous travaillons avec l'équipe d'administration réseaux de la direction informatique ENAFOR pour réaliser une application de monitoring réseau, testée sur une plateforme virtuelle qui simule le réseau informatique de l'entreprise. Cet outil permet de collecter des données sur les routeurs, les serveurs, les commutateurs, et les équipements réseau. Ainsi, il permet de notifier immédiatement par email, en cas de panne, l'administrateur en spécifiant la source de problème.

# Chapitre 1 : Généralités sur les réseaux

# 1. Définitions

## 1.1 Les réseaux

Un réseau est un ensemble d'infrastructures bien organisées permettant de rendre des services à un ou plusieurs usagers. En informatique, un réseau est un ensemble d'entités permettant de faire circuler des données entre plusieurs ordinateurs [1].

## 1.2 Réseaux informatiques

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs en vue d'échanger, de partager des données, des ressources ou des informations. En d'autre terme, c'est une infrastructure de communication reliant des équipements informatiques (ordinateur, concentrateur, commutateur, routeur, imprimante...) permettant de partager desressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles) [1].

## 2. Types des réseaux

### 2.1 Réseau personnel

Un réseau personnel PAN (Personal Area Network) interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, un agenda électronique [1].

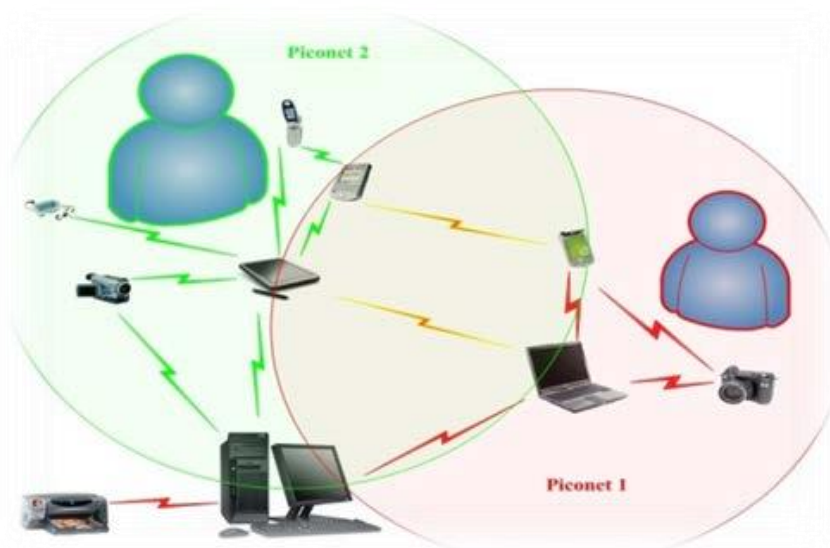


Figure 1: Réseau PAN

## 2.2 Réseau local

Un réseau LAN (Local Area Network) est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). Un réseau local est donc un réseau sous sa forme la plus simple. Des réseaux locaux offrent en général une bande-passant comprise entre 4M bits/s et 1000Mbits/s [1].



Figure 2: Réseau LAN

## 2.3 Réseau métropolitain

Un réseau métropolitain. MAN (Métropolitain Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres) à des débits importants. Ainsi un MAN permet à deux Nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local .un MAN est formé de commutateur ou routeurs interconnectés par des liens hauts débits(en général en fibre optique) [1].

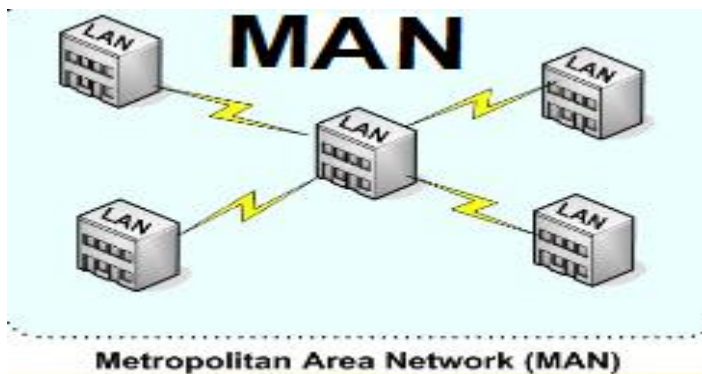


Figure 3: Réseau MAN

## 2.4 Réseau étendu

Un réseau étendu WAN (Wide Area Network) interconnecte plusieurs réseaux locaux à travers de grandes distances géographiques. Les infrastructures physiques peuvent être terrestres ou spatiales à l'aide de satellites de communication. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des trajets le plus approprié pour atteindre un nœud du réseau. Le plus connue des WAN est Internet [1].

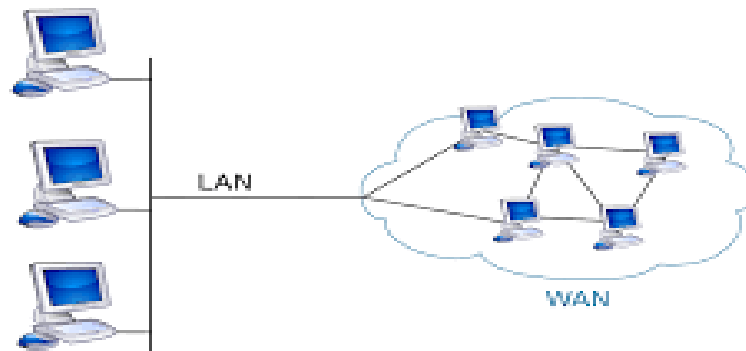


Figure 4: Réseau WAN

## 2.5 Réseau de stockage

Un réseau SAN (Storage Area Network), est un réseau spécialisé permettant de mutualiser des ressources de stockage [].

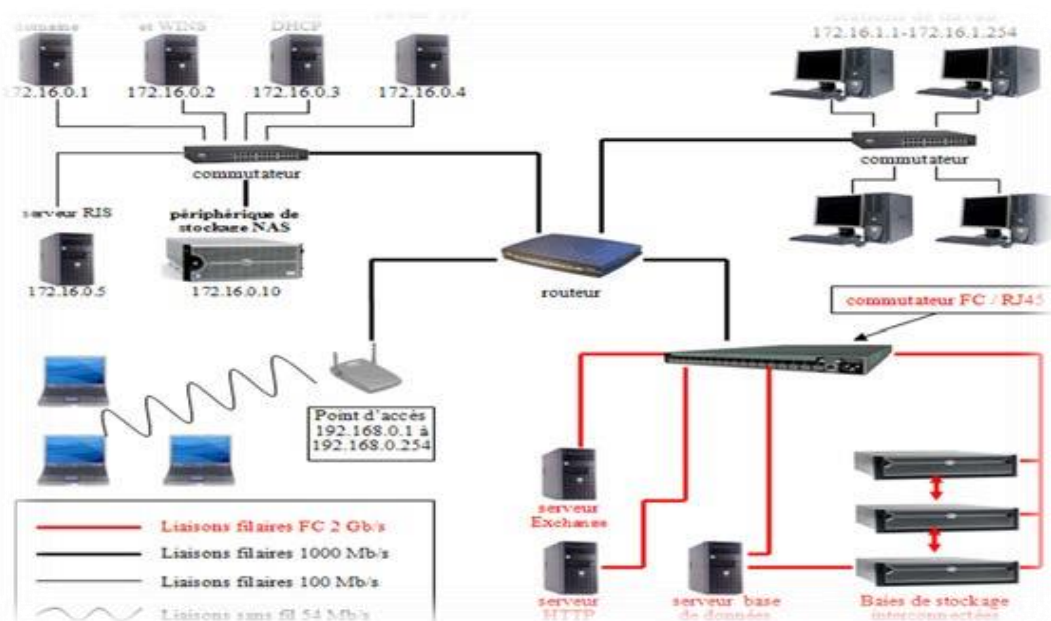


Figure 5: Réseau de stockage

## 2.6 Réseau régional

Un réseau RAN (**R**egional **A**rea **N**etwork) est un réseau de télécommunications, en général sans fil, installé par des utilisateurs d'internet en zone rurale. Un tel réseau permet l'accès internet à haute vitesse dans une zone non desservie par les fournisseurs traditionnels [1].

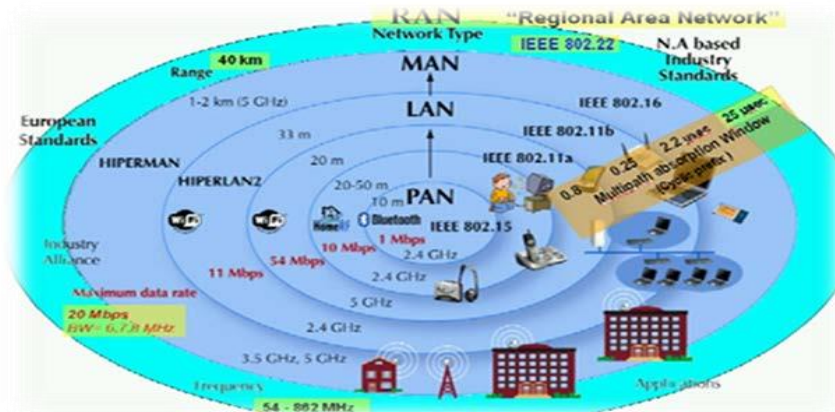


Figure 6 : Réseau RAN

## 3. Le modèle OSI

OSI signifie (Open Systems Interconnect), ce qui se traduit par Interconnexion de systèmes ouverts). Ce modèle a été mis en place par l'ISO afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs. En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire). Ainsi de nombreux réseaux incompatibles coexistaient. C'est la raison pour laquelle l'établissement d'une norme a été nécessaire. Le rôle du modèle OSI consiste à standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles pour peu qu'ils respectent scrupuleusement le modèle OSI [2].

Le modèle OSI comporte sept couches [2] :

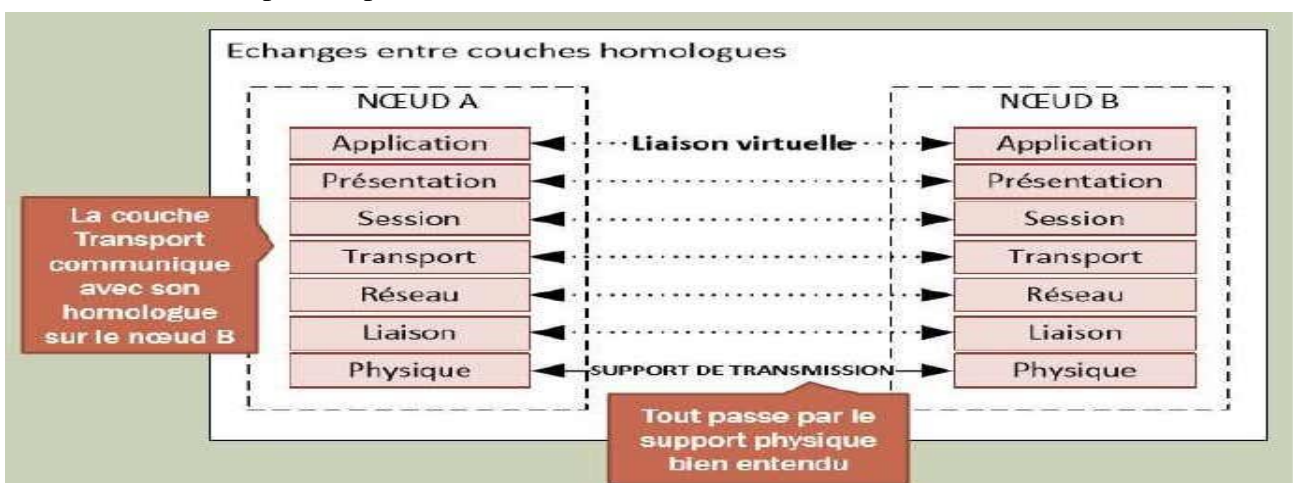


Figure 6: Architecture de modèle (OSI)

### **3.1 Couche Physique**

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit être bien reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données. L'unité d'information typique de cette couche est le BIT, représenté par une certaine différence de potentiel.

### **3.2 Couche Liaison**

Le support n'est pas parfait, il peut se rompre ou générer des erreurs de transmission. Il faut donc le contrôler, c'est le rôle de la couche 2. Elle a pour rôle principal de

S'assurer du transfert de blocs de données entre les équipements directement connectés avec un taux d'erreurs négligeable. L'unité d'information au niveau de la couche Liaison s'appelle TRAME.

### **3.3 Couche Réseau**

Le rôle principal de la couche réseau est la détermination du meilleur chemin qui doit être utilisé pour transporter les Paquets jusqu'à la destination. Le chemin entre la source et la destination peut s'établir de deux manières différentes :

- En mode data gramme : le choix est effectué indépendamment pour chaque paquet,
- En mode circuit virtuel : le choix est fixé à l'établissement de la connexion, et pour toute la durée de la connexion.

L'unité d'information au niveau de la couche réseau s'appelle PAQUET ou DATAGRAMME

### **3.4 Couche Transport**

La couche transport est la quatrième couche du modèle de référence OSI, la dernière couche des services de bas niveau. Elle assure l'interface entre les aspects applicatifs et les aspects liés à la transmission des données sur un réseau informatique. Les entités communicantes ne sont plus des stations mais des processus (programmes). L'unité d'information au niveau de la couche transport s'appelle *Segment*.

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites (on parle de la SEGMENTATION) et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux

### **3.5 Couche Session**

Cette couche organise et synchronise les échanges entre tâches distantes. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.



### 3.6 Couche Présentation

Pour que deux systèmes puissent se comprendre, ils doivent utiliser le même système de représentation des données. La couche présentation gère cette représentation universelle des données échangées par des systèmes. Il existe plusieurs façons de Représenter des données, par exemple, l'ASCII et l'EBCDIC pour les fichiers texte. La Couche présentation utilise un langage commun compréhensible par tous les nœuds du réseau. Cette couche détermine la forme sous laquelle s'échangent les données entre les ordinateurs du réseau. Cette couche gère aussi tous les problèmes de sécurité du réseau offrant des services tels que le cryptage des données. Elle permet aussi la compression des données de façon à réduire le nombre de bits à transmettre

### 3.7 Couche Application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie est la fenêtre par laquelle les processus d'application accèdent aux services du réseau

## 4. Le modèle TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle TCP/IP, comme nous le verrons plus bas, s'est progressivement imposé comme modèle de référence qui remplace le modèle OSI. Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients [4].

L'architecteur modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches [4] :

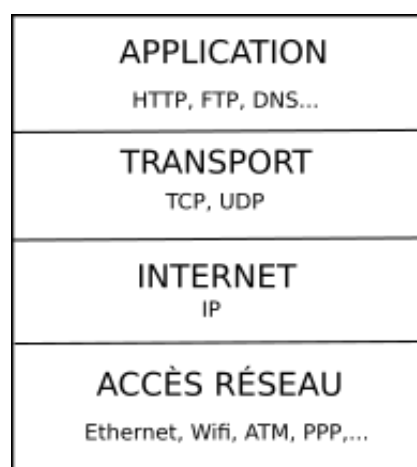


Figure 7: Architecture de modèle (TCP/IP)

## 4.1 La Couche D'application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, tel que :

- **FTP** : (File Transfer Protocol) protocole de transfert de fichiers : protocole qui fournit un moyen efficace de transfert des fichiers d'un ordinateur à un autre.
- **SMTP** : (Simple Mail Transfer Protocol) protocole de transfert de courriers électroniques.
- **HTTP** : (Hyper Texte Transfer Protocol) protocole de transfert hypertexte assure le transfert de page hypertexte entre un serveur web et un client web (navigateur web).
- **TELNET** : permet d'établir une connexion hôte distante et de gérer les données locales.

## 4.2 La Couche Transport

Son rôle est le même que celui de la couche transport du modèle OSI. La couche transport permet à des applications tournant sur des machines distantes de communiquer, elle assure l'acheminement des données ainsi que les mécanismes permettant de connaître l'état de la transmission, elle définit deux protocoles différents TCP et UDP.

- **TCP** : (Transmission Control Protocol) il a été développé pour assurer que les connexions entre deux ordinateurs sont établies et maintenues.
- **UDP** : (User Datagram Protocol) il fournit un service en mode non connecté elle détecte les erreurs mais ne les corrige pas (accusé de réception).

## 4.3 La Couche Internet

La couche Internet est la couche la plus importante du modèle TCP/IP, elle réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

Elle utilise les protocoles suivants :

- **IP** : (Internet Protocol) le protocole IP gère l'adressage logique des ordinateurs.
- **ICMP** : (Internet Control Message Protocol) gère les erreurs et envois des messages d'erreurs au TCP/IP.
- **ARP** : (Adresse Résolution Protocol) établit une correspondance entre les adresses logiques (IP) et les adresses physiques (MAC).

## 4.4 La Couche Accès Réseau

Elle est appelée aussi couche hôte, elle spécifie la forme sous laquelle les données sont acheminées quel que soit le type du réseau, elle assure la conversion des signaux (analogique/numérique), elle contrôle des erreurs à l'arrivée. En effet, elle semble "regrouper" les couches physiques et liaison de données du modèle OSI.

## 5. La différence entre le modèle OSI et le modèle TCP/IP

TCP / IP et OSI sont les deux modèles de réseau les plus utilisés pour la communication. Il existe des similitudes et des différences entre eux. L'une des principales différences est que l'OSI est un modèle conceptuel qui n'est pas utilisé de manière pratique pour la communication, alors que TCP / IP est utilisé pour établir une connexion et communiquer à travers le réseau. Principales différences entre le modèle TCP / IP et OSI est :

- TCP / IP est un modèle client-serveur, c'est-à-dire lorsque le client demande un service, il est fourni par le serveur. Considérant que, OSI est un modèle conceptuel.
- TCP / IP est un protocole standard utilisé pour tous les réseaux, y compris Internet, tandis que l'OSI n'est pas un protocole, mais un modèle de référence utilisé pour comprendre et concevoir l'architecture du système.
- TCP / IP est un modèle à quatre couches, alors que l'OSI comporte sept couches.
- TCP / IP suit l'approche verticale. D'autre part, le modèle OSI prend en charge l'approche horizontale.
- TCP / IP est tangible, alors qu'OSI ne l'est pas.
- TCP / IP suit une approche de haut en bas, tandis que le modèle OSI utilise une approche de bas en haut [4].

OSI	TCP/IP
Application	Application
Presentation	
Session	Transport
Transport	
Network	Network
Data link	Physical
Physical	

Figure 8: Architecture de modèle (OSI-TCP/IP)

## 6. L'adressage IP

L'adresse IP (Internet Protocol) désigne un numéro unique attribué de manière provisoire ou durable à un ordinateur connecté à un réseau informatique qui utilise l'internet protocole. Cette suite de chiffres joue un rôle d'identification du branchement et permet l'acheminement (c'est-à-dire le routage) des paquets de données sur Internet [5].

### 6.1 Les types d'adresse IP

Il existe deux types d'adresses IP qui sont :

- **Adresse statique** : elle est assignée de façon permanente c'est-à-dire ne change jamais.
- **Adresse dynamique** : assignée d'une façon temporaire.

### 6.2 Adressage en classe

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le routage) des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum [7].

