Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations et des sigles

Abréviation	*Description*
ADS-(B/C)	**Automatic Dependant Surveillance (Broadcast/Contract)**
AES	**Advanced Encryption Standard**
AMHS	**Aernautical Message Handling system**
ASTERIX	**All purpose Structured Eurocontrol suRveillance eXchange**
ATC	**Air Trafic Control**
ATM	**Air Trafic Management**
ATN	**Aeronautical Telecommunication Network**
ATS	**Air Trafic Services**
ATSEP	**Air Traffic Safety Electronic personnel**
CADAS	**Comsoft Aeronautical Data Acces System**
CAFSAT	**Central Atlantic FIR SATellite**
CCR	**Centre de contrôle Régional**
CDNA	**Centre National de la défense aérienne**
CNCSA	**Centre National de Contrôle de la Securité Aérienne**
DES	**Digital Encryption Standard**
DNA	**Direction de la Navigation Aérienne**
E&M	**Ear and Mouth**
ESMS	**Enhanced System Managment Station**
FH	**Faiseau Hertzien**
FIR	**Flight Information Region**
FPL	**Flight Plan**
HDLC	**High-Level Data Link Control**

IA5	International Alphabet N° 5
IP	Internet Protocol
ISO	International Organization for Standardization
ITA2	International Telegraph Alphabet N°2
L2TP	Layer 2 Tunniling Protocol
LAN	Local Area Network
LGD	Ligne à Grande Distance
LS	Ligne specialisée
MPLS	MultiProtocol Label Switching
Nm	Nautical mile – Mile nautique
NOTAM	NOTice to Air Men
OACI(ICAO)	Organisation de l'Aviation Civil International
ONDA	Office Nationale des Aéroports
OSI	Open Systems Interconnection
Pan	Procedures for Air Navigations
PPP	NavigationPoint to Point Protocol
PSR	Primary surveillance Radar
QoS	Quality of Service
Radar	Radio Detection And Ranging
RNIS(ISDN)	Réseau Numérique à Intégration de Services
RSFTA(AFTN)	Réseau des Services Fixes de Télécommunication Aéronautique
RTC	Réseau Téléphonique commuté
RTP	Real-time Transport Protocole
SARP	Standards And Recomended Procedures
SIP	Session Initiation Protocol
SR	Site Radar
SR	Site Radio
SSR	Secondary Surveillance Radar
TCP	Transmission Control Protocol
UDP	User Datagramme Protocol
vLAN	Virtual LAN
VPN	Virtual Private Network
V-SAT	Verry Small Aperture Terminal
WAN	Wide Area Network

Remerciements

Je tiens à exprimer ma profonde reconnaissance à El Aouni ZAROIL responsable du service Radar/CIR de la division technique de l'aéroport Marrakech-Menara pour avoir accepté de m'encadrer et pour le soutient et l'aide qu'il m'a accordé.

Je remercie chaleureusement M. Abdellah MECHAQRANE mon encadrant universitaire ainsi que mon professeur à la FST, d'avoir accepté de m'encadrer, assister, orienter durant ma période de stage, les mots ne peuvent décrire à quel point je suis reconnaissant envers M. MECHAQRANE.

Mes remerciements à M. Abdelhadi GOUAAZRI chef de la section Radio-Navigation qui a été plus qu'un encadrant de stage, il m'a guidé et m'a orienté. Son encouragement permanent et son dynamisme organisateur m'ont énormément facilité la tâche. Je le remercie vivement pour tout.

Je tiens à remercier Mlle Sana ACHENOUR, Mme Faiza HAGCHI, Mme Asmae EL BOUKILI, Mme Ghizlane SAADA, M. Abdellatif TIMSAHI, M. Ali TAQBIBT, M. Hamza HAOUMI, M. Soufiane MALKI, M. Mohamed LAMSALHI, Mme Hasnaa HOUSSALI, Mlle Bouchra FARIHI, tous les cadres et les techniciens qui m'ont aidé à profiter des différents travaux sur terrain au cours de mon stage.

Que tous ceux, qui m'ont aidé, de près ou de loin, trouvent ici l'expression de mes sentiments les plus distingués.

Introduction générale

L'office national des aéroports a été fondé dans le but de garantir une gestion et un développement optimaux du secteur aéronautique au Maroc. Afin de réaliser sa mission principale, l'ONDA intègre de diverses outils, système et maintien des partenariats dans le but d'instaurer un niveau de sécurité et de qualité de service dans l'ensemble de son réseau aéroportuaire sur le territoire de notre pays.

Généralement, chaque aéroport suit une structure hiérarchique propre à lui. Marrakech-Ménara est composé de quatre divisions principales: Navigation aérienne, Exploitation aéroportuaire, Ressources humaines et la Division technique dans laquelle se trouve Radar/CIR. Ce service revêt une importance majeur pour la sécurité aérienne assurée par l'aéroport, c'est pourquoi la direction de l'aéroport attend toujours du personnel formant le service l'autonomie, l'efficience, la rapidité, l'efficacité et plus important l'implication totale à la contribution dans la sécurité aérienne.

Outre cet aspect important, la gestion de la sécurité aérienne doit également aspirer à un bon niveau et satisfaire les normes et standards la sécurité aérienne, imposés par l'organisme responsable de la standardisation. Afin d'arriver à cette finalité, la direction de l'aéroport met en collaboration la Division Navigation aérienne avec deux services de la Division technique (RadioNav et Radar/CIR). La première entité est responsable de l'exploitation des équipements et systèmes d'aide ou de surveillance et gestion de la navigation aérienne, alors que la deuxième doit garantir le bon fonctionnement de tous ces équipements et systèmes, tout en répondant aux requêtes du personnel de l'autre division.

