REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud MAMMERI TIZI-OUZOU

Faculté de Génie Electrique et Informatique

Département Informatique

Mémoire de Projet de Fin d'Etudes Master Informatique

Option : ISI

THEME

Etude et supervision du réseau Data Communication Network (DCN)

Dirigé par : Mme BOUAMRA.S

Proposé par et Encadré : Mr BENKAIDALI.M

présenté par : KHALEM Med Amine

LADJ Charafeddine

Jury composé de :

Président :…….

Examinateur 1:……

Examinateur 2 :……..

Promotion: 2011- 2012

Sommaire……I

Liste des figures……VI

Liste des tableaux……VII

Introduction générale…… ……1

Problématique……..2

Cahier de charge……..3

Chapitre I Réseaux et protocoles de communication

I. Introduction……....4

II. Les réseaux.....…....4

II.1. Les différents types du réseau……..4

a. Les réseaux LAN……...4

b. Les réseaux MAN……5

c. Les réseaux WAN……5

II.2. Les équipements réseaux ……5

III. Le modèle de référence OSI de ISO……6

1. La couche physique……7

2. La couche liaison de données……7

3. La couche réseau……..7

4. La couche transport……..7

5. La couche session……8

6. La couche présentation……8

7. La couche application……..8

IV. Description du modèle TCP/IP ……..9

V. L'adresse IP (IPv4)……10

1. Le format des adresses IP……10

2. La technique de découpage d'une classe en sous-réseaux « Subneting »……..12

VI. Le routage……...13

VI. Les Protocoles de routage…….……13

1. Terminologie et distinction…….…….14

2. Composition d'une table de routage……...…….14

2.1 Métrique……..14

2.2 Distance administratif……15

3. Routage statique VS routage dynamique.....…...16

3.1. Objectifs des protocoles de routage……...16

3.2. Routes statiques…….…16

4. Les protocoles de routage……17

4.1. Système autonome, routage intérieur et extérieur…….....17

4.2. Protocole de routage à vecteur de distance, à état de lien et hybride…….17

5. Tableau récapitulatif des protocoles de routage intérieurs……..……18

VII. Le protocole de routage OSPF……..……18

1. Introduction……..…….18

2. Comparative fonctionnelle des protocoles RIP et OSPF…….…….18

3. Les éléments d'OSPF……20

4. Link-State…….20

4.1 Hiérarchie……...……..20

5. Notions de DR et BDR……23

6. Les états OSPF pour la construction des adjacences…….…….23

6.1. Découverte des voisins…….24

a. Down State……..24

b. Init State……24

c. Two-Way state…….25

6.2. Découverte des routes……25

a. ExStart State……25

b. Exchange State……26

c. Loading State……26

d. Full Adjacency……26

7. Topologie OSPF……...26

1. Vue d'ensemble du protocole OSPF « HELLO »……..27

2. Opérations OSPF……28

VIII. Conclusion……31

Chapitre II Les réseaux GSM

I. Introduction……..……..32

II. Architecture du réseau GSM……...……32

III. Fonctions d'un réseau GSM……..….33

1. Le sous système radio (BSS)…….……33

a. Le mobile (MS)……..……..33

b. La station de base BTS (Base Transceiver Station)……...…….33

c. Le contrôleur de station de base BSC (Basic Station Controler)……...…..34

2. Le sous système réseau (NSS)……...….35

a. Le centre de communication Mobile (MSC)……..35

b. L'enregistreur de localisation nominale (HLR)……..35

c. Le centre d'authentification (AuC)…….36

d. L'enregistreur de localisation visiteurs (VLR)……36

e. Le centre d'exploitation et de maintenance (OSS)……..36

IV. Supports de transmission ……..37

V. Technique de multiplexage……..39

1. traitement des vois…….40

2. Le système PDH (Plesiochronous Digital Hierarchy)……..……40

3. Le système SDH (Synchronous Digital Hierarchy)……...41

V. Conclusion…….……..41

Chapitre III Dimensionnement d'un DCN

I. Introduction……...…….42

II. Equipements de transmission SDH et PDH utiliser par Wataniya ……..42

III. MINI-LINK TN (Trafic Node)…….…..43

a. Parties extérieur (OutDoor)……..43

b. Partie intérieur (InDoor) ……..44

IV. Les outils de gestion……..…….46

1. Centralized management…….….47

a. Mini Link manager…….47

b. Mini Link connexion……..47

2. Northbound Management Interfaces……47

3. Local Manager……..……48

4. CLI (Command Line Interface)……49

5. ServiceOn Microwave……..49

V. Les avantages de TN……...…….50

VI. Data Communication Network (DCN)……...50

1. DCN IP…….51

2. Les services du DCN……52

3. Les canaux DCN……..53

4. La capacité DCN…….….53

4. Le calcul de la bande passante BW……..53

VII. Etudes sur un réseau DCN (Exemple)……...56

a. Calcul de la bande passante……..56

b. Adressing IP et Subneting……..……..58

c. Routage……60

d. Les extensions DCN……..……..61

VIII. Conclusion……...……61

Chapitre IV Outils de dimensionnement

I. Introduction …….....62

II. Présentation de Delphi.....62

II.1 Environnement de travail…….....62

II.2. Présentation de l'interface développée sous Delphi.....63

Conclusion…….....76

Conclusion générale……..77

Annexe…….....VII

Glossaire……...XI

Bibliographie……..XIII

Liste des Figures

Chapitre I

Fig.1.1 Le modèle OSI……6

Fig.1.2 Correspondance entre OSI - TCP/IP……..9

Fig.1.3 Les différents types des classes et format d'adresse……11

Fig.1.4 Exemple d'utilisation de la technique « subneting»……13

Fig.1.5. Le fonctionnement d'OSPF dans une zone……22

Fig.1.6. Etape Two-Way state……...25

Chapitre II

Fig.3.1. Architecture du réseau GSM……...32

Fig.2.2. Fonctions du système GSM……33

Fig.3.4. Station de Base BTS……....34

Fig.3.5. Faisceaux hertziens……38

Fig.3.6. Interconnexion VSAT……..38

Fig.3.7. Traitement d'une voie temporelle……....40

Fig.3.8. Trame de base STM1……...41

Chapitre III

Fig.3.1. Mini Link TN……..43

Fig.3.2. La partie extérieure……..43

Fig.3.3. AMM 2p……..44

Fig.3.4. AMM 6p……..44

Fig.3.5. AMM 20p……44

Fig.3.6. MMU……...45

Fig.3.7. NPU……45

Fig.3.8. FAU……45

Fig.3.9. Emplacements des composants d'un MINI LINK TN……46

Fig.3.10. la philosophie de gestion de Mini-Link TN……..46

Fig.3.11. Northbound Management interfaces……47

Fig.3.12. Embedded Element Manager (EEM)……48

Fig.3.13. Gestion locale……48

Fig.3.14. Outils de gestion……49

Fig.3.15. ServiceOn MicroWive……...49

Fig.3.16. Le trafic et réseau de DCN……50

Fig.3.17. The DCN connects the NEs to the management system……...51

Fig.4.18. les services DCN……52

Liste des Tables

Chapitre I

Tab.1.1. Exemple : adresse IP **192.168.1.1**……...10

Tab.1.2. Espace d'adressage……12

Tab.1.3. Distance administrative……...15

Tab.1.4. Récapitulatif des protocoles de routage intérieurs…...……18

Tab.1.5. Types de paquet OSPF……24

Tab.1.6. Topologie OSPF……..……26

Tab.1.7. les valeurs par défaut du coût/ type de média sur les IOS Cisco…...……30

Chapitre II

Tab .2.1. Les interfaces du réseau GSM……...37

Chapitre III

Tableau 3.1. O&M Payload……...55

Tableau 3.2. BW Calculassions…….55

Tableau 3.3. Table des nœuds……59

Introduction générale

De jour en jour, la télécommunication joue un grand rôle à l'échelle mondiale et ne cesse d'évoluer en fonction de la demande sur les medias et les moyens de télécommunication, pour subvenir au besoin du client et du consommateur.

Ce dynamisme a poussé la technologie de télécommunication à se développer d'une façon considérable, en évoluant recherche par recherche pour se combiner et réunir l'ensemble nécessaire à l'industrie de la télécommunication. L'outil le plus important qui a donné naissance a ces réalisations historiques c'est bien le réseau de transmission, avec ses diverses solutions de transport d'information (voix, vidéo,….). Ce dernier est une façon fiable et efficace de relier un émetteur et un récepteur quelle que soit la distance qui sépare l'un de l'autre.

Malgré la fiabilité des réseaux de transmission, la nécessité d'un réseau de supervision est primordiale afin d'assurer une meilleur disponibilité des services d'un opérateur de télécommunication.

Il est essentiel d'avoir la maitrise des technologies de télécommunication ou des réseaux de transport de données au moyen d'un système de gestion pour éviter les interruptions et les perturbations dans le trafic. Le système de gestion communique avec chacun des éléments du réseau (Network Elément NE) pour la création de la configuration des paramètres et pour la collecte de l'état et le rendement.

C'est toutefois, une condition préalable à la communication que le système de gestion est relie a touts les NEs. Ces connexions constituent le Data Communication Network (DCN).

Wataniya Télécom Algérie ne cesse d'acquérir des nouvelles solutions, ce qui la contraint à un problème d'interopérabilités de protocoles de supervision de plusieurs plateformes, Fiabilités, Disponibilité, Adaptation des équipements futures sur le réseau de supervision existant.

Le but de notre travaille est d'étudier le DCN et de trouver des solutions pour bien assurer la fiabilité de la supervision du réseau de transmission appartenant à l'opérateur de la téléphonie mobile Wataniya Télécom Algérie.

Pour cela, les objectifs suivant ont été tracés :

1. Garantir l'interopérabilité entre les équipements.
2. Assurer une meilleure supervision
3. Analyser, optimiser le réseau DCN de WTA.
4. Assurer la bande passante suffisante pour le trafic.

Apres avoir étudié les différents équipements et technologies, nous avons envisagé des solutions qui sont aptes pour le cas réseau actuel et en cas d'extension.

Ce mémoire est structuré selon quatre chapitres :

- Dans un premier temps, nous aborderons le sujet des réseaux informatiques et les différents modèles ISO, TCP/IP ainsi que les différents types de routages qui existaient déjà et utilisés dans le domaine comme la téléphonie Mobile, avec quelques exemples et comparaisons entre eux.
- Dans un deuxième temps, nous allons nous pencher sur des préambules importants de GSM telle que l'architecture du réseau GSM. Nous décrivons brièvement les supports de transmission, puis nous aborderons les thèmes du multiplexage PDH, SDH.
- Dans le troisième chapitre, nous nous concentrerons sur le réseau de supervision DCN de Wataniya Télécom Algérie (Nedjma). Nous étudierons les différentes étapes de conception de ce réseau ainsi que les solutions pour garantir la visibilité, la flexibilité et la fiabilité.
- On finalise avec une application DELPHI qui nous à été proposée et qui apportera plusieurs aides au niveau du dimensionnement du réseau DCN lors du calcul de la bande passante.

Notre cahier des charges consiste :

1. Garantir l'interopérabilité entre les équipements.
2. Assurer une meilleure supervision
3. Analyser, optimiser le réseau DCN de WTA.
4. Garantir la bande passante suffisante pour le trafic.

CHAPTRE I

I. Introduction

Un réseau permet à plusieurs machine de communiquer entre elles afin d'assurer des échanges d'informations: du transfert de fichiers, du partage de ressources, de la messagerie ou de l'exéc ution de programmes à distance. Du point de vue de l'utilisateur, le réseau doit être le plus transparent possible: ses applications doivent être capables de communiquer toutes seules avec le reste du réseau, sans intervention. Le défi consiste donc à 'interconnecter' ces différents matériels. Le protocole TCP/IP s'impose comme langage de communication *espéranto* permettant de fédérer un environnement hétérogène. On peut classer les réseaux en trois catégories, principales, selon le type et l'origine de l'information :

- Réseaux téléphoniques des opérateurs télécommunications.
- Réseaux informatiques.
- Réseaux de diffusion acheminant les programmes audiovisuels.

II. Les réseaux :

Les personnes communiquent en ligne à partir de n' importe où (exemple : communication téléphonique). Une technologie efficace et fiable permet au réseau d'être disponible n'importe quand et n' importe où. Alors que notre réseau humain continue de s'étendre, la plateforme qui relie ce réseau et le prend en charge doit également se développer.

II.1 Les différents types de réseau :

a. Les réseaux LAN :

LAN signifie Local Area Network (en français Réseau Local). Appelé aussi réseau local d'entreprise ou Privé, Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et souvent reliés entre eux grâce a la technologie la plus rependue, l'Ethernet. Avec à ce type de réseau, l'entreprise ou l'organisation dispose d'un système qui lui permet :

- Le partage des données (base de données industrielles, informations...)
- L'accès aux Ressources du réseau (imprimantes, serveurs)
- L'accès aux applications disponibles sur le réseau (logiciel) Un réseau local relie des ordinateurs et des périphériques tels que des unités de stockages ou des imprimantes à l'aide de support de transmission par câble (coaxial ou paire torsadée) ou radio-fréquences sans fil sur une circonférence d'une centaine de mètres. Au-delà, on considère que le réseau fait partie d'une autre catégorie de réseau appelé (MAN - Métropolitan Area Network), pour laquelle les supports de transmission sont plus adaptés aux grandes distances...

b. Les réseaux MAN :

Les MAN (Metropolitan area Network) permettent de connecter plusieurs LAN proches entre elles. Pour les relier entre elles, on fait appel à des routeurs et des câbles de fibre optique permettant des accès à très haut débit.

c. Les réseaux WAN :

Les WAN (Wide area Network qui signifie réseau étendu) permettent de connecter plusieurs LAN éloignées entre elles. Le débit devient de plus en plus faible en fonction de la distance. Internet est un regroupement de WAN.

II.2 Les équipements réseaux :

L'interconnexion de réseaux peut être locale : les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard suffit à réaliser physiquement la liaison.

L'interconnexion peut aussi concerner les réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc..).

Les équipements qui sont utilisé en général sont :

- ✓ Le répéteur (Repeater)
- ✓ Le pont(Bridge)
- ✓ La passerelle(Gateway)
- ✓ Le concentrateur(HUB)
- ✓ Le commutateur(Switch)
- ✓ Le routeur (Router) : Un Routeur Equipement d'interconnexion dans un réseau. Matériel « intelligent » qui détermine une route à suivre pour l'acheminement des données.

Un routeur doit être connecté à au moins deux réseaux informatiques pour être utile, sinon il n'aura rien à router. L'appareil crée et/ou maintient une table, appelée *table de routage*, laquelle contient les meilleures routes vers les autres réseaux, via les métriques associées à ces routes.

Un routeur moderne est un boîtier regroupant une carte mère, avec un microprocesseur, mémoire ROM, RAM ainsi que les ressources réseaux nécessaires (Wifi, Ethernet...). Il s'agit donc d'un ordinateur minimal dédié, dont le système d'exploitation est d'ailleurs souvent un dérivé allégé de Linux. De même, tout ordinateur disposant des interfaces adéquates (au minimum deux, souvent Ethernet) peut faire office de routeur s'il est correctement configuré (certaines distributions Linux minimales sont spécialisées pour la fonction).

La fonction de routage consiste à traiter les adresses IP en fonction de leur adresse réseau définie par le masque de sous-réseaux (par défaut ou personnalisé) et à les diriger en fonction de l'algorithme de routage et de sa table de routage (celle ci contient la correspondance des adresses réseau avec les numéros de port physique du routeur ou sont connectés les autres réseaux).

III. Le modèle de référence OSI d'ISO :

Pour visualiser l'interaction entre différents protocoles, un modèle en couche est généralement utilisé. Un modèle en couche décrit le fonctionnement des protocoles au sein de chacune des couches, ainsi que l'interaction avec les couches supérieures et inférieures.

Le modèle OSI a été conçu par l'organisation internationale de normalisation (ISO, International Organizaion for Standardization). L'idée était que cet ensemble de protocoles serait utilisé pour développer un réseau international qui ne dépendrait pas de systèmes propriétaires. Il se décompose en sept couches :

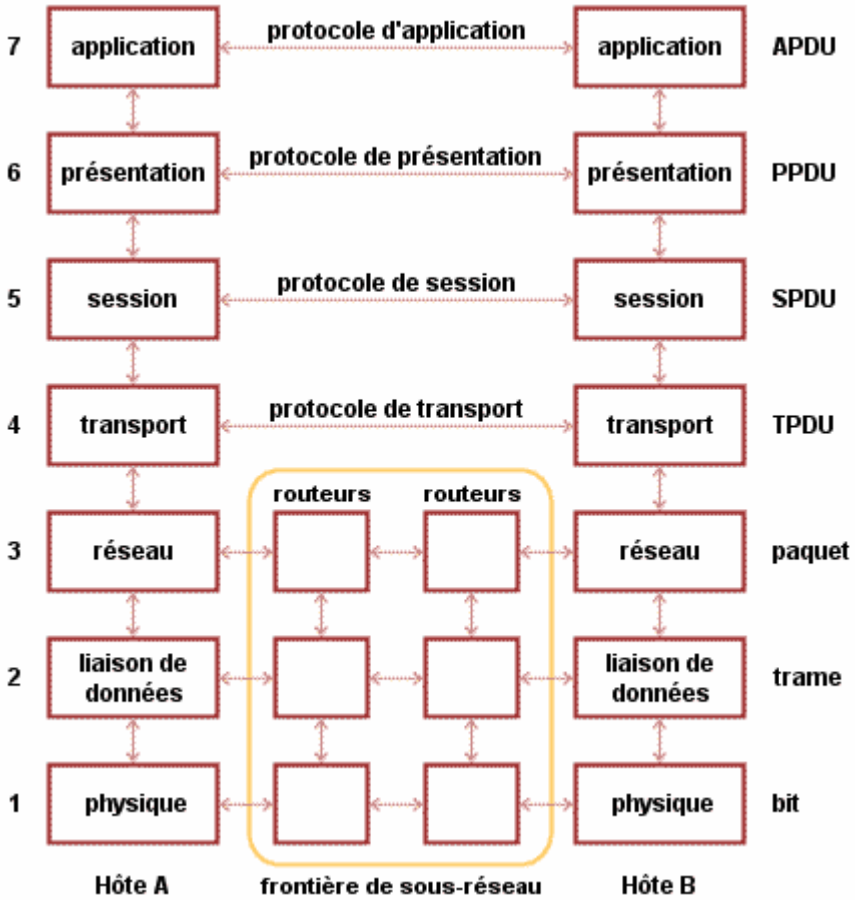


Fig.1.1. Le modèle OSI.

1. La 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 bien être 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. **[12]**

2. La couche liaison de données

Son rôle est un rôle de "liant" : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données. La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

L'unité d'information de la couche liaison de données est la trame qui est composée de quelques centaines à quelques milliers d'octets maximum. **[12]**

3. La couche réseau

C'est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...).
La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat. L'unité d'information de la couche réseau est le paquet. **[12]**

4. Couche transport

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 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. Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session. Cette couche est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois... Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau. Un des tous derniers rôles à évoquer est le contrôle de flux.

C'est l'une des couches les plus importantes ; car c'est elle qui fournit le service de base à l'utilisateur, et par ailleurs, c'est elle qui gère l'ensemble du processus de connexion avec toutes les contraintes qui y sont liées. L'unité d'information de la couche réseau est le message. **[12]**

5. La couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. 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. **[12]**

6. La couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser. **[12]**

7. La 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... **[12]**

IV. Description du modèle TCP/IP :

Appelé également « modèle DoD » ou « darpa », le modèle TCP/IP a été initialement développé par l'agence ARPA (Advanced Research Projects Agency) sous le nom « arpanet».

Destiné à une utilisation militaire, TCP/IP est devenu un standard aussi bien au niveau des réseaux locaux que des réseaux étendus comme l'internet.

Le modèle TCP/IP correspond a une simplification du modèle OSI plus pragmatique et représentatif des technologies existantes. On parle de réseau TCP/IP lorsque la famille de protocole TCP/IP est utilisée.

Donc la figure suivant décrit les quatre couches du modèle TCP/IP en correspondance avec le modèle OSI ainsi que les protocoles utilisés pour chaque couche de ce modèle. [11]

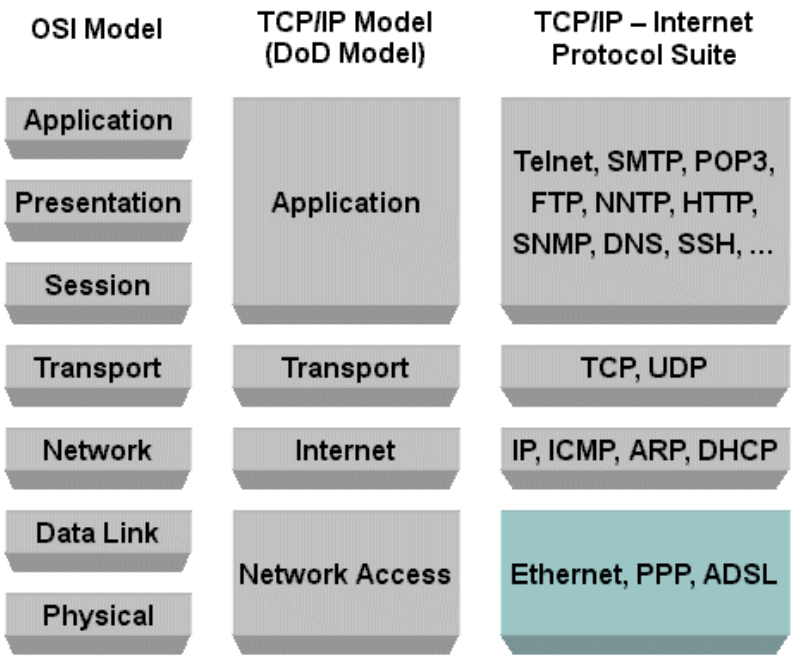


Fig.1.2.correspondance entre OSI - TCP/IP.

Le rôle fondamental de la couche réseau (niveau 3 du modèle OSI) est de déterminer la *route* que doivent emprunter les paquets. Cette fonction de recherche de chemin, nécessite une identification de tous les hôtes connectés au réseau. De la même façon que l'on repère l'adresse postale d'un bâtiment à partir de la ville, la rue et un numéro dans cette rue. On identifie un hôte réseau par une *adresse* qui englobe les mêmes informations.

Le modèle TCP/IP utilise un système particulier d'adressage qui porte le nom de la couche réseau de ce modèle : *l'adressage IP*. Le but de cet article est de présenter le fonctionnement de cet adressage dans sa version la plus utilisée IPv4.

De façon très académique, on débute avec le format des adresses IP. On définit ensuite les classes d'adresses IP, le premier mode de découpage de l'espace d'adressage. Comme ce mode de découpage ne convenait pas du tout au développement de l'Internet, on passe en revue la chronologie des améliorations apportées depuis 1980 : les sous-réseaux ou *subnetting*, la traduction d'adresses ou *Native Address Translation* (NAT) et enfin le routage inter-domaine sans classe. [11]

V. L'adresse IP (IPv4) :

1. Le format des adresses IP :

Les adresses IP sont composées de 4 octets. Par convention, on note ces adresses sous forme de 4 nombres décimaux de 0 à 255 séparés par des points.
L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

- La partie réseau (netid) est commune à l'ensemble des hôtes d'un même réseau [11].
- La partie hôte (hostid) est unique à l'intérieur d'un même réseau [11].