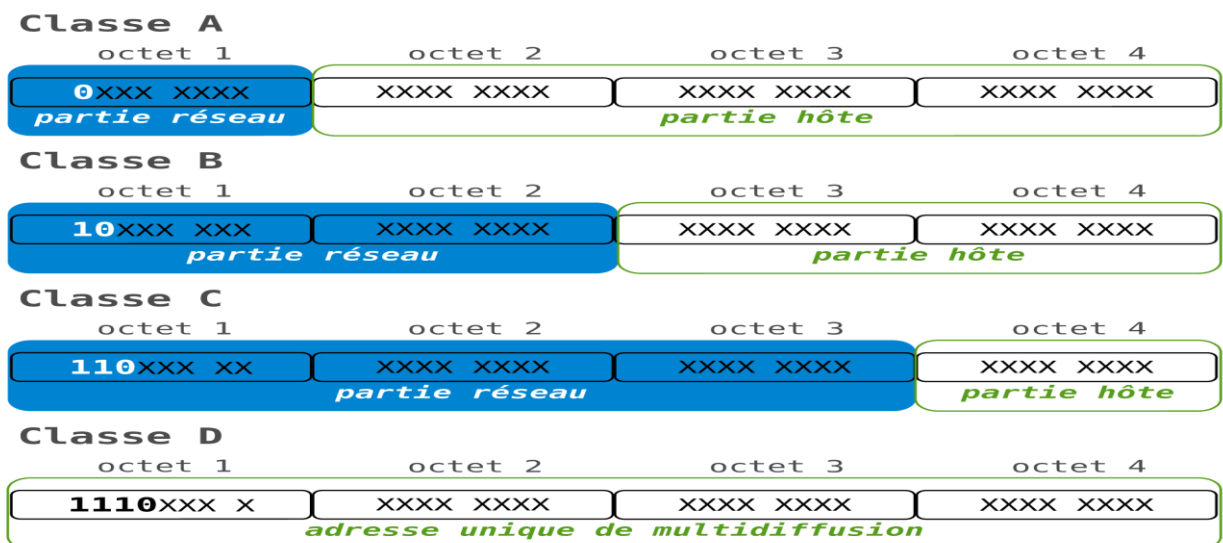


Figure 9: Les classes de réseau

Le tableau ci-dessus montre les 5 classes de réseaux utilisés sur Internet.

Tableau 1: Les classes de réseau

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	127.255.255.255	/08	255.0.0.0

<b>Classe B</b>	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
<b>Classe C</b>	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
<b>Classe D</b> (multi diffusion)	1110	224.0.0.0	239.255.255.255	/04	non défini
<b>Classe E</b> (réservée)	1111	240.0.0.0	255.255.255.255		non défini

### 6.3 Masque de sous-réseau

Cette donnée indique la partie de votre adresse qui caractérise le réseau local sur lequel votre hôte est connecté, et lui permet de déterminer, pour n'importe quelle adresse IP, si celle-ci fait ou non partie du réseau local. Le masque de sous-réseau permet d'identifier une partie de l'adresse IP.

C'est un nombre à 32 bits qui se compose d'un ensemble de 1 suivi d'un ensemble de 0. Les 0 indiquent la partie machine

Les masques de sous réseaux par défaut, suivant les classes des adresses IP [6] :

Tableau 2: Classes et masques réseau

Class d'adresse	Masque de sous réseau
<b>Class A</b>	255.0.0.0
<b>Class B</b>	255.255.0.0
<b>Class C</b>	255.255.255.0

### 6.4 Passerelle par défaut

En informatique, une passerelle (Gateway) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents [7].

## 7. Les supports de transmission

Il existe différents types de câbles [8] :

## 7.1 Le câble coaxial

Il a un revêtement extérieur en plastique contenant 2 conducteurs parallèles ayant chacun un couvercle de protection isolé séparé. Le câble coaxial transmet les informations en deux modes : le mode bande de base (bande passante de câble dédiée) et le mode large bande (la bande passante du câble est divisée en plages distinctes). Les télévisions par câble et les réseaux de télévision analogiques utilisent largement les câbles coaxiaux.

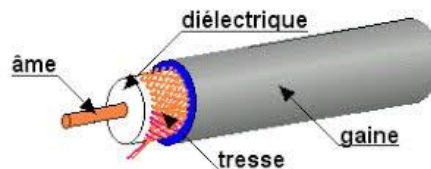


Figure 10: câble coaxial

## 7.2 La paire torsadée

Il se compose de 2 fils conducteurs isolés séparément enroulés l'un sur l'autre. Généralement, plusieurs de ces paires sont regroupées dans une gaine protectrice. Ce sont les supports de transmission les plus utilisés.

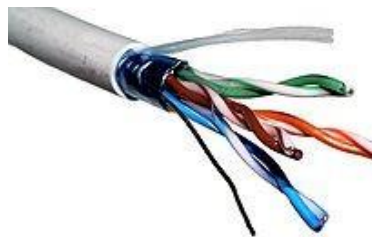


Figure 11: Paire torsadée

## 7.3 La fibre optique

Il utilise le concept de réflexion de la lumière à travers un noyau composé de verre ou de plastique. Le noyau est entouré d'un revêtement en verre ou en plastique moins dense appelé revêtement. Il est utilisé pour la transmission de gros volumes de données.

Le câble peut être unidirectionnel ou bidirectionnel. Le WDM (Wavelength Division Multiplexer) prend en charge deux modes, à savoir le mode unidirectionnel et bidirectionnel.



Figure 12: Fibre optique

## 8. Les topologies

La topologie d'un réseau informatique reprend la méthode de connexion des ordinateurs entre-eux, la méthode de câblage

Il y a différentes topologies [9] :

- **Le réseau en anneau :**

La topologie en anneau permet d'avoir un débit bande passante proche de 90%.

Contrairement à la topologie en bus, le signal est régénéré par chaque station. Par contre, la panne d'une station rend l'ensemble du réseau inutilisable (du moins dans un sens). Cette architecture étant la propriété d'IBM, les prix sont élevés.

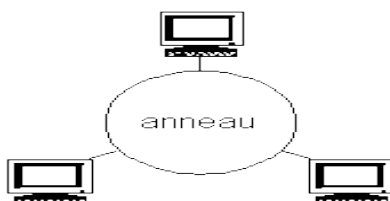


Figure 13: Topologie en anneau

- **Le réseau en bus :**

Topologie en bus c'est la connexion est constituée d'une seule ligne de communication qui relie l'ensemble des ordinateurs du réseau. A chaque extrémité, un "bouchon" élimine permet d'éliminer la réverbération (le retour) des données sur le câble et éviter.

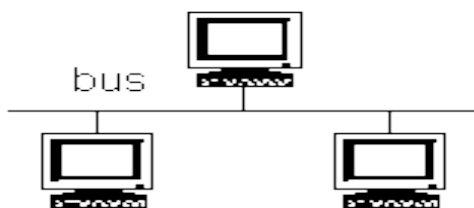


Figure 14: Topologie en anneau

- **Le réseau en étoile :**

C'est est la plus courante (réseaux Ethernet) avec la topologie maillée (Internet), les trois autres (en anneau, en bus et FDI) ne sont quasiment plus employés.

Le premier avantage de cette méthode de connexion est la facilité pour le câblage : un simple câble vers le concentrateur permet de relier l'équipement au réseau.

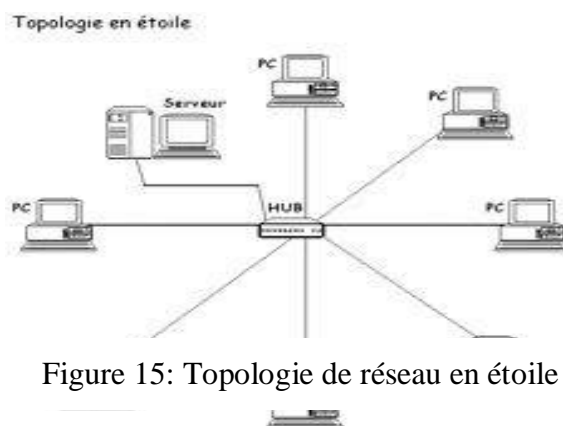


Figure 15: Topologie de réseau en étoile

- **Le réseau maillé :**

La topologie maillée est une topologie réseau (architecture) hybride de type étoile mais avec différents chemins pour accéder d'un nœud à un autre (contrairement à un réseau Ethernet).

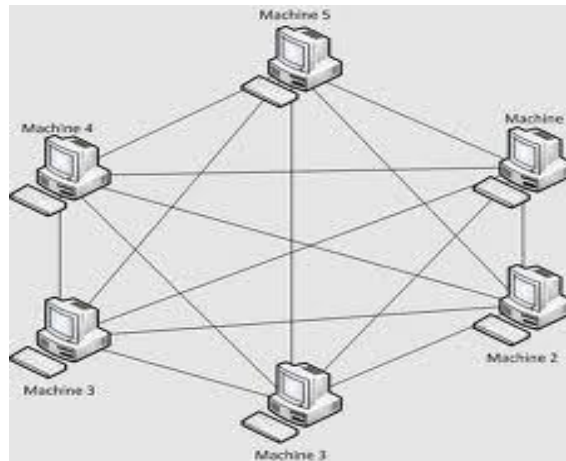


Figure 16: Topologie de réseau maillé

## 9. Les Méthodes d'accès

Nous envisageons ici les méthodes utilisées par ordinateurs pour savoir quand ils peuvent émettre des données sans déranger les transmissions des autres utilisateurs du réseau. Les deux méthodes citées ci-dessous font partie du protocole de communication [10] :

- **Méthodes d'accès aléatoire :**

La méthode d'accès CSMA/CD (Carrier Sensed Multiple Access/Collision Détection", en français : "Accès Multiple avec Ecoute de Porteuse/Détection de Collision").

Le poste qui veut émettre vérifie qu'un autre n'est pas déjà en train d'utiliser le réseau au même moment. Il n'envoie ses données que si la voie lui semble libre. Ensuite, Il vérifie que cet envoi n'est pas perturbé par un autre équipement qui lui aussi, pensant que le câble est inutilisé, aurait entrepris d'y envoyer des données. Dans ce cas, on dit qu'il y a collision et chacun des équipements en cause attend un temps aléatoire avant de répéter l'envoi. Le temps d'attente étant aléatoire de part et d'autre il est fort peu probable que les nouveaux envois soient à nouveau simultanés.

- **Méthodes d'accès déterministe :**

La méthode du token-ring est une méthode d'accès déterministe. Aucune machine ne commence à émettre sur le réseau si elle n'en a pas le droit. Aucun ordinateur ne dirige le "débat" mais un peu à la manière d'un tour de table lors d'une réunion, chaque machine attend son tour pour "prendre la parole". C'est le passage d'une information appelée jeton (token) qui détermine l'équipement qui a le droit d'initier une transmission.



## 10. Equipements réseau

Les principaux équipements matériels mis en place dans les réseaux locaux sont [11] :

### 10.1 Les modems

Le modem est un équipement électrique qui effectue une double conversion des signaux (analogique-numérique) dans le sens ligne téléphonique vers ordinateur et numérique-analogique dans le sens ordinateur vers ligne téléphonique. Il est surtout caractérisé par son débit binaire qui peut être de 512Kbits/s, 256Kbits/s, 56Kbits/s. Il permet à un ordinateur d'accéder au réseau Internet à partir d'une ligne téléphonique classique



Figure 17: Modem

### 10.2 Les concentrateurs (Hubs)

Le concentrateur est un équipement qui intervient au niveau de la couche 1 du modèle OSI. Son avantage est qu'il autorise plusieurs entrées et sorties des signaux (4, 8, 16 ou 24 ports), cet équipement est aussi appelé "hub". Il est surtout utilisé dans les réseaux locaux ayant une topologie en étoile. Il peut avoir une alimentation autonome permettant son fonctionnement même en cas de coupure de courant. Le concentrateur joue le rôle de répéteur en plus plusieurs entrées et sorties.



Figure 18: Hub

### 10.3 Les commutateurs (Switch)

Le commutateur est une variante du pont. On appelle parfois pont multi port. Il possède des acheminements sélectifs des informations vers certaines machines du réseau en utilisant les adressages correspondants. Par contre le hub réalise un acheminement non sélectif des informations sur le réseau. Toutes les machines reçoivent les mêmes informations, seules celles qui reconnaissent leur adresse effectuent la tâche qui leur incombe. Cette technique s'appelle aussi diffusion des données dans un réseau. C'est une technique facile à mettre en œuvre mais elle devient inadaptée, lorsque le nombre de machine devient important et supérieur à 10.



Figure 19: Commutateur

### 10.4 Le routeur

Le routeur est un équipement qui intervient au niveau 3 du modèle OSI, il intervient surtout dans la régulation du trafic dans les grands réseaux. Il analyse et peut prendre des décisions et peut prendre des décisions (c'est un équipement intelligent). Son rôle principal consiste à examiner les paquets entrants, à choisir le meilleur chemin pour le transporter vers la machine destinataire. On peut relier un routeur à un ordinateur afin de permettre sa configuration (mot de passe, type de réseau).



Figure 20: Routeur

## 11. Sécurité informatique

La sécurité informatique, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité informatique vise généralement cinq principaux objectifs [12] :

- **La confidentialité** : La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- **L'intégrité** : L'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- **La disponibilité** : L'objectif de La disponibilité est de garantir l'accès à un service ou à des ressources.

- **La non-répudiation** : La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

- **L'authentification** : L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre l'accès à des ressources uniquement aux personnes autorisées. La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue. Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

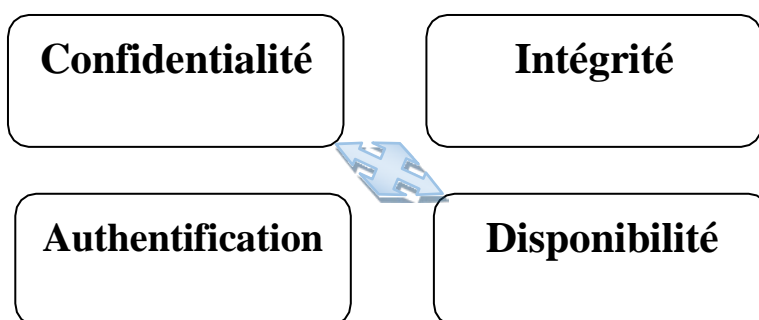


Figure 21: Sécurité de l'information

Dan notre travail , seul l'aspect du disponibilite est pris en consédération. Les autre a cose des contrainte temporelle, les autre aspects de securiter sont hors la porté de ce mémoir

- **La sécurité logique**, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- **La sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.**
- **La sécurité physique**, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.

## Chapitre 2 : Réseau ENAFOR

# 1. Historique

L'entreprise nationale de forage par abréviation « ENAFOR » a été créée par décret N° 81-170 du 1er Août 1981.

Devenir une société de services pétroliers de dimension internationale référencée pour ses services de forage et de Workover », c'est le but d'ENAFOR, Entreprise Nationale de Forage.

Membre du groupe **SONATRACH**, ENAFOR est une entreprise qui réalise pour le compte des opérateurs nationaux et internationaux, des opérations forage aux fins de reconnaissance et d'exploitation de gisements d'hydrocarbures et/ou de nappes d'eau, ainsi que des opérations d'entretien de puits producteurs d'huiles ou de gaz (Workover).

Ayant été une compagnie mixte entre SONATRACH et SEDCO elle était connue sous le nom

« **ALFOR** » avec un capital détenu par la **SONATRACH** à 51% et par SEDCO (USA) à 49%. En 1981 ALFOR s'est dissolu et ENAFOR voit le jour avec un capital 100% algérien.

**En 1989**, ENAFOR devient autonome sous forme d'une société par actions à un capital détenu par le Fond Mine à 40%, le Fond Chimie/Pétrochimie/Pharmacie à 30% et le Fond agroalimentaire à 30%.

**En 1995** le fond des mines devient l'unique actionnaire d'ENAFOR. Après presque une année, les actions d'ENAFOR seront détenues par RGT (réalisation et grands travaux)

**En 1998** SONATRACH devient l'actionnaire principal avec 51% par le biais de SSP et le reste détenu par RGT, ce dernier va être remplacé par RMC (réalisation et matériaux de construction)

**En 2002** le holding SPP se substitue au holding SSP et SGP-TRAVENS remplace RMC.

**2004** ENAFOR est certifié ISO 9001 – Version 2000. En Novembre 2004 - ENAFOR lance l'installation du système de gestion intégré (E.R.P) SAP.

**2005** Le Holding SPP "INDJAB" se substitue au Holding SGP TRAVEN et devient actionnaire de 49% des parts.

**2006** La SONATRACH devient le principal et unique actionnaire par le rachat des 49% des parts du Holding SPP "INDJAB".

**2008** Augmentation du capital social de 4 milliards de DA à 14 Milliards 800 Millions de DA

[15].

## 2. Direction Technologies de Communication et de l'Information

La Direction Technologies de Communication et de l'Information dans l'organigramme des grandes organisations devient indispensable vu le rôle que joue cette cellule dans le développement des solutions facilitant l'accès à l'information et réalisant ainsi un gain en matière de temps d'accès et en matière de cout d'accès surtout que ENAFOR doit rassembler périodiquement des données provenant de plus de 50 chantiers distant à travers le grand sud algérien. Ces données qui lui auraient coutaient des journées de déplacements pour faire la collecte sans parler des moyens que couteraient tous ces déplacements [15] .

## 3. Département Administration Système et Réseau

Le département administration système et réseau est chargé des tâches suivantes (structure responsable) [15]

- ✓ Data center : centre de données, est une infrastructure composée d'un réseau d'ordinateurs et d'espaces de stockage
- ✓ La virtualisation : s'appuie sur les logiciels pour simuler une fonctionnalité matérielle et crée un system informatique virtuel
- ✓ La sauvegarde des données : La sauvegarde en réseau ou en ligne est un moyen qui permet une décentralisation des données immédiates
- ✓ Assurer la veille technologique : La veille technologique ou veille scientifique et technique consiste à s'informer de façon systématique sur les techniques les plus récentes et surtout sur leur mise à disposition commerciale
- ✓ Elaborer et mettre à jour la documentation technique.