Parfaitement conscient de ces enjeux, et en tant que deuxième plus important aéroport du Maroc après l'aéroport Mohammed V de Casablanca, Marrakech-Ménara vise toujours à améliorer la qualité de sécurité qu'il offre, en lançant des appels d'offre dans ce cadre et organisant des formations du personnel et répondant aux standards de sécurité imposé par l'OACI.

C'est dans ce cadre que s'inscrit mon projet de fin d'études. Il a pour objet l'étude du système de contrôle et de surveillance de la sécurité du trafic aérien utilisé à l'aéroport et la proposition d'une solution qui réponde aux normes et standards de sécurité imposés par l'OACI.

Le présent mémoire est structuré en cinq chapitres:

Le premier définit le contexte général du projet. Il comporte une présentation de l'organisme d'accueil.

Le deuxième chapitre porte sur le contexte théorique et l'étude des radars de surveillance aérienne.

Puis vient la partie de l'étude de l'existant, mise à part du système de contrôle du trafic aérien de l'aéroport. Ce chapitre commence par dresser les points que j'ai suivi durant mon étude et les points que j'ai suivi pour aborder la proposition de la solution.

Par la suite le document s'oriente vers la partie de la solution suggérée. Le quatrième chapitre représente une sorte de catalogue des technologies WAN et des solutions opérateurs ainsi que les exigences de l'OACI, sur lesquelles je me suis basé dans le choix de l'amélioration proposée, amélioration basée sur l'utilisation de plusieurs sources de détection pour n'en plus dépendre en une seule.

Le dernier chapitre traite en détail les parties de la conception du réseau VPN, qui est la solution que j'ai jugée optimale pour l'aéroport.

Le document se termine par une synthèse du travail réalisé.

Chapitre 1

Présentation de l'organisme d'accueil

Chapitre 1 : Présentation de l'organisme d'accueil

1. Présentation de l'ONDA :

1.1. Introduction :

La naissance de l'Office National Des Aéroports (ONDA), en 1990, procède d'une philosophie résolument orientée vers le futur, et qui pourrait tenir dans une trilogie : Développer le réseau aéroportuaire de manière à renforcer la liaison des différentes régions entre elles et avec l'extérieur, moderniser les infrastructures afin de doter le royaume des moyens les plus performants susceptibles d'assurer le maximum de sécurité, d'efficacité et de confort aux utilisateurs des aérogares et enfin, mettre en place une gestion rationnelle à même d'optimiser l'exploitation des ressources.

L'ONDA est un établissement public à caractère industriel et commercial doté de la personnalité et de l'autonomie financière. Il est placé sous la tutelle du Ministère du Transport et le contrôle du Ministère des Finances.

La mission de l'ONDA s'articule autour de 5 principaux axes stratégiques:

- Restauration de la confiance avec les parties prenantes
- Recadrage stratégique du plan d'Investissement
- Renforcement de la culture client
- Gouvernance, Organisation & RH
- Coopération internationale

L'ONDA encourage sans relâche la collaboration entre les aéroports et joue un rôle de coordination, ainsi par exemple, après avoir été à l'origine de la création des associations des aéroports arabes et maghrébins, il en assure aujourd'hui la présidence de même, il plaide en faveur d'une coopération interafricaine. Les compétences de son institut de formation, l'IFGEA (Institut de Formation en Gestion et Exploitation Aéroportuaires) sont constamment sollicitées par d'autres pays. A ce titre, l'IFGEA, sera amené à développer, dans le cadre de relations de partenariat des programmes pédagogiques pour le compte de pays tiers. Enfin ; c'est encore l'ONDA qui a participé, à titre d'organisme conseil, à l'édification des structures de l'aviation palestinienne et à la construction de son réseau d'aéroports.

L'extension progressive des attributions de l'ONDA est la meilleure preuve du bien - fondé de ses options stratégiques de départ.

1.2. Historique :

Jusqu'en 1980, les aéroports et les services de navigation aérienne étaient directement gérés par l'administration (Ministère du Transport).

Avec la construction et la mise en service du terminal de l'aéroport Mohammed V à cette date, le Gouvernement décida d'opter pour l'autonomie de gestion, avec la création en 1980 du premier établissement public de gestion aéroportuaire ; l'OAC (Office des Aéroports de Casablanca), dont les attributions ont été initialement limitées aux aéroports de Casablanca.

L'OAC a constitué la première étape du nouveau régime de gestion aéroportuaire : il a été mis en place conformément à la haute vision Royale de Feu le Roi Hassan II : « Nous nous sommes résolus à développer, à élargir et à moderniser le réseau des communications, à multiplier les aéroports et à les rehausser au niveau des aéroports occidentaux les plus prestigieux » Discours du trône du 03 mars 1981.

Ce bilan positif a été un facteur déterminant dans la décision d'extension de cette première expérience à l'ensemble des aéroports nationaux.

Ainsi, les prérogatives de l'OAC ont été graduellement et progressivement étendues pour couvrir finalement à partir de 1990 la totalité des aéroports et des services de la Navigation Aérienne.

Ce renforcement par paliers des compétences de l'Etablissement, découle d'un choix délibéré, et d'une vision stratégique, en vue d'assurer le développement optimal du secteur aéronautique.

L'ONDA est créée en vertu du décret n° 2-89-480 du 1er joumada II 1410 (30 décembre 1989) pris pour l'application de la loi n° 14-89 transformant l'Office aéroports de Casablanca en Office National Des Aéroports.