Prenons un exemple d'adresse IP pour en identifier les différentes parties :

Tableau 1. Exemple : adresse IP 192.168.1.1

Adresse complète	**192.168.1. 1**
Masque de réseau	255.255.255. 0
Partie réseau	192.168.1.
Partie hôte	1
Adresse Réseau	192.168.1.0
Adresse de diffusion	192.168. 1.255

Tab.1.1 Table d'adressage.

- **Le masque de réseau :**

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau.

- **L'adresse de diffusion :**

Chaque réseau possède une adresse particulière dite de *diffusion*. Tous les paquets avec cette adresse de destination sont traités par tous les hôtes du réseau local. Certaines informations telles que les annonces de service ou les messages d'alerte sont utiles à l'ensemble des hôtes du réseau.

- **Les classes d'adresses :**

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.

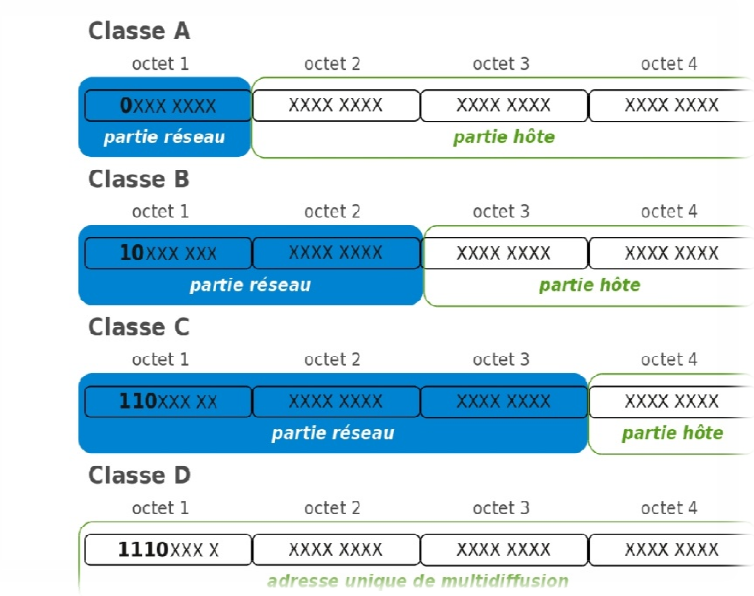


Fig.1.3. les différents types des classes et format d'adresses.

Les adresses de Classe A :

Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte. L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

Les adresses de Classe B :
Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

Les adresses de Classe C :
Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

Les adresses de Classe D :
Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (*host groups*).

Les adresses de Classe E :
Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Tableau 2. Espace d'adressage

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques

Tab.1.2. Espace d'adressage.

Le tableau ci-dessus montre que la distribution de l'espace d'adressage est mal répartie. On ne dispose pas de classe intermédiaire entre A et B alors que l'écart entre les valeurs du nombre d'hôte par réseau est énorme.

2. La technique de découpage d'une classe en sous-réseaux « subnetting » :

Pour compenser les problèmes de distribution de l'espace d'adressage IP, la première solution utilisée consiste à découper une classe d'adresses IP A, B ou C en sous-réseaux. Cette technique appelée *subnetting* a été formalisée en 1985 avec le document RFC950.

Si cette technique est ancienne, elle n'en est pas moins efficace face aux problèmes d'exploitation des réseaux contemporains. Il ne faut jamais oublier que le découpage en réseaux ou sous-réseaux permet de cloisonner les domaines de diffusion. Les avantages de ce cloisonnement de la diffusion réseau sont multiples.

Pour illustrer le fonctionnement du découpage en sous-réseaux, on utilise un exemple pratique. On reprend l'exemple de la classe C 192.168.1.0 dont le masque réseau est par définition 255.255.255.0. Sans découpage, le nombre d'hôtes maximum de ce réseau est de 254. Considérant qu'un domaine de diffusion unique pour 254 hôtes est trop important. On choisit de diviser l'espace d'adressage de cette adresse de classe C. On *réserve* 3 bits supplémentaires du 4ème octet en complétant le masque réseau. De cette façon on augmente la partie réseau de l'adresse IP et on diminue la partie hôte. **[12]**

Fig.1.4 : Exemple d'utilisation de la technique « Subnetting».

VI. Le Routage :

Le terme routage désigne le mécanisme par lequel les données d'un équipement expéditeur sont acheminées jusqu'à leur destinataire, même si aucun des deux ne connait le chemin complet que les données devront suivre. Avoir une procédure de routage efficace est particulièrement important pour les réseaux décentralisé.

Tous les appareils connectés à Internet contiennent une table de routage. Du point de vue du routage, on distingue deux types logiques d'appareils :

- Les terminaux, ou hôtes qui sont reliés à un seul réseau et qui ont par conséquent une table de routage simple.
- Les routeurs qui relient au moins deux réseaux et possèdent une table de routage plus complexe.

a. Routage statique et dynamique :

Les tables de routage peuvent être configurées en dur sur le routeur. On parle alors de « routage statique ». Elles peuvent aussi être mises à jour automatiquement et dynamiquement, c'est le « routage dynamique ».

VI.1 Les protocoles de routage :

On trouvera ici une vue d'ensemble sur le routage. On aborde de manière synthétique les notions de tables de routage, de métrique, de distance administrative, de protocole de routage dynamique et de routage statique, de convergence, de routage à vecteur de distance à état de liens et hybride.

1. Terminologies et distinctions :

- On distinguera la notion de métrique et de distance administrative dans une table de routage dont on connait la composition.
- On définira les objectifs des protocoles de routage
- On distinguera le routage statique du routage dynamique (protocole de routage).
- On distinguera les protocoles de routage intérieurs et les protocoles de routage extérieurs ainsi que la notion de système autonome.
- Parmi les protocoles de routage, on distinguera les protocoles de routage à vecteur de distance, les protocoles de routage à état de liens, ainsi que les protocoles de routage hybride.

2. COMPOSTION D'UNE TABLE DE ROUTAGE :

Une table de routage est une sorte de "panneau indicateur" qui donne les routes (les réseaux) joignables à partir du "carrefour" que constitue un routeur. Les paquets arrivent sur une interface de la machine. Pour "router" le paquet, le routeur fondera sa décision en deux temps : d'abord il regarde dans l'entête IP le réseau de destination et compare toutes les entrées dont il dispose dans sa table de routage; ensuite, si le réseau de destination est trouvé, il commute le paquet sur le bon port de sortie; si ce réseau n'est pas trouvé, le paquet est rejeté.

Une table de routage réside en RAM. Elle constituée des éléments suivants :

- Méthode de routage : type de protocole qui a appris la route.
- Réseau et masque : destination.
- Distance administrative : Préférence d'une route par un protocole sur un autre. Chaque protocole a sa valeur par défaut.
- Valeur de métrique : valeur d'une route sur une autre parmi toutes celles apprises par un protocole de routage.
- Via prochaine interface (Gateway).
- Interface de sortie du routeur.

2.1. Métrique :

La métrique d'une route est la valeur d'une route en comparaison d'autres routes apprises par le protocole de routage. Plus sa valeur est faible, meilleure est la route. Chaque protocole dispose de sa méthode de valorisation.

On peut trouver toute une série de composante de métrique parmi :

- nombre de sauts (RIP)
- bande passante (IGRP - EIGRP)
- délai (IGRP - EIGRP)
- charge (IGRP - EIGRP)
- fiabilité (IGRP - EIGRP)
- MTU (IGRP - EIGRP)
- coût (OSPF - ISIS)

2.2 Distance administrative :

La distance administrative est la préférence dans une table de routage des routes apprises par un protocole de routage par rapport aux mêmes routes apprises par un autre protocole de routage. Plus la valeur est faible et plus le protocole est préféré. Chaque protocole dispose de sa valeur par défaut sur les routeurs Cisco :

Méthode de routage	**Distance administrative**
Interface directement connectée	0
Route statique	1
Ext-BGP	20
Int-EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Int-BGP	200
Inconnu	255

Tab.1.3. Distance Administrative.

3. Routage statique et routage dynamique :

Une route statique est une entrée manuelle dans la table de routage. Une route dynamique est apprise dynamiquement par un protocole commun.

3.1. Objectifs des protocoles de routage

- Découvrir dynamiquement les routes vers les réseaux d'un inter-réseau et les inscrire dans la table de routage.
- S'il existe plus d'une route vers un réseau, inscrire la meilleure route dans la table de routage.
- Détecter les routes qui ne sont plus valides et les supprimer de la table de routage.
- Ajouter le plus rapidement possible de nouvelles routes ou remplacer le plus rapidement les routes perdues par la meilleure route actuellement disponible.
- Empêcher les boucles de routage

3.2. Routes statiques

Une route statique est une entrée manuelle dans une table de routage. Contrairement aux routes apprises dynamiquement, leur maintenance est plus lourde pour les administrateurs. Elles servent d'alternatives aux routes dynamiques surtout quand la situation le permet ou l'exige en termes de facilité, de simplicité ou de sécurité.

Voici la commande de configuration des routes statiques :

(config)#**ip route** *network mask {address|interface} [AD]*

Ou :

network : est l'adresse du réseau à joindre

mask : est le masque du réseau à joindre

address : est l'adresse du prochain routeur directement connecté pour atteindre le réseau

interface : est l'interface de sortie du routeur pour atteindre le réseau

AD : distance administrative optionelle (1, par défaut)

Par exemple, à partir du routeur A, le réseau 200.150.75.0/24 est joignable par l'interface de Serial 0/0 par la passerelle (prochaine adresse IP) 192.168.1.2 :

RA(config)#ip route 200.150.75.0 255.255.255.0 serial 0/0

Ou

RA(config)#ip route 200.150.75.0 255.255.255.0 192.168.1.2

On peut vérifier le routage statique dans la configuration courante du routeur via la commande #show running-config .

Notons qu'une route a toujours une métrique de 0. Le réseau à joindre est censé être directement connecté.

4. Les protocoles de routages :

La convergence est le temps pour qu'un ensemble de routeurs puissent avoir une vision homogène, complète et efficace de l'ensemble des routes d'un inter-réseau. Le temps de convergence est particulièrement éprouvé lorsqu'il y a des modifications topologiques dans l'inter-réseau.

4.1. Système autonome, routage intérieur et extérieur :

Un **système autonome (AS)** est un ensemble de réseaux sous la même autorité administrative (autorité de gestion). Au sein d'un système autonome, les routes sont générées par des **protocoles de routage intérieurs** comme RIP, IGRP, EIGRP, OSPF ou ISIS. Les protocoles de routage qui permettent de connecter les systèmes autonomes entre eux, sont des **protocoles de routage extérieurs** comme EGP ou BGP. Dans le contexte de l'interconnexion mondiale des réseaux, l'IANA assigne un numéro d'AS (16 bits). Un AS peut éventuellement être découpé en zones (*areas*) selon le protocole de routage (OSPF et ISIS).

4.2. Protocole de routage à vecteur de distance, à état de lien et hybride :

Sans entrer dans les détails, nous allons définir les notions de protocole de routage à vecteur de distance, à état de lien et hybride.

- **Un protocole de routage à vecteur de distance** est celui qui utilise un algorithme de routage qui additionne les distances pour trouver les meilleures routes (Bellman-Ford). Souvent ils envoient la totalité de leur table de routage aux voisins. Ils sont sensibles aux boucles de routage. Dans ce type de protocole, aucun routeur ne remplit de fonction particulière. On parlera de connaissance "plate" de l'inter -réseau ou de routage non-hiérarchique. Ces protocoles convergent lentement. On citera RIP et IGRP.
- **Un protocole de routage à état de liens** utilise un algorithme plus efficace (Dijkstra ou Shortest Path First). Les routeurs collectent l'ensemble des coûts des liens et construisent de leur point de vue l'arbre de tous les chemins. Les meilleures routes sont

alors intégrées à la table de routage. On parlera de routage hiérarchique. On citera OSPF et ISIS. Ils convergent très rapidement.

- **Un protocole de routage hybride** est un protocole de routage à vecteur de distance qui reprend des concepts d'états de liens. On citera EIGRP.

5. Tableau récapitulatif des protocoles de routage intérieurs :

X	**Vecteur de distance**	**Etat de liens**	**Hybride**
TCP/IP	RIP Routing Information Protocol	OSPF Open Shortest Path First	/
Cisco	IGRP Interior Gateway Routing Protocol	/	EIGRP Ehanced Interior Gateway Routing Protocol
OSI	/	ISIS Intermediate System to Intermediate System	/

Tab.1.4. Protocole de routage intérieur.

Parmi les protocoles de routage dynamiques indiqués plus haut, on trouve le protocole OSPF (Open Shortest Path First).

VII. Le protocole de routage OSPF :

1. Introduction :

Le protocole OSPF (Open Shortest Path First) a été développé suite au besoin de la communauté Internet d'utiliser un protocole intérieur IGP (Internal Gateway Protocol) dans la pile des protocoles TCP/IP non-propriétaires et hautement fonctionnels. Les discussions sur la création d''un IGP commun et inter-opérable pour l'Internet, commença en 1988 et ne fut pas formalisé avant 1991. La prescription la plus récente est la **RFC 2328 (avril 1998 version 2)**. OSPF est un protocole de couche 3, annoncé dans le paquet IP avec le numéro de protocole 89. Il n'utilise pas TCP pour la fiabilité qu'il assure par des mécanismes propres.

2. Comparative fonctionnelle des protocoles RIP et OSPF :

La croissance rapide et l'expansion des réseaux à poussé RIP a ses limites. RIP comporte certaines restrictions qui peuvent causer des problèmes dans les réseaux larges :

- **RIP a une limite de 15 sauts**. Un réseau qui comporte plus de 15 sauts (15 routeurs) est considéré comme inaccessible.
- **RIP ne supporte pas les masques à longueur variable (VLSM : Variable Length Subnet Mask)**. Compte tenu du manque d''adresses IP et de sa flexibilité, le VLSM comporte des avantages considérables dans les plans d''adressage.
- **L'envoi périodique de l'entièreté des tables de routage en diffusion *(broadcast)* consomme une grande quantité de bande passante**. Il s'agit d'un véritable problème dans les réseaux larges et spécifiquement sur les liaisons lentes et les nuages WAN.
- **RIP converge plus lentement qu'OSPF**. Dans les très grands réseaux, la convergence doit être rapide.
- **RIP ne prend pas en compte les paramètres de délais et de coût**. Les décisions de routage sont uniquement basées sur le nombre de sauts quelque soit la bande passante ou les délais des lignes.
- **Les réseaux RIP sont des réseaux plats**. Il n'y a pas de concept d'area (zone) ou de boundarie (frontière). Avec l'introduction du routage classless et l'utilisation intelligente de l'agrégation et de la summurization des routes, les réseaux RIP ont moins de succès.

Certaines améliorations ont été introduites dans une version nouvelle de RIP, appelée RIP2. RIP2 supporte le VLSM, permet l'authentification et les mises à jour de routage multicast. Toutefois, ces améliorations restent faibles car RIP2 est encore limité par le nombre de sauts et une convergence lente qui conviennent mal aux réseaux étendus.

Voici les caractéristiques comparatives d'OSPF :

- **Il n'y a pas de limite du nombre de sauts**. OSPF étant un protocole de routage à état de lien, chaque routeur possède une connaissance complète des réseaux au sein d'une zone (*area*). Aussi, le danger de boucles de routage n'étant *a priori* plus présent, la limite du nombre de sauts n'est plus nécessaire.
- **L'utilisation intelligente du VLSM améliore les plans d'adressage** (allocations d''adresses IP). Il supporte aussi l'agrégation et la summarization de routes.
- **Il utilise IP multicast pour envoyer ses mises à jour d'état de lien**. Cette méthode prend moins de ressources aux routeurs qui n'écoutent pas les paquets OSPF. Aussi, ces mises à jour sont envoyées uniquement lors d''un changement de topologie. On économise de manière évidente la bande passante. Les mises à jour sont seulement incrémentielles.
- **OSPF a une meilleure convergence que RIP ;** parce que les changements de routage sont propagés instantanément et non périodiquement de manière incrémentielle grâce aux relations de voisinage entretenues.
- **OSPF est meilleur pour la répartition de charge** *(load balancing*).
- **Le choix du meilleur chemin est basé sur le coût (la bande passante inversée).** Cette métrique peut être définie manuellement sur les interfaces.
- **OSPF permet une définition logique des réseaux** où les routeurs peuvent être

répartis en zones (*area)*. Cela évitera une explosion de mises à jour d'états de lien sur l''ensemble du réseau. On peut également ainsi fournir un mécanisme d'agrégation des routes et stopper la propagation inutile des informations de sous-réseaux existants.

- **Il permet l'authentification de routage** par l'utilisation de différentes méthodes d'identification avec mots de passe.
- **Il permet le transfert et l'étiquetage des routes extérieures injectées dans un Système Autonome (AS)** pour permettre de les maintenir par des EGPs comme BGP.

3. Les éléments d'OSPF :

- Les routeurs OSPF entretiennent une relation orientée connexion avec les routeurs d'un même segment physique. Dans la terminologie OSPF, on parlera d'*adjacency*, en français, d'adjacence ou de contiguïté.
- Au lieu d'envoyer des mises à jour entières lors d'un changement topologique, OSPF envoie des mises à jour incrémentielles.
- OSPF n'est pas limité par une segmentation dépendante de l'adressage IP ou des sous-réseaux. il utilise la notion d'*area* pour désigner un groupe de routeurs.
- OSPF supporte entièrement les possibilités du VLSM et de la *summarization* manuelle des routes.
- Grâce à la possibilité de donner des rôles particuliers aux routeurs, la communication inter-routeurs est efficace.
- Bien qu'OSPF permette une communication *inter-area*, il reste un protocole de routage intérieur (IGP).

4. QUE SIGNIFIE LINK-STATES / ETATS DE LIENS ?

OSPF est un protocole à état de lien. Nous pouvons penser qu'un lien est l'interface d'un routeur. L'état d'un lien est une description de cette interface et de la relation qu'elle entretient avec ses routeurs voisins. Une description de cette interface pourrait comprendre, par exemple, son adresse IP, le masque, le type de réseau connecté, les routeurs connectés, etc. L'ensemble de ces états de liens forme la *link-state database*. **La *link-state database* ou, dite aussi, *topology table*, est identique sur tous les routeurs d'une zone.** [9]

4.1 Hiérarchie :

Une caractéristique principale d'OSPF est de supporter des inter-réseaux très larges. Elle est possible grâce au regroupement des routeurs dans des entités logiques appelées area ou zone.

La communication inter-zones ne laisse passer l'échange d'informations minimales de routage, uniquement pour que les zones restent connectées. Il en résulte que tous les efforts de calcul de routes ne s'opèrent qu'au sein d'une même zone. Les routeurs d'une zone ne sont pas affectés par les changements intervenus dans une autre zone. Dans un contexte où OSPF demande beaucoup de ressources en CPU et en mémoire, cette notion de conception est très importante. [9]

Un routeur OSPF peut prendre en charge trois types d'opérations :

- Opération dans une zone.
- Connexion inter-zone.
- Connexion entre systèmes autonomes (AS).

Comme cité plus haut, pour remplir ces tâches, un routeur doit remplir un rôle et une responsabilité particulière qui dépend de l'hiérarchie OSPF établie. [9]

- **Internal Router (IR)** – Un IR remplit des fonctions au sein d'une zone uniquement. Sa fonction primordiale est d'entretenir à jour sa base de données avec tous les réseaux de sa zone et sa base de données d'états de lien (link-state database), qui est identique sur chaque IR. Il renvoie toute information aux autres routeurs de sa zone. Le routage ou l'inondation (flooding) des autres zones requiert l'intervention d'un Area Border Router (ABR). [9]

- **Backbone Router (BR)** – Une des règles de conception OSPF est que chaque zone dans l'inter-réseau doit être connectée à une seule zone, la zone 0 ou la backbone area. La plupart des BR ont une interface connectée à la backbone area et une ou plusieurs interfaces à d''autres zones. [9]

- **Area Border Router (ABR)** – Un ABR connecte deux ou plusieurs zones. Un ABR possède autant de bases de données d'états de lien qu'il y a d''interfaces connectées à des zones différentes. Chacune des ces bases de données contiennent la topologie entière de la zone connectée, peut donc être summarizée ; c'est-à-dire agrégée en une seule route IP. Ces informations peuvent être transmises à la zone de backbone pour la distribution. Un élément clé, est qu'un ABR est l'endroit où l'agrégation doit être configurée pour réduire la taille des mises à jour de routage, qui doivent être envoyées ailleurs. Donc quand on parle des capacités d'OSPF de minimiser les mises à jour de routage, on peut directement penser au rôle rempli par les ABR. [9]

- **Autonomous System Boundary Router (ASBR)** – Il faut bien retenir qu'OSPF est un IGP (Interior Gateway Protocol), autrement dit qu'il devra être connecté au reste de l''Internet par d''autres AS. Ce type de routeur fera en quelque sorte office de passerelle vers un ou plusieurs AS. L'échange d'information entre un AS OSPF et d'autres AS, est le rôle d'un ASBR et les informations qu'il reçoit de l'extérieur seront redistribuées au sein de l''AS OSPF. [9]

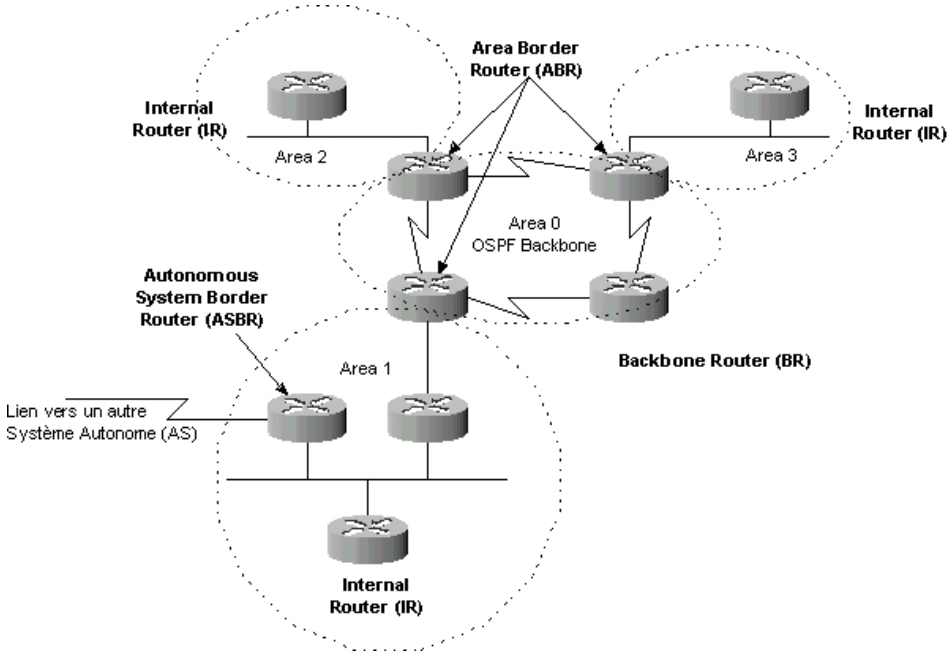


Fig.1.5. Le fonctionnement d'OSPF dans une zone

Cette section traite du fonctionnement d'OSPF au sein d'une seule zone et de la manière dont la topology table ou la link-state database est construite. La table de routage est constituée à partir de cette base de données. Ce résultat est obtenu grâce à l'application de l'algorithme de routage SPF. En voici les différentes étapes : [9]

a. D'abord, un routeur doit trouver ses voisins. Pour ce faire, il utilise des paquets Hello. Dès son initialisation ou à la suite d'un changement de routage, un routeur va générer un link-state advertisement (LSA). Cette annonce représentera la collection de tous les états de liens de voisinage du routeur.

b. Tous les routeurs vont s'échanger ces états de liens par inondation (flooding). Chaque routeur qui reçoit des mises à jour d'état de lien (link-state update), en gardera une copie dans sa link-state database et propagera la mise à jour auprès des autres routeurs.

c. Après que la base de données de chaque routeur soit complétée, le routeur va calculer l'arbre du chemin le plus court (Shortest Path Tree) vers toutes les destinations avec l'algorithme Dijkstra. Il construira alors la table de routage (routing table), appelée aussi forwarding database, en choisissant les meilleures routes.

d. S'il n'y a pas de modification topologique, OSPF sera très discret. Par contre en cas de changement, il y aura échange d'informations par des paquets d'état de lien et l'algorithme Dijkstra recalculera les chemins les plus courts.