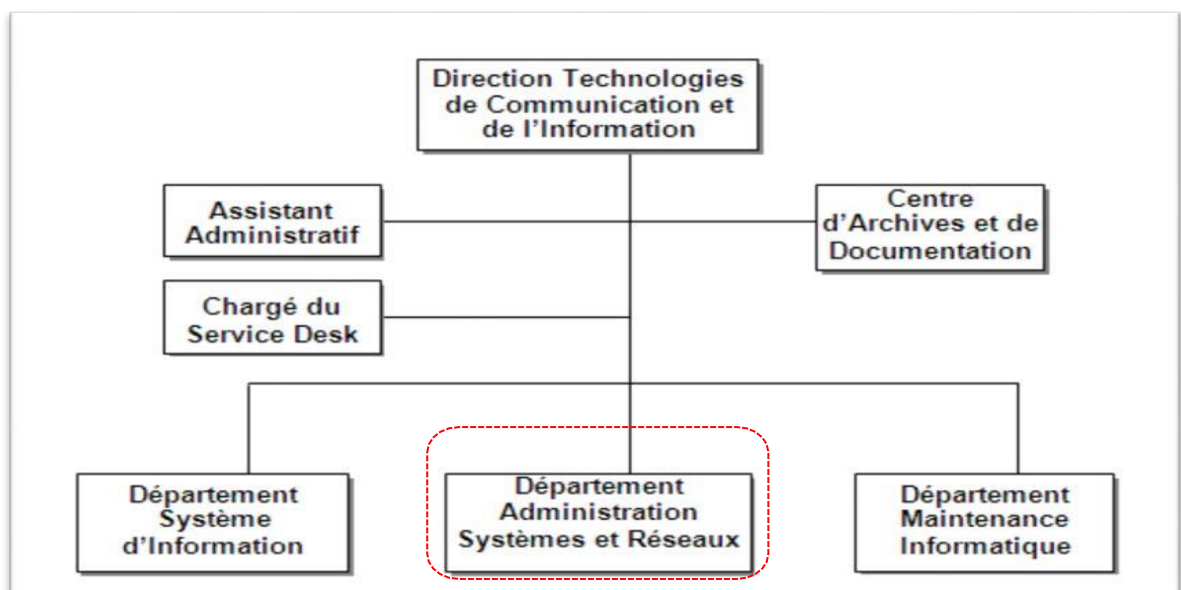


Figure 22: Organigramme de la direction Technologie de communication et de l'Information

Le département Administration Système et Réseau est divisé en trois groupes (Figure23) : Administration Réseaux, Administration Systèmes, et Administration ERP

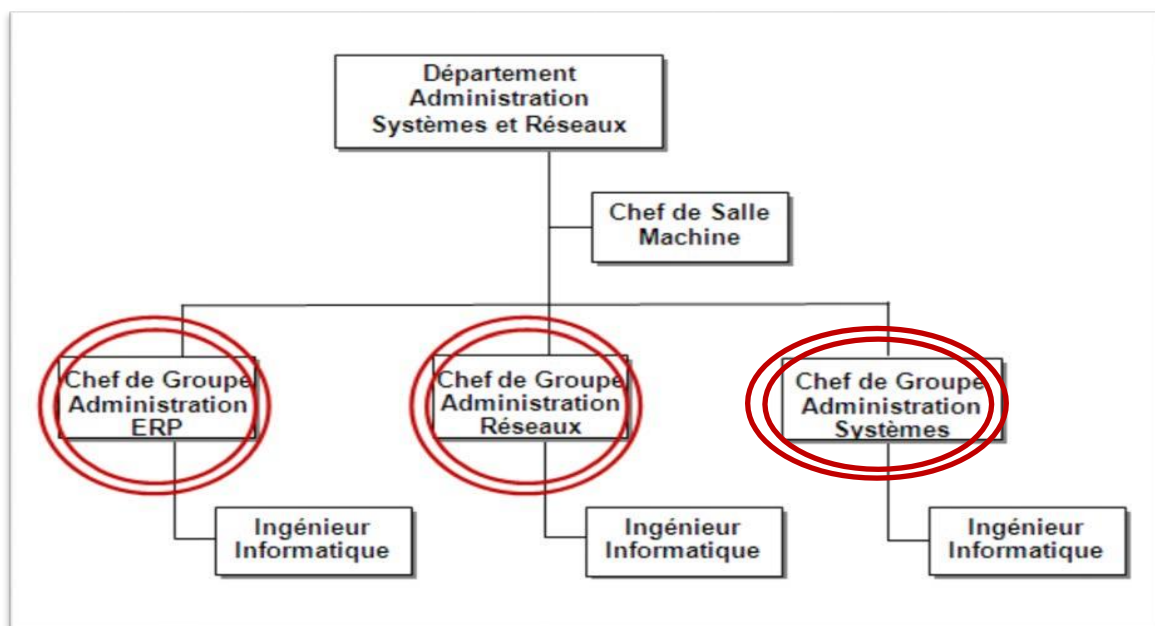


Figure 23: Organigramme Département Administration Systèmes et Réseaux

### 3.1 Administration Réseaux

Cette division assure :

- le contrôle d'authentification des utilisateurs pour l'accès au réseau de l'Entreprise ;
- le maintien de l'infrastructure d'active directory ;
- l'accès et la disponibilité des services Internet ;
- la prise en charge du réseau SAN ;
- la prise en charge du NAS ;
- la disponibilité et la fluidité du Réseau ;
- la migration, extension et adaptation vers aux besoins futurs du réseau de l'entreprise ;
- la disponibilité de la connexion VPN ;
- les sauvegardes relatives aux composants réseaux (Config, AD, ISA, etc.) ;
- Monitoring, audit et sécurité ;

### 3.2 Administration Systèmes

Cette division assure :

- l'administration et la disponibilité des serveurs Antivirus et serveur Windows ;
- l'administration et la disponibilité des serveurs de mise à jour automatique ;
- l'administration et la disponibilité du système de messagerie ;

- la migration des systèmes ;
- l'administration et la disponibilité du système de Contrôle d'Accès ;
- l'administration et la disponibilité du système vidéo ;
- les sauvegardes relatives aux systèmes gérés (AV, WSUS, EXCHANGE, etc.) ;
- Monitoring, audit et sécurité.

### 3.3 Administration ERP

Cette division assure :

- la disponibilité du système ERP ;
- l'entretien préventif périodique du système ERP (diagnostique, nettoyage) ;
- la maintenance du système ERP (Patchs, Mise à jours composants systèmes, etc.) ;
- la gestion des autorisations et des ordres de transport pour maintenir la cohérence du système ;
- la migration des systèmes ERP ;
- l'évolution du système à travers la Marketplace SAP (Licences serveurs, clés Abapeurs, Troubleshooting, etc.) ;
- les sauvegardes relatives aux systèmes SAP ;
- Monitoring, audit et sécurité ;

ENAFOR à Hassi-Messaoud est subdivisée en cinq sites, tous reliés au siège social et administrés par ce dernier.

**Siège Social** : situé près de BIR MESSAOUD, il occupe le sommet de l'architecture, c'est la direction générale de l'entreprise.

**Base Logistique** : située à quelques kilomètres du siège social, elle occupe la deuxième place.

**Base Workover** : c'est une base qui est chargée des services qu'ENAFOR propose à ses clients. Ces deux services sont FORAGE et WORK OVER qui sont respectivement rattachées aux deux directions qui portent leurs mêmes noms de service : Direction FORAGE et Direction WORKOVER.

**Base Transport** : elle s'occupe de tout ce qui est transport et déménagement de chantiers, de ce fait elle a une certaine importance au sein de l'entreprise.

**Base Maintenance** : elle se charge de la remise en œuvre des appareils de forage et de l'approvisionnement.

**Chantiers** : actuellement ENAFOR compte trente-cinq chantiers mobiles à travers le grand sur de l'ALGÉRIE. Chacun de ces appareils est chargé pour une période bien spécifiée d'accomplir une tâche bien aux bénéfices des clients



## 4. Schéma du réseau ENAFOR

En premier temps on va s'intéresser à expliquer de manière générale l'architecture sans trop s'attarder sur les détails [15].

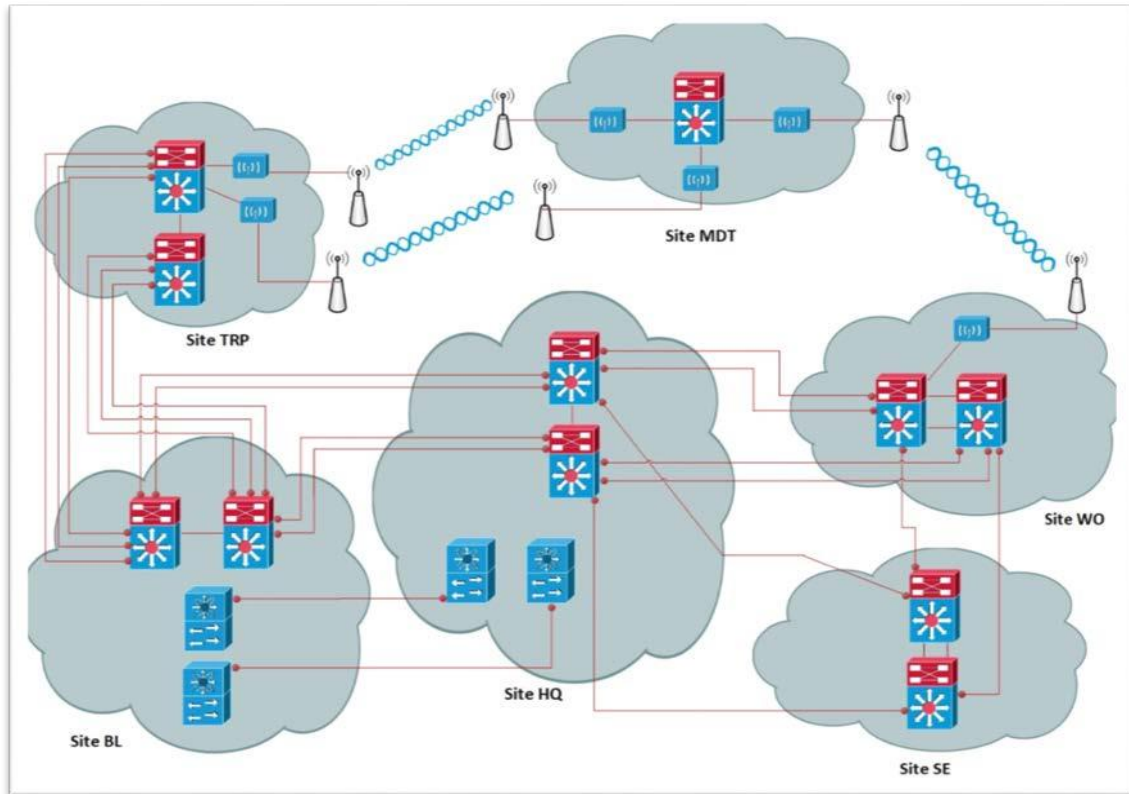


Figure 24: Schéma du réseau ENAFOR

Occupant Le poste le plus important au sein de l'entreprise, le siège social représente le **NOYEAU** du réseau de l'entreprise en logeant dans une salle appelée Salle Machine ayant une température ambiante, des armoires qui forment les réacteurs du réseau ENAFOR

Liées au siège social à travers de la fibre optique à 1GB chacune, les bases Logistique et Workover sont obligées de passer par la salle machine pour solliciter un service pour les employés, et ce point-là constitue le point fort de **ENAFOR** du fait qui lui permet de centraliser ces données pour éviter les redondances d'informations.

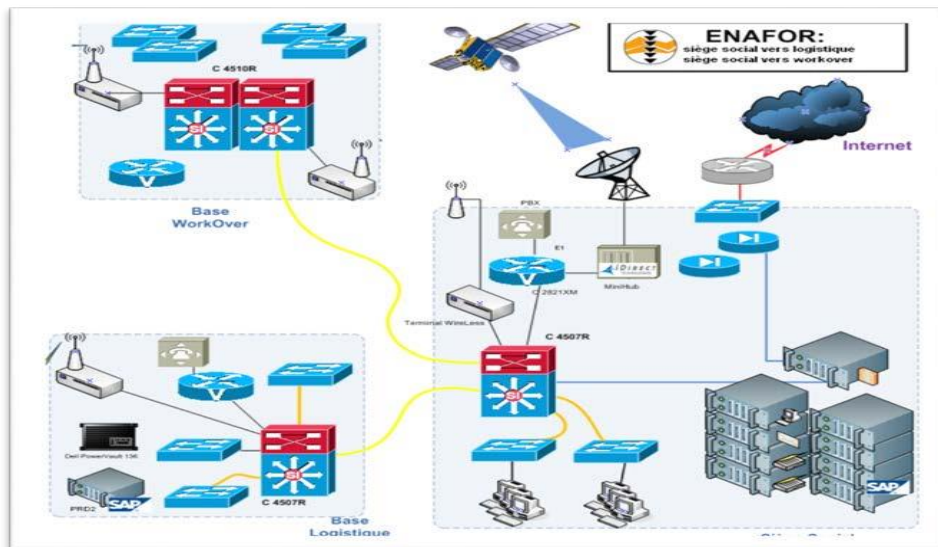


Figure 25: La liaison entre le siège Workover et la base logistique

Les ingénieurs d'ENAFOR ont prévu une connexion secours Wireless entre le Workover et le Siège Social pour faire face aux conditions météorologiques, à titre d'exemple les vents de sable. Un peu plus loin de chacune des deux bases qu'on vient de citer, se trouvent les deux bases Transport et Maintenance qui sont reliées respectivement à travers un réseau Wireless à la base Logistique et Workover.

Pour créer un circuit et parer aux pannes qui risquent d'handicaper l'entreprise, ENAFOR a relié la base Maintenance à la base Transport à travers un réseau Wireless.

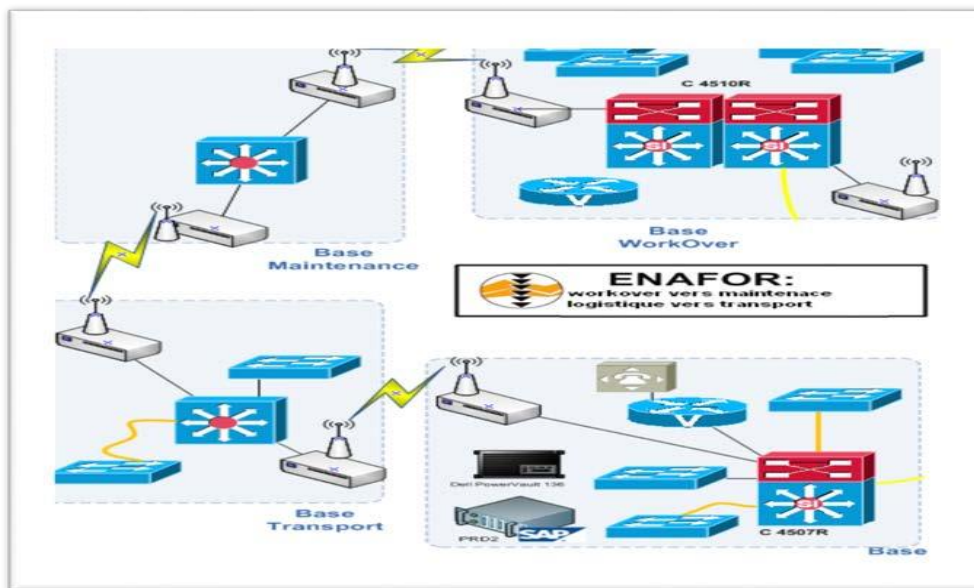


Figure 26 : Comment relier la base maintenance & le base transport avec un réseau Wireless

L'architecture générale qui connecterait et rassemblerait tous ce qu'on vient de voir est cijointe :  
 Comme on peut le constater, ENAFOR fait appel à un satellite **Panam SAT PAS1R** pour diffuser

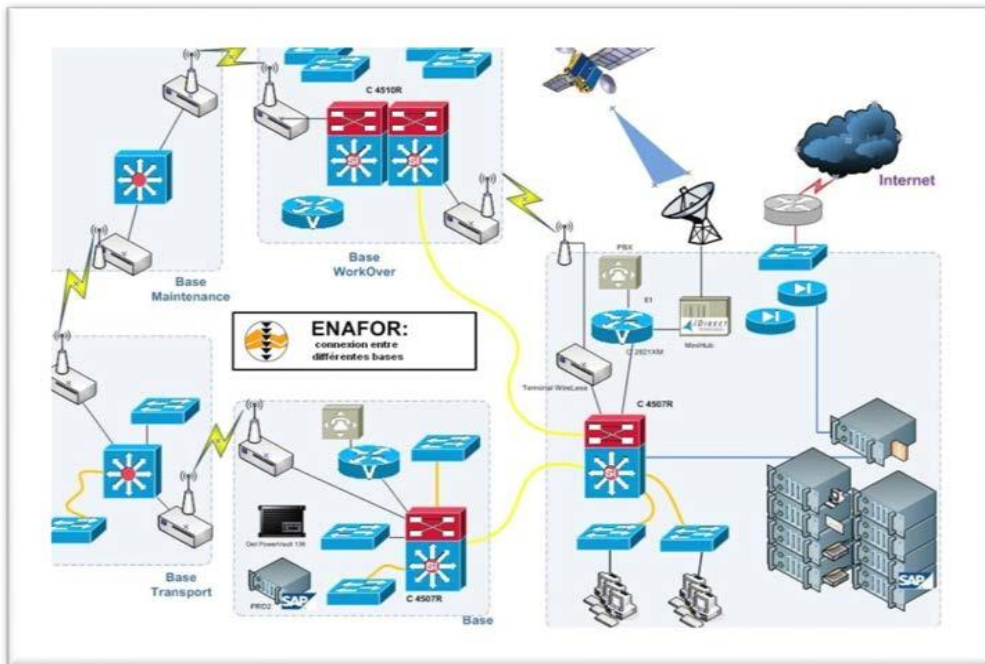


Figure 27: L'architecture générale

ses fréquences pour les chantiers dont on va spécifier l'architecture dans ce qui suit.

#### 4.1 Connexion entre siège social et chantiers distants

Le besoin des chantiers d'ENAFOR se résume aux besoins en matière de téléphonie IP et le service de messagerie, et les applications de SAP surtout qu'ENAFOR est l'une des rares pourn pas dire la seule en Algérie à réussir l'utilisation du système S.A.P. Le schéma qui va suivre résume toutes les connexions entre siège social et chantiers distant [15].

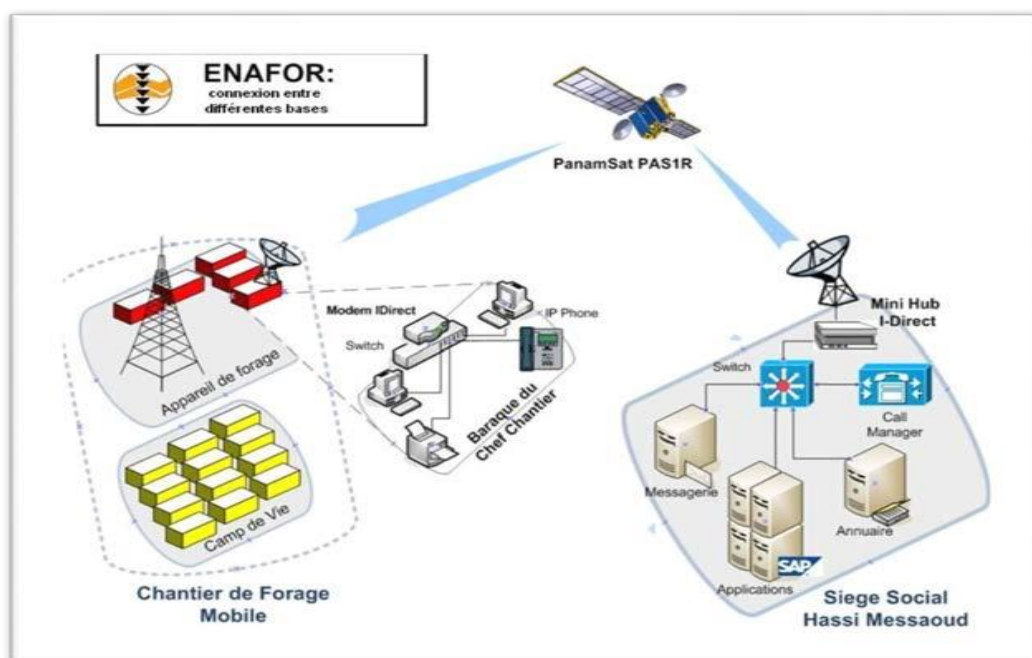


Figure 28: Connexion entre siège social et chantiers distants

## 4.2 Architecture du siège social

Pour réaliser une étude approfondie sur le réseau on va s'intéresser à étudier chaque site à part et chaque équipement du site à tour de rôle pour pouvoir assimiler les connaissances [15].

Comme précédemment mentionné, le siège social loge dans l'une de ses grandes salles du rais dechaussée la salle machine qui comprend dans ces armoires de trésors, des équipements variant entre Switch, Switch de niveau trois, Router allant jusqu'aux Mini hubs et les Terminaux Wireless.