La démarche de développement de cet important Office fut couronnée par la Décision Royale intervenue en 1991, rattachant l'ensemble des services de la Navigation Aérienne à l'ONDA, en vue de consolider le rôle de l'établissement pour une action plus large en faveur du secteur aéronautique.

1.3. Les directions de l'ONDA

1.3.1. La Logistique et du Développement Commercial

La direction est chargée de :

- Instruire les dossiers à caractère général qui lui sont confiés par la Direction Générale
- Gérer les affaires à caractère médical et social
- Etablir et exécuter un programme d'audit et de contrôle des unités
- Traiter les questions d'ordre juridique
- Evaluer et gérer le patrimoine foncier de l'Etablissement
- Coordonner l'activité des salons dans les aéroports.

1.3.2. Direction de la Communication et des Affaires Générales

La direction est chargée de :

- Instruire les dossiers à caractère général qui lui sont confiés par la Direction Générale
- Gérer les affaires à caractère médical et social
- Etablir et exécuter un programme d'audit et de contrôle des unités
- Traiter les questions d'ordre juridique
- Evaluer et gérer le patrimoine foncier de l'Etablissement
- Coordonner l'activité des salons dans les aéroports.

1.3.3. Direction d'Ingénierie

Elle se charge de :

- tout ce qui est planification technique, notamment :
- Les études techniques des programmes d'investissement
- Les entretiens et les études planifiés et préventifs des équipements et infrastructures

1.3.4. Direction de la Navigation Aérienne

La Direction de la Navigation aérienne a pour missions :

- Définir et mettre en œuvre le dispositif de la navigation aérienne de l'Office qui satisfait aux exigences de sécurité et de services de l'ensemble des usagers aériens
- Apporter un support permanent aux entités opérationnelles de la Navigation Aérienne par tous les moyens appropriés et notamment des procédures et normes de contrôle aérien.

1.3.5. Direction de la Qualité, de la Sûreté et de la Sécurité

La Direction de la Navigation aérienne a pour missions :

- définir et mettre en œuvre le dispositif de la navigation aérienne de l'Office qui satisfait aux exigences de sécurité et de services de l'ensemble des usagers aériens
- Apporter un support permanent aux entités opérationnelles de la Navigation Aérienne par tous les moyens appropriés et notamment des procédures et normes de contrôle aérien.

2. Aéroport de Marrakech :

L'aéroport international Marrakech-Ménara (code AITA : RAK • code OACI : GMMK) est l'aéroport principal de Marrakech. En 2014, c'est le deuxième plus important aéroport du Maroc : plus de 4 millions de passagers y transitent chaque année.

2.1. Fiche technique de l'aéroport :

TABLEAU 1 : FICHE TECHNIQUE DE L'AEROPORT MARRAKECH MENARA

	Aéroport Marrakech Mènera
Avion critique	**B. 747 - Pax : 400**
MTOW	**370000**
Longueur piste (m)	**3100**
LDA (m)	**3100**
Largeur de piste (m)	**45**
Largeur taxiway (m)	**23**
Sécurité incendie	**Cat 7**
Air Trafic Contrôle	**D**
Equipements aéronautiques ILS/VOR/DME	**10 CAT I ILS/VOR/DME**
Equipements aéronautiques Papi / Vasis	**28 Papi 2,5° - 10 papi 3°**

2.2. Organigramme de l'aéroport :

L'aéroport Marrakech Ménara suit la forme ci-dessus, Un **Directeur délégué de l'aéroport** qui communique directement avec des chefs de divisions et des responsables de services particuliers. **Les chefs de division** jouent le rôle d'interface entre le DPT/Commandant de l'aéroport et les chefs de services, ainsi ils leurs rôles se voit très nécessaires dans la gestion du bon fonctionnement de l'aéroport. Alors qu'un **chef de service** est supposé de gérer, superviser et orienter le travail de toute une équipe d'opérateurs, techniciens ou contrôleurs. Les services particuliers ont chacun leurs missions à exécuter, par exemple **le service de permanence** remplace le DPT/Commandant de l'aéroport lors de son absence ; **Le Service système Management Qualité et Environnement** à pour taches de maintenir le niveau de qualité certifié pour l'aéroport conforme à la norme ISO 9001/2000 ; **le Service gestion de la sûreté** n'est d'autre que l'intermédiaire entre la direction de l'aéroport et l'extérieur, les organisme de sûreté ; et dernièrement **le Service CIR** se charge de gérer les formations.