5. Notions de DR et BDR :

Dans un réseau multi-accès, beaucoup de routeurs peuvent être connectés. Si chaque routeur doit établir une adjacence complète (*Full Adjacency*) avec tous les autres routeurs et échanger des informations à état de lien avec chaque voisin, les machines pourraient subir des surcharges. S'il y a 5 routeurs, 10 relations d''adjacence seront nécessaires et 10 états de lien envoyés. S'il y a 10 routeurs, 45 adjacences seront nécessaires. En général, pour *n* routeurs, *n*(n-1)/2* adjacences seront formées.

La solution à cette surcharge est l'organisation de l'élection d'un routeur désigné (*designated router*, DR). Ce routeur devient adjacent à tous les autres routeurs dans un segment de broadcast. Tous les autres routeurs sur le même segment envoient leurs informations d'état de lien au DR. Le DR agit comme porte-parole pour le segment. En utilisant les exemples chiffrés exposés ci-avant, seulement 5 et 10 ensembles de *link-state* seront envoyés. Le DR se chargera de renvoyer les informations d'état de lien à tous les autres routeurs du segment avec l'adresse multicast 224.0.0.5.

Malgré tout le bénéfice en efficacité de cette procédure d'élection, il y a un désavantage : le DR sera un point unique de rupture. Un second routeur est aussi élu comme routeur désigné de sauvegarde (*backup designated routeur*, BDR). Pour être sûr que les DR et BDR voient l'état de lien de tous les routeurs sur le segment, l'adresse multicast 224.0.0.6 est utilisée pour tous les routeurs désignés (DR). Les autres routeurs qui ne sont ni DR ni BDR sont appelés DROTHER et s'arrêtent à l'état *Two Way*, sans échange d'informations de routage.

Sur un réseau point-à-point, seuls deux points existent. **Il n''y a pas d''élection de DR ou BDR**. Chaque routeur devient entièrement adjacent avec l'autre. [9]

6. Les états OSPF pour la construction des adjacences :

Avant de s''échanger des informations de routage, les routeurs OSPF établissent des relations ou des états avec leurs voisins afin de partager efficacement les informations d'états de lien.

Les protocoles à vecteur de distance, comme RIP, utilisent aveuglément le broadcast ou le multicast en envoyant par chaque interface leur table de routage complète toutes les 30 secondes (par défaut). A contrario, les routeurs OSPF comptent 5 différents types de paquets pour identifier les voisins et mettre à jour les informations de routage à état de lien.

Type de paquet OSPF	Description
Type 1 – Hello	Etablit et maintient les informations de contiguïté (*adjacency information*) avec les voisins.
Type 2 – Database Description packet (DBD)	Décrit le contenu des bases de données d'état de liens (*link-state database*) des routeurs OSPF.
Type 3 – Link-state request (LSR)	Demande des éléments spécifiques des bases de données d'état de liens (*link-state database*) des routeurs OSPF.
Type 4 – Link-state update (LSU)	Transporte *les link-sate advertisements*, les LSA, aux routeurs voisins.
Type 5 – Link-state acknowledgment (LSAck)	Accusés de réception des LSA des voisins.

Tab.1.5. Type de paquet OSPF

Ces cinq types de paquets font en sorte qu'OSPF soit capable de communications complexes et sophistiquées. Les interfaces OSPF peuvent rencontrer sept états et correspondent à deux moments : d'une part, la découverte des voisins et d'autre part, la découverte des routes. En voici brièvement le descriptif : [9]

6.1 découverte des voisins :

Les trois premières étapes visent à découvrir le voisin :

a. Down State :

Dans cet état, il n'y a pas d'échange d'informations entre les voisins. OSPF attend le prochain état qui est l'*Init State.*

b. Init State :

Les routeurs OSPF envoient des paquets Type 1 (*Hello*) à des intervalles réguliers (d''habitude 10 secondes) pour établir une relation avec les routeurs voisins. Quand une interface reçoit le premier paquet Hello, le routeur entre en *Init State*, ce qui signifie que le routeur sait qu'il y a un voisin en face et il attend d'entrer en relation avec lui dans la prochaine étape.
Il y a deux catégories de relations : *Two-Way* et *Full Adjacency*. Un routeur doit de toute façon recevoir un Hello d'un voisin avant d'établir une relation.

c. Two-Way State :

Utilisant des paquets Hello, chaque routeur OSPF tente d'établir un *Two-Way State* ou une communication bidirectionnelle avec chaque voisin qui est dans le même réseau IP. En d'autres termes, les paquets Hello incluent la liste des voisins OSPF connus de l'envoyeur. Un routeur entre en *Two-Way State* quand il se voit dans le Hello d'un voisin.

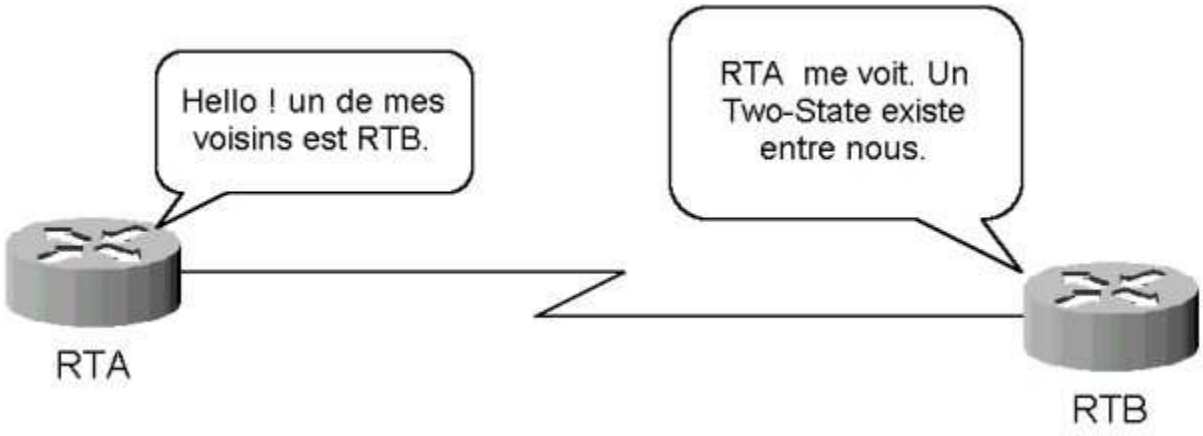


Fig.1.6. Etape Two-Way State

Le *Two-Way State* est la relation la plus basique qu'un voisin OSPF peut établir. Mais dans cette relation aucune information de routage n'est partagée. Pour apprendre l'état des liens des autres routeurs et construire une table de routage, chaque routeur doit former une contiguïté entière (*adjacency*). Une *adjacency* est une relation avancée entre des routeurs OSPF qui implique une série d'états progressifs qui ne comptent pas seulement des paquets Hello, mais aussi les quatre autres types de paquets. Les routeurs qui tentent de devenir contigus ou *adjacents* avec un autre, échangent des informations de routage avant que toute *adjacency* soit entièrement établie. La première étape est le *ExStart State*.

5.2 Découverte des routes :

Toute interface OSPF "non problématique" est au moins en état "Two Way". Selon les circonstances, elles pourront atteindre l'état "Full Adjacency" en passant par d'autres étapes intermédiaires. Les connaître est très utile pour le diagnostic. [9]

a) ExStart State :

Techniquement, quand un routeur entre en Exstart State, la conversation est caractérisée par une contiguïté (*adjacency*) mais les routeurs ne sont pas encore entièrement adjacents. **L**'*ExStart* est établi en utilisant des paquets de Type 2 database description (DBD). Les deux routeurs voisins utilisent ces paquets pour négocier qui sera le « maître » et qui sera l''« esclave » dans la relation.

Le routeur avec la plus haute OSPF ID « gagnera » et deviendra « maître ». Quand ces rôles de « maître » et « esclave » sont définis, l''état *Exchange* intervient et l'envoi d'informations de routage peut commencer.

b) Exchange State :

Dans cet état, les routeurs voisins utiliseront des *Type 2 DBD packets* pour s'envoyer l'un à l'autre des informations. En d'autres mots, Les routeurs décrivent leur *link-state database* aux autres. Les routeurs comparent ce qu'ils apprennent avec ce qu'ils connaissent déjà de leur *link-state database*. S'ils apprennent des informations sur des liens qu'ils ne possèdent pas, ils demandent une mise à jour complète à leurs voisins. Les informations de routage complètes sont échangées dans le *Loading State*.

c) Loading State :

Après que la base de données ait été décrite à chaque routeur, ils peuvent demander des informations plus complètes en utilisant des *Type 3 packets*, appelés *link-state requests* (LSRs). Quand un routeur reçoit un LSR, il répond avec une mise à jour en utilisant un *Type 4 link-state update* (LSU) *packet*. Ces paquets Type 4 LSU contiennent les *link-sate advertisements* (LSAs) qui sont le cœur du protocole de routage à état de lien. Les LSU sont accusés de réception par des LSAcks, *link-state acknowledgments*.

d) Full Adjacency :

Lorsque le Loading State est complet, les routeurs sont entièrement *adjacents*. Chaque routeur garde une liste de ses routeurs voisins appelée *adjacency database*. Elle ne doit pas être confondue avec la *link-state database* ou la *forwarding database*.

7. Topologies OSPF :

Une relation de voisinage est nécessaire pour que les routeurs OSPF partagent des informations de routage. Un routeur va tenter de devenir adjacent (contigu) avec au minimum un autre routeur d'un réseau IP auquel il est connecté. Certains routeurs essaient de devenir adjacents à chaque routeur voisin. D'autres essaient d'être adjacents à seulement un ou deux routeurs. Tout ceci est déterminé par le type de réseau auquel ils sont connectés. Lorsqu'une adjacence est formée entre deux voisins, les informations à état de lien sont alors échangées. [9]

Topologie	Caractéristiques	Election DR
Broadcast Multiacces	Ethernet, FDDI, Token Ring	Oui
NBMA (Non Broadcast MA)	Frame Relay, X.25, SMDS	Oui
Point-to-Point	PPP, HDLC	Non
Circuit à la demande	Configuré par un administrateur	Non

Tab.1.6. Topologie OSPF

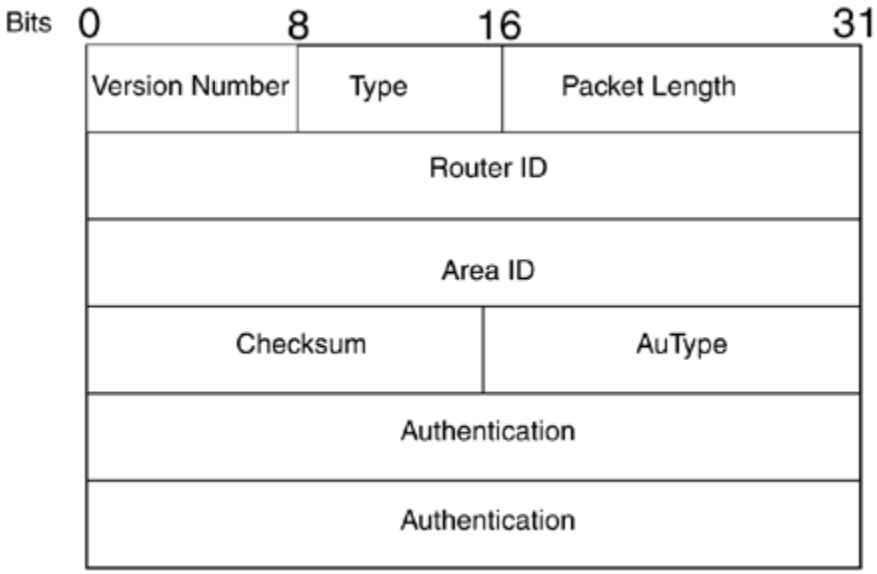
Les interfaces OSPF reconnaissent automatiquement deux types de réseaux :

- Broadcast multi-access, comme Ethernet
- Point-to-point networks

Contrairement aux réseaux NBMA et Circuits à la demande, il n'y a pas besoin de les configurer. [9]

1. Vue d'ensemble du protocole OSPF« HELLO » :

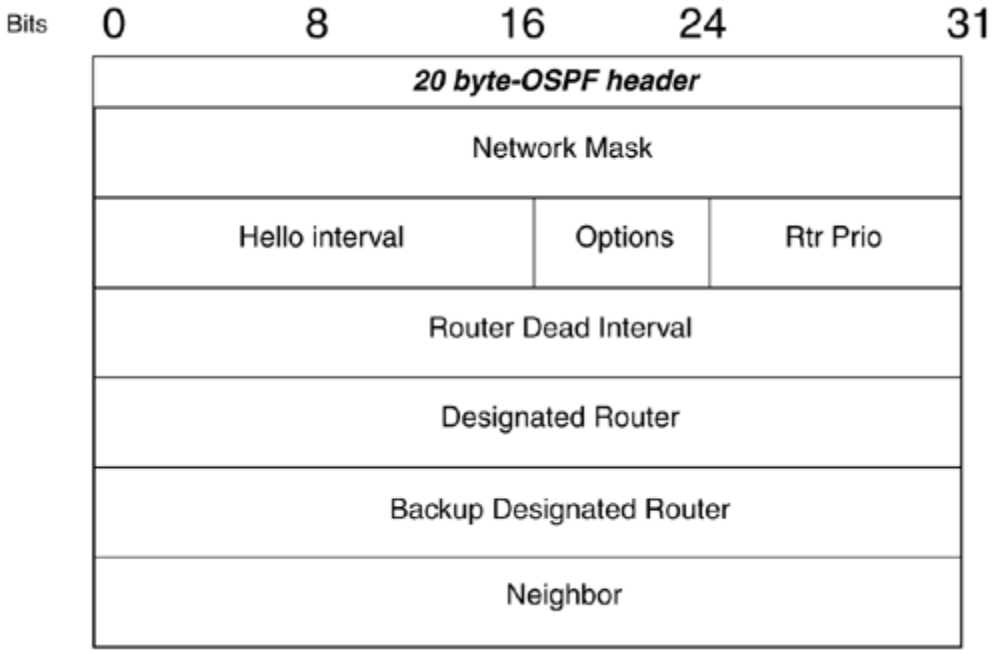
Quand un routeur commence un processus de routage OSPF sur une interface, il envoie un paquet Hello et continue à envoyer ces paquets à intervalles réguliers. La règle qui gouverne l'échange des paquets Hello OSPF est appelée le protocole Hello.
A la couche 3 du modèle OSI, les paquets *Hello* sont adressés en multicast 224.0.0.5. Cette adresse est « tous les routeurs OSPF ». Les routeurs OSPF utilisent ces paquets *Hello* afin d'initier de nouvelles adjacences et pour s'assurer que les routeurs voisins sont fonctionnels. Les paquets *Hello* sont envoyés toutes les 10 secondes par défaut sur un réseau multi-accès et point-à-point et toutes les 30 secondes sur un NBMA.
Dans un réseau multi-accès, le protocole *Hello* élit un DR et un BDR.
Bien qu'un paquet Hello soit petit (moins de 50 Bytes), il est en fait l'entête d'un paquet OSPF qui prend la valeur de 1 dans le champ type.



Remarquons ici particulièrement le champ Router ID dont nous avons parlé plus haut et dont nous reparlerons encore. Ce champ est utilisé pour identifier de manière unique un routeur OSPF. Il prendra la valeur de la plus haute adresse IP du routeur (32 bits). Puisqu'une adresse IP est censée être unique dans un réseau, elle convient bien pour remplir ce champ. Aussi, parce qu'un routeur supporte de multiples adresses IP assignées

pour l'interconnexion des réseaux, on utilisera volontiers l'adresse IP d'interfaces de *loopback* (virtuelles) qui ne participeront pas nécessairement au routage. Leur avantage est aussi dans le fait que ces interfaces ne tombent jamais (en fonction d'une dépendance à un lien physique). Notons enfin que les IOS Cisco prendront toujours en compte l'IP de l'interface de *loopback* quand bien même des interfaces physiques auraient une IP plus élevée. Par contre, en absence d'interface de *loopback*, sur du matériel Cisco, l'IP la plus élevée d''une interface physique sera prise.

Un Paquet *Hello* transporte des informations que tous les voisins doivent agréer avant qu'une adjacence soit formée et avant que les informations d'état de lien soient échangées.



Notons le champ « Rtr Prio », « Router Priority » qui intervient dans la désignation des rôles entre routeurs OSPF.

2. Opérations OSPF :

Il est maintenant nécessaire de reprendre l'ensemble des concepts vu dans les sections précédentes et d'envisager globalement les opérations de fonctionnement OSPF au sein d'une zone configurée.

Etape 1 : Etablir l'adjacence des routeurs.

Cette étape correspond à un des 7 états décrits dans la section 5, ***Les états OSPF*.** Dans des conditions de configuration correcte, les routeurs iront au moins jusqu'au *Two-Way State*. Si la liaison est point-à-point, les routeurs voisins deviendront adjacents. Dans le cas d'un réseau multi-accès, les routeurs vont entrer dans un processus d'élection pour devenir DR, BDR ou aucun des deux (DROTHER).

Si une élection est nécessaire, autrement dit si les interfaces partagent un réseau-multi accès, les routeurs entrent dans l''étape 2 : Election d'un DR et d'un BDR. Sinon, les routeurs entrent dans l'état *ExStart* (cf. section 5.A) décrit dans l''étape 3 : Découverte des routes.

Etape 2 : Election d'un DR et d'un BDR.

Parce que les réseaux multi-accès peuvent comporter plus de deux routeurs, OSPF élit un DR pour être le point central des mises à jour *link-state*. Le rôle du DR est critique. Pour cette raison, un BDR est élu comme remplaçant immédiat du DR. Cette élection est fonction d'un type de réseau (une interface LAN dans un réseau multi-accès). Cela signifie qu'un routeur qui a trois interfaces LAN OSPF pourrait prendre trois rôles OSPF à la fois

Le processus électoral du DR ou du BDR peut être truqué … Ainsi, les paquets *Hello* contiennent un champ « *Router Priority* » (8 bits) qui pourra déterminer une élection. Le routeur avec la plus haute priorité par rapport à ses routeurs voisins gagnera l'élection DR. Le second avec la plus haute priorité gagnera l'élection BDR. Une fois que l'élection est terminée, les rôles sont déterminés jusqu'au moment où l'un est en panne, même si de nouveaux routeurs s'ajoutent au réseau avec une plus haute priorité. Les paquets *Hello* informent les nouveaux venus de l'existence et de l'identification des DR et BDR.

Par défaut, tous les routeurs OSPF ont la même priorité d'une valeur de 1. Une priorité prendra une valeur de 8 bits, de 0 à 255. Elle est assignée sur une interface, le cas échéant, manuellement. Une priorité de 0 assurera un routeur qu'il ne gagnera pas une élection sur une interface tandis qu'une priorité de 255 assurera sa victoire. Le champ « Router ID » est utilisé pour départager des routeurs qui auraient éventuellement la même priorité. On a vu plus haut que ce champ prendra la valeur de l'adresse IP la plus élevée sur le routeur, avec sur les IOS Cisco, une préférence absolue pour les interfaces de *loopback*.

Quand une élection est finie et qu'une communication bidirectionnelle est établie, les routeurs sont prêts à échanger des informations de routage avec les routeurs adjacents et à construire leur base de données de liens.

Etape 3 : Découverte des routes.

Les routeurs sont maintenant prêts à s'engager dans le processus *Exchange* décrit plus haut. Dans l'état *ExStart*, les routeurs détermineront qui commence à envoyer les informations. Ici, le principe est d'établir une relation Maître/Esclave entre deux routeurs. Le routeur qui déclare la plus haute ID (la priorité n'intervient plus) commencera et orchestrera l'échange en tant que maître.

Une fois que ces rôles sont établis, les routeurs entrent dans l'état *Exchange* à proprement dit. Le maître mène l'esclave à un échange de paquets *Database Description* (DBDs) qui décrivent la base de données de liens de chaque routeur dans les détails. Ces descriptions comportent le type d'état de lien, l'adresse du routeur qui fait la publicité, le coût du lien et un numéro de séquence.

Les routeurs confirment la réception des DBDs en envoyant des paquets LSAck (Type 5), qui contiennent une correspondance aux numéros de séquences envoyés dans les DBDs. Chacun compare les informations qu'il reçoit avec ce qu'il sait déjà. Si des DBDs annoncent des nouveaux états de lien ou des mises à jour d'état de lien, le routeur qui les reçoit entre alors en état *Loading* et envoie des paquets LSR (Type 3) à propos des nouvelles informations. En réponse aux paquets LSR, l'autre enverra des informations complètes d'état de lien des paquets LSUs (Type 4). En fait, les LSUs transportent des LSAs.

Quand l'état *Loading* est terminé, les routeurs entrent en *Full Adjacency*. Il faudra qu'ils entrent dans cet état d'adjacence totale avant de créer leur table de routage et de router le trafic. A ce moment, les routeurs d'une même zone ont une base de données d'état de lien identique.

Etape 4 : Sélection des bonnes routes appropriées.

Après qu'un routeur ait complété *sa link-state database*, il peut créer sa table de routage et commencer à transférer le trafic. Comme mentionné plus haut, OSPF utilise comme métrique le coût (*Cost*) pour déterminer le meilleur chemin vers une destination. La valeur par défaut du coût dépend de la valeur de la bande passante d'un lien. En général, plus la bande passante diminue, plus le coût est élevé. Voici les valeurs par défaut du coût par rapport au type de média sur les IOS Cisco :

Medium	Coût
Ligne série 56kbps	1785
T1 (ligne série 1544kbps)	64
E1 (ligne série 2048kbps)	48
Token Ring 4 Mbps	25
Ethernet	10
Token Ring 16Mbps	6
Fast Ethernet 100Mbps, FDDI	1

Tab.1.7. les valeurs par défaut du coût/ type de média sur les IOS Cisco

Où la formule est : 10^8 / bandwidth = 100 000 000 /bandwidth

Pour calculer le coût le plus faible vers une destination, le routeur exécutera l'algorithme SPF. Pour simplifier, l'algorithme SPF fait la somme des coûts à partir de lui-même (*root*) vers tous les réseaux de destination. S'il y a plusieurs chemins possibles vers une destination, celle qui a le coût le plus faible est choisi. Par défaut, OSPF inscrit quatre routes équivalentes dans sa table de routage pour permettre la répartition de charge (*Load Balancing*).