Cette salle machine est alimentée par cinq connexions vers le monde extérieur voire six

1. Connexion satellite avec les différents camps de chantiers.
2. Connexion avec les postes du siège social à travers de la fibre optique multi modes à des Switch.
3. Connexion avec la base LOGISTIQUE à travers de la fibre optique mono mode à 1G.
4. Deux connexions avec la base WORKOVER la première à travers de la fibre optique mono mode à 1G, la deuxième avec un réseau point à point Wireless.
5. Une connexion à internet via un fournisseur de service unique **MPLS** (Algérie Tél

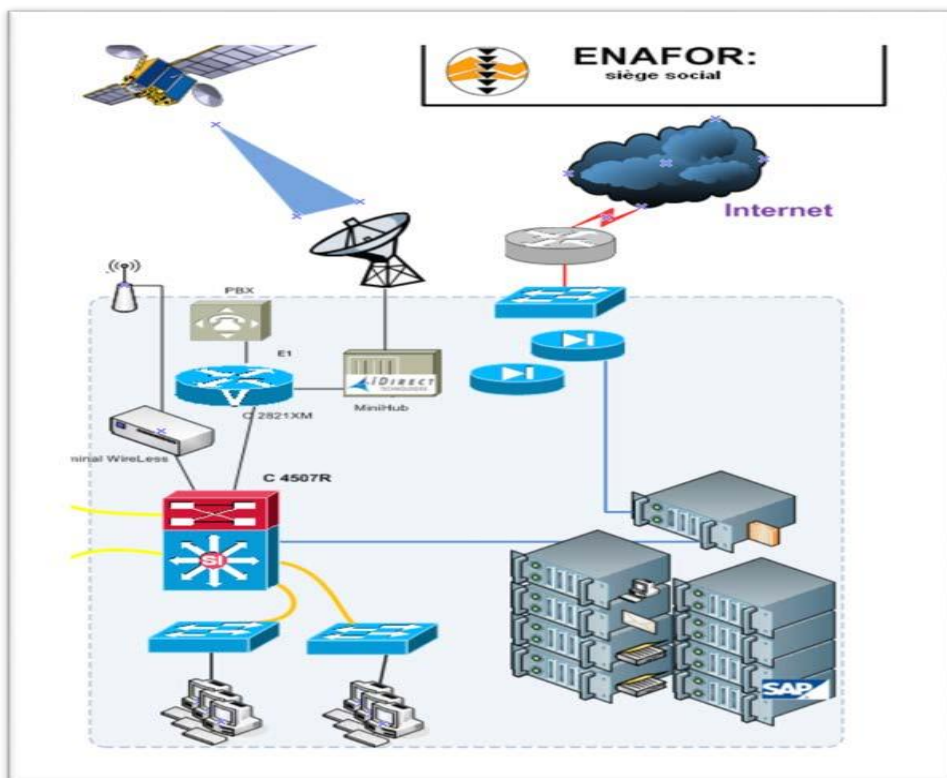


Figure 29: Connexion entre les sites

## 5. Data Center

Les connexions précédemment mentionnées sont réalisées par des équipements répartis dans des armoires bien structurées dans une salle d'environ trente mètres carrés (30 m<sup>2</sup>) isolée par une salle de séparation dite SAS afin de garder la température de la salle dans un degré bas pour éviter le réchauffement des équipements dû aux résistances des micros composants qui sont intégrés.

On compte cinq armoires au niveau de la salle machine, Dans notre rapport on a cité uniquement trois armoires suites à la confidentialité interne de l'Entreprise Nationale de Forage[15].

Tableau 3: Armoire des Switch & Routeurs

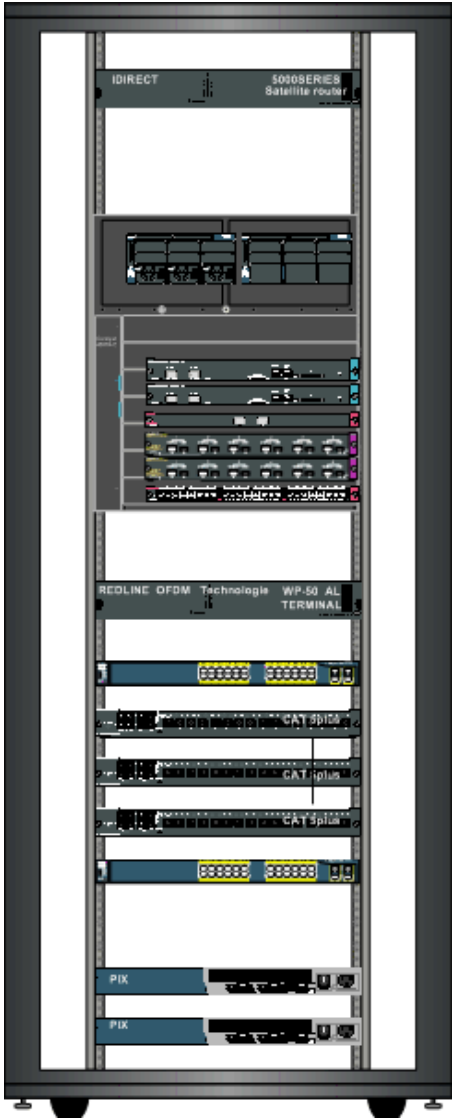
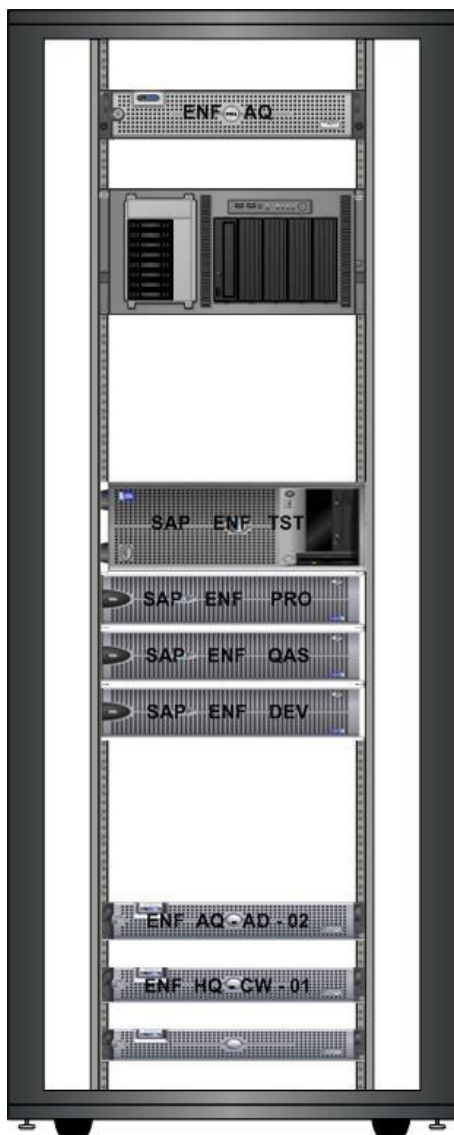
	<p>On remarque sur le haut de l'armoire la présence d'un router satellite placé sur le haut de l'immeuble du siège.</p> <p>Les référence de se router sont « IDIRECT 5000 séries ».</p> <p>Se Router permet la connexion aux chantier a un débit théorique de deux mégabits par seconde.</p> <p>Sous le router on remarque un Switch dit de troisième niveau pour l'option qui lui est intégrée et qui lui permet de jouer le rôle du routeur faisant ainsi l'opération du routage.</p> <p>Pour permettre aux employés d'en profiter, les administrateurs réseau on mit en place des Switch en cascades de types « CISCO2900 séries » qui vont permettre à l'aide des Hub qui sont placé entre les Switch sur l'armoire.</p> <p>De rassembler tous les postes des travailleurs.</p> <p>Pour plus de sécurité il y'a eu lieu d'ajouter des PIX pour la sécurité du réseau, c'est des PIX CISCO PIX515E.</p>
--	--

Tableau 4: Armoire des serveurs ERP



Cette armoire est l'armoire la plus couteuse vue la technologie matérielle du coté serveurs qui sont placés sur ses support et cote logiciel qui sont installé sur ces serveurs, Il existe plusieurs serveurs dans cette armoire répartis selon les caractéristiquessur plusieurs taches.

HP PROLIANT ML350 : prochainement pour la messagerie.

DELL POWER EDGE 1800 : pour le test des applications pour SAP sensibles nécessitant plusieurs contrôles avant la mise en place.il est étiqueté SAPENFTST.

DELL POWER EDGE6800 : pour la production car une fois l'application contrôlée elle doit être installée sur le serveur de production, il est dit ENFSAPPRO.

DELL POWER EDGE6800 : pour essayer la qualité deservices avant de mettre l'application sur ENFSAPPRO.

DELL POWER EDGE6800 : pour l'équipe de développement et réalisation des applications qui seront aux services aux utilisateurs finaux de l'entreprise.

DELL POWER EDGE2950 : pour les données de l'entreprise.

Tableau 5: Armoire des Serveurs Messageries & Antivirus

	<p>Czzsette armoire comprend des serveurs pour différentes tâches.</p> <p>CISCO S7800 séries : pour le management des appels IP et tous ce qui se réfère.</p> <p>HP PROLIANT ML350: serveur de données pour le SIEGE SOCIAL.</p> <p>DELL POWER EDGE 1600SC: serveur de données lui aussi.</p> <p>DELL POWER EDGE 2850: pour la messagerie.</p> <p>DELL POWER EDGE 2850: pour le control de domaine « active directory »</p> <p>DELL POWER EDGE 1600SC: server proxy.</p> <p>DELL POWER EDGE 1600SC: server de données et aussi un serveur ISA.</p>
--	--

## 6. Les chantiers distants

D'après les ingénieurs réseaux et systèmes d'ENAFOR le besoin des chantiers en matière de communication et l'accès au siège se résume en trois nécessités [15]. :

- La première représente l'accès aux **Serveurs SAP** pour bénéficier des applications qui ont été intégrées dans ces serveurs pour que tout le monde optimise sa qualité de services fonctionnel. Ces serveurs SAP sont du type « SAP ECC6 » et sont gérés par les Ingénieurs Administrateurs ERP.
- La deuxième application sollicitée par les chantiers concerne **la messagerie**, pour bénéficier de la possibilité de valider des documents à distances par les hauts responsables de l'entreprise pour que ces décisions soient valables.

- Le troisième besoin des chantiers c'est l'accès aux **annuaires et à la téléphonie IP** pour être en contact avec les sites d'ENAFOR soit d'une manière directe avec le Siège Social ou bien à travers ce dernier avec le reste des pôles.

Comme le but des chantiers est d'exécuter les ordres venant de niveau un peu plus haut, la possibilité de communiquer avec le monde extérieur n'est permise qu'aux chefs de chantiers ou bien au bureaux de secrétariat au même temps le médecin avec l'équipe de maintenance (Electricien et Mécanicien ) pour cela on trouve cinq ordinateurs pour les applications et la messagerie et à côté de ça on trouve un téléphone IP les reliant directement au serveur CALL MANAGER se trouvant au niveau des salles machines et bien sûr une imprimante réseau.

Toutes les communications dont on vient de parler sont transmises via un satellite **PanamSAT PAS1R** qui offre à ENAFOR une certaine plage de bande passante.

Donc deux émetteurs récepteurs assurent cette technique de communication avancée qui dépasse 64 kilo. Cette connexion étant largement suffisante, elle accomplit la tâche qui lui est affectée sachant que la communication IP consomme environ 3 à 4 kilo et les applications un peu plus que ça.

Comme on l'a mentionné du côté des chantiers on trouve des modems de types IDIRECT qui jouent le rôle de modulateurs/démodulateurs et transmettent les signaux. Ces derniers connectés à des Switch, ils permettent d'envoyer les paquets au **Panam SAT PAS1R** qui se chargera par la suite de les transmettre au SIEGE SOCIAL.

Les Switch utilisés permettent la connexion de deux ordinateurs, un téléphone IP et une imprimante muni d'une carte réseau pour permettre aux chefs de chantiers de communiquer avec les employés des chantiers à travers des imprimés.

Donc en quelques sortes l'architecture côté chantiers se présente comme suit

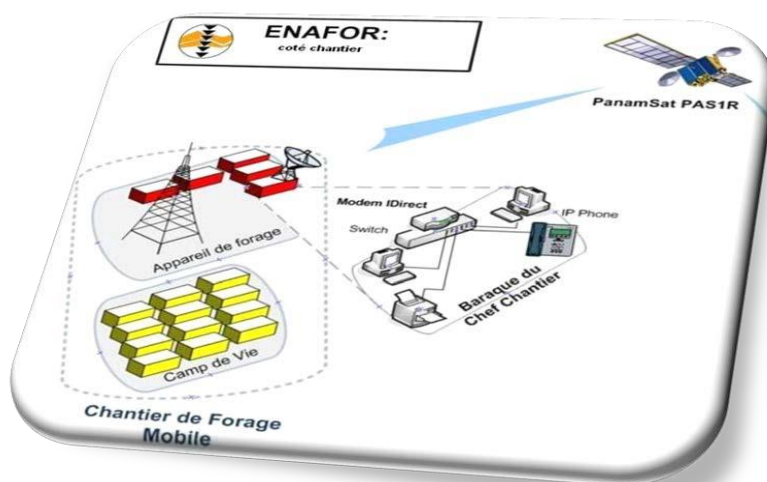


Figure 30: Réception et émission coté chantiers distant



# Chapitre 3 : Simulation basée-GNS3 du réseau ENAFOR

# 1. Présentation de GNS3

**GNS3** (Graphical Network Simulator) est un simulateur de réseau graphique qui permet l'émulation des réseaux complexes. VMware ou Virtual Box sont utilisées pour émuler les différents systèmes d'exploitation dans un environnement virtuel. Ces programmes permettent d'exécuter plusieurs systèmes d'exploitation tels que Windows ou Linux dans un environnement virtuel. GNS3 permet le même type de d'émulation à l'aide de Cisco Inter network Operating System. Il permet d'exécuter un IOS Cisco dans un environnement virtuel sur votre ordinateur. GNS3 est une interface graphique pour un produit appelé Dynagen. Dynamips est le programme de base qui permet l'émulation d'IOS. DynAgen s'exécute au-dessus de Dynamips pour créer un environnement plus convivial, basé sur le texte environnement. Un utilisateur peut créer des topologies de réseau de Windows en utilisant de simples fichiers de type ini. Il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment Open Source et multi-plates-formes. Il est possible de le trouver pour Mac OS , windows et évidemment pour les distributions Linux [13].

## 2. Installation et Configuration de GNS3 :

Cette section présente les étapes d'installation et de configuration de GNS3. Il est téléchargé<sup>1</sup> et installé (figure 31,32,33,34,35,36 et37) sur un PC doté d'un système d'exploitation Windows 8 64 bits [13].



Figure 31: Lancement GNS3

---

<sup>1</sup> <https://www.gns3.com/>

Le GNS3 exige d'autres composants d'aide pour assurer une bonne simulation du réseau comme

- **WinPCAP et Npcap** : bibliothèque Windows qui opèrent sur la couche réseau pour traiter les paquets
- **Wireshark** : Le logiciel à avoir pour capturer et analyser des trames réseaux.
- **SolarWinds Response** : Logiciel qui permet des analyses plus approfondies depuis vos captures wireshark.
- **Dynamips** : Le logiciel qui émule les images à proprement parlé.
- **QEMU** : Permet l'émulation des firewalls Cisco ASA.
- **VPCS** : Permet de simuler des PC dans les topologies.
- **Cpulimit** : produit permet d'optimiser l'utilisation CPU.
- **GNS3** : L'interface graphique du programme en lui-même.
- **TightVNC** : Utilitaire permettant de se connecter sur des PC à distance (avec vnc server d'installé).

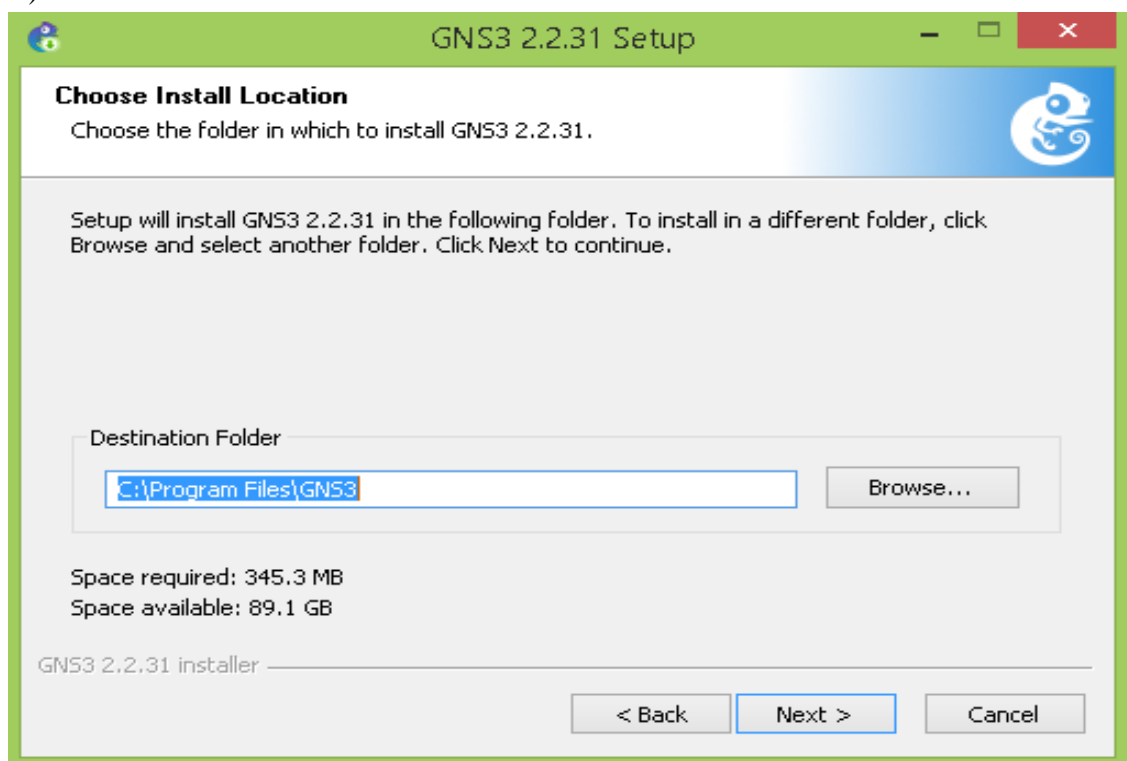


Figure 32 : Installation

La première dépendance pour GNS3 est WinCAP qui doit être installée via l'assistant d'installation WinPcap