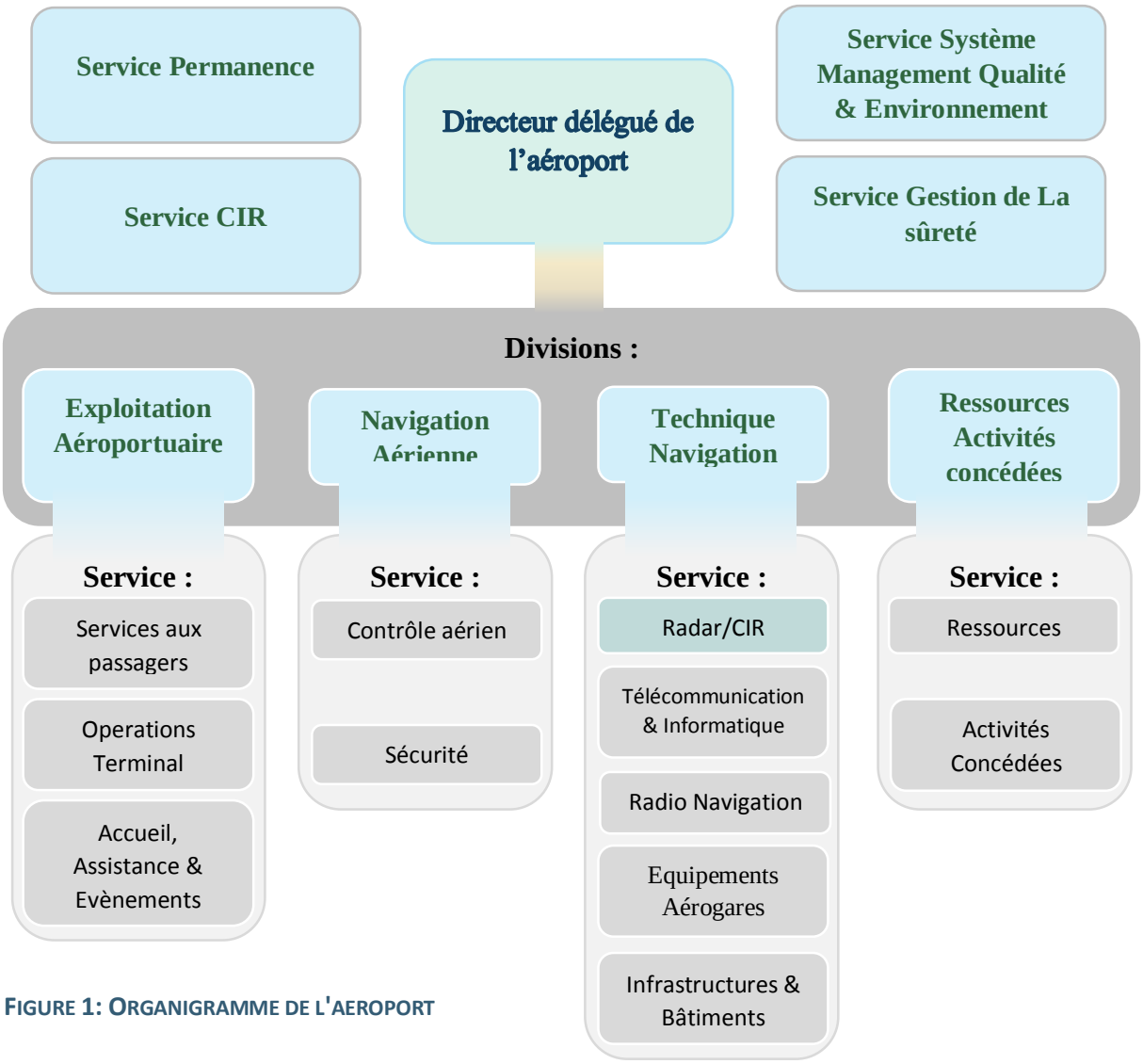


FIGURE 1: ORGANIGRAMME DE L'AEROPORT

2.3. Division technique :

Cette division a pour rôle principale de maintenir tous les équipements de l'aéroport en état de fonctionnement. Les équipements qu'ils soient informatique, de supervision, contrôle, télécommunication, électrique ou électronique et qui sont utilisés par les autres divisions.

2.4. Service Radar/CIR (lieu de mon stage) :

Ce service se compose principalement des ingénieurs électroniciens des systèmes de la sécurité aérienne (ESA), supervisés par un chef de service et chef de division. Le travail des ESA consiste à maintenir le bon fonctionnement de tout équipement dédié au système Radar de l'aéroport, qui a pour utilité aider, guider, et assister les aéronefs dans leur tâches (décollage, atterrissage).

Chapitre 2

Contexte théorique : les Radar de contrôle aérien

Chapitre 2 : Contexte théorique : les systèmes de surveillance du contrôle aérien

1. Les systèmes de la surveillance du trafic aérien :

La surveillance est l'outil de base des contrôleurs aériens pour gérer d'une façon sûre et efficace le trafic aérien. Les systèmes de surveillance du trafic aérien dont dispose la DNA (Direction Nationale Aérienne) sont utilisés pour le contrôle d'en route et d'approche et sont principalement le Radar primaire, le Radar secondaire et l'ADS. Les informations de surveillance telles que la position, l'identification, l'altitude et la vitesse des avions vont permettre de réduire l'espacement entre les avions tout en conservant le niveau de sécurité requis pour l'espace aérien concerné.

Ainsi les systèmes de surveillance jouent un rôle capital dans la gestion et le contrôle du trafic aérien. Les données de surveillances fournies par les différentes stations de surveillances sont reçus au niveau du CNCSA et sont ensuite traitées et associées aux données plans de vol, ou itinéraires de vol, avant de les produire sur des stations de visualisation permettant ainsi de disposer d'informations complètes sur le trafic aérien évoluant dans le ciel marocain.

1.1 Surveillance indépendante – Radar primaire :

Un radar primaire (**P**rimary **S**urveillance **R**adar) utilise le principe de la réflexion des ondes électromagnétiques, c'est un système de surveillance indépendante. La station mesure l'écart de temps entre l'émission de l'impulsion et la réception de l'onde réfléchie sur la cible pour en déduire la distance de celle-ci. La position de la cible est déterminée en mesurant l'azimut de l'antenne à l'instant de la réception.

Les réflexions se produisent sur les cibles (les avions), mais aussi sur des objets fixes (immeubles) ou mobiles (camions) non désirés, ce qui tend à créer des parasites. La fonction "traitement" du radar est chargée de l'élimination de ceux-ci.