Il arrive que certaines lignes, comme des lignes sérielles, montent ou descendent rapidement (*flapping*). Le *flapping* provoquera l'envoi de LSUs qui pousseront les routeurs destinataires à ré-exécuter l'algorithme SPF pour recalculer les routes. Le*flapping* prolongé peut toucher sévèrement les performances des machines. Les calculs SPF répétés prendront beaucoup de ressources en CPU. Aussi, elles pourraient empêcher la base de données de lien de converger.

Pour combattre ce problème, l'IOS Cisco utilise un compteur de retenue SPF (*SPF hold timer*). Après avoir reçu un paquet LSU, le compteur ne commencera le calcul SPF qu'après un certain laps de temps. La commande *timers spf* active l'ajustement de ce temps qui est de 10 secondes par défaut.

Etape 5 : Maintien des informations de routage.

Quand un routeur a installé ses routes dans la table de routage, il doit maintenir minutieusement ses informations de routage. Lorsqu'il y a changement d'un état de lien, les routeurs OSPF utilisent un processus d'inondation (*flooding*) pour avertir les autres routeurs. L'intervalle de mort (*dead interval*) du protocole *Hello* fournit un mécanisme simple pour déclarer un lien rompu. Quand une interface n'a plus de nouvelles d'un lien après cette période (habituellement 40 secondes), le lien est réputé *down*. (au sens OSPF cf. flooding)

Le routeur qui a constaté le lien down envoie un LSU avec les nouvelles informations d'état de lien. Oui, mais à qui ?

- Sur un réseau point-à-point, il n'y ni DR ni BDR. Les nouvelles informations d'état de lien sont envoyées sur l'adresse Multicast 224.0.0.5. Tous les routeurs OSPF écoutent à cette adresse.
- Sur un réseau multi-accès, un DR et un BDR existent et maintiennent les adjacences avec tous les autres routeurs du réseau. Si un DR ou un BDR a besoin d'envoyer une mise à jour d'état de lien, il le fera à destination de l'adresse 224.0.0.5. Quoi qu'il en soit, les autres routeurs du réseau sont adjacents uniquement au DR ou au BDR et n'envoient des LSUs qu'à ceux-ci. C'est pour cette raison que les DR et BDR ont leur propre adresse de destination multicast 224.0.0.6. Les routeurs qui ne sont pas DR/BDR envoient leurs LSUs sur 224.0.0.6, autrement dit, « tous les routeurs DR/BDR ».

Quand un DR reçoit et accuse réception d'un LSU destiné à 224.0.0.6, il inonde de LSU tous les autres routeurs du réseau sur 224.0.0.5. Chaque routeur accusera réception du LSU avec un LSAck.

Si un routeur OSPF est connecté à un autre réseau, il inonde de LSU les autres réseaux en transférant le LSU au DR d'un réseau multi-accès ou au routeur adjacent sur un réseau P2P. Le DR, à son tour, « multicaste » le LSU à ses routeurs non DR/BDR de son propre réseau …

Dès qu'un routeur reçoit un LSU, il met à jour sa *link-state database* et met en œuvre l'algorithme SPF pour calculer les nouvelles routes à inscrire dans sa table de routage. Après l'expiration du compteur SPF, la route est inscrite dans la table de routage.

Sur les routeurs Cisco, une vieille route est toujours utilisée pendant que l'algorithme SPF calcule la nouvelle route et jusqu'au moment où le calcul sera terminé.

Il est important de remarquer que même si aucun changement topologique n'intervient, les informations de routage OSPF sont régulièrement rafraîchies. Chaque entrée LSA a sa propre durée de vie. Le compteur a une durée par défaut de 30 minutes. Après que sa durée de vie soit écoulée, le routeur à l'origine de cette information renvoie un LSU au réseau pour vérifier que le lien est toujours actif.

VIII. CONCLUSION :

Dans ce chapitre on a pu voir que le TCP/IP est devenu un standard aussi bien au niveau des réseaux locaux que des réseaux étendus. De ce fait, il est très important de comprendre les mécanismes et les protocoles avec les différentes couches du modèles OSI.

Le Modèle TCP/IP correspond à une simplification du modèles OSI plus pragmatique et représentatif des technologies existantes.

Les technologies passerelles permettent aux réseaux non IP d'assurer la transmission de données IP (IP sur PDH par exemple).

CHAPITRE II

I. Introduction :

GSM (Global System for Mobile communication) très largement utilisé est la première norme de téléphonie cellulaire qui soit pleinement numérique. C'est la référence mondiale pour les systèmes radio mobile. Le réseau GSM offre à ses abonnés des services qui permettent la communication de stations mobiles de bout en bout à travers le réseau. La téléphonie est la plus importante des services offerts. Ce réseau permet la communication entre deux postes mobiles où entre un poste mobile et un poste fixe. Les autres services proposés sont la transmission de données à faibles débits et l transmission de messages alpha numériques courts.

Ce chapitre présente les caractéristiques essentielles du système, ainsi que son architecture générale, son interface radio qui constituait à l'époque de sa création l'une de ses principales innovations, et les protocoles mis en œuvre.

II. Architecture du réseau GSM :

Un réseau GSM a pour premier rôle de permettre des communications entre abonnés mobiles et des abonnés du réseau téléphonique commuté (RTC), il s'interface avec le RTC et comprend des commutateurs. Il est caractérisé par un accès très spécifique : La liaison radio.

Enfin, comme tout réseau il doit offrir à l'opérateur des facilités d'exploitation et de maintenance [15]. L'architecture d'un réseau GSM peut être divisée en *trois* sous-systèmes :

1. Le sous-système radio contenant la station mobile, la station de base et son contrôleur.

2. Le sous-système réseau ou d'acheminement.

3. Le sous-système opérationnel ou d'exploitation et de maintenance.

Les éléments de l'architecture d'un réseau GSM sont repris sur le schéma de la figure 2.1.

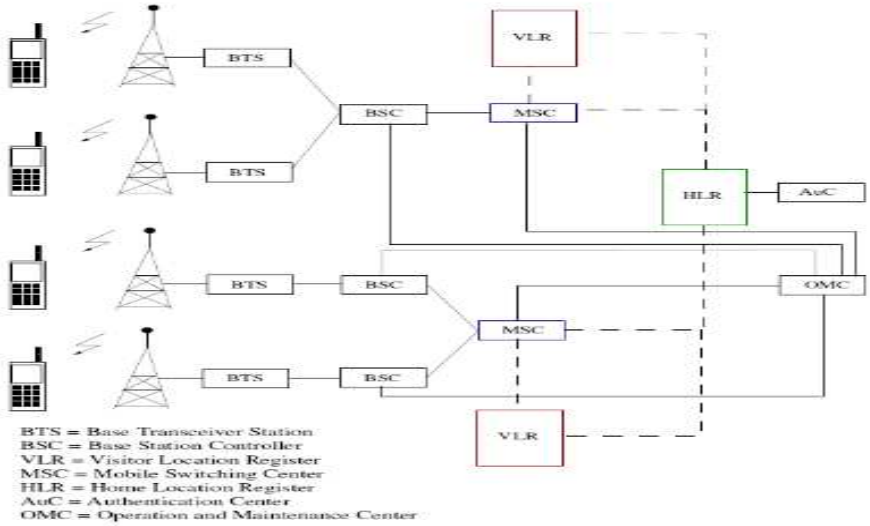


Fig.2.1. Architecture du réseau GSM.

III. Fonctions d'un système GSM :

Les fonctions que doit remplir un réseau GSM comprennent non seulement la transmission des données mais également l'enregistrement, l'authentification, le routage et la mise à jour de la localisation. Ces fonctions sont réalisées par le sous- système réseau en utilisant le protocole (MAP).

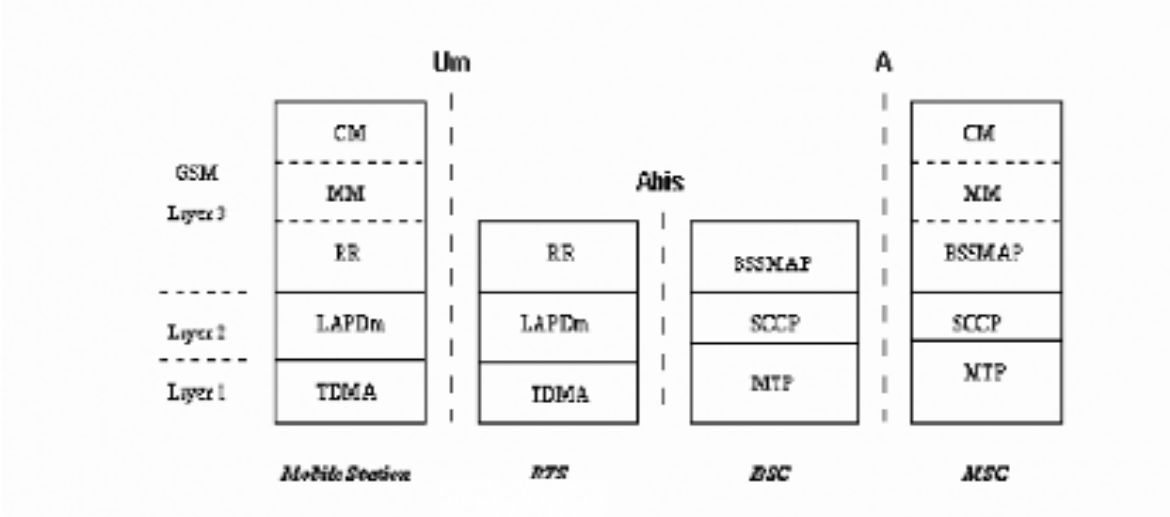


Fig.2.2. Fonctions du système GSM.

1. Le sous-système radio (BSS) :

Le sous-système radio (BBS Base Station Sub-system) gère la transmission radio. Il est constitué de plusieurs entités dont :

a. Le mobile (MS) :

Le téléphone et la carte SIM (Subcriber Identity Module) les deux seuls éléments que l'utilisateur a directement accès. Ces deux éléments suffisent à réaliser l'ensemble des fonctionnalités nécessaires à la transmission et à la gestion des déplacements.

b. La station de base BTS (Base Transceiver Station) :

La BTS est un ensemble d'émetteurs-récepteurs appelés TRX(Transceiver). Elle a la charge de la transmission radio : modulation, démodulation, égalisation, codage, correcteur d'erreur, pilotant une ou plusieurs cellules. Elle permet le dialogue avec le mobile sur l'interface Air (aussi appelée interface Radio ou interface Um), elle dialogue également avec son BSC grâce à l'interface A-Bis. Cette liaison est une liaison MIC (Modulation par Impulsions Codées) à 2 Mb/s réalisée sur ligne cuivre classique, parfois sur faisceaux hertziens (2, 4 ou 8 Mb/s).

La Capacité maximale d'une BTS est typiquement de 12 porteuses, en zone urbaine une BTS à 4 porteuses peut écouler environ 28 communications simultanées [15].

Fig.2.4. Station de Base BTS.

c. Le contrôleur de station de base BSC (Base Station Controller) :

Le contrôleur de station de base gère une ou plusieurs stations de base BTS et communique avec elles par le biais de l'interface A-bis. Ce contrôleur remplit différentes fonctions tant au niveau communication qu'au niveau exploitation.

Il remplit à la fois le rôle de relais pour les différents signaux d'alarme destinés au centre d'exploitation et de maintenance et de banque de données des données installées sur les stations base.

En effet, le contrôleur gère les transferts intercellulaires des utilisateurs dans sa zone de couverture, c'est-à-dire quand une station mobile passe d'une cellule à une autre. Il doit communiquer avec les stations de base qui va prendre en charge l'abonné et lui communiquer les informations nécessaires tout en avertissant la base de données locale VLR (Visitor Location Register) de nouvelle localisation de l'abonné [15].

Il assure le contrôle d'une ou de plusieurs BTS. Il gère la ressource radio, exploite les mesures effectuées par la BTS pour contrôler les puissances d'émission du mobile et/ou de la BTS**.** La plupart des fonctions intelligentes du BSS sont implantées à son niveau, notamment les fonctions de gestion des ressources radioélectriques tels que :

- L'allocation des canaux
- La gestion de la configuration des canaux.
- Le traitement des mesures et la décision de handovers intra BSC.

Le BSC est relié au NSS par le biais de l'interface A. c'est une liaison à grand débit (32Mb/s) sur fibre optique, elle est acheminée via le réseau public. Le BSS est relié au serveur de l'OMC-R par l'Interface REM. Cette liaison suivant le protocole X25, utilise habituellement une ligne cuivre classique.

d. Le sous-système réseau (NSS) :

Le sous-système réseau, appelé Network Switching Sub-system (NSS), joue un rôle essentiel dans un réseau mobile. Les éléments du NSS prennent en charge toutes les fonctions de contrôle et d'analyse d'information contenues dans des bases de données nécessaires à l'établissement de connexion [15]. Le NSS assure principalement les fonctions de commutation et de routage. C'est lui qui permet d'établir les communications entre mobile d'un même PLMN ou de PLMN différent et entre mobile et PSTN. En plus des fonctions indispensables de commutation, on y retrouve les fonctions de gestion de la mobilité, de la sécurité et de la confidentialité qui sont implantées dans la norme GSM.

Le NSS est constitué de :

1) Le centre de communication mobile (MSC) :

Le centre de communication mobile MSC (Mobile Switching Center) a pour rôle principal d'assure la communication entre les abonnés du réseau mobile, et entre le réseau mobile et le réseau commuté public (RTC) ou autre réseau.

De plus, il participe a la fourniture des différents services aux abonnés tels que la téléphonie, les services supplémentaires et services de messageries.

Les commutateurs MSC d'un opérateur sont reliés entre eux pour commutation interne des informations. Des MSC servent de passerelle (Gateway Mobile Switching Center, GMSC) sont placées en périphérie du réseau d'un opérateur de manière à assurer une interopérabilité entre réseau d'opérateurs. [1]

2) L'enregistreur de localisation nominale (HLR) :

Il existe au moins un enregistreur de localisation (HLR) par réseau. Il faut le voir comme une base de données avec des informations essentielles. Plus la réponse du HLR est rapide plus le temps d'établissement de la connexion sera petit.

Le HLR contient à la fois :

- Toutes les informations relatives aux abonnés : le type d'abonnement, la clé d'authentification Ki cette clé est comme d'un seul HLR et d'une seule carte SIM les services souscris, le numéro de l'abonné (IMSI) etc.
- Ainsi qu'un certain nombre de données dynamiques telles que la position de l'abonné dans le réseau, son VLR et l'état de don terminal (allumé, éteint, en communication, libre,…). [2]

3) Le centre d'authentification (AuC) :

Lorsqu'un abonné passe une communication, l'opérateur doit pouvoir s'assurer qu'il ne s'agit pas d'un usurpateur. Le centre d'authentification remplit cette fonction de protection des communications.

On distingue trois niveaux de protection :

- La carte SIM qui empêche un utilisateur non enregistré d'avoir accès au réseau.
- Le codage des communications est destiné a à empêcher l'écoute.
- La protection de l'identité de l'abonné. [2]

4) L'enregistreur de localisation des visiteurs (VLR) :

Cette base de données ne contient que des informations dynamiques liées à un MSC. Il y en a donc plusieurs dans un réseau GSM. Elle contient des données dynamiques qui lui sont transmises par le HLR avec lequel elle rentre en communication lorsqu'un abonné entre dans la zone de couverture du centre de communication mobile auquel elle est rattachée. Lorsque l'abonné quitte cette zone de couverture, ses données sont transmises à un autre VLR suivent l'abonné. [2]

5) Le centre d'exploitation et de maintenance(OSS) :

Le réseau de maintenance technique s'intéresse au fonctionnement des éléments du réseau. Il gère notamment les alarmes, les dysfonctionnements, la sécurité,…ce réseau s'appuie sur un réseau de transfert de données, totalement dissocié du réseau de communication GSM.

Il se compose d'un sous système d'exploitation de maintenance réseau OMC-N (Operating and Maintenance Center-Network) qui supervise le NSS et d'un sous-système d'exploitation et de maintenance radio OMC-R (Operating and Maintenance Center-Radio) qui supervise le BSS.

Présentation des interfaces :

Interface	Equipements	Fonction principale
Um	BTS-Mobile	Interface radio FDMA/TDMA. Cette interface est normalisée.
Abis	BTS-BSC	Supervision de la BTS. Activation, désactivation des ressources radio. Cette interface n'est pas normalisée.
A	BSC-MSC	Etablissement et libération de la communication, Allocation de ressources et gestion du Handover.
B	MSC-VLR	Echange d'information usager et mise à jour de zone de localisation. Cette interface est non normalisée car les fonctions du MSC et du VLR sont souvent intégrées dans un seul équipement.
C	GMSC-HLR	Interrogation du HLR pour joindre un abonné mobile.
D	VLR-HLR	Le VLR informe le HLR de la localisation du mobile. Le HLR fournit au VLR les informations relatives à l'abonné.
E	MSC-MSC	Gestion du Handover.
	MSC-GMSC	Transport des SMS.
F	MSC-EIR	Vérification de l'identité du terminal.
G	VLR-VLR	Gestion du changement de zone de localisation.
H	HLR-AuC	Echange des informations nécessaires au chiffrement et à l'authentification.

Tab.2.1. Les Interfaces du réseau GSM. [1]

IV. Supports de transmission :

Il y a plusieurs, on cite :

- **Les lignes spécialisées :**

Ce sont des lignes louées qui permettent la transmission de données à moyens et hauts débits (2,4 Mb/s à 140 Mb/s) en liaison point à point ou multipoints.

- **Les Faisceaux Hertziens :**

Un faisceau hertzien est un système de transmission de signaux entre deux points fixes. Il utilise comme support les ondes radioélectriques, avec des fréquences porteuses de 1GHz à 40GHz (domaine des micro-ondes), très fortement concentrées.

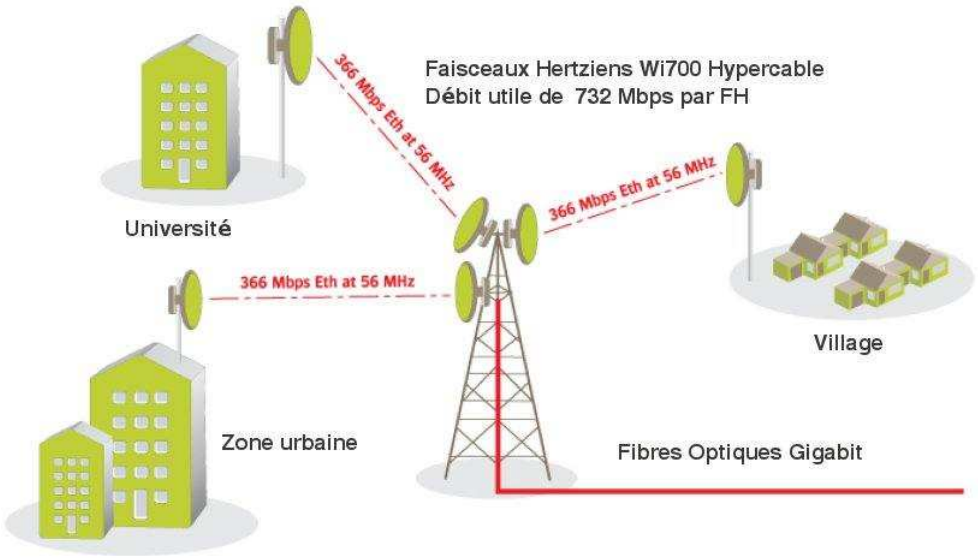


Fig.2.5. Faisceaux hertziens.

Ces ondes sont principalement sensibles au masquage (relief, végétation, bâtiments…) ; aux précipitations, aux conditions de l'atmosphère.

Elles supportent de grandes distances et de grandes capacités pour une propagation en visibilité directe (entre 50 et 80 Km). Les débits sont très élevés mais les transmissions sont sensibles aux perturbations et les possibilités d'écoute sont nombreuses.

- **Le VSAT (V**ery **S**mall **A**perture **T**erminal):

La transmission en VSAT consiste à envoyer l'information d'une BTS à une autre via un satellite.

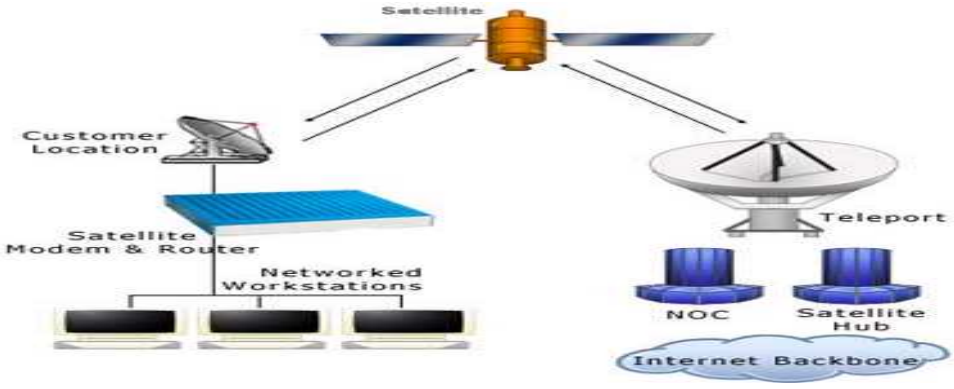


Fig.2.6. Interconnexion VSAT.

- **La fibre optique :**

La fibre optique est un support physique de transmission de données IP à très haut débit. Fin et souple comme un cheveu, un brin de fibre optique véhicule de manière guidée un signal lumineux qui a la particularité d'atteindre des vitesses élevées sur de grandes distances, en ne subissant ni affaiblissement ni perturbation électro-magnétique.

Grâce à la fibre optique, la vitesse d'une connexion Internet peut dépasser plusieurs Gigabits par seconde en émission (upload) et en réception (download). Concrètement, les débits commerciaux annoncés aujourd'hui sont de l'ordre de 100 Mbit/s mais ils sont amenés à progresser dans les années à venir.

Contrairement à la paire de cuivre et aux technologies xDSL qui subissent une atténuation importante au bout de quelques kilomètres, le signal de la fibre optique ne décline presque pas avec la distance (affaiblissement de l'ordre de 0.2 dB/km à comparer aux 15 dB/km du cuivre). **[13]**

V. Les techniques de multiplexage :

Les techniques de multiplexage consistent à fusionner plusieurs données numériques en un signal.

Les débits élémentaires sont :

- 1,5 Mbits/s (T1), pour la hiérarchie utilisée aux USA.
- 2 Mbits/s (E1) pour celle utilisée en Europe. **[3]**

1. Traitement d'une voie :

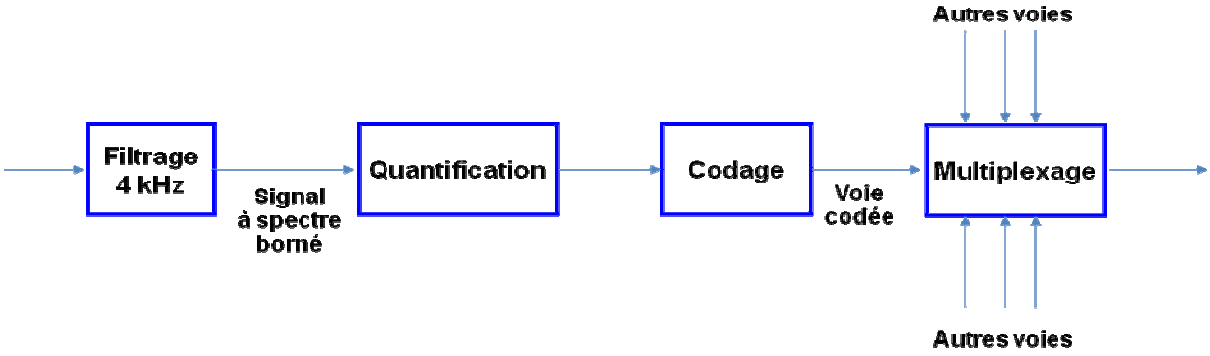


Fig.2.7. Traitement d'une voie temporelle.