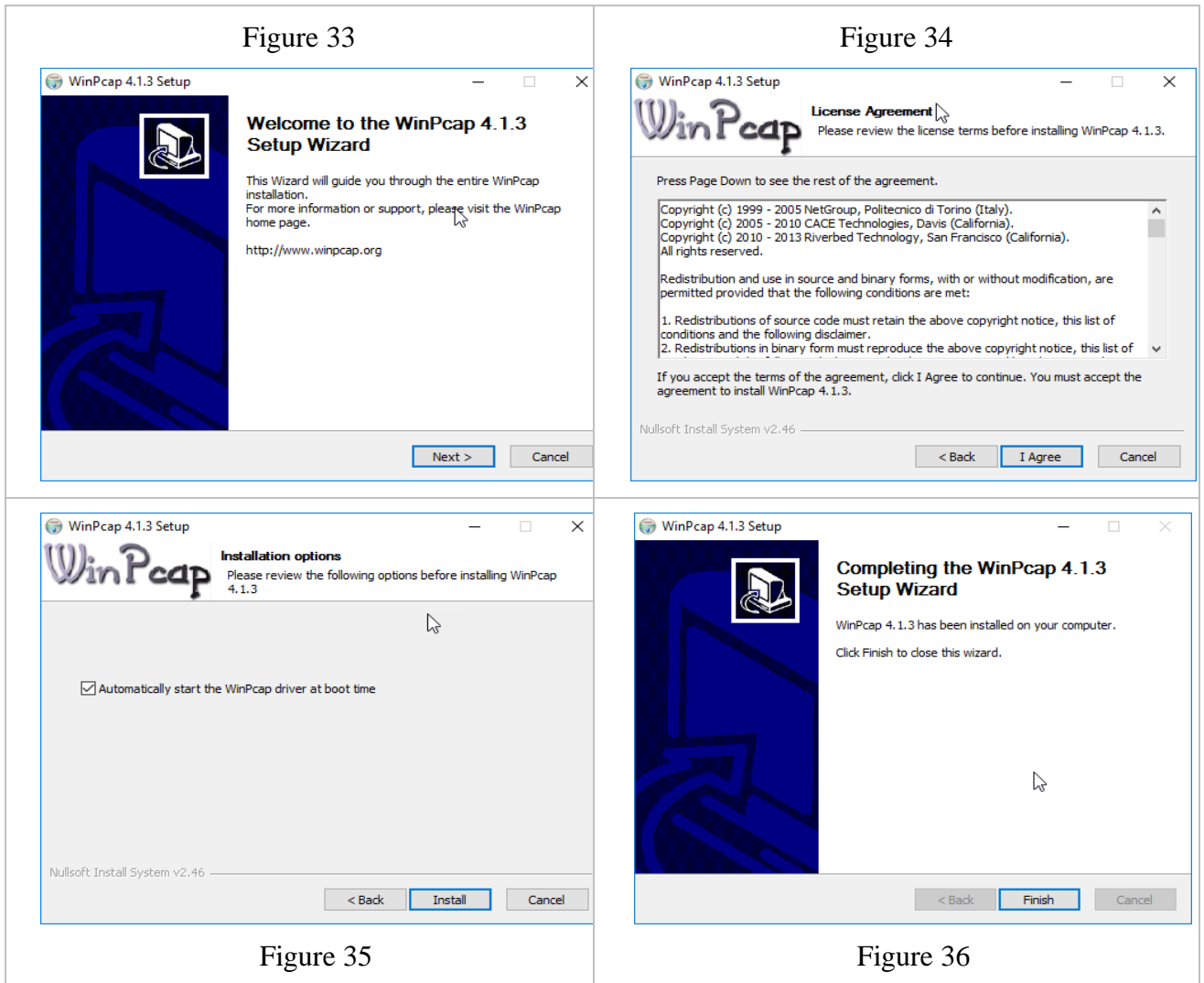


Figure 37-34-35-36 : installation WinPcap



Figure 38 : Terminer l'installation de GNS3

La figure 39 montre la fenêtre principale de GNS3.

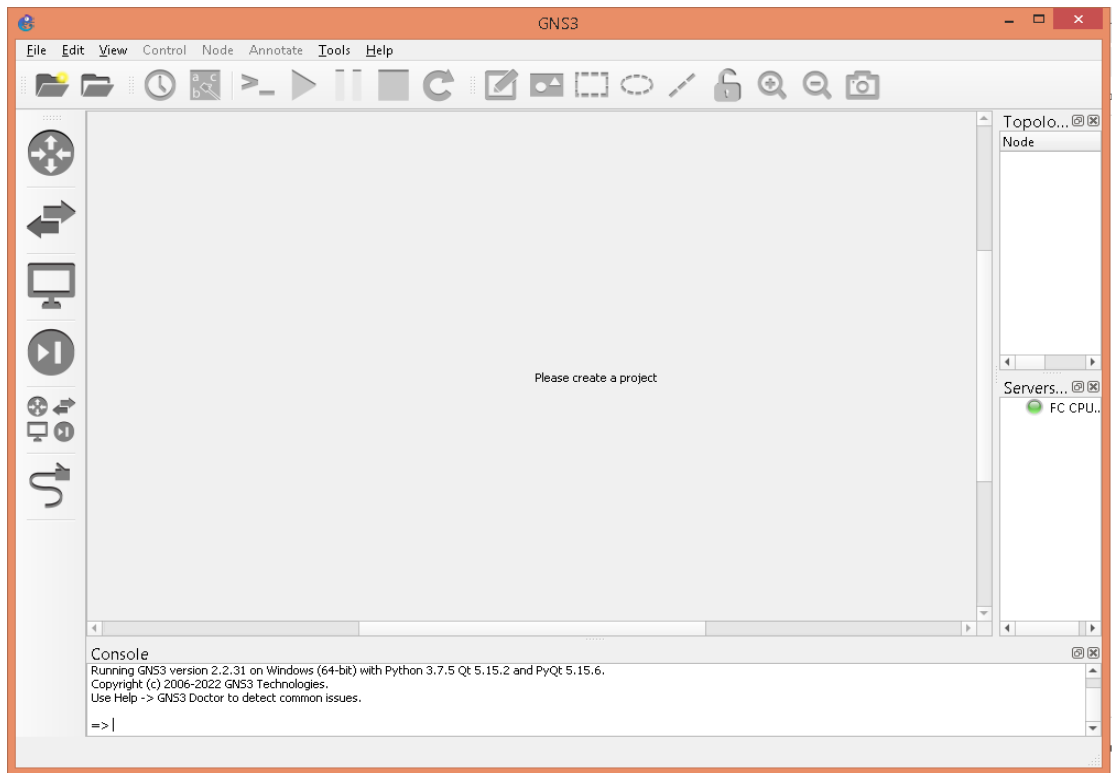


Figure 39 : Lancement de simulateur Cisco (GNS3)

GNS3 est destiné à être utilisé dans un environnement de laboratoire pour tester et apprendre. Pour fournir les routeurs à utiliser avec GNS3, il faut installer le logiciel Cisco IOS pour l'une des plates-formes supportées. A travers ce logiciel, il est possible de télécharger et ajouter manuellement les routeurs Cisco IOS sous forme de fichiers comme le montre les figures 40 et 41 [14].



Figure 40: Exemple d'un routeur Cisco IOS téléchargé

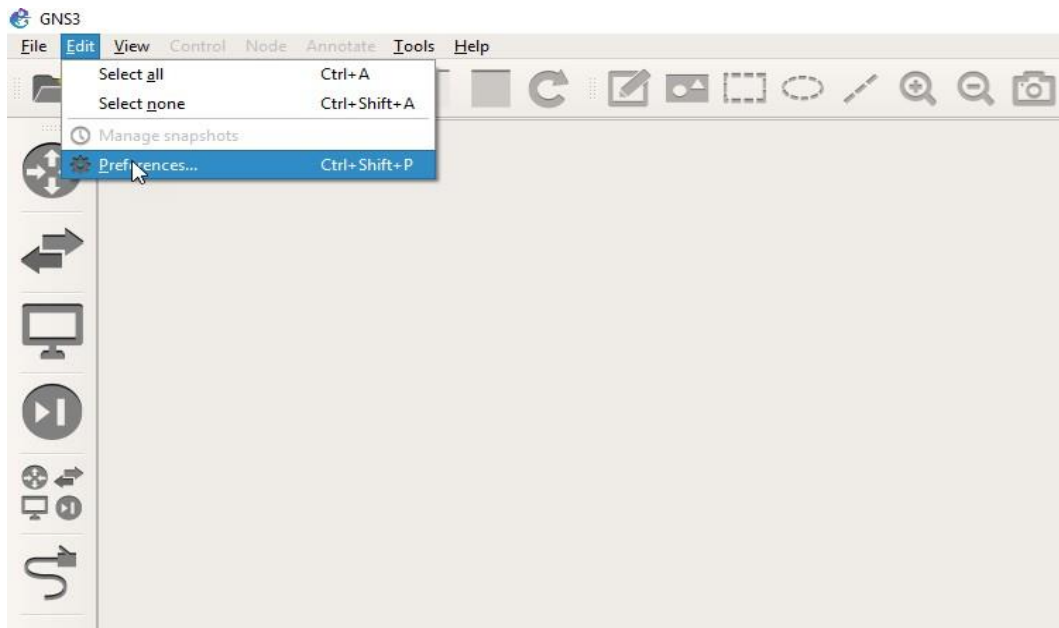


Figure 41 : Chargement manuel IOS image

Le fichier du routeur à télécharger peut-être un fichier « *bin* » ou une « *image* ». Si le fichier choisi est une image, l'utilisateur doit l'importer et la décompresser. Dans notre simulation, on a utilisé uniquement le routeur C7200. GNS3 donne à l'administrateur la possibilité de configuration les routeurs (ex. RAM, NVRAM, Adaptateurs).

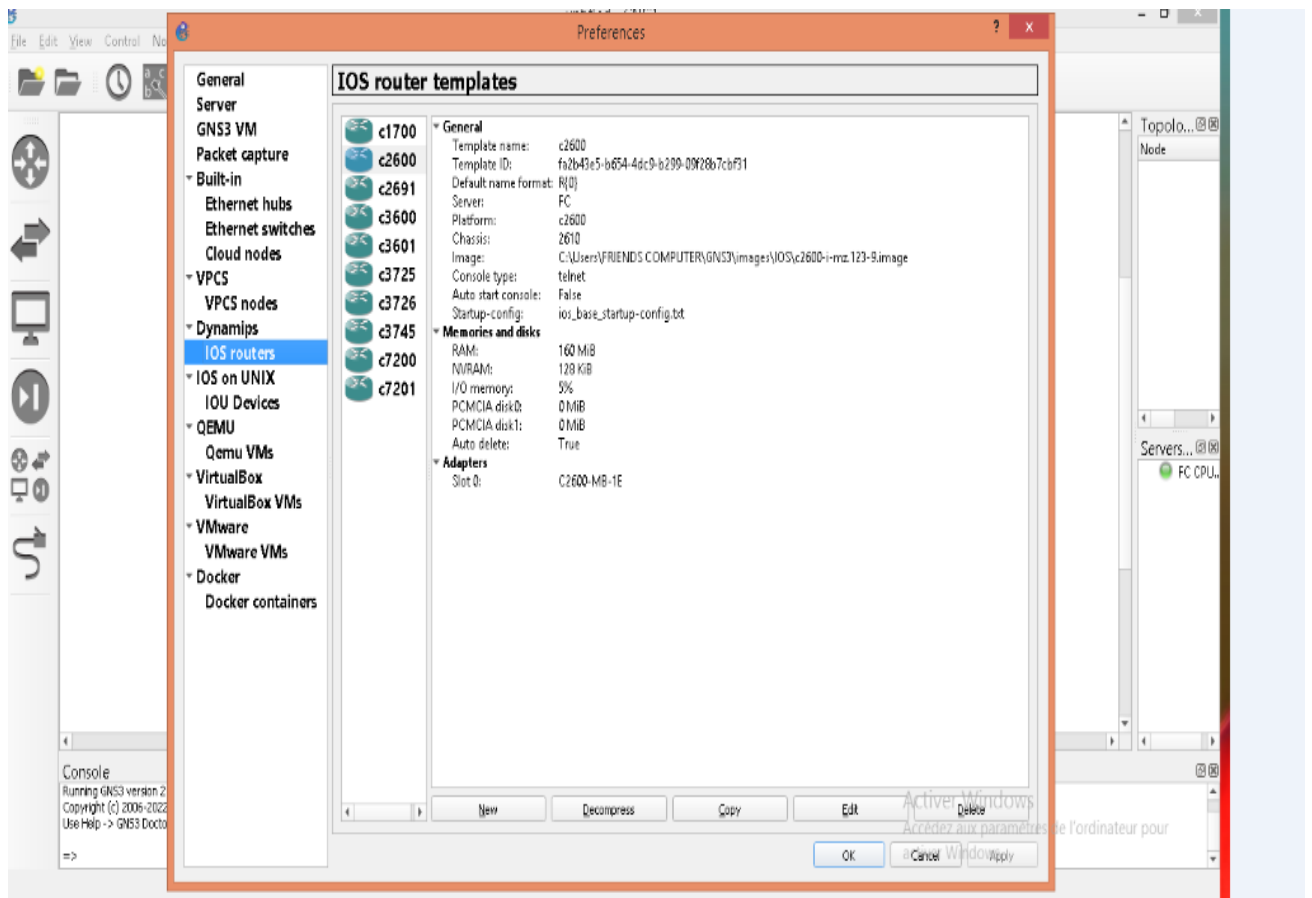


Figure 42: Importer et décompresser des images

### 3. Simulation du réseau informatique ENAFOR

Cette section présente les différentes étapes suivies pour simuler la topologie réseau ENAFOR. Les ressources utilisées dans cette simulation incluent des routeurs, des switches, des câbles réseau et des PCs. Le travail commence par la création d'un nouveau projet sous GNS3 (figure 43)

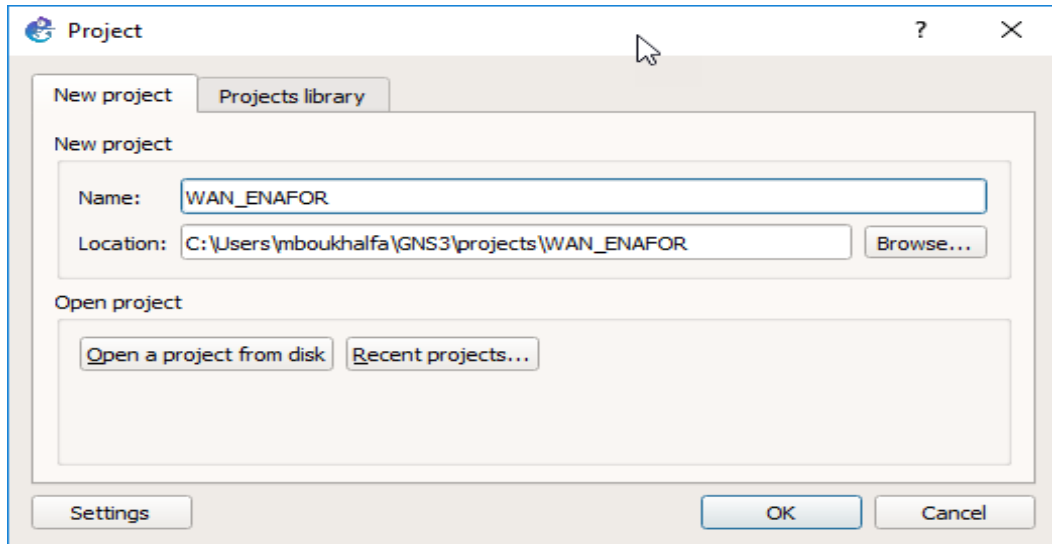


Figure 43 : Création d'un projet sous GNS3

On ajoute ensuite le modèle du routeur CISCO C7200 à partir de la section gauche de la fenêtre illustrée à la figure 44.

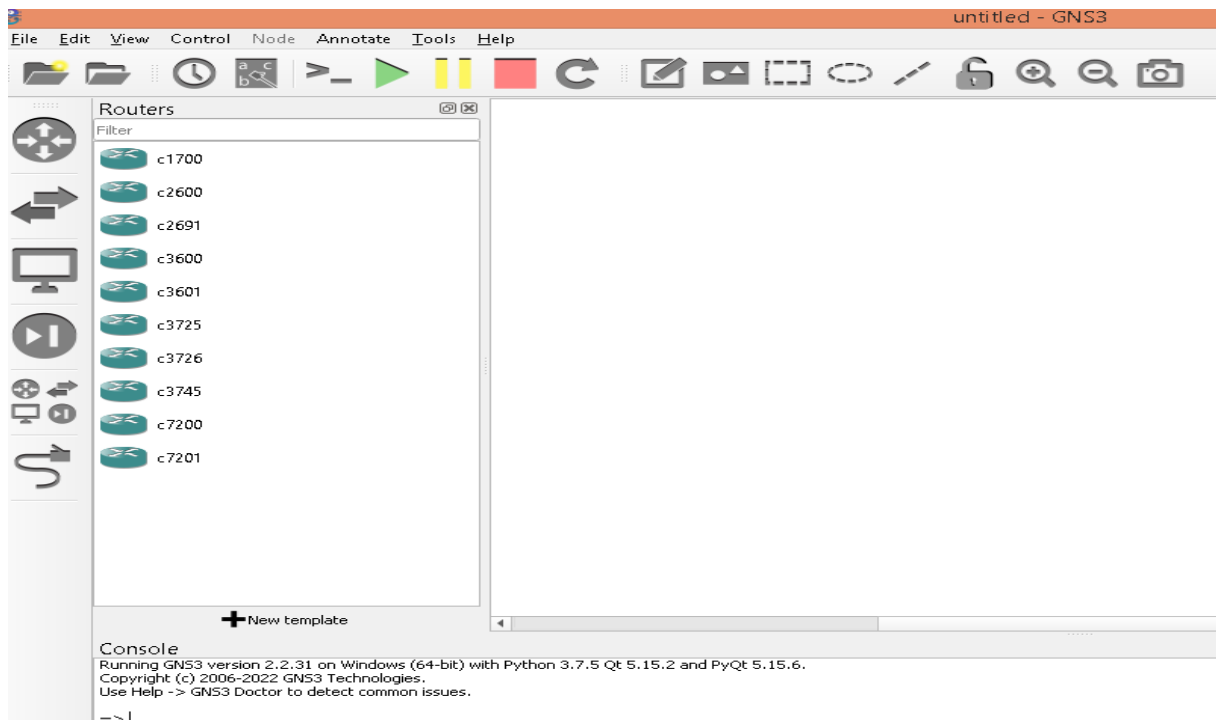


Figure 44 : Ajout des routeurs sous GNS3

A Hassi-Messaoud, ENAFOR est subdivisée en cinq sites, tous relié au Siège Social. Dans notre cas d'étude, on a utilisé cinq routeurs C7200 pour représenter les cinq sites, en exultant la Base Maintenance (choix de conception).



Figure 45: Les cinq routeurs représentant les cinq sites ENAFOR

Une fois les routeurs sont insérés, ils sont reliés au routeur principal Siege via leurs slots *FastEthernet* (voir figures 46 et 47).