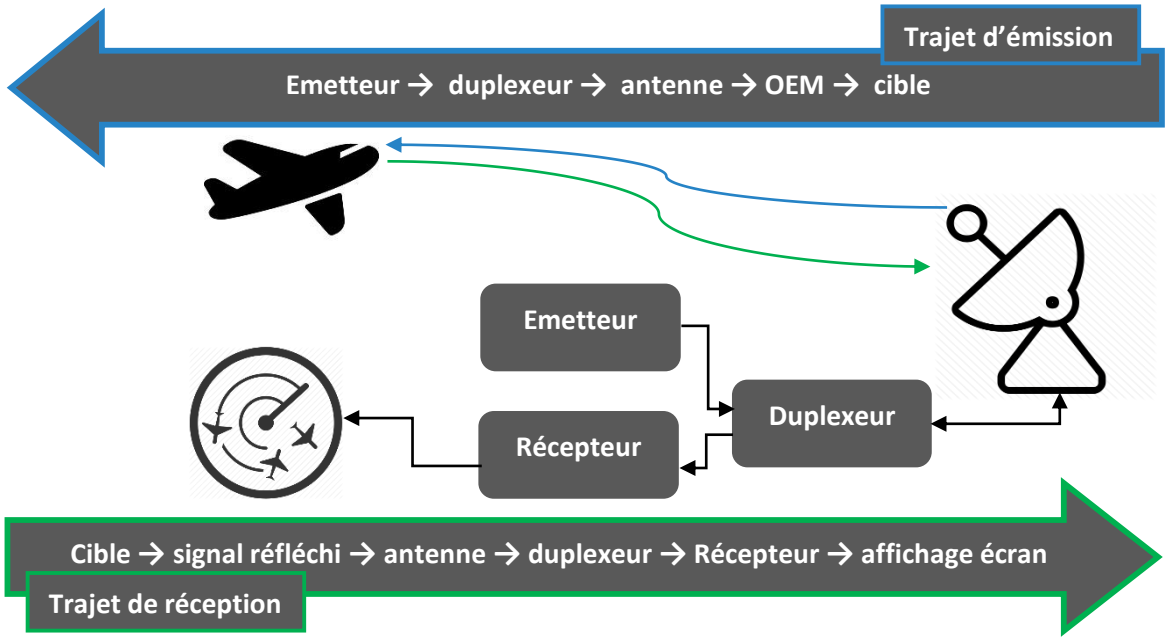


FIGURE 2: PRINCIPE DU RADAR PRIMAIRE

Les avantages du radar primaire sont :

- Aucun équipement embarqué n'est nécessaire pour la détection de la cible, ce qui permet la détection des cibles non-coopératives
- Il peut être utilisé pour la surveillance au sol

Les inconvénients du radar primaire sont :

- La détection d'échos indésirables (Clutter, brouillage, bruit de fond…)
- La nécessité d'un traitement complexe
- Il nécessite des émissions puissantes, ce qui tend à limiter la portée (60 NM)

1.2. Surveillance semi-dépendante – Radar secondaire:

Un radar secondaire (**S**econdary **S**urveillance **R**adar) est composé de deux éléments : **une station sol** interrogatrice et un **transpondeur** embarqué dans l'avion. Le transpondeur répond aux interrogations de la station, la renseignant sur sa distance et son azimut. Le radar secondaire permet les fonctions de détection, mesure de la distance et d'azimut sans collaboration avec l'aéronef, alors que le transpondeur offre les données supplémentaires comme l'indentification et l'altitude, ce qui le classe dans la catégorie de la surveillance semi-dépendante.

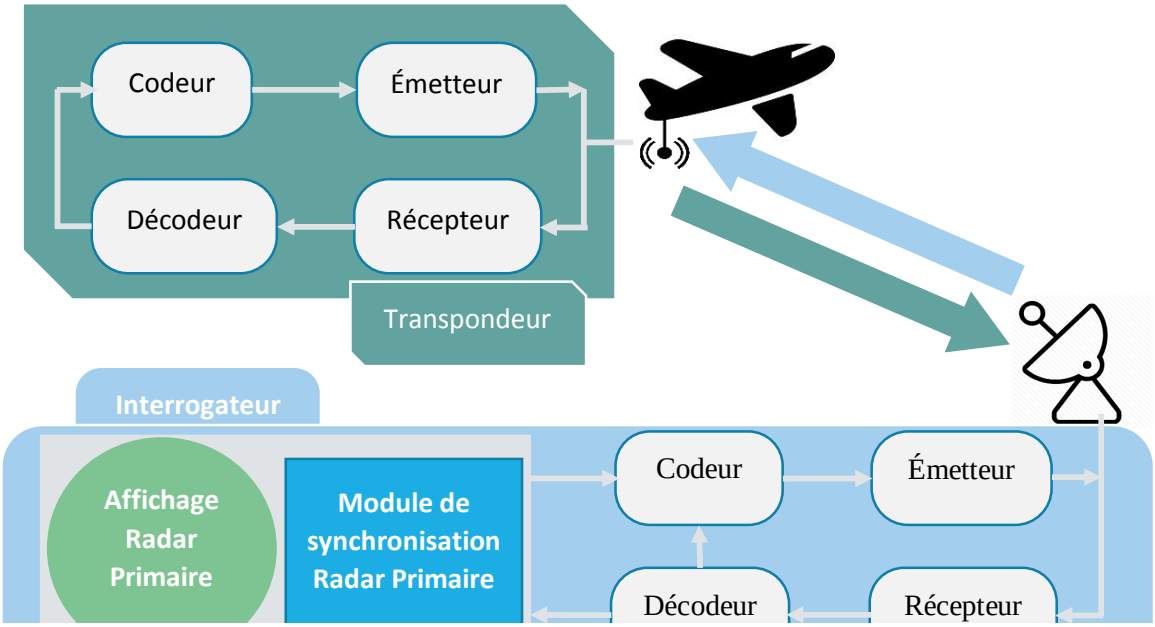


FIGURE 3: PRINCIPE DE FONCTIONNEMENT DU SSR

Interrogateur :

- Le mode est choisi par le codeur (par des modes différents différentes questions peuvent être posés).
- Ces impulsions sont modulées par le transmetteur.