- Filtrage
- Echantillonnage quantification
- Codage
- Multiplexage temporelle (TDM) : La trame MIC ou E1 est conçue pour transmettre simultanément 30 voies téléphoniques (voie de donnée à 64K bps), en utilisant les temps libre entre deux échantillonnages successifs d'une voie pour intercaler les échantillons des autres voies.
  Chaque voie dispose dans la trame d'un intervalle de temps correspond à 8 bits (en abrégé IT). Dans une trame nous avons 30 IT (ou time slot) d'information ou 30 mots de 8 bits à transmettre en 125 microsecondes.
  Finalement la trame contient 32IT (en ajoutant un IT de verrouillage de trame « VT » et un IT supplémentaire de signalisation au milieu de la trame « IT16 »). Le débit numérique est donc de 32 voies à 64 Kbps soit 2048 kbps, ce format est appelé **E_1.**

2. Le système PDH (Plesiochronous Digital Hierarchy) :

La hiérarchie numérique plésiochrone ou PDH (Plesiochronous Digital Hierarchy) est une technologie utilisée dans les réseaux de télécommunication. Le terme « plésiochrone » vient de grec plesio (proche) et chronos (temps), il reflète le fait que les réseaux PDH soit presque parfaitement synchronisé : afin de constituer des systèmes de débits plus élevés, un multiplexage temporel des trames MIC est effectué 4 par 4.

Le deuxième échelon de la hiérarchie numérique, par exemple, est constitué de 4 signaux E1 et présente un débit de 8448 Kbits/s permettant 120 voies téléphoniques. (2048*4=8192).La hiérarchie numérique plésiochrone est basée sur le signal E1, les niveaux supérieurs de la hiérarchie sont réalisés par multiplexage bit à bit de 4 signaux de niveau immédiatement inférieur. Chaque niveau supérieur est obtenu en multiplexant 4 affluents de niveau inférieur.

L'incapacité d'identifier un canal individuel dans un flot à haut débit, l'absence des moyens efficaces pour la surveillance de la qualité de transmission et la structure de la trame non dimensionnée pour transporter les informations de gestion du réseau- et des équipements sont les limitations principales de PDH. Elles peuvent être acceptables en téléphonie, mais pas dans un réseau de services. Par exemple, pour fournir une ligne à 2Mbit/s plusieurs

multiplexages et démultiplexages doivent être faits pour l'extraire d'un canal rapide à 140Mbit/s. [4]

3. Le système SDH (Synchronous Digital Hierarchy) :

SDH « Synchronous Digital Hierarchy », ce terme désigne un ensemble de protocoles reliés à l'utilisation de la fibre optique dans les réseaux. La hiérarchie numérique synchrone (SDH) est la version européenne du réseau optique synchrone (SONET) qui est un protocole d'origine américaine. La structure de multiplexage s'articule autour d'une trame de base : le signal STM-1(Synchronous Transfert Mode d'ordre 1). Cette trame a une longueur totale de 2430 octets, une fréquence de transmission de 125 µs, soit une résultante de 155,520 Mbit/s. 9octets étant réservés à la gestion et à l'adressage ; il reste une charge utile de 150,336 Mbits/s. [4]

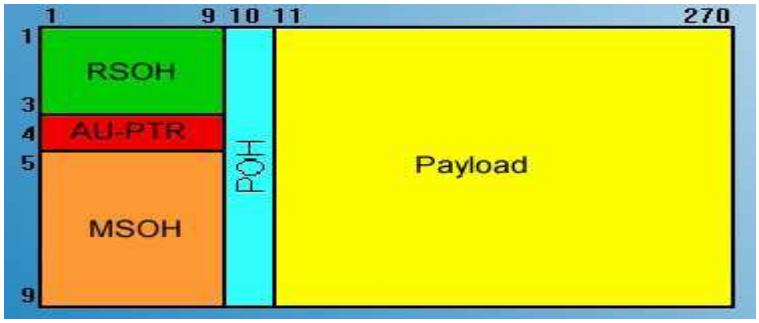


Fig.2.8. Trame de base STM1.

VI. Conclusion :

Les réseaux de type GSM sont des réseaux complètement autonomes. Ils sont interconnectables aux RTCP (Réseaux Terrestres Commutés Publics) et utilisent le format numérique pour la transmission des informations, qu'elles soient de type voix, données ou signalisation.

En finalité, il existe plusieurs technologie de transmission tel que la hiérarchie SDH et PDH sur différents supports tel que : faisceaux hertziens, fibre optique, câble coaxial… etc.

CHAPITRE III

I. Introduction :

La transmission des données désigne un transfert d'informations de type voix, image vidéo, texte... d'un point à un autre mais à travers le réseau de télécommunications. Pour qu'un réseau de téléphonie mobile soit en mesure de transmettre les données, il doit avoir un débit élevé ainsi que la largeur de bande passante élevée capable de prendre en charge toutes les applications mobiles. Telles que les appels, envoie des messages… etc. En effet l'optimisation du réseau de transmission consiste à contrôler les différents équipements utilisés par le système de gestion afin de détecter les intrusions, le statut du trafic et la performance de l'information.

Un réseau DCN bien conçu assure la fiabilité, la performance ainsi que la mise à jour de l'état du réseau.

II. Equipements de transmission SDH et PDH utilisés par WTA :

On s'intéresse aux équipements SDH et PDH de **WTA** qui se trouvent en interface Abis et Ater. Ils garantissent le bon transport des différents trafics vers leurs directions voulues, suivant le chemin conçu. exemple : de la BTS jusqu'aux Switch (MSC).

90% des liens exploités par **WTA** sont en fuseau hertzien. Ils offrent des débits variables de 2Mb/s à quelque Gb/s.

La technologie de FH a permit a **WTA** de couvrir 98% le territoire nationale (en 2010) d'après l'ARPT. Ce dernier partage la bande de fréquence entre les opérateurs de télécommunication du marché algérien. L'UITT (télégraphie télécommunication) s'occupe de la normalisation des bandes de fréquences des réseaux de transmission SDH et PDH. WATANIYA dispose des licences pour le SDH (6,11 et 15 GHz) et pour le PDH (15,23 et 38GHz).

La transmission constitue la dorsale d'un réseau GSM, d'où la nécessiter de superviser (à distance) en permanence ces équipements afin de parer en temps réel aux pannes de ces dernières pour assurer une meilleur disponibilité du réseau.

Les paramètres de supervision DCN

- Les performances (l'état des liens), fonctionnement rupture, saturation…
- Les alarmes (alarme de trafic)
- La mise à jour logicielle sur les équipements.
- Gestion des licences.
- Investigation des problèmes réseaux.

La majorité des équipements FH de WTA sont fournis par le constructeur **Ericsson** dans le centre et l'est, pour l'ouest c'est **Siemens** et **NEC.**

Au début, la gamme d'**Ericsson** était constituée que de MINI LINK E ensuite WTA introduit le MINI LINK TN.

III. MINI-LINK TN (Trafic Node) :

Le MINI-LINK Trafic Node fournit un DCN basé IP pour le transport des données d'opération et de maintenance. Chaque MINI-LINK Trafic Node a un routeur pour le traitement du trafic IP. Il se compose de deux parties :

Fig.3.1. Mini Link TN.

a. **La partie extérieure (Outdoor) :** est constituée d'une unité radio RAU qui fait la transmission des fréquences et l'amplification du signal qui sera émis par une antenne.

Fig.3.2. La partie extérieure.

b. La partie intérieure (Indoor) : On peut avoir plusieurs types. les figures suivantes montrent les composantes de la partie intérieure d'un MINI-LINK TN.

- **AMM 2p :** approprié en site finale, il comprend un ou deux MMUs,

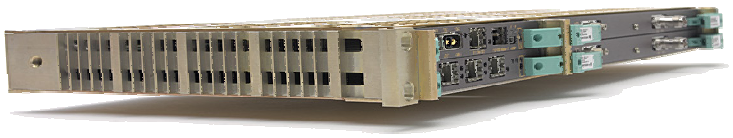


Fig.3.3. AMM 2p.

- **AMM6p :** approprié pour des sites de taille moyenne.

Fig.3.4. AMM 6p.

- **AMM 20p :** approprié pour des sites à grand trafic

Fig.3.5. AMM 20p.

- **MMU (Modem Unite) :** Elle détermine la capacité du trafic et fait la modulation et la démodulation.

Fig.3.6. MMU.

- **NPU (Node processor Unit) :** est toujours indispensable dans un AMM pour les fonctions suivantes :
  - ✓ Traitement du trafic
  - ✓ Traitement du DCN.
  - ✓ Il a un agent SNMP
  - ✓ Interface Ethernet 10base-T pour la connexion à un site LAN.
  - ✓ Stockage et administration des données de configurations.

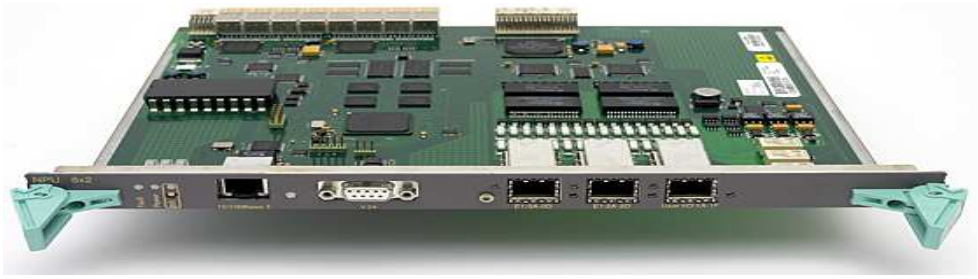


Fig.3.7. NPU.

- **PFU (Power Filter Unit) :** distribuent la puissance interne aux unités de modules d'extension via la carte mère.
- **FU (Fan Unit) :** fournit le refroidissement pour la partie intérieure.

Fig.3.8. FAU.

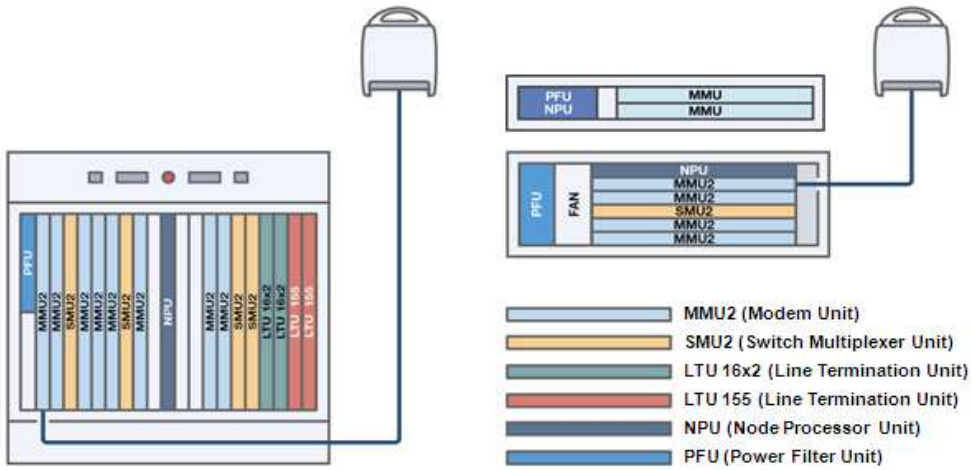


Fig.3.9. Emplacements des composants d'un MINI LINK TN.

IV. Les outils de gestion :

Ericsson peut fournir des solutions de gestion pour toutes les couches de gestion : Customized solutions for Business Management, Service Management, and Network Management layers est fournit comme un service.

La gestion de Mini-Link TN est divisée en 3 phases comme le représente la figure suivante :

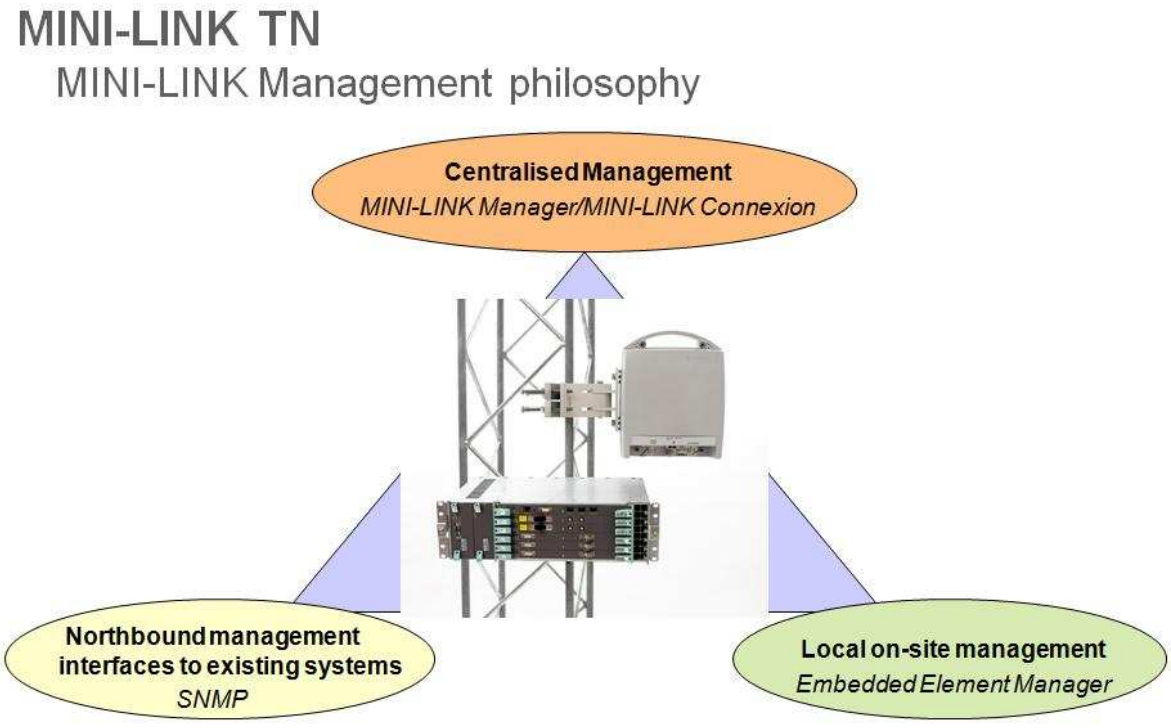


Fig.3.10. la philosophie de gestion de Mini-Link TN.

1. **Centralized management:**

NMS (network management system) est capable de superviser un réseau d'un point central. Il fournit les outils de gestion au niveau des nœuds et des circuits :

- ✓ Fault management.
- ✓ La gestion de performance.
- ✓ La gestion de configuration.
- ✓ La gestion de l'inventaire.
- ✓ Remote software Upgrade.
- ✓ La gestion de sécurité.
- ✓ Administration du system.

La gestion centralisée consiste :

a. Mini Link Manager :

La gestion d'éléments d'un réseau est capable de superviser les différents types de Mini Link (ML E, ML TN, ML HC...etc.)

b. Mini Link connexion :

Est utilisé pour la gestion de topologie du réseau et la connexion de transmission end-to-end, dans un réseau Mini-Link, dans le but de mettre en œuvre les avantages de la manipulation du nouveau trafic dans un Mini Link TN. On peut dire que Mini Link connexion est vu comme une extension optionnelle de Mini Link Manager fournissant les fonctionnalités des éléments de gestion de réseaux pour un réseau Mini-Link TN.

2. **Northbound Management interfaces:**

Chaque élément de réseau fournit un agent SNMP permettant une intégration facile à la configuration avec toute version SNMP (v1/v2/v3) basé system de gestion.

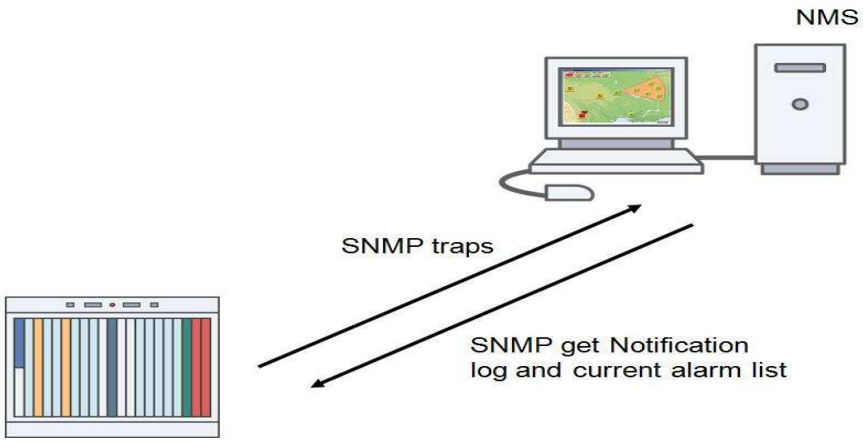


Fig.3.11. Northbound Management interfaces.

3. Local Management:

La fonction d'élément de gestion est implémentée comme une application EEM (Embedded Element Manager). The EEM est accédé en utilisant un navigateur web standard. The EEM fournit des outils pour : site en installation, configuration management, fault management, performance management and software upgrade. Il est aussi utilisé pour la configuration du fonctionnement du trafic routage, protection et DCN.

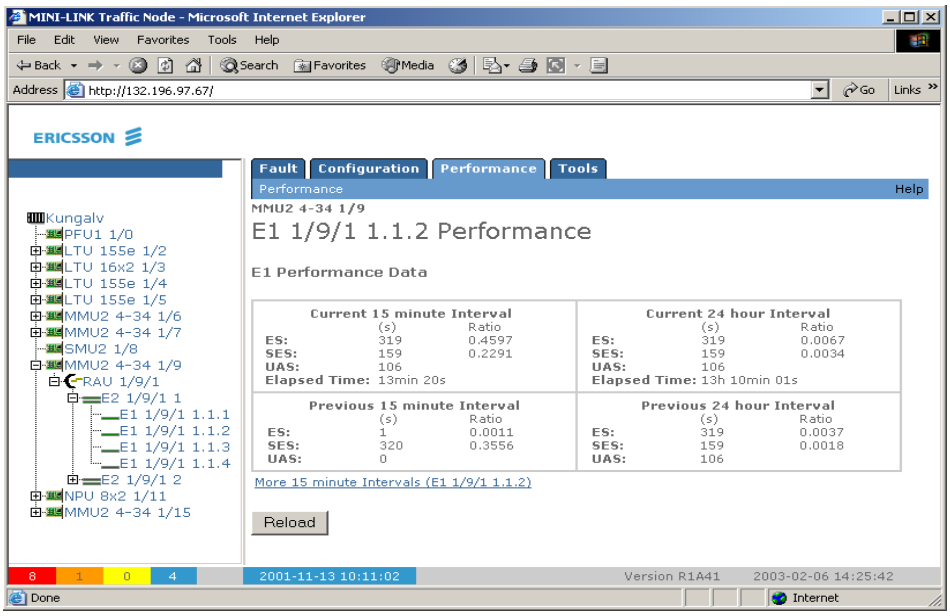


Fig.3.12. Embedded Element Manager (EEM).

Concernant le local craft terminal LCT, il est employé pour la gestion locale. Cela en connectant un pc au NPU avec un câble Ethernet (AMM6p, 20p) ou câble USB (AMM20p)

On peut accéder à L'EMM à distance, en entrant l'adresse IP comme URL dans le navigateur Internet avec une connexion au port 10 BASE-T sur l'un des nœuds du réseau.

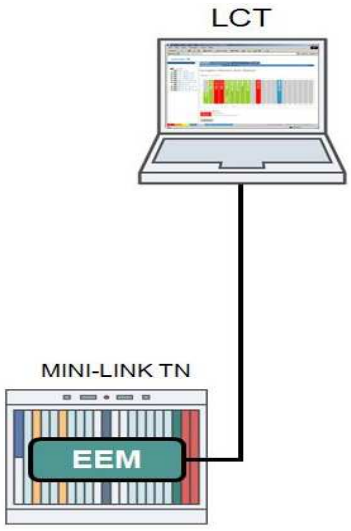


Fig.3.13. Gestion local.

4. **CLI (Command Line Interface) :** est une interface conçue pour la configuration du routeur IP.

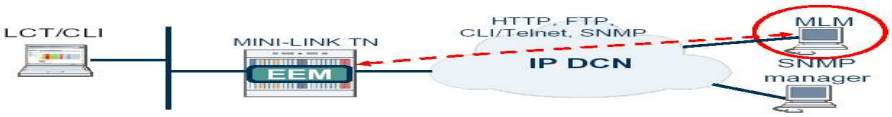


Fig.3.14. Outil de gestion.

5. **ServiceOn Microwave :**

Il est l'élément de gestion pour tout Produits de radio à micro-ondes d'Ericsson. ServiceOn Microwave nous permet de gérer notre réseau de transmission à micro-ondes.

Il fonctionne comme gestionnaire de faute et contrôleur de performance. Plusieurs utilisateurs peuvent avoir accès à n'importe quelle partie du réseau dans des différents sites en même temps et voir l'information de plusieurs serveurs. ServiceOn Microwave fournit une interface graphique facile à utiliser. [8]

Fig.3.15. ServiceOn MicroWave.

Remarque :

Toutes les gestions (locales et éloignées) sont protégées par un utilisateur et un mot de passe.

V. Les avantages du TN :

- Plus de modem dans le même AMM
- Le câblage est réduit
- Flexibilité
- Haute capacité
- Elément de gestion incorporé
- DCN basé IP avec configuration facile
- Mécanisme avancé de protection

VI. Data Communication Network (DCN) :

Les réseaux d'accès optiques et à large bande, peut être divisé en deux réseaux: le réseau de trafic et réseau de communication de données (DCN).

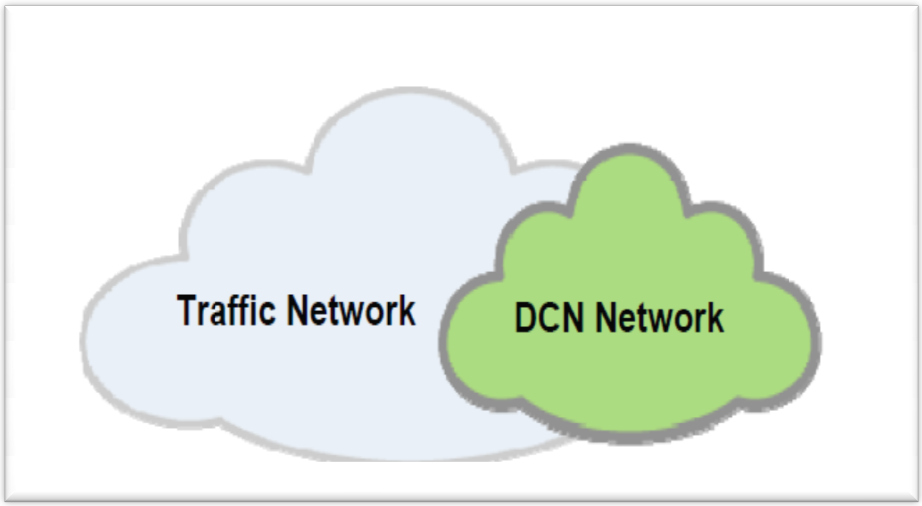


Fig.3.16. Le trafic et réseau de DCN.