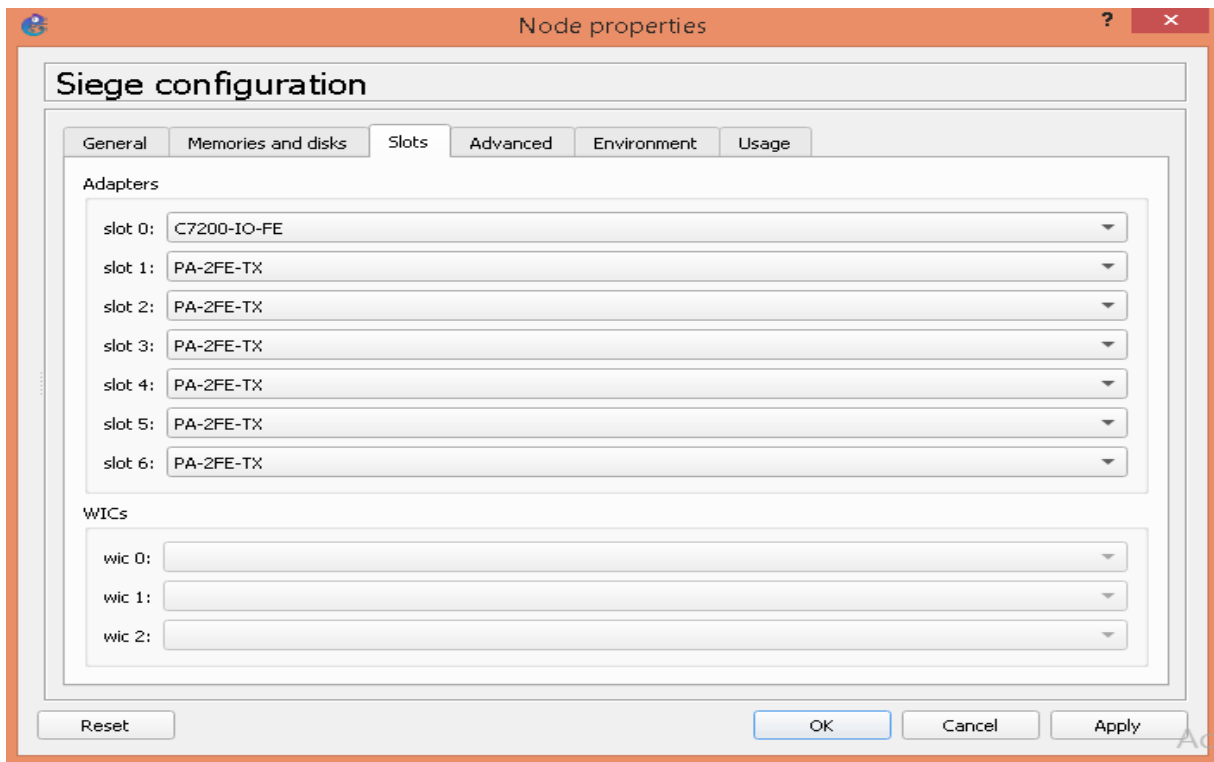


Figure 46: Connexion du routeur Siège aux différents sites (routeurs)



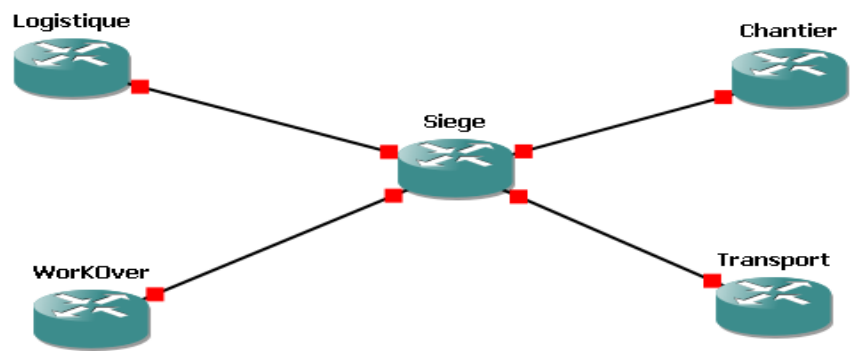


Figure 47: connexion des équipements par un câble FastEthernet

On utilise la console de chaque routeur pour Configurer ses interfaces en :

- Affectant des adresses IP ;
- Spécifiant les masques réseau ;
- Sauvegardant sa configuration.

La figure 48 illustre la configuration du routeur Siege via sa console.

```

et4/1, changed state to down
*Jun  4 01:45:21.219: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Jun  4 01:45:21.231: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state
to administratively down
*Jun  4 01:45:21.243: %LINK-5-CHANGED: Interface FastEthernet1/1, changed state
to administratively down
*Jun  4 01:45:21.255: %LINK-5-CHANGED: Interface FastEthernet2/0, changed state
to administratively down
*Jun  4 01:45:21.263: %LINK-5-CHANGED: Interface FastEthernet2/1, changed state
to administratively down
*Jun  4 01:45:21.271: %LINK-5-CHANGED: Interface FastEthernet3/0, changed state
to administratively down
*Jun  4 01:45:21.279: %LINK-5-CHANGED: Interface FastEthernet3/1, changed state
to administratively down
*Jun  4 01:45:21.291: %LINK-5-CHANGED: Interface FastEthernet4/0, changed state
to administratively down
*Jun  4 01:45:21.299: %LINK-5-CHANGED: Interface FastEthernet4/1, changed state
to administratively down
Siege#
Siege#
Siege#en
Siege#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Siege(config)#int f0/0
Siege(config-if)#ip add 192.168.5.1 255.255.255.0
Siege(config-if)#
  
```

Figure 48: Console du routeur siège

Le protocole de routage utilisé pour chaque routeur est RIP (Le protocole de routage RIP fait partie des protocoles de routage de vecteur de distance). Il permet de tester la connectivité entre les routeurs par la commande *Ping*.

La figure 49 résume les différents éléments constituant la topologie du réseau ENAFOR.

Topology Summary	
Node	Console
▶ C1	telnet localhost:5015
▶ C2	telnet localhost:5016
▶ Chantier	telnet localhost:5013
▶ L1	telnet localhost:5000
▶ L2	telnet localhost:5001
▶ Logistique	telnet localhost:5011
▶ Mon_Pc	none
▶ Siege	telnet localhost:5005
▶ Switch1	none
▶ Switch-Chantier	none
▶ Switch-Logistique	none
▶ Switch-Transport	none
▶ Switch-WorkoVer	none
▶ T1	telnet localhost:5019
▶ T2	telnet localhost:5018
▶ Transport	telnet localhost:5006
▶ W1	telnet localhost:5002
▶ W2	telnet localhost:5014
▶ WorkOver	telnet localhost:5012

Servers Summary	
▶ FC	CPU 32.0%, RAM 97.0%

Figure 49 : Résumé de topologie

Le schéma de la figure 50 représente la simulation complète du réseau informatique **ENAFOR**.

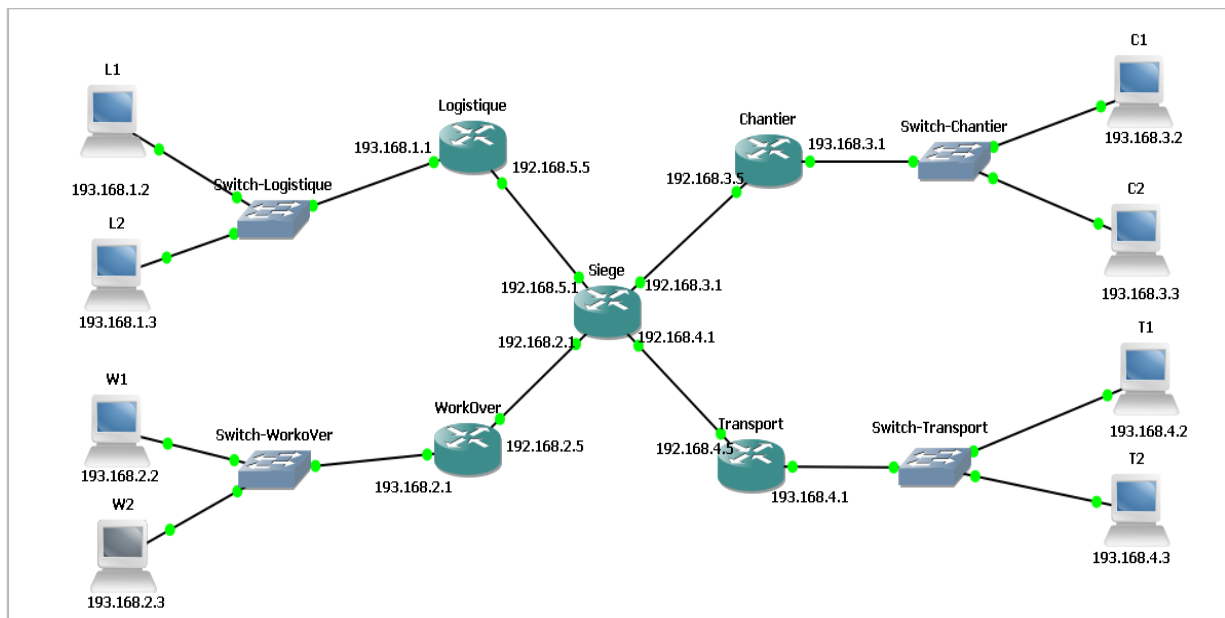


Figure 50: Le réseau ENAFOR

Les tableaux suivants introduisent la configuration détaillée de chaque routeur du réseau. La commande « **Enable** » ou « **ENA** » ou « **en** » est utilisée pour passer en mode administrateur sur l'équipement réseau. Toutes les commandes indiquées ci-dessous sont à effectuer en mode administrateur.

Tableau 6 : Commandes pour configurer un routeur

Command	Descriptions
<b>configure terminal</b> <b>conf t</b> <b>conf term</b>	Entre dans le mode de configuration globale
<b>interface Ethernet</b>	Entre dans le mode de configuration de
<b>int f</b>	l'interface
<b>ip address &lt;address&gt; &lt;mask&gt;</b> <b>ip add</b>	Configure l'interface avec l'IP et le masque de réseau
<b>no shutdown</b> <b>no shut</b>	Active ou Désactive l'interface
<b>Exit</b>	Sort et remonte d'un cran dans la hiérarchie des menus
<b>Exit</b>	Sort et remonte d'un cran dans la hiérarchie des menus
<b>copy running-config startup-config ou</b> <b>copy run star ou write mem</b>	Sauvegarde la configuration courante en NVRAM

Tableau 7 : Configuration du Protocol de routage RIP

Commandes	Descriptions
<b>Name router# conf t</b>	Entre dans le mode de configuration globale
<b>Name router (config)# router rip</b>	Le protocole de routage
<b>Name router (config-router)# version 1-2</b>	La version 2 apporte le routage CIDR et L'utilisation de VLSM, un nombre de sauts à 128
<b>Name router (config-router)# network</b> <b>network-number</b>	Configure l'interface avec l'IP et le masque de réseau
<b>Name router (config-router)# Exit</b>	Sort et remonte d'un cran dans la hiérarchie des Menus
<b>Name router (config)# Exit</b>	Sort et remonte d'un cran dans la hiérarchie des Menus
<b>Name router#Show ip rout</b>	Affiche la table de routage

<b>Name router#wr</b>	Sauvegarde la configuration courante en NVRAM
-----------------------	---

Les adresses IP utilisés pour chaque routeur d'un site sont citées dans le tableau suivant :

Tableau 8: Adresse IP utilisés pour chaque routeur d'un site

Sites	Add IP	Int F	Masque réseaux	Int F	IP add siege
<b>Workover</b>	192.168.2.5	0/1	255.255.255.0	0/0	192.168.2.1
<b>Transport</b>	192.168.4.5	1/0	255.255.255.0	2/0	192.168.4.1
<b>Logistique</b>	192.168.5.5	0/0	255.255.255.0	0/1	192.168.5.1
<b>Chantiers</b>	192.168.3.5	2/0	255.255.255.0	1/0	192.168.3.1

Sites	Transport	Logistique	Workover	Chantiers
<b>Add IP</b>	193.168.4.1	193.168.1.1	193.168.2.1	193.168.3.1
<b>Add pc</b>	T5 : 193.168.4.2 T6 : 193.168.4.3	L1 : 193.168.1.2 L2 : 193.168.1.3	W3 : 193.168.2.2 W4 : 193.168.2.3	C7 : 193.168.3.2 C8 : 193.168.3.3

# Chapitre 4 : Développement et mise en œuvre de l'application Monitoring Réseau

# 1. La mise en relation de l'administrateur avec GNS3

## 1.1 Le Cloud

Pour relier la machine locale (l'administrateur) avec le projet GNS3 (**Wan\_enafor**), il est nécessaire d'utiliser un Cloud (figure 51) qui représente un ensemble de serveurs sur le réseau. Cette opération exige l'installation d'une carte réseau de bouclage

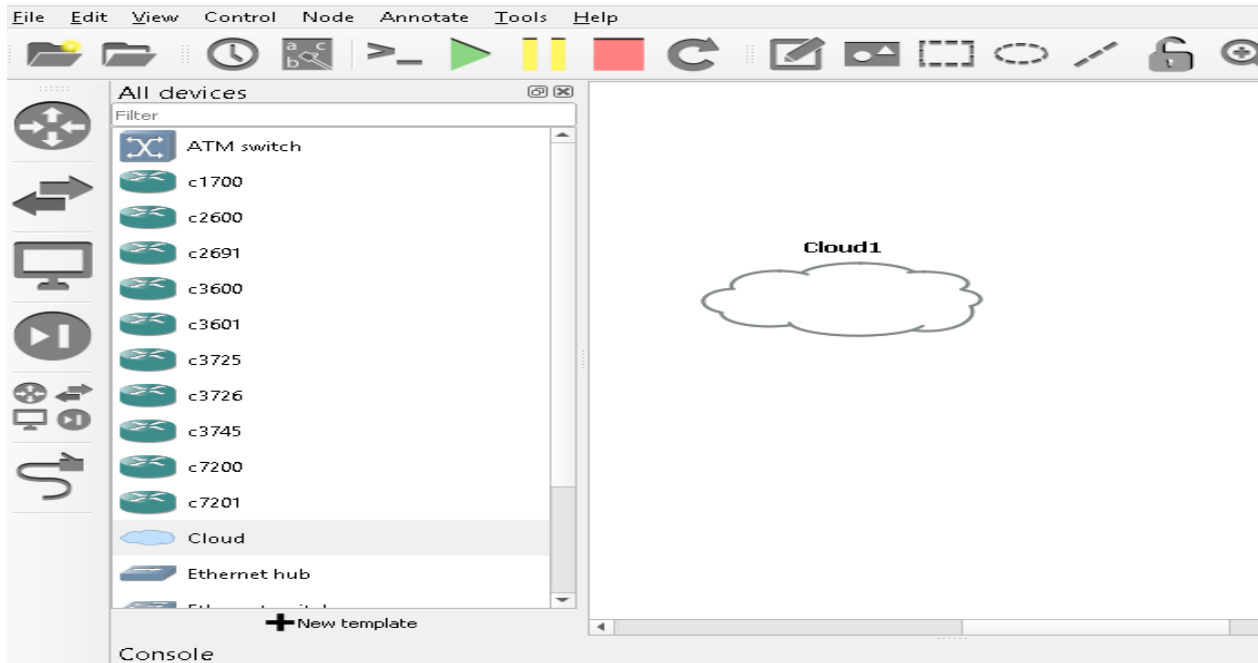


Figure 51: Création Cloud

## 1.2 La carte de bouclage

La carte de bouclage est un outil de test dans un environnement virtuel de réseau comme GNS3 dans lequel l'accès à un réseau n'est pas possible. Elle permet de simuler la présence d'une carte réseau active sur la machine administrateur. La figure 52 présente la configuration de la carte de bouclage installée sur la machine administrateur.

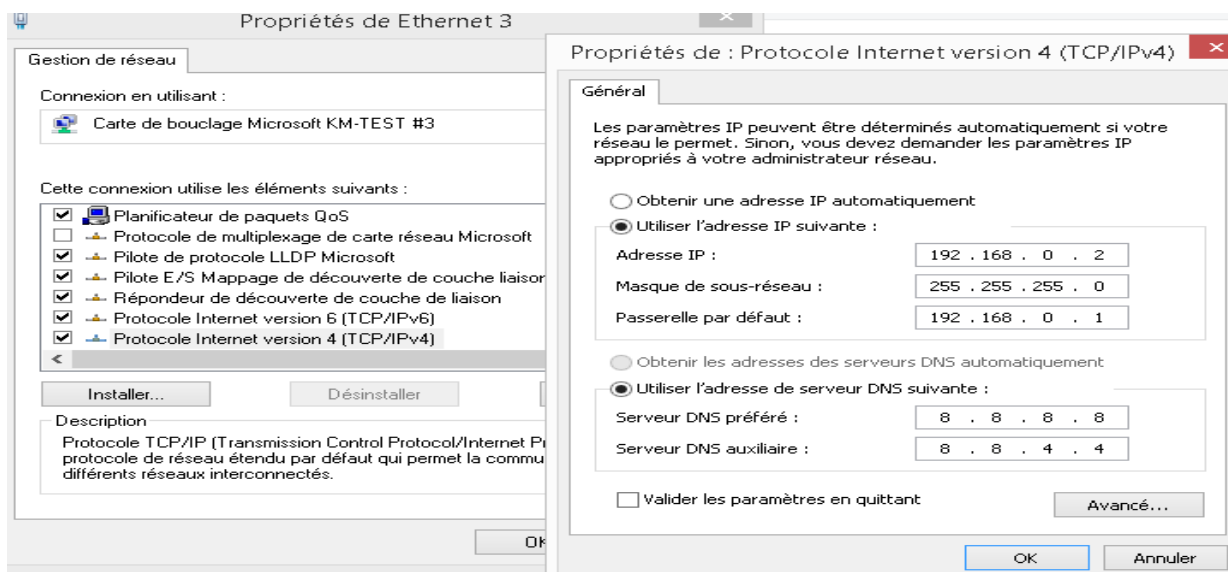


Figure 52: Configuration de la carte réseau

La configuration de la carte de bouclage doit être suivie de l'établissement d'une liaison entre la machine administrateur et le Cloud (figure 52)

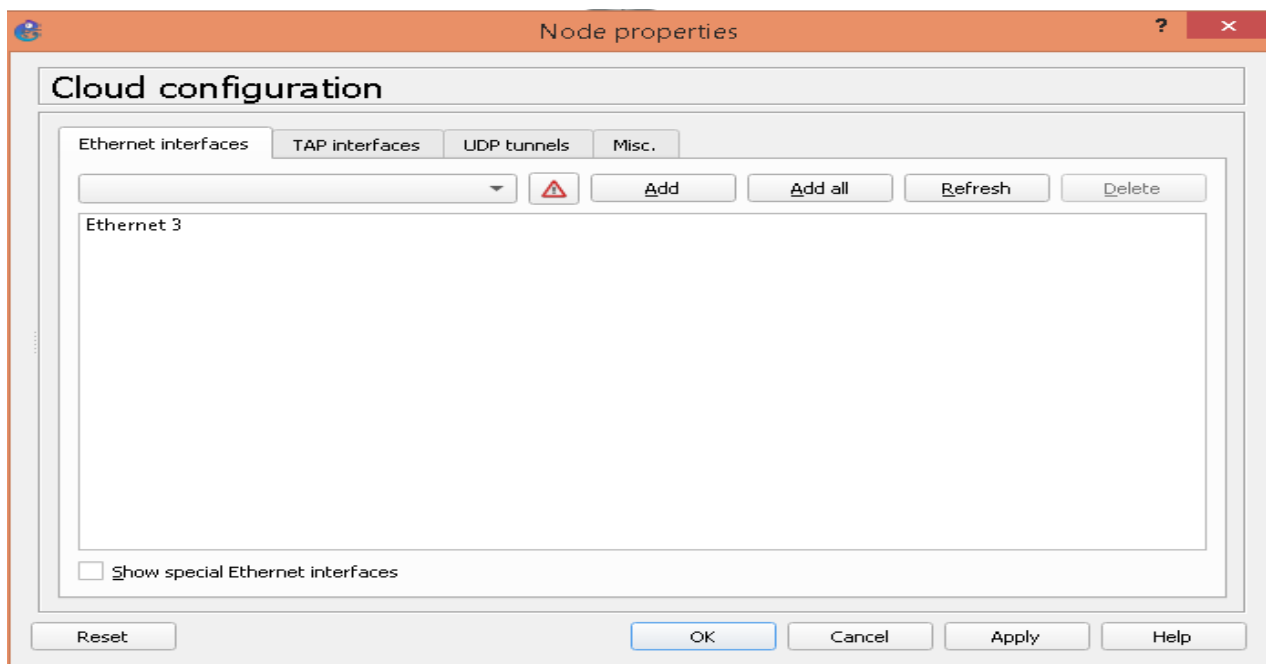


Figure 53: Configuration du Cloud

Le Cloud est connecté au routeur Siege pour donner à la machine administrateur la possibilité d'accéder au réseau simulé comme le montre la figure suivante :