Transpondeur :

Une antenne réceptrice et un transpondeur se trouvent au bord de l'avion.

- Le récepteur amplifie et démodule les interrogations.
- Le décodeur décode les questions propres à chaque information voulue et induit le codeur à préparer les réponses souhaitées.
- Ces impulsions sont modulées et amplifiées par le transmetteur.

L'émetteur Radar émet trois impulsions P1, P2 et P3 et interroge la cible de son identification (Δt (P1, P3)= 8µs) et de son altitude (Δt (P1, P3)= 21µs). Le transpondeur répond par un train de 12 impulsions indiquant le code réponse souhaitée. L'impulsion P2 est utilisée pour inhiber les interrogations et réponses sur les lobes secondaires de

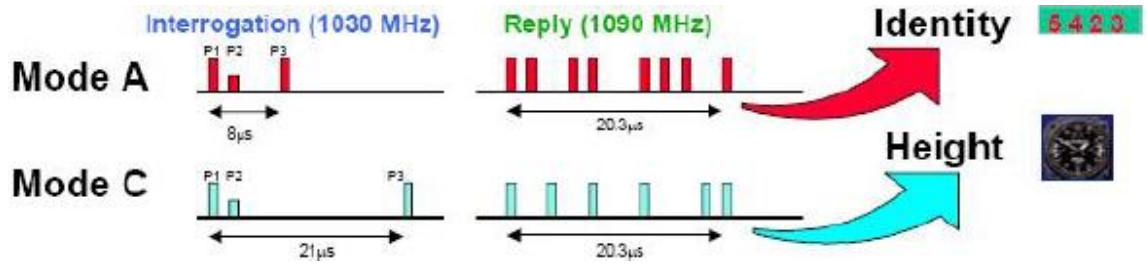


FIGURE 4: EXEMPLE D'INTERROGATION REPONSE

l'antenne Radar, il faut mentionner que la portée du Radar secondaire atteint les 255 NM.

Les avantages du SSR sont :

- La détermination de l'identité et de l'altitude, en plus de la distance et de l'azimut.
- Il est beaucoup moins sujet aux parasites que le radar primaire.
- Sa portée est beaucoup plus importante que celle du radar primaire, étant donné que l'interrogation et la réponse n'ont que la distance aller à parcourir.
- Le Mode S introduit l'avantage de liaison de données air/sol.

Les inconvénients du SSR sont :

- Il ne convient pas à la surveillance au sol, à cause de la perte de précision introduite par le délai de traitement du transpondeur.
- Les systèmes mode A/C connaissent de nombreux problèmes d'enchevêtrement des réponses et de réception de réponses non-sollicitées. Le Mode S résout ces problèmes en interrogeant sélectivement les cibles.

Le mode S :

Le Mode S est une amélioration du Mode A/C. Il en contient toutes les fonctions, mais permet également une interrogation sélective des cibles grâce à l'utilisation d'une adresse unique codée sur 24 bits, ainsi qu'une liaison de données bidirectionnelle permettant l'échange d'informations air/sol.

- **S** pour **S**électif pour interrogation unique (en anglais: Selective Unique Interrogation). Il permet une adresse unique de 24-bits attribuée par l'autorité nationale de l'aviation ;
- Il augmente la qualité des données en utilisant une bit de parité dans les mots informatiques ;
- Il augmente la précision de la donnée d'altitude à 25 pieds (8 mètres) au lieu de 100 pieds antérieurement.

Donc le SSR Mode S est un système de surveillance enrichie (qui résout les problèmes du Radar secondaire), il permet au système au sol d'acquérir automatiquement les indicatifs d'appel des aéronefs, surmontant ainsi les problèmes liés à l'allocation et à l'assignation des codes SSR, en plus d'une liaison de données permettant au système au sol d'acquérir automatiquement certaines données de bord qui améliorent la poursuite au sol de l'aéronef.