Le réseau de trafic assure l'émission des données d'utilisateur. Par exemple ; entre des stations de base radio dans le réseau d'accès mobile ou entre un MSAN et un routeur de base.
La DCN n'est pas seulement composée de réseaux entre le système de gestion et la passerelle NE, mais aussi le transport entre NE à l'aide soit en bande ou hors bande de canaux de communication.

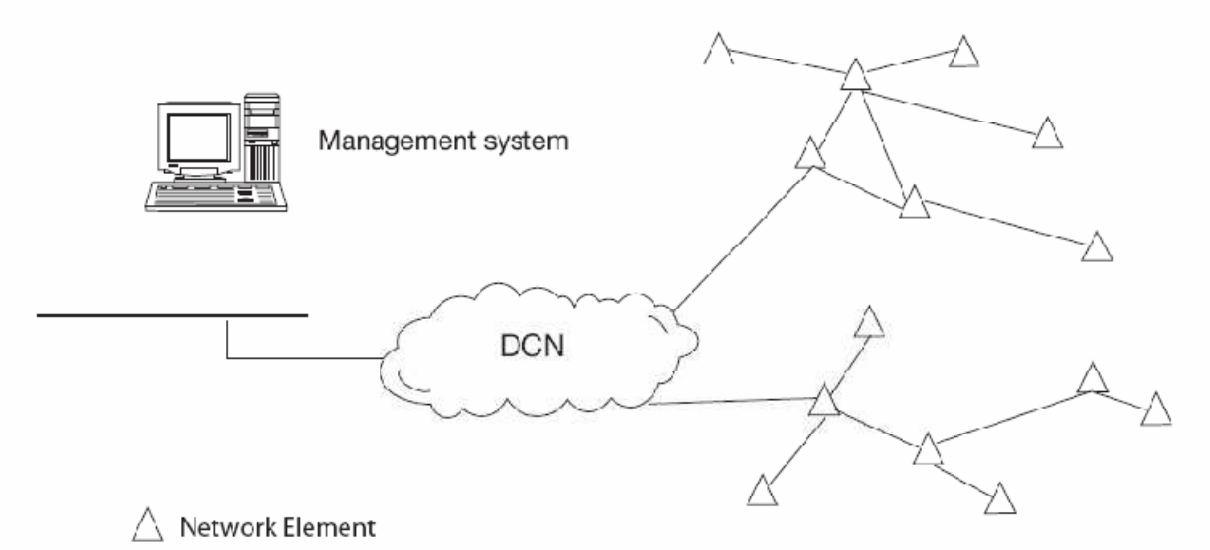


Fig.3.17. The DCN connects the NE's to the Management System.

Accès à large bande optique, micro-ondes, et le tiers d'autres produits (si la famille spécifique NE a la capacité) peuvent supporter IP, et / ou OSI basé DCN.

Quel que soit le protocole supporté, la DCN peut être reportée sur l'ensemble du réseau par la voie DCN embarquée ou via une infrastructure externe.

Nœuds à micro-ondes peuvent utiliser les serveurs Terminal Server pour fournir la connectivité DCN.

Les éléments du réseau sont affectés individuellement, OSI et / ou les adresses IP pour la connexion à la DCN. Beaucoup de NE ont également intégré des routeurs pour le traitement du trafic entre la DCN et NE. Ce qui réduit la quantité de routeurs et des commutateurs externes nécessaires.

1. DCN IP :

Certains principes doivent être utilisés lors de la planification d'une DCN IP pour Service On et l'OMS. Pour concevoir un réseau efficace, IP DCN exige une certaine compréhension de la base des deux capacités de la IP DCN de NE et IP en général. Assurez-vous que cela est en place avant de prendre la tâche de la construction du réseau IP DCN.

Le processus du désigne exige certaines décisions à prendre. Ces décisions auront un impact sur les performances de la DCN IP et devrait donc prendre en compte les principaux objectifs suivants :

• **Plan pour l'expansion :** Lorsqu'on démarre le déploiement du réseau DCN, il est important de regarder vers l'avenir pour planifier la mise à niveau et l'expansion future. Sinon, on sera confronté à un remaniement coûteux à un stade ultérieur.

• **Stabilité :** on doit faire une conception de réseau robuste qui assurera la stabilité.
• **routage efficace et rapide :** Le routage IP doit être rapide et efficace. Les petites tables de routage sont un moyen pour y parvenir.
• **Minimiser les frais généraux :** Gardez les messages généraux utilisés pour le routage IP avec des mises à jour minimum.

• **Peu d'entretien :** Faire une conception du réseau dans la mesure du possible, c'est l'épreuve du futur afin de minimiser la nécessité d'une maintenance active. L'utilisation d'un routage dynamique est une façon d'aborder cet objectif.

Lorsque le DCN IP est terminé et déployé, on doit faire en sorte que les différentes NEs soient accessibles depuis le centre OMC. Cela peut être fait avec la commande «Ping». Ceci permettra de vérifier que le routage IP fonctionne et de découvrir des problèmes de routage IP. Il est important de faire cette vérification, car il n'y a pas de messages d'erreur fournis par le routage IP SW, pour informer que les tables de routage IP ne sont pas mises en place comme on le désire. La conséquence d'une mauvaise configuration d'une table de routage IP, entraîne que les paquets IP ne seront pas capables d'atteindre leurs destinations.

2. Les services de DCN :

Les standards externes suivants des services de réseau IP sont pris en charge comme suit :

- Toutes les horloges utilisées par exemple pour les alarmes d'horodatage et d'événements, peuvent être synchronisées avec un Network Time Protocol (NTP).
- File Transfer Protocol (FTP) est utilisé comme un mécanisme de transfert de fichiers pour, la mise à niveau logiciel, la sauvegarde et la restauration de la configuration du système.
- Domain Name System (DNS) permet l'utilisation de noms d'hôte.
- Dynamic Host Configuration Protocol (DHCP) est utilisé pour allouer des adresses IP dans le DCN. Le NE a un agent de relais DHCP pour servir d'autres équipements sur le réseau local du site.

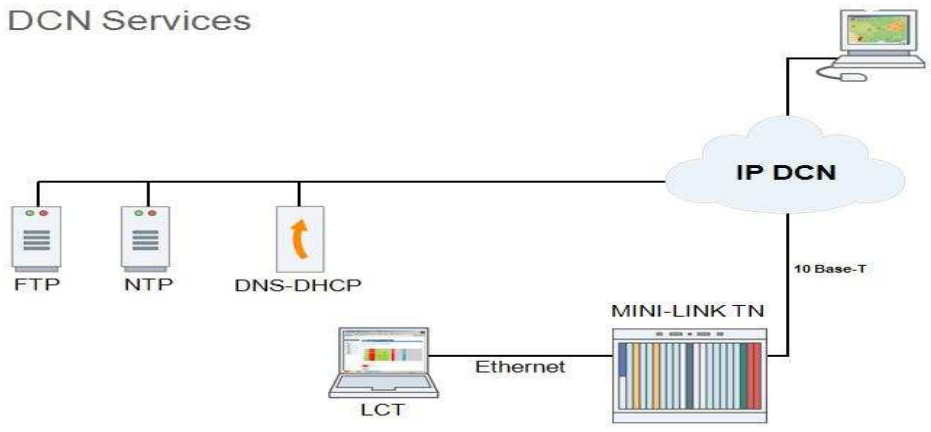


Fig.3.18. Les services DCN.

3. Les canaux de DCN :

Un sous-réseau de Mini Link regroupe plusieurs nœuds reliés en utilisant des vois de transmission consacrées. Les canaux DCN permettent le transfert des données de gestion entre les différents Mini Link connectés.

- **Node communication Channel (NCC) :** Employer pour la distribution de la gestion de données en utilisant le protocole GNM entre les AMMs. La connexion NCC entre deux MMUs dans un même AMM est faite par la carte mère.
- **Ethernet :** un port pour le RJ45.
- **External Alarm Channel (EAC):** Les données entre AMMs et autres équipements Mini Link dans un site peuvent être distribuées par cette connexion.
- **Remote Alarm Channel (RAC) :** Il est employé pour la connexion de deux AMMs qui ne sont pas sur le même site.
- **Hop Communication Channel (HCC) :** La transmission des données entre deux terminaux, à travers un hop, est envoyée sur des canaux séparés, HCC (8kbit/s).
- **Operation and Maintenance (O&M) port:** Il est disponible sur chaque unité intérieure dans l'AMM de Mini Link. Il est employé pour la lecture et l'installation des données de maintenance et d'opérations.

4. La capacité DCN :

Il existe plusieurs types du trafic dans un réseau IP DCN :

- Le trafic Background
- Les sessions de gestion
- Les Alarmes

Si on assure le bon fonctionnement des opérations précédentes, on peut dire qu'un réseau DCN est fiable. Cela vient avec une capacité suffisante de la bande passante dans le réseau et pour chacune des opérations (background, Alarmes, sessions).

5. Le Calcul de la bande passante BW :

Pour chaque type de trafic, on doit assurer la bande passante suffisante qui supporte le maximum du transport dans le réseau. D'une manière générale, on peut calculer la bande passante dans le pire des cas (Worst case) qui assure le minimum de transport du trafic dans notre réseau DCN, et on peut le citer comme suite :

Worst case BW = n /7 *64 [kbps]…….. (1)

n= nombre d'E1 des NEs.

Alors qu'une autre formule mieux adapter pour le réseau DCN on a :

DCN BW $_{(to\ OMC)}$ = 32*p [kbps] …….. (2)

DCN BW $_{(from\ OMC)}$ = 128*q [kbps] …….. (3)

P = nombre des sessions LCT actives.

q = nombre des sessions SUG actives.

Si on veut être plus précis, on doit calculer la bande passante pour chaque opération. Et ce qui est notre but. en plus, c'est la manière la plus fiable et la plus sûre.

- **Background :** le trafic background se passe entre l'OMC et les NEs. Ce sont des messages qui seront envoyés pour vérifier si le nœud qui contient les NEs est toujours connecté au réseau, et ceci dans un temps déjà défini (pas moins de 1000 sec). Les messages surviennent des deux cotés, OMC et le nœud NEs. on peut calculer la bande passante de ce trafic comme suite :

Background BW $_{(from/to\ OMC)}$ = (n*2400)/t [bps] …….. (4)

n = le nombre des nœuds.

t = intervalle d'interrogation.

Remarque : dans le cas ou le nœud sera plus petit, le concept de la bande passante sera sans importance.

- **Les sessions de gestion (Management terminals):** une session de la gestion dans le réseau IP DCN, est une opération de maintenance des équipements concernant le Software en utilisant les outils de gestions (voir IV). Chaque session nécessite un protocole, une charge utile, et un temps spécifique. et bien sûr une bande passante suffisante qui peut transporter tout le paquet. Le calcule de la bande passante se fait dans les deux sens vers/de l'OMC.

Management BW $_{(from\ OMC)}$ = n*128 [kbps] …….. (5)

Management BW $_{(to\ OMC)}$ = m*32 [kbps] …….. (6)

n = le nombre des sessions simultanées de SUG (Software Upgrade).
m = le nombre de sessions simultanées de management des terminaux.

O&M terminals	Payload	Protocol
MINILINK Manager(MLM) – Single parameter change – Single parameter view(FM/PM) – Single parameter view (other) – Multi parameter view (FM/PM) – SW upgradee single TN	 5-15Kbyte 300Byte 5-15Kbyte 550Byte 9-12MByte	 http SNMP get one(1object) http SNMP get bulk (10object) ftp
Local management (LCT-TN) – Parameter change/view – CLI – SW upgraded – Alarm bar update	 5-15Kbyte 50-100Byte 9-12 MByte 5Kbyte	 http telnet ftp http (every x second)
SNMP based manager – Single parameter change – Single parameter view – Multi parameter view – CLI – SW upgrade	 300Byte 300Byte 550Byte 50-100Byte 9-12MByte	 http SNMP get one(1object) http SNMP get bulk (10object) ftp

Tab.3.1. O&M payloads.

O&M terminal	BW	Response time
MINILINK Manager(MLM) – All operations except SW upgraded – SW upgrade activity	 32kbps 128kbps	 3-2s 10 min
Local management (LCT-TN) – All operations except SW upgraded – SW upgrade activity	 32kbps 128kbps	 3-2s 10 min
SNMP based manager – All operations except SW upgraded – SW upgrade activity	 32kbps 128kbps	 3-2s 10 min

Tab.3.2. BW Calculation.

- **Les Alarmes :** les alarmes ce sont des alertes qui indiquent le disfonctionnement ou des dégradations de performance des liens. Et dans le pire des cas, un arrêt total du réseau, ce qui est rare. Dans ce cas, la bande passante se calcule de la manière suivante :

$$\textbf{Alarms BW}_{\text{(to OMC)}} = (n + m*4)*o*p / t \text{ [bps]} \ldots\ldots\ldots\ldots\ldots\ldots \textbf{(7)}$$

n = nombre de radio hop.
m = nombre d'E1 affectés.
o = Facteur d'élimination pour les pertes dues aux liens (alarmes présente).
p = la taille du paquet alarmes = 365 byte= 2920 bits.
t = intervalle de Pooling……t = 200 sec (théorique)
t = (5- 10) min (pratique)

  - Le pire des cas n'existe pas en réalité.
  - La situation la plus réelle, c'est qu'une partie du nœud est affectée. Ce qui fait que la bande passante va diminuer énormément.
  - On prend les recommandations par défaut. Pour calculer la bande passante demandée pour les alarmes dans le pire des cas (the worst case), on a les suppositions suivantes :
    - Tous les E1 sont affectés.
    - 10% des radios hop dans un nœud sont affectés
    - Les alarmes sont générées chaque 10 sec.
    - 20 % des alarmes sont perdues pour le mal fonctionnement des liens.

D'où la loi du Worst case :

$$\textbf{Worst case alarms BW}_{\text{(to OMC)}} = 233*n + 93{,}2*m \text{ [bps]} \ldots\ldots\ldots\ldots\ldots\ldots \textbf{(8)}$$

n = nombre de radio hop.
m = nombre d'E1 affectés.

VII. Etude sur un exemple d'un réseau DCN :

Dans cette partie on énumère les différentes étapes du dimensionnement et de construction d'un réseau DCN. On a choisi une wilaya parmi les wilayas d'Algérie pour faire notre travail.

Dans notre exemple nous avons le nombre de n= le nombre d m. donc on à calculé le nombre des E1 qui égale à 36.

a. Calcule numérique de la bande passante :

N=m=36 donc le pire des cas (worst case) de la bande passante (BW) peut être calculé de la manière suivante :

Worstcase BW = n/7*64

=36/7*64

=329.14 Kbps

De la même manière on peut calculer the average background BW :

Average background BW = n*2400/T (le chargement utile pour BW payload est égale à 2400KByte et le temps T écoulé par défaut si l'on peut dire pour le faire est égale à 1000s).

Average background BW =36*2400/1000

Average background BW = 86.4 bps.

- ✓ **Les sessions de gestion (Management terminals) :**

Pour faire les calcules sur le management terminals, c'est-à-dire ; calculer le mangement BW dans les deux cas (from OMC and to OMC), on a qu'à appliquer les deux règles :

Nombre de SUG=1

Nombre de LCT=1

Management BW $_{(from\ OMC)}$ = n*128 [kbps]

Management BW $_{(from\ OMC)}$ = 1*128

Management BW $_{(from\ OMC)}$ =128Kbps

Management BW $_{(to\ OMC)}$ = m*32 [kbps]

Management BW $_{(to\ OMC)}$ = 1*32

Management BW $_{(to\ OMC)}$ = 32Kbps

- ✓ **The Alarms:**

Pour calculer l'impact d'IP DCN à partir des scénarios des alarmes, on établit les formules suivantes :

D'abord on utilise la formule par défaut pour calculer the BandWidth utilisé dans le dimensionnement de l'IP DCN.

Worst case Alarms BW=233*n+93.2*m

- n= m=36
- dans ce cas on a utilisé une seule Alarme pour les deux areas.

Worst case Alarms BW=233*36+93.2*36=11.74 Kbps

Alarms BW $_{(to\ OMC)}$ = (n + m*4)*o*p / t [bps]

Application numérique :

- n= m=36
- o=on a une élimination de perte à 80% donc ça reste 20% de perte.
- P=le chargement utile pour l'alarme est égale à 365Byte=2920 b.
- t= l'intervalle de Pooling on le prend par défaut à 200s.

Alarms BW $_{(to\ OMC)}$ = (36+36*4)*0.8*2920/200

Alarms BW $_{(to\ OMC)}$ = 2.10 Kbps

Nous avons deux areas dans cet exemple dont on fait un calcule sur les alarmes pour chaque Area. Pour cela, on garde toujours la même formule d'Alarme BW. ce qui change, c'est le nombre des n et m :

Pour l'area 1 on a pris un seul E1, et le nombre des nœuds qui appartient a ce réseau est de m=n=6.

Area 1 Alarms BW $_{(to\ OMC)}$ = (6 + 6*4)*0.8*2920 / 200 [bps]
Area 1 Alarms BW $_{(to\ OMC)}$ =0.35 Kbps

Pour l'area 2 on a pris un seul E1 pour chaque ML et le nombre des nœuds qui appartient à ce réseau est de m=n=30.

Area 2 Alarms BW $_{(to\ OMC)}$ = (30 + 30*4)*0.8*2920 / 200 [bps]
Area 2 Alarms BW $_{(to\ OMC)}$ = 1.75 Kbps

b. Adressing IP et Subneting :

Pour cette wilaya, on a la plage d'adressage 10.3.0.0 et on a utilisé le masque 255.255.252.0 pour la BSC de cette wilaya, ensuite on divise par la méthode de subneting en 2 plages d'adressage pour chacun des LAN. C'est-à-dire le LAN1 prend une plage de 10.3.4.1/28 et le LAN2 prend une seconde plage qui est 10.3.6.1/28. Maintenant dans chaque LAN se situe des nœuds NEs qu'on va encore diviser les plages d'adressage qui prendra un AREA ID de 10.3.4.0/23 pour le BSC_TN2, NET : 10.3.4.0 et un MASK : 255.255.254.0. Même chose pour BSC_TN1 avec un AREA ID : 10.3.6.0, NET : 10.3.6.0 et un masque: 255.255.254.0. Et enfin pour terminer le reste des 2 sous réseaux, elle prend la plage d'adressage de /30 avec un masque de : 255.255.255.252 qui satisfait notre exemple et laisse quelque nœud vide pour la mise à jour à l'avenir.

La table des nœuds :

	Nom Site	Adresse IP NE	OSPF Areas	
			OSPF Area	OSPF Area Type
Area 1	BSC TN1	10.3.0.4/28	10.3.0.0/23	STUB
	C1	10.3.0.17/30	10.3.0.0/23	STUB
	C2	10.3.0.21/30	10.3.0.0/23	STUB
	C3	10.3.0.25/30	10.3.0.0/23	STUB
	C4	10.3.0.29/30	10.3.0.0/23	STUB
	C30	10.3.0.33/30	10.3.0.0/23	STUB
	C31	10.3.0.37/30	10.3.0.0/23	STUB
Area 2	BSC TN2	10.3.2.4/28	10.3.0.0/23	STUB
	C5	10.3.2.17/30	10.3.0.0/23	STUB
	C6	10.3.2.21/30	10.3.0.0/23	STUB
	C6	10.3.2.24/30	10.3.0.0/23	STUB
	C7	10.3.2.29/30	10.3.0.0/23	STUB
	C8	10.3.2.33/30	10.3.0.0/23	STUB
	C9	10.3.2.37/30	10.3.0.0/23	STUB
	C10	10.3.2.41/30	10.3.0.0/23	STUB
	C11	10.3.2.45/30	10.3.0.0/23	STUB
	C12	10.3.2.49/30	10.3.0.0/23	STUB
	C13	10.3.2.53/30	10.3.0.0/23	STUB
	C14	10.3.2.57/30	10.3.0.0/23	STUB
	C15	10.3.2.61/30	10.3.0.0/23	STUB
	C16	10.3.2.65/30	10.3.0.0/23	STUB
	C17	10.3.2.69/30	10.3.0.0/23	STUB
	C18	10.3.2.73/30	10.3.0.0/23	STUB
	C19	10.3.2.77/30	10.3.0.0/23	STUB
	C20	10.3.2.81/30	10.3.0.0/23	STUB
	C21	10.3.2.85/30	10.3.0.0/23	STUB
	C22	10.3.2.89/30	10.3.0.0/23	STUB
	C23	10.3.2.93/30	10.3.0.0/23	STUB
	C24	10.3.2.97/30	10.3.0.0/23	STUB
	C25	10.3.2.101/30	10.3.0.0/23	STUB
	C26	10.3.2.105/30	10.3.0.0/23	STUB
	C27	10.3.2.109/30	10.3.0.0/23	STUB
	C28	10.3.2.113/30	10.3.0.0/23	STUB
	C29	10.3.2.117/30	10.3.0.0/23	STUB
	C32	10.3.2.121/30	10.3.0.0/23	STUB
	C33	10.3.2.125/30	10.3.0.0/23	STUB
	C34	10.3.2.129/30	10.3.0.0/23	STUB
	C35	10.3.2.133/30	10.3.0.0/23	STUB
	C36	10.3.2.137/30	10.3.0.0/23	STUB

Tab.3.3. Table des nœuds.

Remarque :

Les masques des différentes étapes du tableau sont les suivants :

/28 : Masque 255.255.255.240

/30 : Masque 255.255.255.252

/23 : Masque 255.255.254.0

/22 : Masque 255.255.252.0

c. Routage :

On utilise en générale le routage dynamique dans les clusters et le routage statique pour connecter l'OMC aux clusters.

- **Routage dynamique**

On a employé le protocole OSPF avec des Areas reliées à un ABR. On utilise un Backbone 0.0.0.0 pour relier les 2 Mini-Link TN au routeur qui est relié directement à l'OMC. Le type d'aires est STUB Area où le routeur communique avec un seul MINI LINK Trafic Node qui joue le rôle d'un ABR. On a choisi un ABR dans tout le site, puisque on a pris une petite zone de 36 nœuds.

- **Recommandation de routage**

L'ABR dans une zone de stub se propage uniquement entre les routes area dans une zone. Tous les autres types de routes seront bloqués. Les routeurs dans une zone de stub auront des informations de routage sur les routeurs dans son propre secteur et les autres sous zones.

Une route DGW, pointant à l'ABR, sera automatiquement générée dans une zone tampon pour tous les routeurs interne. La route DGW sera utilisée pour le routage IP en dehors propre OSPF.

- **Routage statique**

  - Pour un petit réseau de l'IP DCN.
  - Pour la connexion de l'OMC vers les domaines OSPF.
  - Pour un DGW.

Une fois que notre IP DCN est complète, on utilise la commande PING pour faire la vérification du bon fonctionnement et la détection des problèmes.

d. Les extensions DCN :

L'un des défis de l'opération du DCN est l'extension du réseau dû aux nouveaux sites, équipements ou l'amélioration de capacité. Comme un général guide, il est recommandé de planer pour l'extension en même temps que l'initiale installation du DCN.

On peut citer quelques recommandations :

- Travailler avec les Totally stub-area.
- Résumer les routes en utilisant l'ABR.
- Travailler avec le routage dynamique OSPF.
- Diviser les aires si elles-mêmes dépassent 45_50 nœuds.
- Utiliser les « virtuels Link ».
- Diviser les aires en petites aires logiques.
- Travailler avec le routage statique et dynamique.