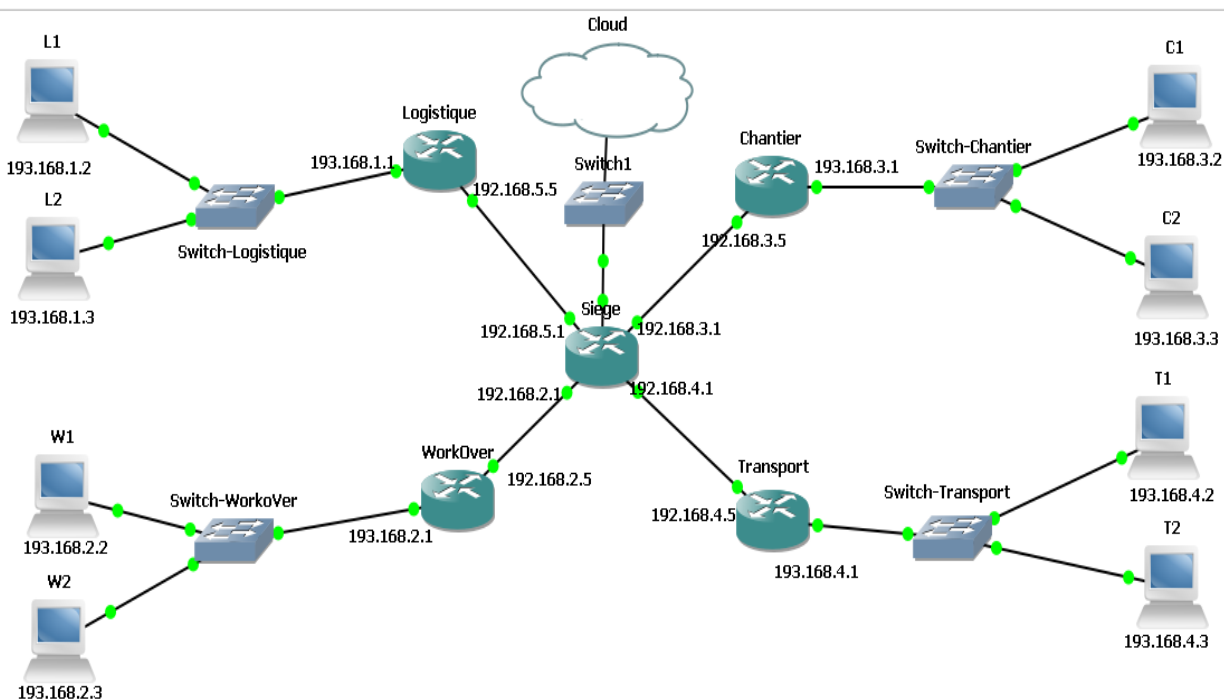


Figure 54: Connexion du Cloud avec le réseau ENAFOR

## 2. Développement de l'application de Monitoring Réseau

### 2.1 Langage de programmation

Notre application est implémentée en utilisant le langage de programmation C# et Visual Studio. C# est choisi pour son efficacité et sa simplicité.

Visual Studio est un ensemble complet d'outils de développement permettant de générer des applications Web ASP.NET, des Services Web XML, des applications bureautiques et des applications mobiles. Visual Basic, Visual C++, Visual C# et Visual J# utilisent tous le même environnement de développement intégré (IDE, Integrated Development Environment), qui leur permet de partager des outils et faciliter la création de solutions faisant appel à plusieurs langages. Par ailleurs, ces langages permettent de mieux tirer parti des fonctionnalités du Framework .NET, qui fournit un accès à des technologies clés simplifiant le développement d'applications Web ASP et de Services Web XML grâce à Visual Web Développeur [15] :

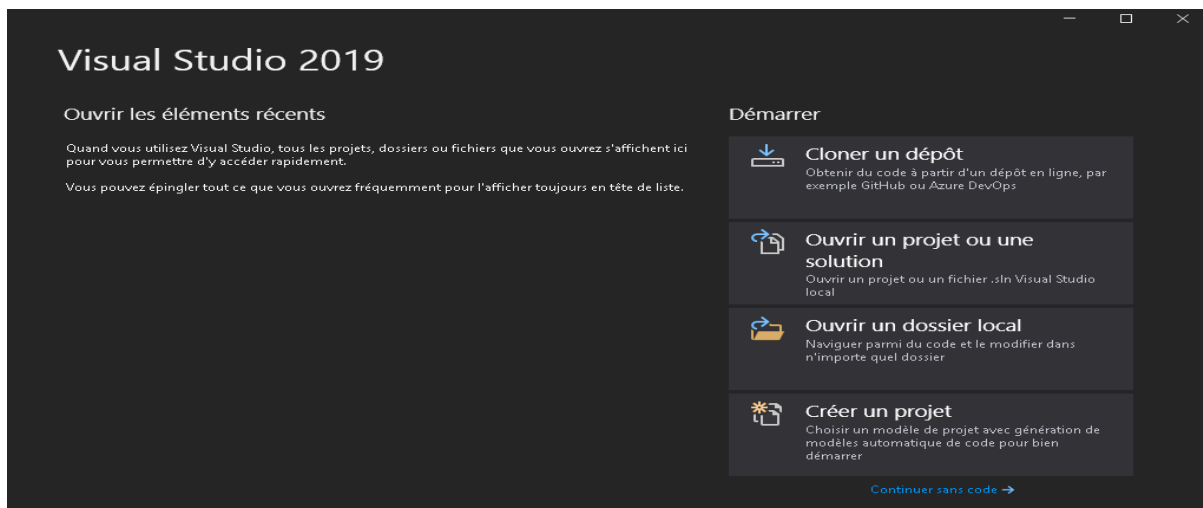


Figure 55: la plateforme de programmation Visual Studio 2019

## 2.2 Les fonctionnalités de l'application

L'application Monitoring Réseau est un outil réseau qui permet à l'administrateur de surveiller les équipements du réseau (Routers, PCs, Switchs, etc.) afin de tester leur disponibilité et leur connectivité. Elle récupère un large éventail de statistiques utiles quidevraient aider l'administrateur réseau.



Figure 56: l'interface de l'application Monitoring Réseau



Les fonctionnalités de l'application sont représentées par les boutons de l'interface graphique de la figure 56. Les éléments numérotés de la fenêtre d'application sont :

1. Démarrage en masse de Ping pour plusieurs équipements
2. Arrêt en masse de Ping pour plusieurs équipements
3. Réinitialisation en masse des statistiques Ping pour plusieurs équipements
4. Ping d'un seul équipement
5. Arrêt de Ping pour un équipement
6. Réinitialisation des statistiques Ping pour un équipement
7. Ajouter un équipement
8. Supprimer un équipement
9. Paramétrage du programme Ping
10. Scanneur IP réseaux
11. Tracer IP route
12. Sauvegarder la configuration
13. Option d'affichage
14. Ecran de contrôle des activités des équipements réseau

Pour tester et faire fonctionner l'application, on commence par le lancement de GNS3. Son démarrage implique le démarrage de tous les équipements du réseau (routeurs, Switchs et PCs)

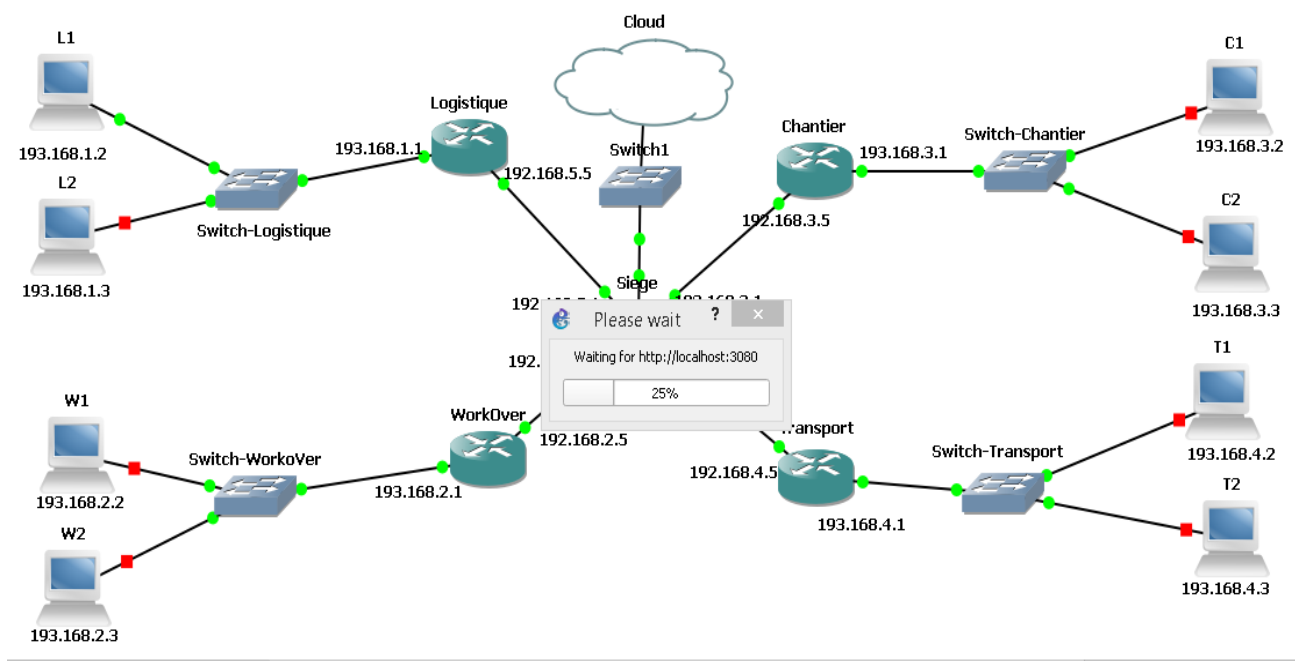


Figure 57: Lancement de GNS3

L'administrateur doit ajouter les adresses IP des équipements du réseau soit manuellement soit automatiquement. L'ajout automatique se fait en utilisant *Scanneur IP réseaux*. L'ajout manuel se fait en utilisant le bouton *ajouter un équipement*, comme l'illustre la figure 58

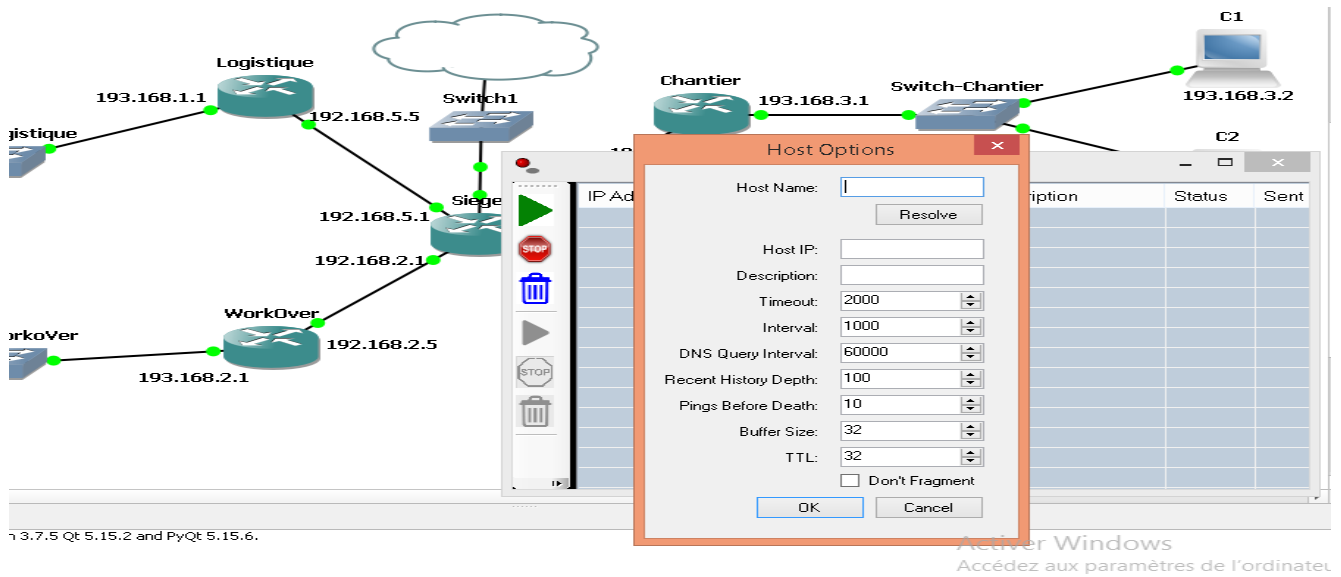


Figure 58: Ajout d'un équipement à l'application

La figure 59 donne une vue globale sur l'état de l'application après le lancement de GNS3 et l'ajout des équipements.

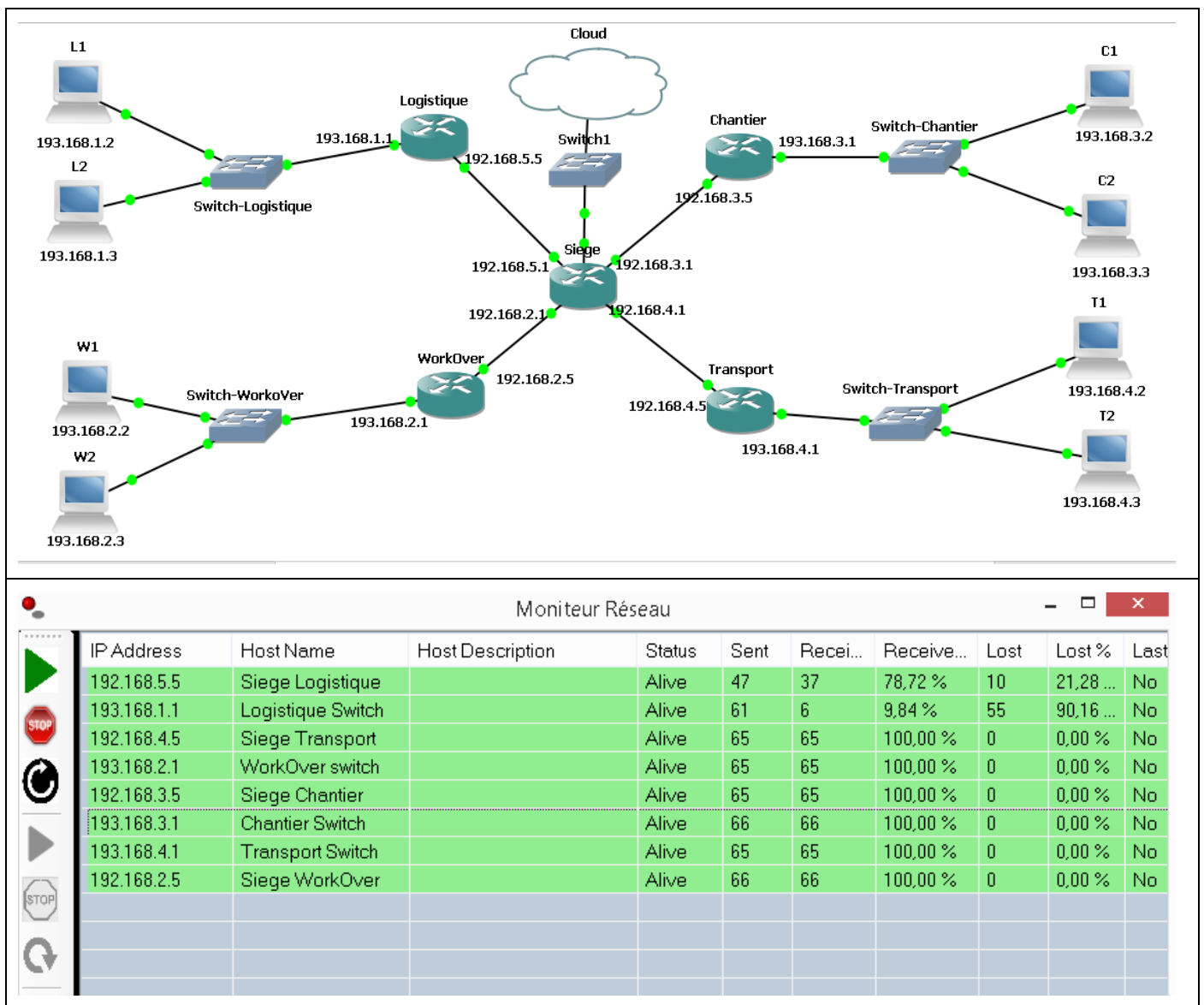


Figure 59: Le schéma final du réseau avec le moniteur Réseau

### 3. Les problèmes réseau détectés par l'application

Notre application, dans son état actuel couvre trois types de problèmes :

- problème de câblage.
- problème de conflit d'adressage.
- Problème de disponibilité

#### 3.1 Problème de connectivité

La défaillance au niveau du câblage ou n'importe quel support de transmission au sein d'un réseau informatique est un scénario très probable. Notre application facilite la détection rapide de ce problème, en localisant la source de la panne d'une manière précise. Nous présentons dans ce qui suit un scénario d'une coupure d'un câble qui relie le routeur Siege avec le routeur Chantier.