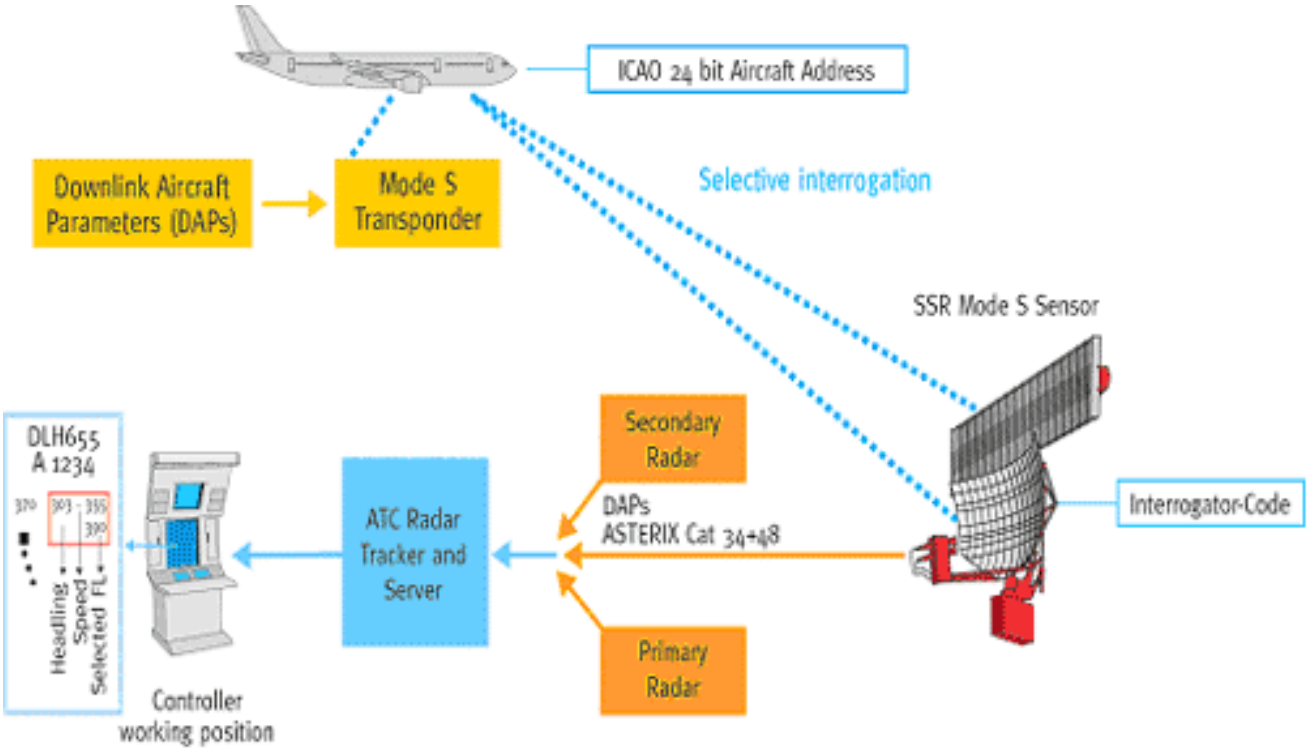


FIGURE 5: PRINCIPE DE FONCTIONNEMENT EN MODE S DE MSSR

Chapitre 3

Le système radar de l'aéroport Marrakech-Ménara

Chapitre 3 : Le système Radar de l'aéroport Marrakech-Ménara :

I. Cahier des charges :

1. Présentation du sujet de stage

Mon stage comporte comme objectif, la réalisation d'une étude d'une solution d'amélioration de la sécurité du système de surveillance du trafic aérien installé à l'aéroport Marrakech-Ménara. Ceci rentre dans le cadre du projet de la migration des du réseau de télécommunications aéronautiques, qui est utilisé pour le transport des données de surveillance – plans de voles – données vocales opérationnelles, vers la technologie IP et de proposer une conception de ce réseaux IP qui regroupe fiabilité et robustesse tout en restant dans les normes et exigences de l'OACI.

En effet ce projet doit permettre de :

- Renforcer l'autonomie et la continuité du système de surveillance en reliant l'aéroport Marrakech-Menara avec les plateformes aéroportuaires nationales et les différentes stations radio et radars des sites adjacents.
- Relier les plateformes aéroportuaires nationales entre elles et garantir un accès facile pour elles aux données Radar brutes et traitées.
- Diminuer le coût lié à l'utilisation des services opérateur de type liaisons louées.
- Répondre d'une façon flexible aux besoins de communications des futures extensions, modifications et intégration de nouveaux systèmes

2. Etude de l'existant

Pour proposer une solution permettant une migration vers un réseau IP, je suggère d'abord d'étudier le système actuel pour le déport des données de surveillance, messages de vol ainsi que les communications vocales et ce dans le but de repérer les vulnérabilités de ce dernier et de les prendre en compte dans le choix du réseau envisagé.

L'étude du système actuellement en exploitation est scindée en trois parties dont chacune traitera un type de données (surveillance, messages de vol ou voix), cette étude s'articule essentiellement autour des points suivants :

- Sources de données
- Moyens de déport
- Format ou interface utilisé

II. l'étude de l'existant :

1. le système de surveillance :

1.1. La surveillance indépendante - ATCR-33S :

ATCR-33S un radar primaire de la société Selex-SI qui assure la surveillance du trafic aérien supérieur des phases décollage/atterrissage, est utilisé à l'aéroport de Marrakech pour rester conforme aux normes internationales radar primaire (exigé soit par l'OACI ou l'Eurocontrol), et garantir un haut degré d'**autonomie** et de continuité de service.

Il fournit des capacités de traitement et de suivi de la performance prolongée afin de soutenir 24h d'exploitation. La surveillance et le contrôle des activités sont effectués à partir de stations locales (in-situ) ou distantes (salle IFR) à l'aide d'interface d'opérateur.

Le système ATCR-33S utilise une large gamme de techniques de traitement, qui optimisent automatiquement la performance opérationnelle sous la plus sévère Conditions environnementales.

La section de réception est entièrement **redondante**, avec les deux canaux de réception séparés et indépendants inclus au sein d'une seule armoire, ce qui permet d'adapter l'équipement aux exigences d'installation les plus critiques.

Le traitement est contrôlé par la méthode cell-by-cell, par un système de cartographie géographique très sophistiqué. Un canal météo intégré est inclus, offrant six niveaux des informations météorologiques selon la Direction Nationale de la Météorologie.

L'émetteur est modulaire et tolérant aux pannes, avec 8 modules d'alimentation inclus dans une seule armoire. L'étage de puissance RF utilise la plus récente technologie de transistor qui est basée sur le Nitrure de Gallium (GaN), permettant ainsi, d'augmenter en même temps puissance transmise, efficacité et fiabilité. Chaque module peut être retiré durant le fonctionnement « on-line » et il est muni d'une alimentation séparée pour une meilleure **autonomie**.