VIII. Conclusion :

Le dimensionnement du DCN est très important pour la bonne supervision d'un réseau de transmission. Le Mini Link Trafic Node offert une solution optimale pour un réseau DCN IP et assure une extension future, et compatibilité avec des nouvelles Technologies.

CHAPITRE IV

I. Introduction :

Le présent chapitre décrit notre logiciel que nous avons proposé après avoirs terminer notre travail principal. Ce logiciel permet d'aider les ingénieurs a facilité le dimensionnent d'un cluster DCN.

Pour se faire, on a choisi le langage orienté objet Delphi, qui prend en charge le maintien automatique d'une partie du code source. Ces raisons nous amènent de préférer cet outil pour concevoir notre logiciel.

Nous allons en premier lieu, présenter, brièvement, l'outil d'aide au développement

Delphi, puis, en second lieu, on va présenter d'une manière succincte la manipulation de l'application développée.qui permet d'aider les ingénieurs à faciliter le dimensionnent d'un cluster DCN.

II. Présentation de Delphi :

Delphi est un environnement de programmation permettant de développer des applications pour Windows 95, Windows 98/2000, Windows XP, Windows7.Il incarne la suite logique de la famille turbo Pascal.

Delphi est un langage de programmation qui comprend certaines caractéristiques :

- Programmation objet.
- Outils visuels bidirectionnels.
- Compilateur produisant du code natif.
- Traitement complet des exceptions.
- Possibilités de créer des exécutables et des DLL.
- Bibliothèque de composant extensible.
- Débogueurs graphique intégré.
- Support de toutes les API de Windows : OLE2, DDE, VBX, OCX,…

II.1 Environnement de travail :

Après son lancement Delphi se présente sous la forme de quatre fenêtres. Cette présentation n'est pas courante parmi les applications Windows. Elle se révèle relativement pratique.

La première fenêtre occupe la partie supérieure de l'écran elle correspond à l'environnement de programmation proprement dit. Cette fenêtre contient :

• La barre d'outils.

• La barre de menu de Delphi.

• Une zone « barre d'outil ».

• Une zone contenant les divers composants regroupés par famille.

La seconde fenêtre se trouve par défaut à gauche de l'écran : c'est l'inspecteur d'objet, il permet de visualiser, pour chaque objet un composant, les propriétés et les événements auxquels l'objet peut répondre.

La troisième fenêtre constitue la fiche principale de la future application Delphi .Im s'agit, au départ, d'une fenêtre vide dans laquelle on placera les divers objets.

La dernière fenêtre, cachée sous la précédente constitue « l'éditeur » proprement dit contenant le code source de l'application.

Puisque Delphi permet de créer les applications de deux façons différentes, il est appelé (TWO WAYS TOOLS /un outil à double usage) :

- La première méthode consiste en une programmation traditionnelle.
- La deuxième méthode consiste en une programmation orientée objet.

Toutes ces raisons et ce haut degré de performance de Delphi nous ont poussés à choisir Delphi comme un langage de programmation.

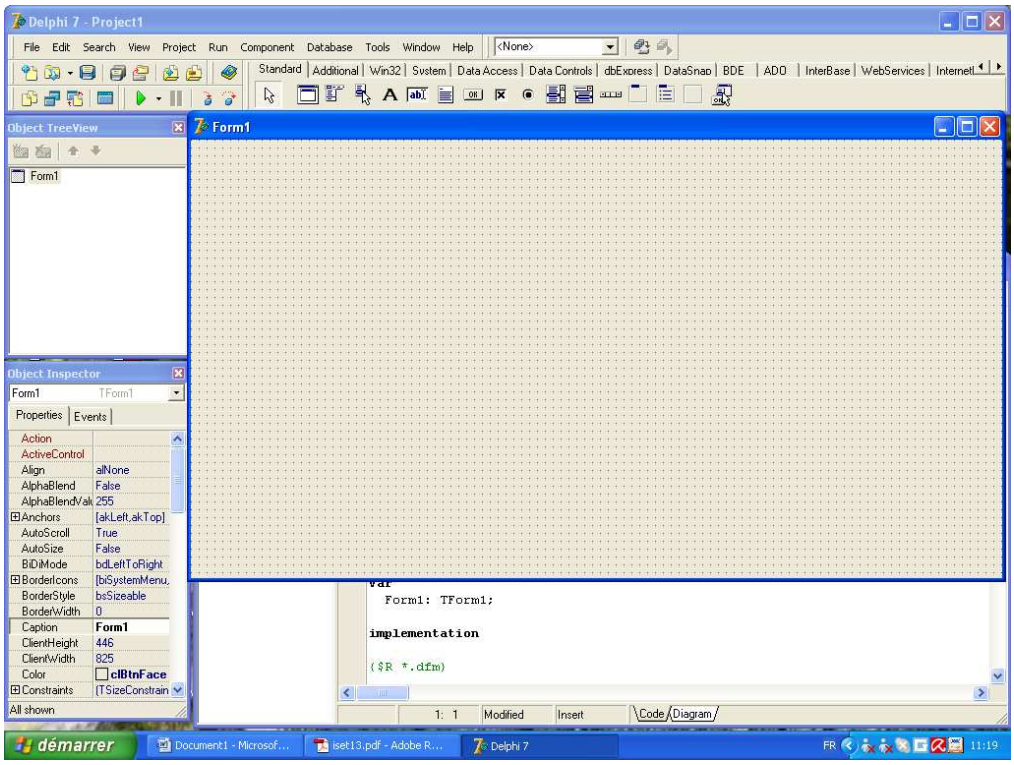


Fig.4.1. Les principaux outils de l'environnement de Delphi

II.2. Présentation de l'interface développée sous Delphi :

Notre programme se compose des fenêtres suivantes :

2-1 Fenêtre principale :

Dans la fenêtre principale, on a tout un menu contenant trois unités. Elle permet d'accéder à l'IP database, au calcul de BW et pour quitter l'application.

Fig.4.2. La fenêtre principale

- ✓ **IP database, GO:** ont le même rôle, c'est d'afficher la fenêtre des choix des BSC.

```
procedure TForm13.IPdatabase1Click(Sender: TObject);
begin
form1.showmodal;
end;
```

- ✓ **BW :** il a le rôle d'afficher la fenêtre du calcul de la BW.

```
procedure TForm13.BW1Click(Sender: TObject);
begin
form14.showmodal;
end;
```

- ✓ **EXIT:** ont pour rôle de fermer l'application.

```
procedure TForm13.EXIT1Click(Sender: TObject);
begin
close;
```

end;

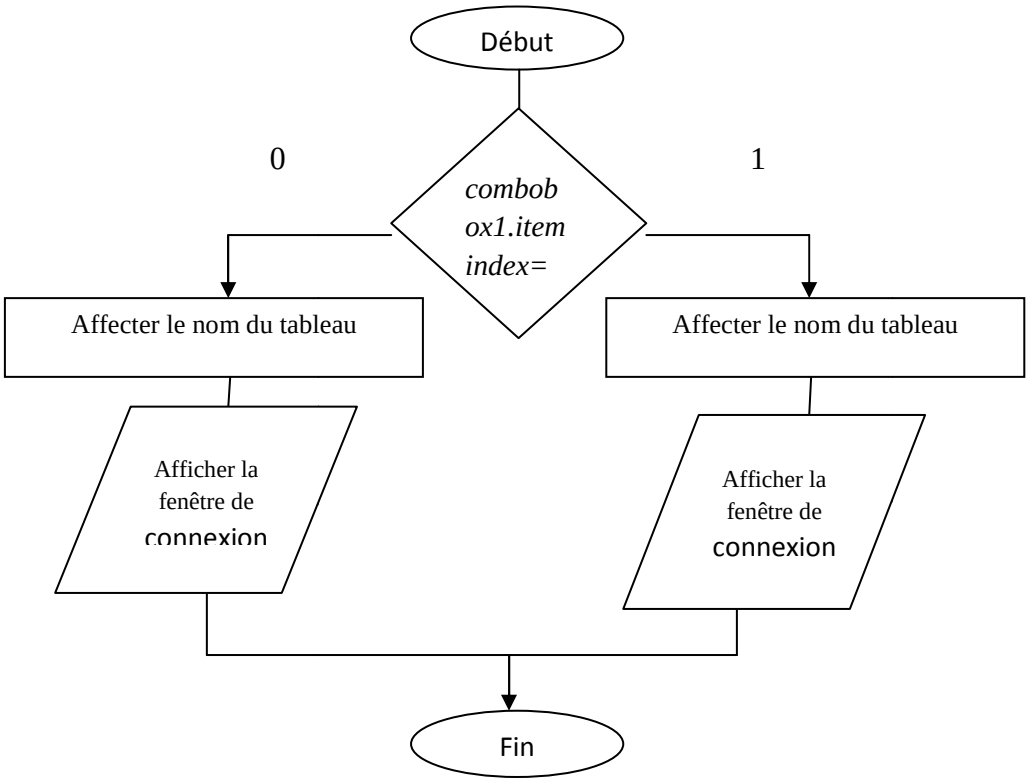
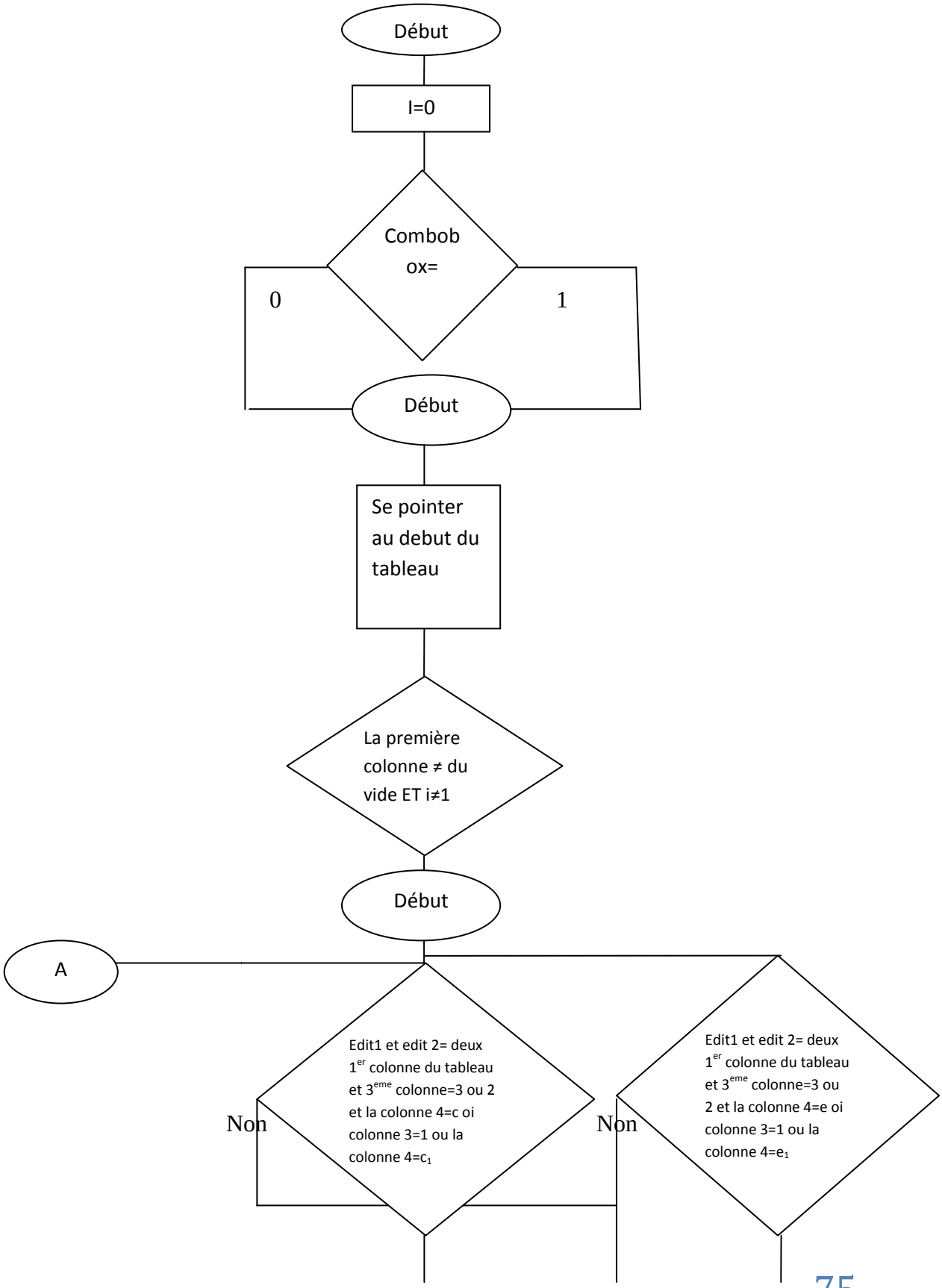


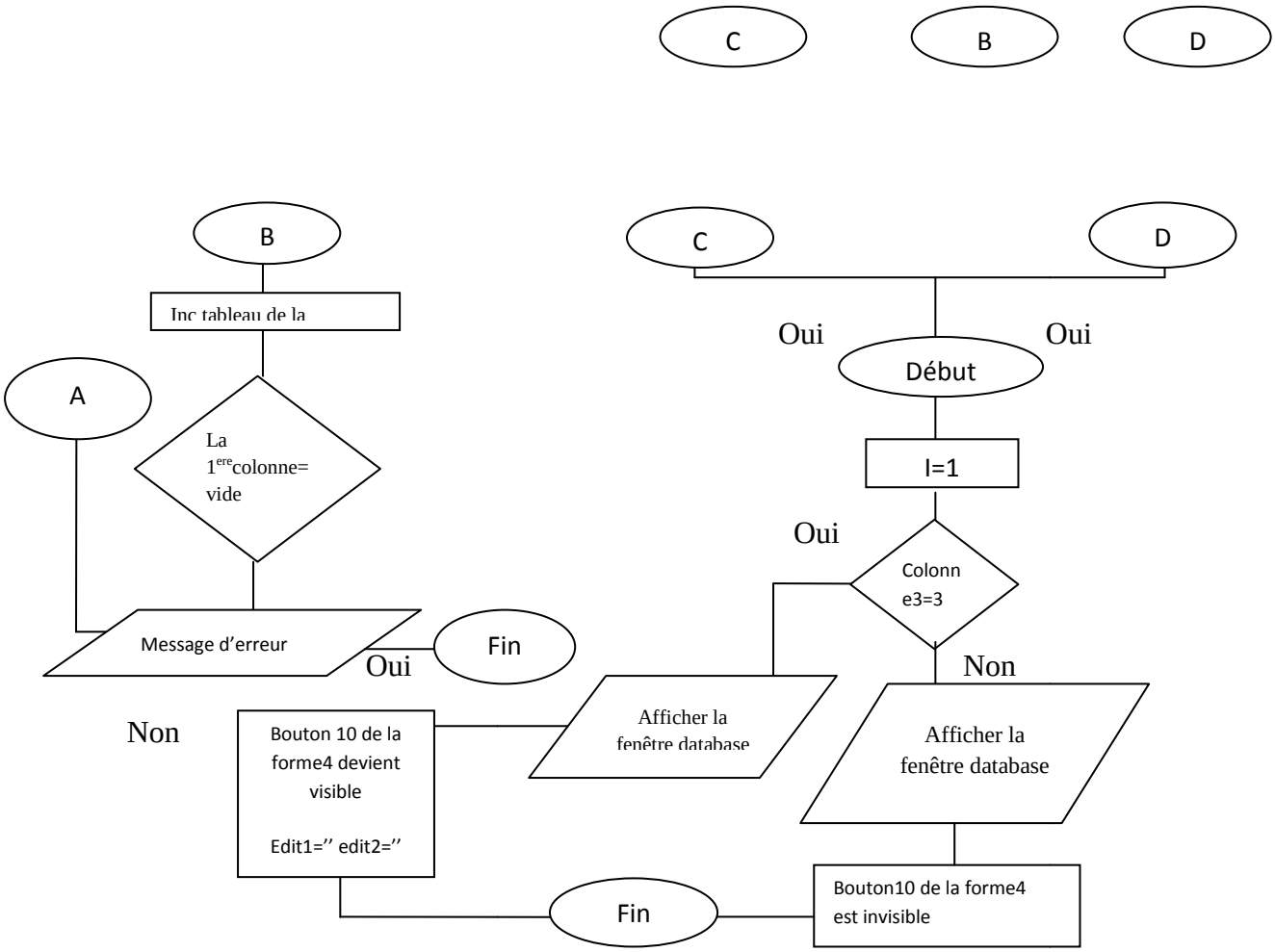
Fig.4.3. La fenêtre de connexion

- ✓ **OK :** a pour rôle de vérifier la validité du mot de passe en sélectionnent les propriétés a l'aide d'un tableau.

```
procedure TForm2.Button1Click(Sender: TObject);

var i,j:integer;

begin

i:=0;

 if form1.ComboBox1.ItemIndex=0 then begin

form11.ADOTable1.First;

while (form11.ADOTable1.Fields[0].AsString<>'') and (i<>1) do

begin if ((edit1.Text= form11.ADOTable1.Fields[0].AsString) and (edit2.Text=
form11.ADOTable1.Fields[1].AsString)

and ((form11.ADOTable1.Fields[2].asstring='3')

or ((form11.ADOTable1.Fields[2].AsString='2')

and
(form11.ADOTable1.Fields[3].AsString='c'))

or ((form11.adotable1.fields[2].asstring='1')

and (form11.adotable1.fields[3].asstring='c1'))))

then

begin

i:=1;

if form11.ADOTable1.Fields[2].asstring='3' then
form4.Button10.Visible:=true

else form4.Button10.Visible:= false;

form4.showmodal;

edit1.Text:='';

edit2.text:='';

close; end;

 form11.adotable1.Next; end;

if i=0 then begin edit1.Text:=''; edit2.text:='';form23.show; end;
```

end;


Début
I=0
Combob ox=
0
1
Début
Se pointer au debut du tableau
La première colonne ≠ du vide ET i≠1
Début
A
Edit1 et edit 2= deux 1er colonne du tableau et 3eme colonne=3 ou 2 et la colonne 4=c oi colonne 3=1 ou la colonne 4=c1
Non
Edit1 et edit 2= deux 1er colonne du tableau et 3eme colonne=3 ou 2 et la colonne 4=e oi colonne 3=1 ou la colonne 4=e1
Non



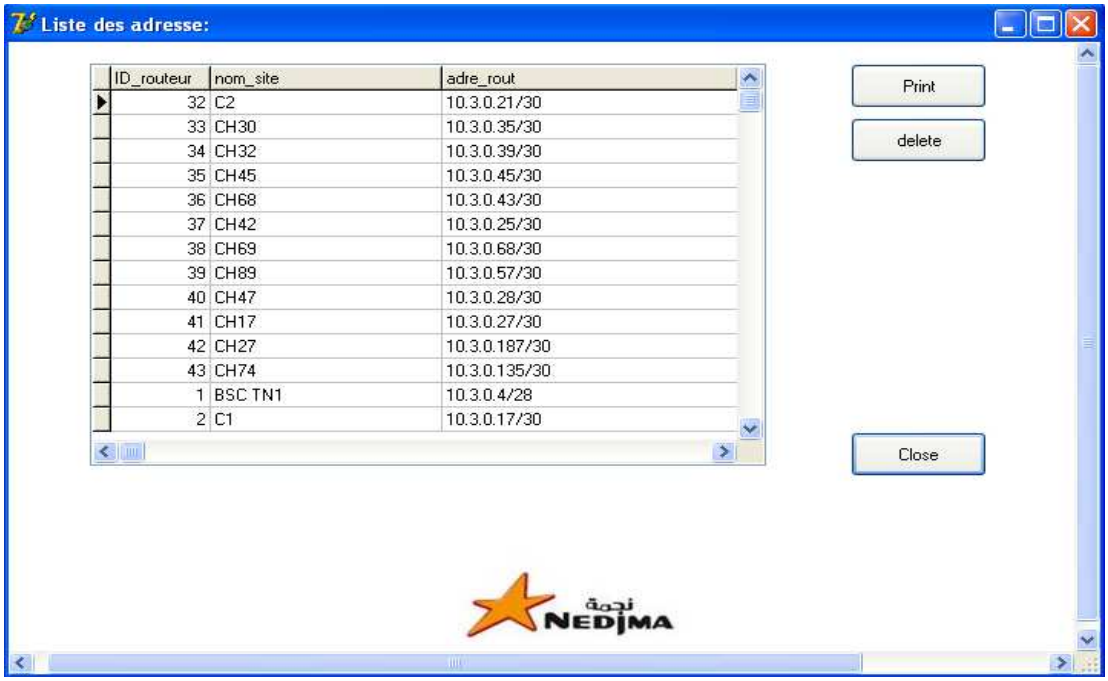
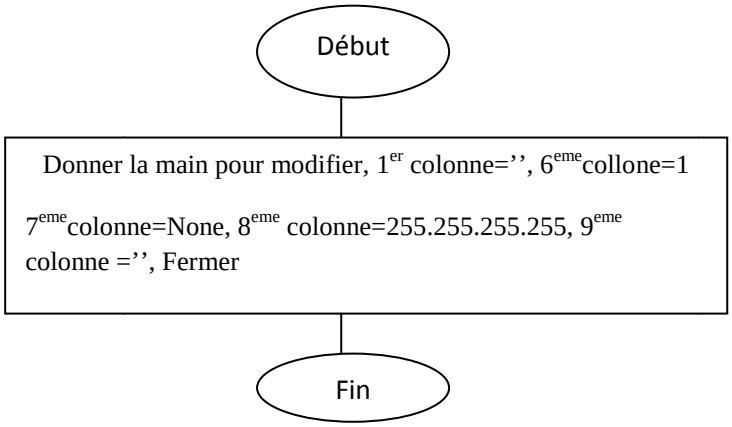


Fig.4.4. Listes des adresses

- ✓ **Delete site:** pour supprimer un site

```
procedure TForm9.Button1Click(Sender: TObject);
begin
form4.ADOTable1.Edit;
form4.ADOTable1.Fields[0].AsString:='';
form4.ADOTable1.Fields[5].AsString:='1';
form4.ADOTable1.Fields[6].AsString:='None';
form4.ADOTable1.Fields[7].AsString:='255.255.255.252';
form4.ADOTable1.Fields[8].AsString:='';
close;
end;
```