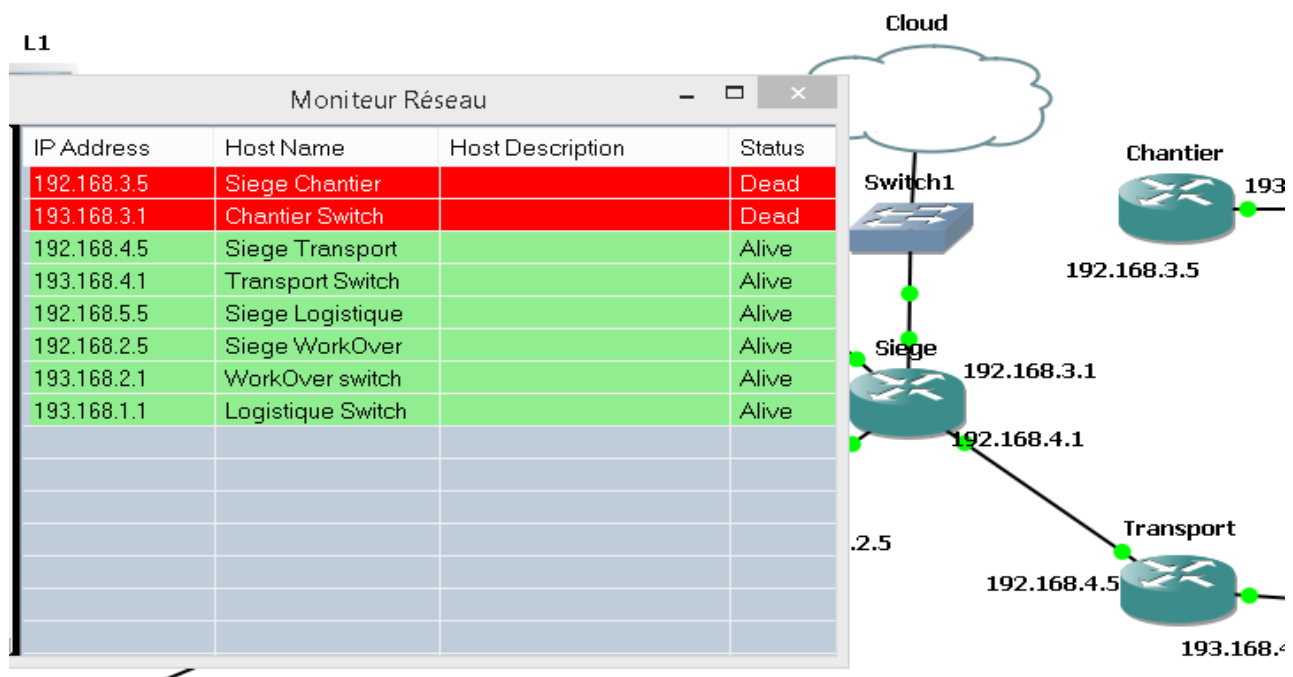


Figure 60: problème de câblage

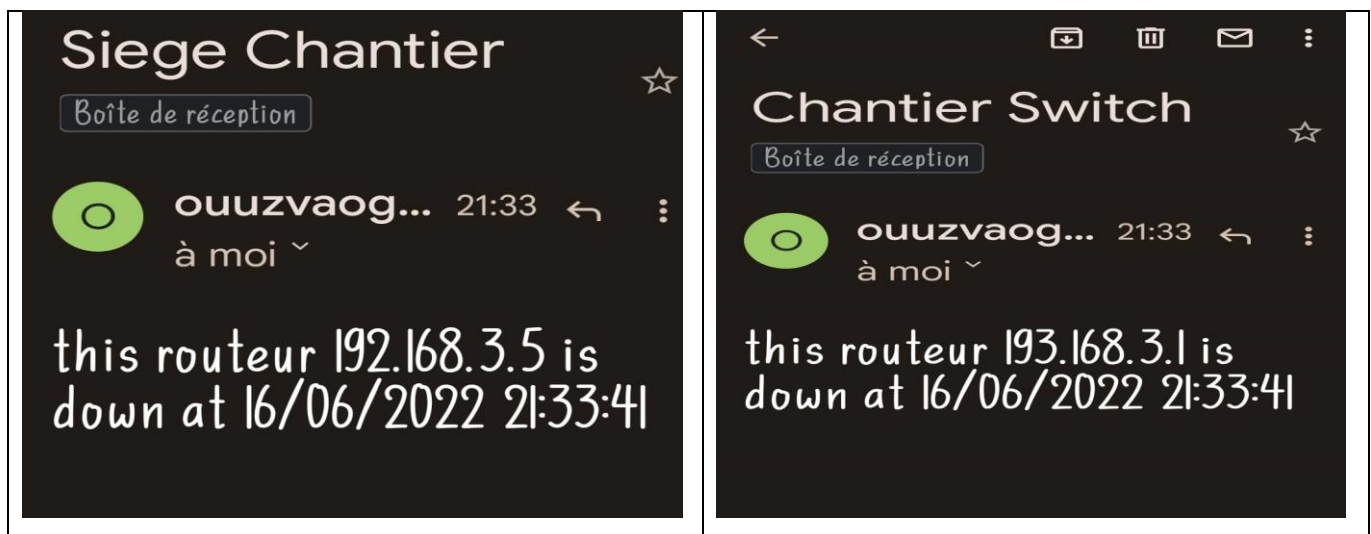


Figure 61: notification par email d'un problème de câblage

### 3.2 Problème de disponibilité des équipements

Il est possible qu'un ou plusieurs équipements du réseau tombent en panne, ce qui peut engendrer la chute d'un sous réseau ou même le réseau entier. Nous présentons l'exemple d'un scénario où un routeur (Transport) cesse de fonctionner.

Le moniteur détecte dans quelques secondes l'arrêt de la passerelle entre le siège et le site de transport, et informe ensuite l'administrateur du réseau immédiatement par une notification (par email) comme le montre la figure 63.

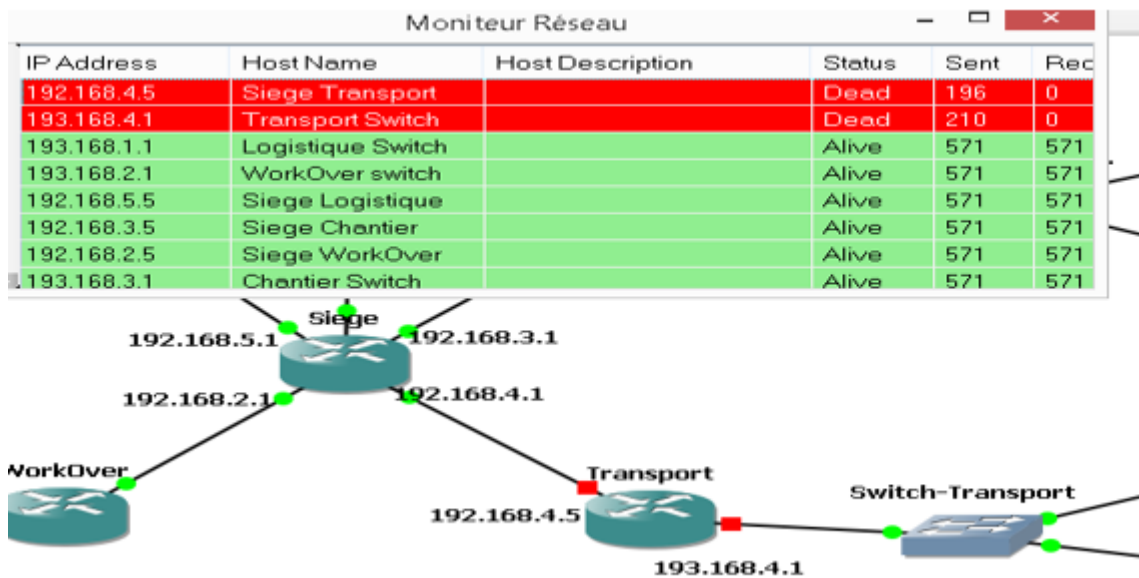


Figure 62: Arrêt du routeur Transport

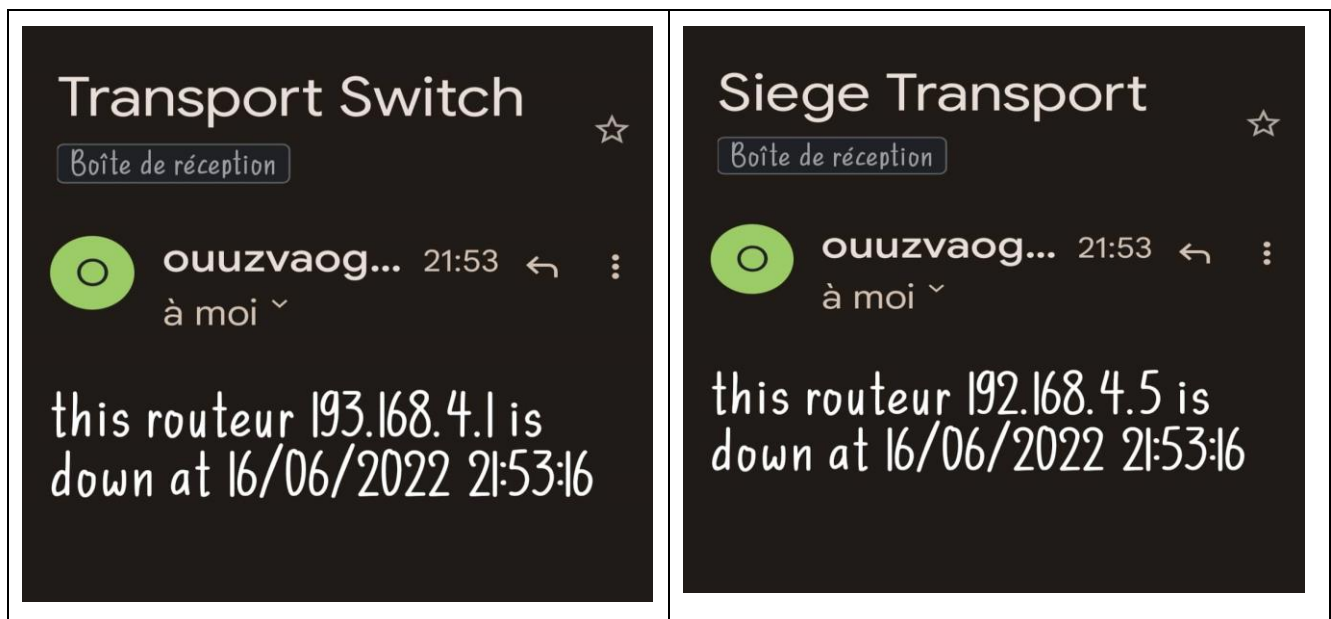


Figure 63: notification par email

### 3.3 Problème de conflit d'adressage

Le conflit d'adressage est rencontré très souvent après l'affectation des adresses IP aux équipements du même réseau. Par exemple, nous présentons le scénario d'un conflit d'adressage

entre le routeur Workover et le routeur Siege. Par conséquent, le routeur workover n'est plus fonctionnel et doit avoir une nouvelle adresse IP.

L'application détecte ce conflit (figure 64) et envoie une notification immédiate (figure 65) à l'administrateur qui va affecter une nouvelle adresse IP.

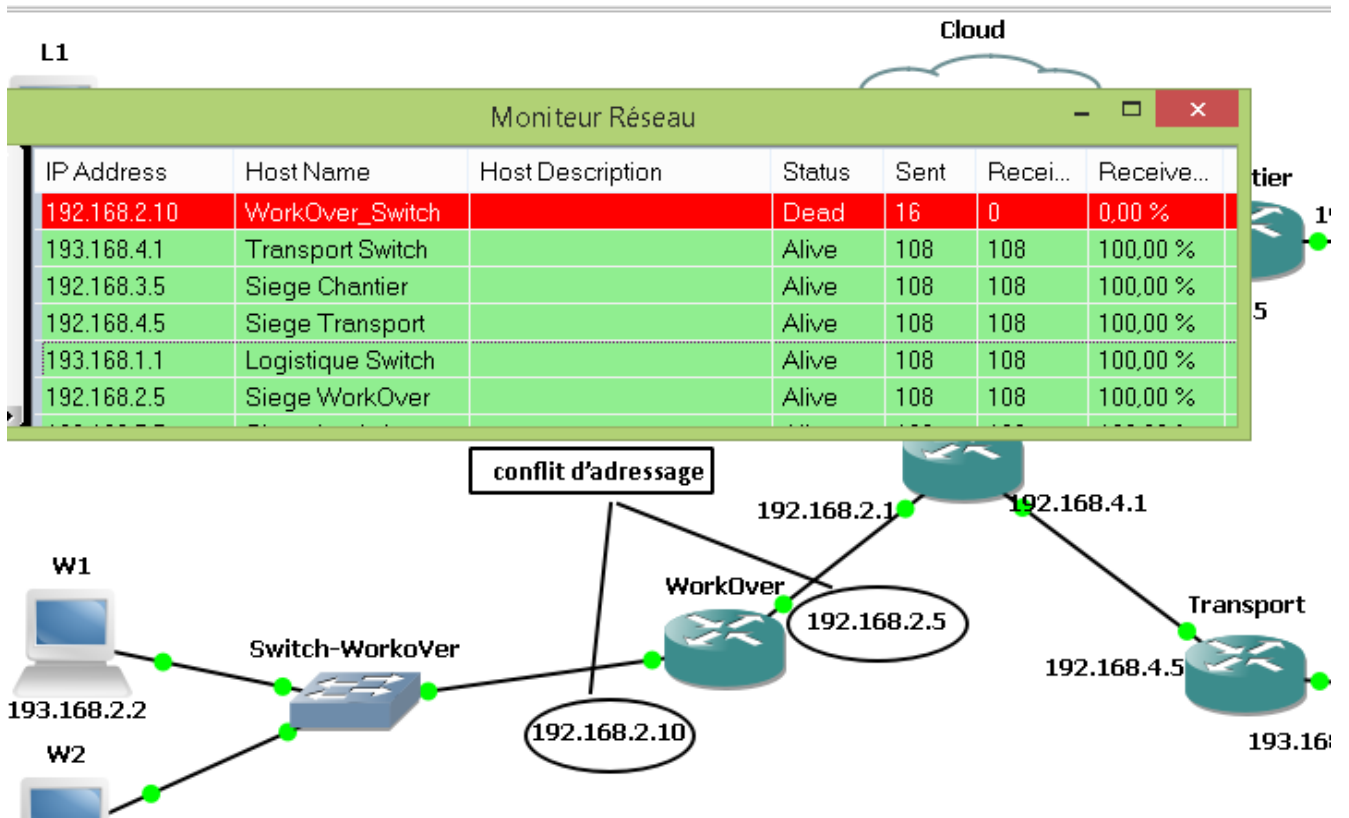


Figure 64 : détection d'un conflit d'adresses

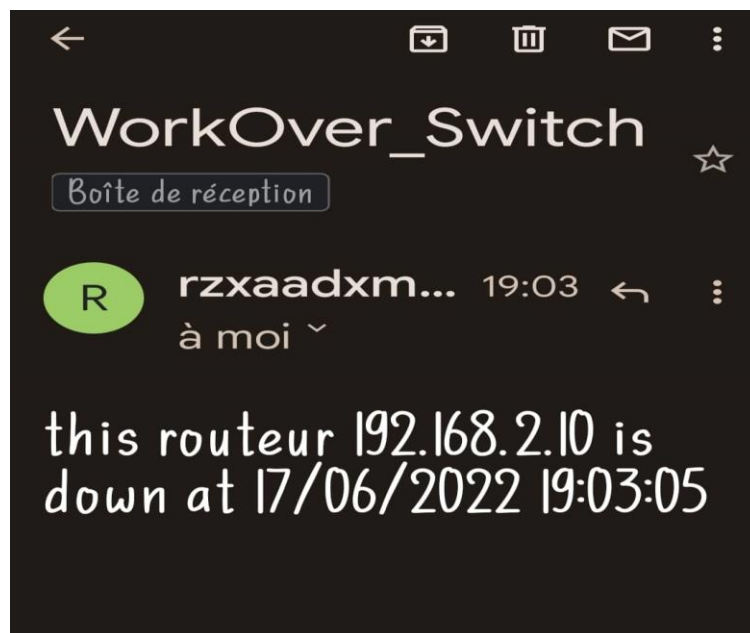


Figure 65: notification par email d'un problème de conflit d'adressage

# Conclusion générale

Un réseau informatique qui fournit des services essentiels à une entreprise doit toujours être disponible et fonctionnel. Par rapport aux objectifs initiaux de ce projet, on a pu développer une application de monitoring réseau sur une plateforme GNS3. Notre travail propose une solution logicielle permettant de reproduire et d'enrichir les fonctionnalités du système supervision et d'administration réseau de l'ENAFOR.

Cette expérience nous a permis d'acquérir des connaissances pratiques sur la supervision et l'administration réseau grâce aux facilités que l'ENAFOR nous a offertes pour réaliser ce travail. L'amélioration de l'outil (en ajoutant d'autres fonctionnalités) ainsi que sa mise en pratique (i.e., passer du virtuel à la pratique) feront l'objet d'un futur projet.

# Références

N °	Référence
[1]	Devaloua E ,(2007) .Mise en place d'un réseau local avec connexion internet cas du CESTIA-2EP.,«Mémoire-online», sur le site <a href="https://www.memoireonline.com/02/12/5375/m_Mise-en-place-dun-reseau-local-avec-connexion-internet-Cas-du-CESTIA-2EP0.html">https://www.memoireonline.com/02/12/5375/m_Mise-en-place-dun-reseau-local-avec-connexion-internet-Cas-du-CESTIA-2EP0.html</a>
[2]	Bernard KABUATILA,(2020).RESEAUX INFORMATIQUES G2 1920 , «academia »,sur le site <a href="https://www.academia.edu/42818698/RESEAUX_INFORMATIQUES_G2_1920_-_Copie">https://www.academia.edu/42818698/RESEAUX_INFORMATIQUES_G2_1920_-_Copie</a>
[3]	Jean-F ,(2012). Partage des connaissances « frameip » <a href="https://www.frameip.com/tcpip/#:~:text=Ce%20qu'on%20entend%20par,l'impl%20la%20plus%20courante">https://www.frameip.com/tcpip/#:~:text=Ce%20qu'on%20entend%20par,l'impl%20la%20plus%20courante</a>
[4]	Cadget-info (10/04/2022),« cadget-info.com », <a href="https://fr.gadget-info.com/difference-between-tcp-ip">https://fr.gadget-info.com/difference-between-tcp-ip</a>
[5]	Newsletter Q, (2019), « journaldunet JDN », <a href="https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203389-ip-adresse-ip-internet-protocol-definition/">https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203389-ip-adresse-ip-internet-protocol-definition/</a>
[6]	Philippe Latu, (2019), Interconnexion réseau et Logiciel Libre, « inetdoc.net »,sur le site <a href="https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html">https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html</a>
[7]	Les réseaux, Guy Pujolle, Édition 2005, Eyrolles, chap. 27
[8]	Hajar NB, (2018) , les type de réseaux,«slideplayer »sur le site <a href="https://slideplayer.fr/slide/13975107/">https://slideplayer.fr/slide/13975107/</a>
[9]	Materiel-informatique.be,(10/04/2022), Materiel-informatique.be, sur le site, <a href="http://www.materiel-informatique.be/topologie.php">http://www.materiel-informatique.be/topologie.php</a>
[10]	CoursTechInfo, (2008) , Provisoirement présentée uniquement sous forme abrégée et schématique , « courstechinfo», sur le site <a href="https://www.courstechinfo.be/Reseaux/Methode.html#:~:text=La%20m%C3%A9thode%20d'acc%C3%A8s%20d%C3%A9terministe&amp;text=C'est%20le%20passage%20,droit%20d'initier%20une%20transmission">https://www.courstechinfo.be/Reseaux/Methode.html#:~:text=La%20m%C3%A9thode%20d'acc%C3%A8s%20d%C3%A9terministe&amp;text=C'est%20le%20passage%20,droit%20d'initier%20une%20transmission</a>
[11]	Bords ,(2021), réseaux informatiques,« MongoSuKulu », sur le site <a href="https://www.mongosukulu.com/index.php/contenu/informatique-et-reseaux/reseaux-informatiques/639-les-equipements-reseaux-informatiques">https://www.mongosukulu.com/index.php/contenu/informatique-et-reseaux/reseaux-informatiques/639-les-equipements-reseaux-informatiques</a>
[12]	Dark P,(2021), leader de la sécurité informatique en Afrique sub-saharienne , « intrapole », sur le site, <a href="https://www.intrapole.com/spip.php?article18">https://www.intrapole.com/spip.php?article18</a>
[13]	Clairvo, (2012) , network informatique, « NETWORK INFORMATIQUE» sur le site <a href="http://network-informatique.blogspot.com/2013/02/gns3-installation.html">http://network-informatique.blogspot.com/2013/02/gns3-installation.html</a>
[14]	Microsoft,(2010). Visual Studio - Définition et Explications, « Techno-Science.net » ,sur le site <a href="https://www.techno-science.net/glossaire-definition/Visual-Studio.html">https://www.techno-science.net/glossaire-definition/Visual-Studio.html</a>
[15]	ENAFOR , Ismail Boulifa ,(10/02/2013).Réseau Informatique Enafor, rapport technique