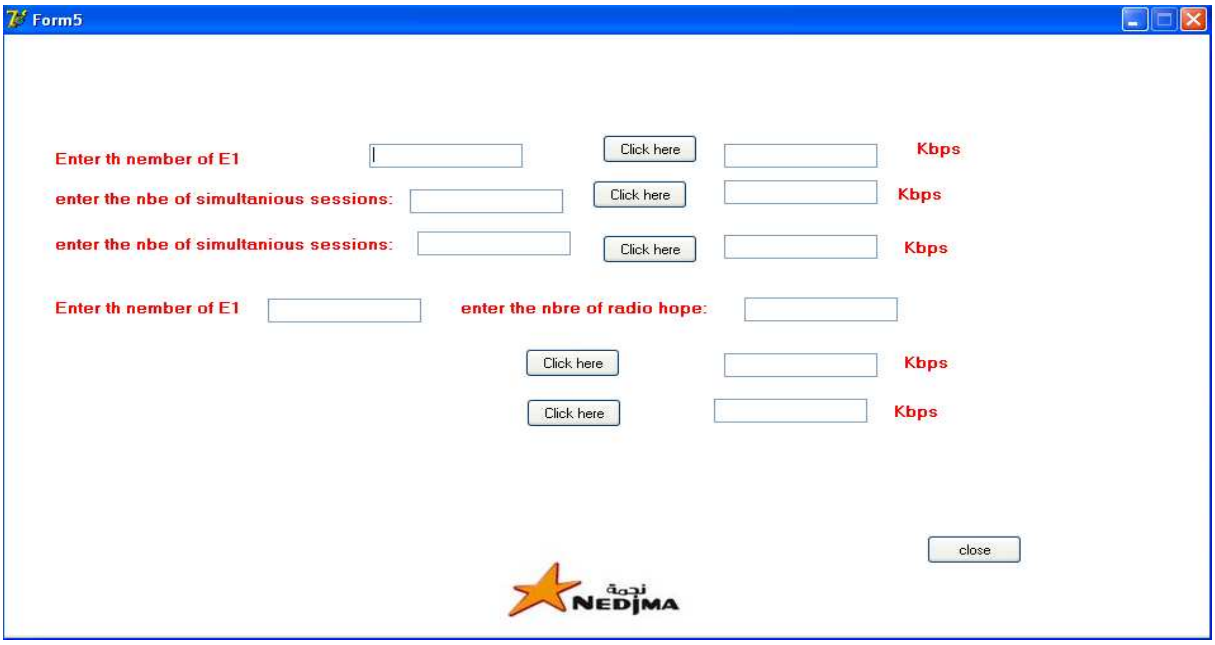
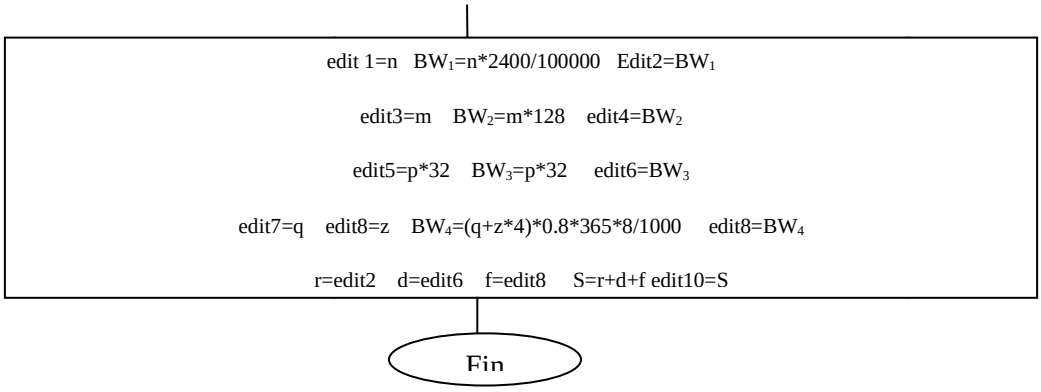


Fig.4.6. Calcul de BW

- ✓ **BW** : pour calculer la bande passante dans le pire cas.

```
procedure TForm13.Button1Click(Sender: TObject);
var  n,BW1:real;
begin
n:=strtofloat(edit1.text);
BW1:=(n*2400)/1000;
BW1:=BW1/100;
edit2.Text:=floattostr(BW1);
end;
procedure TForm13.Button2Click(Sender: TObject);
var  n,BW2:real;
begin
m:=strtofloat(edit3.text);
BW2:=n*128;
edit4.Text:=floattostr(BW2);
end;
```

```
procedure TForm13.Button3Click(Sender: TObject);
var  n,BW3:real;
begin
p:=strtofloat(edit5.text);
BW3:=n*32;
edit6.Text:=floattostr(BW3);
end;
procedure TForm13.Button4Click(Sender: TObject);
var  n,BW4,m:real;
begin
q:=strtofloat(edit7.text);
z:=strtofloat(edit9.text);
BW4:=(n+m*4)*0.8*365*8/10;
BW4:=BW4/100;
edit8.Text:=floattostr(BW4);
end;
procedure TForm13.Button5Click(Sender: TObject);
var m,n,S,z:real;
begin
r:=strtofloat(edit2.text);
d:=strtofloat(edit6.text);
f:=strtofloat(edit8.text);
S:=n+m+z;
edit10.Text:=floattostr(S);
end;
 end.
```



III. Conclusion :

Nous pouvons constater que cette application va économiser beaucoup de temps aux ingénieurs de WTA, car elle apporte beaucoup de facilité par rapport aux fichiers EXCEL.

Conclusion générale

La convergence des réseaux est devenue le refrain marketing à la mode de toutes les entreprises œuvrant dans les réseaux de télécommunications et sachant qu'ils représentent l'épine dorsale informationnelle des entreprises par extension de l'économie. Et en raison de la forte concurrence qui règne dans le domaine des télécommunications, la nécessité d'une planification efficace du réseau de supervision DCN est primordiale afin d'avoir un réseau fiable et sécurisé.

Un réseau DCN bien conçu assure la fiabilité, la performance ainsi que la mise à jour de l'état du réseau. Après l'étude que nous avons abordée à travers ce mémoire, on peut conclure les points suivants :

- Les considérations prises dans notre conception pour éliminer les difficultés de l'exploitation des réseaux des opérateurs téléphonique sont :

Efficacité : L'équipement de réseau devrait être utilisé de telle manière que la charge inutile et la congestion de la gestion du trafic dans le réseau et ses NE peut être évitée.

Flexibilité : Le DCN devrait- si possible- être préparé pour les variations de la topologie existante.

Disponibilité : La capacité des systèmes de gestion ainsi que la conception de la DCN détermine le nombre de NE_S gérés.

Ce mémoire apporte une aide à la conception du réseau DCN. Il donne une connaissance de base des différentes possibilités de se connecter un MINI-LINK à un système de gestion. En outre, il décrit les voies de communication pour la distribution des gestions des données.

La grande souplesse du réseau DCN prendra alors tout son intérêt. Le choix de cette technique représente une véritable révolution pour WATANIYA, mais cela implique une conduite et une maîtrise d'un vaste programme : budget, formation, expérimentations, mise en œuvre et une gestion du réseau.

Enfin, l'évolution du réseau DCN vers un réseau « allOver IP » est un challenge nécessaire dans le futur. L'équipe technique de Wataniya cherche toujours de nouvelle technologie afin d'améliorer leurs service et toujours de satisfaire leurs aimable clients.

Annexe

On va voir les différentes fenêtres de « SOM » qui nous aident à superviser le Mini-Link, visualiser ces alarmes et faire sa maintenance.

La fenêtre apparente quand on lance le « SOM » , on clique sur Network + ouvrir un fichier ID pour visualiser les alarmes est la suivante :

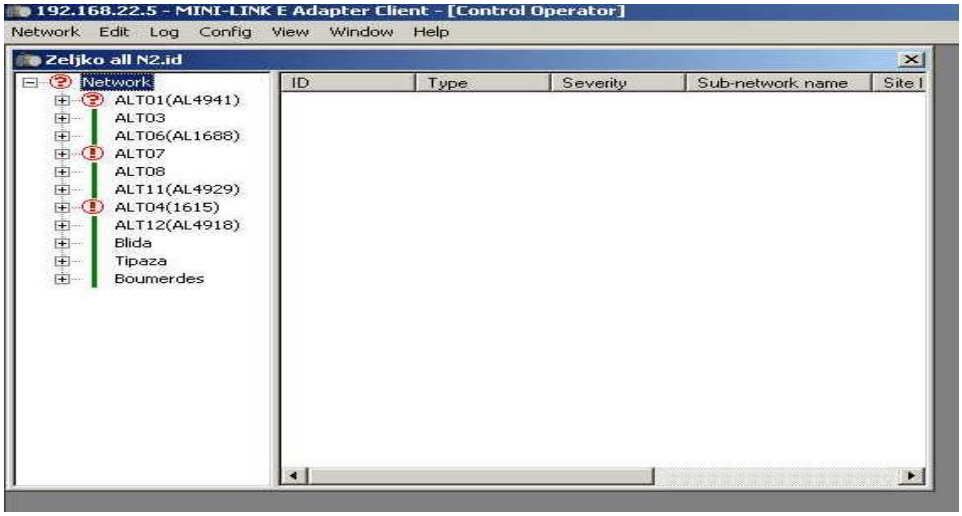


Fig.1. visualiser les alarmes.

? : On ne voit pas le site. (La connexion physique n'est pas fonctionnelle).

! : On a une alarme Majeure

. : On a une alarme mineure

Si on ne trouve pas des ponctuations précédentes c-à-d que le site est en fonctionnement normal.

Le signe + devant les sites signifie que y on a d'autres sites qui sont raccordés à chacun de ces sites. En cliquant sur le signe +, on peut visualiser les sites raccordés

En cliquant sur le « nom de site », on peut avoir des informations telles que le type de Mini-Link, l'état normal ou en alarmes….etc

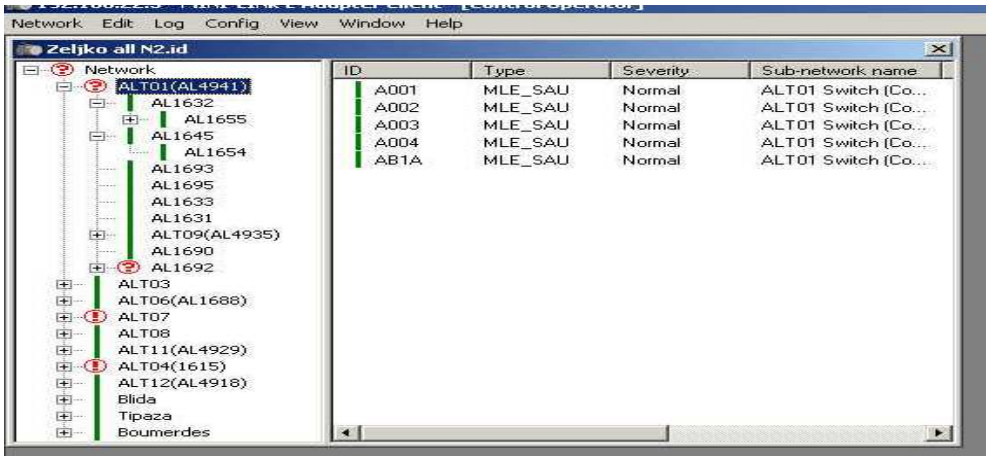


Fig.2. Visualisation des sites raccordés.

1.Exemple d'un site en fonctionnement normal :

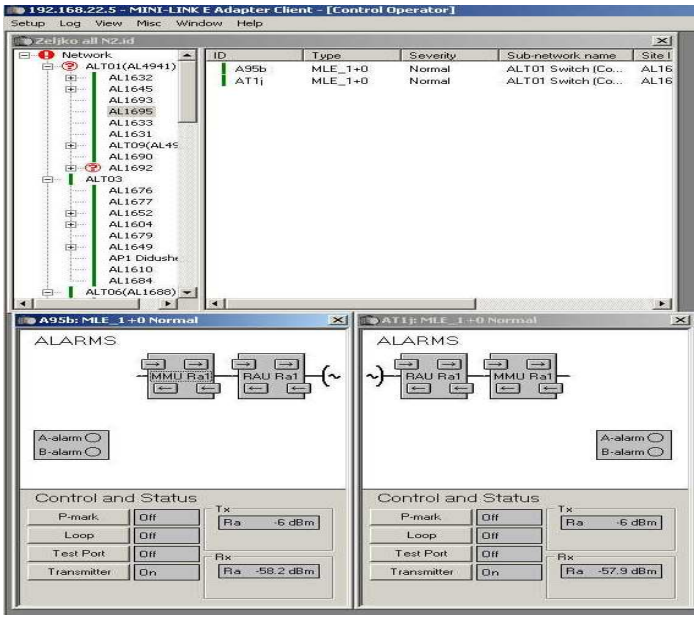


Fig.3: site en fonctionnement normal.

2. Exemple d'un site en alarme :

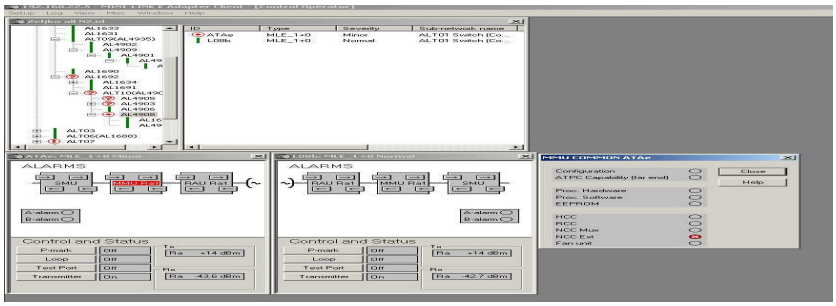


Figure.4: site en alarme

Le Help nous donne plus de détails sur la nature de cette alarme.

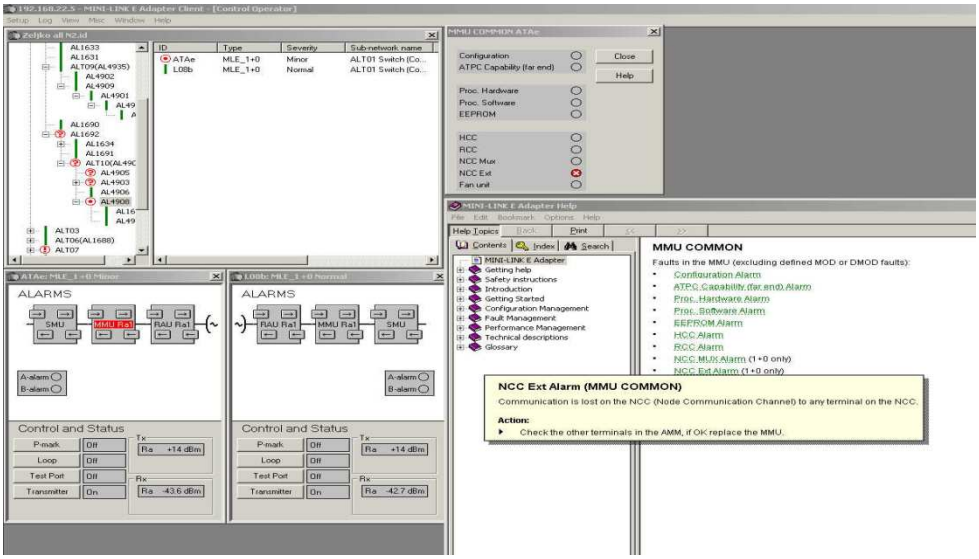


Fig.5. Option du help.

Exemple d'un site 1+1, le rôle de SMU dans ce cas est de Switcher entre ces modules MMUs selon la meilleure qualité de signal et de faire aussi le Multiplexage et le démultiplexage en 2Mb/s. Ce site, comme indiqué par le (!), est une alarme MAJOR .A l'aide de Help, on peut avoir plus de détails sur cette alarme ainsi ce qu'on doit faire pour y remédier.

Pour voir l'état des niveaux d'émission et de réception SETUP ⟶HOP

La visualisation de toutes les alarmes ainsi que leurs degrés de gravité peut se faire aussi en cliquant sur LOG⟶ALARM

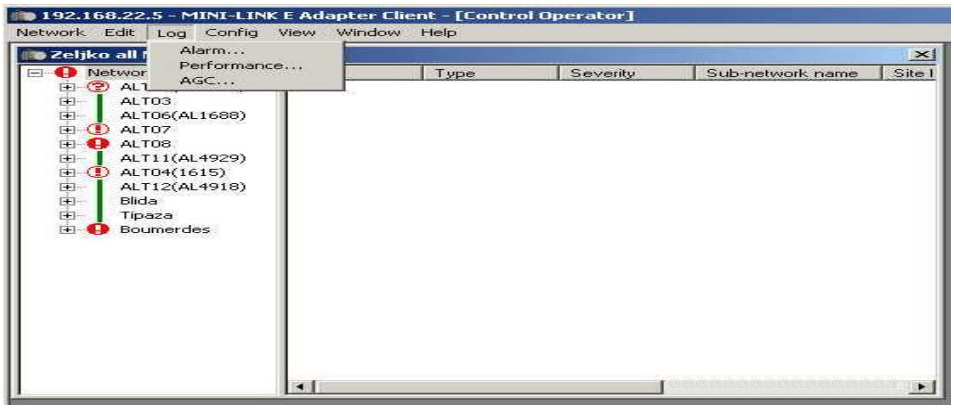


Fig.6. Visualisation des alarmes.

- **<u>Exemple d'un site en fonctionnement normal</u>**

(Commande LOG⟶ALARM)

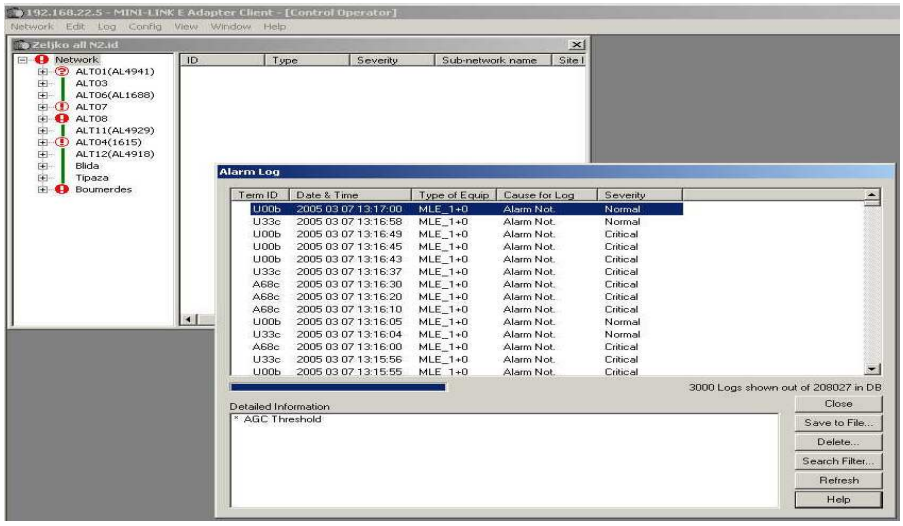


Fig.7. Site en fonctionnement normal par la commende LOG.

- **Exemple d'un site en Alarme**

Commande LOG ⟶Alarm.

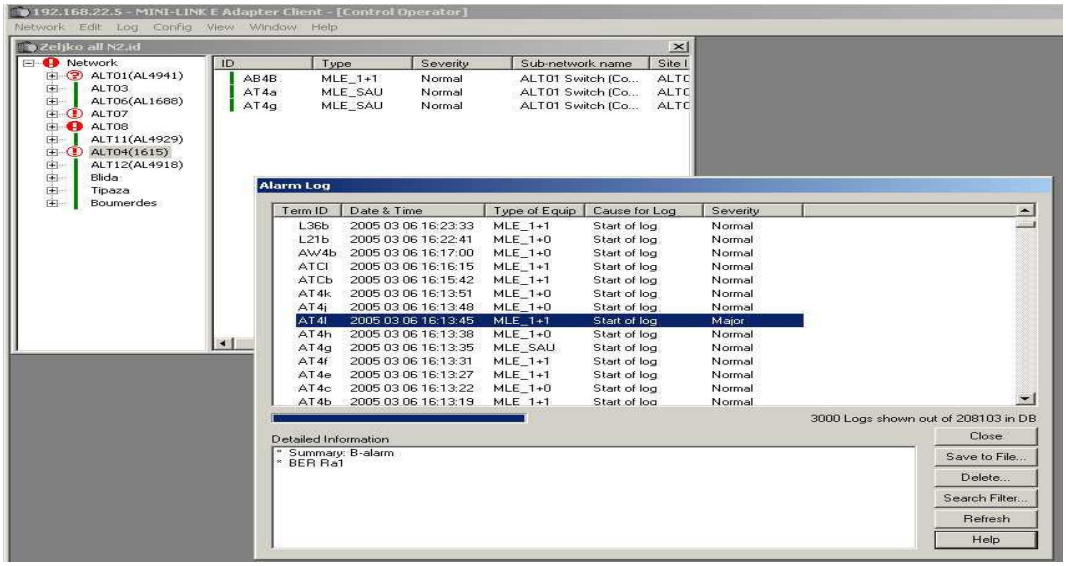


Fig.8. site en alarme par la commende LOG.

Glossaire

ABR: Area Border Router

AS: Autonomous System

ASBR: Autonomous System Border Router

AuC: Authentification Center

BDR: Backup Designated Router

BP: Bande Passante

BSC: Base Station Center

BSS: Base Station Sub-System

BTS : Base Transceiver Station

CLUSTER de MINI-LINK : un groupe de différents nœuds de MINI-LINK

DBD: Data Base Description

DCN: Data Communication Network

DGW: Default Gate Way

DR: Designated Router

FTP: File Transfer Protocol.

GSM: Global System for Mobile Communications

HC: Heigh Capacity

HLR: Home Localisator Regester

HTTP: Hyper Text Transport Protocol.

IGMP: Internet Group Management Protocol.

ICMP: Internet Control Message Protocol.

ISO: International Organization for Standardization

LAN: Local Area Network

LCT: Local Crafts Terminal

LSA: Link State Advertisement

LSAak: Link Sate Acknowledgement

LSR: Link State Request

LSU: Link State Update

MAN: Metropolitan Area Network

MLM: Mini-Link Manager

MMUs : Modem Unit

MS: Mobile Système

MSC: Mobile Switching Center

NSS: Network Switching Sub system

OMC: Operation and Maintenance Centre

OSI: Open System Interconnection.

OSS: Operation Sub System

OSPF: Open Short Path First

PDH: (Plesiochronous Digital Hierarchy)

PPP: Point-to-Point Protocol

QOS: Quality of Service

RBS: Radio Base Station

RNC: Radio Network Control

SAU: Service Access Unit

SDH: Synchronous Digital Hierarchy

SMU: Switch Multiplexer Unit

SMTP: Simple Mail Transfer Protocol

SOM: ServiceOn Microwave

SUG: Software UpGrade (Mise à niveau de logiciel)

TCP/IP: Transmission Control Protocol/Internet Protocol

TN: Trafic Node

TS: Terminal Server

UITT: Union Internationale de Télégraphie et Télécommunication

USB: Autobus de publication périodique universelle

WAN: Wilde Area Network

Bibliographie

Ouvrage:

 [1] réseaux GSM-DSC, GoDlewski, Langage, HEREMES [1997].

 [2] les architectures des réseaux mobiles: Charles Hartmann ; Remi Thomas [2003] ENST

 [3] system de communication, Base de transmission, PG fontolliet, dunod, 1984.

 [4] SDH (norme, réseaux et services). Tayeb ben Meriem, springer, 2000.

Documents:

[5] MINI-LINK DCN. Dsign and dimensioning, description, Ericsson.

[6] DCN_GUIDE LINES_1_15443-FGB101004_1_EN_G_PDFV1R4, Ericsson.

[7] ML-TN R4-ML-EProduct Catalog, Outdoor & Accessories ETSI.

[8] DCN_REF_NETWORK_1_19583-FGB101004_1_EN_PDFV1R4, Ericsson.

Sites web:

[9] http://cisco.goffinet.org

[10] http://www.ariase.com/fr/guides/fibre-optique.html

[11] http://www.memoireonline.com/sommaires/informatique-telecommunications.html

[12] http://www.frameip.com

[13] http://www.ariase.com/fr/guides/fibre-optique.html

[14] www.cisco.fr/go/documentation/

Thèses d'ingéniorat d'état en télécommunication :

[15] Sécurité et Gestion de la Mobilité dans le Réseau GSM,

Présenté par : Mr. BOUTIOUTA Aboubakr

Encadré par : Mr. MEKALICHE Lahouari

Institut de télécommunication ABDELHAFID BOUSSOUF -ORAN-2005 « ITO »