Les interfaces du système ATCR-33S équipées avec le groupe d'antennes du type **S-Band**, qui comprend l'antenne réflecteur parabolique G-33 en bande S, largement utilisé dans applications de la circulation aérienne civile et militaire dans le monde entier.

1.2. La surveillance semi-dépendante - Le radar SIR-S :

Le radar secondaire de l'aéroport de Marrakech SIR-S de la société Selex-SI, est un système modulaire entièrement conforme aux recommandations de l'OACI et EUROCONTROL, à propos du fonctionnement en Mode-S.

Ce système à double canal (dual channel) avec commutation automatique, émetteur et récepteur à l'état solide, conçu pour un fonctionnement sans pilote. Offre une configuration simple de canaux. Chaque canal SSR se compose d'un émetteur, un récepteur et un automate/extracteur programmable.

La plate-forme de traitement puissant est basée sur le matériel COTS, totalement programmable par logiciel, afin d'exploiter l'amélioration des plates-formes commerciales et prévenir les problèmes obsolètes. En outre, il fournit toutes des fonctions programmables des unités émettrices et réceptrices.

L'antenne généralement utilisé en conjonction avec le capteur de l'antenne LVA ALE-9, conçu pour une utilisation complètement Monopulse. Elle fournit des propriétés hautement directionnelles et la « vertical aperture », comme c'est recommandé par l'OACI, également nécessaire pour la surveillance en mode S améliorée (EHS).

SIR-S est la partie pertinente du système Mode-S SELEX SI et, selon la configuration du système, il peut fonctionner en SSR mode conventionnel, Surveillance primaire, surveillance améliorée jusqu'à Mode S complet opérant sur le Data-link et employant des transpondeurs niveau 5.

Aucun changement de matériel n'est nécessaire pour mettre à niveau le système d'une configuration à une autre.

d) les équipements du SIR-S :

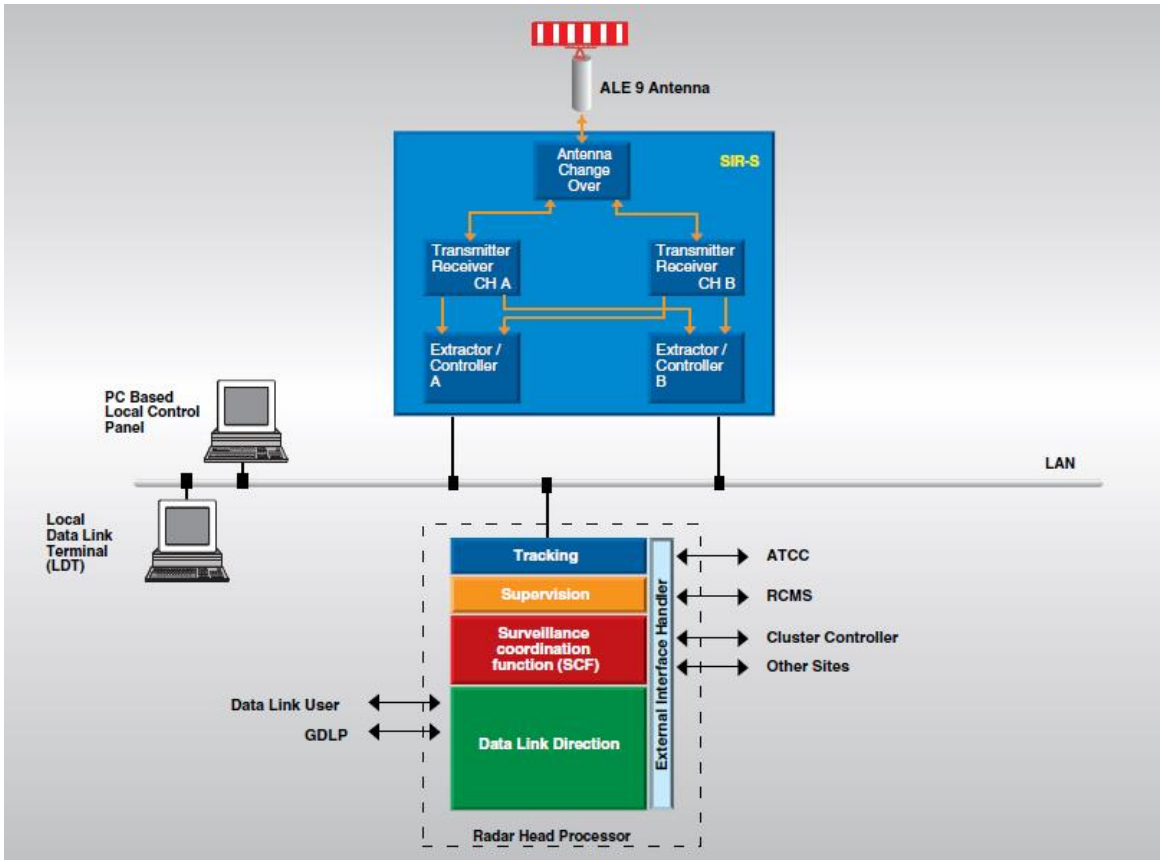


FIGURE 6 : SYSTEME MODE-S (SIR-S + RADAR HEAD PROCESSOR) CONFIGURATION DU MODE-S COMPLET

1.3. Couverture et sites au Maroc :

La couverture de notre espace aérien est assurée par sept stations radars nationale MSSR mode S niveau 2 installées dans les villes suivantes : Agadir, Casa, Ifrane, Safi, El Jadida, Oujda, Tantan, Marrakech, Fes et Tanger et par deux station internationales de

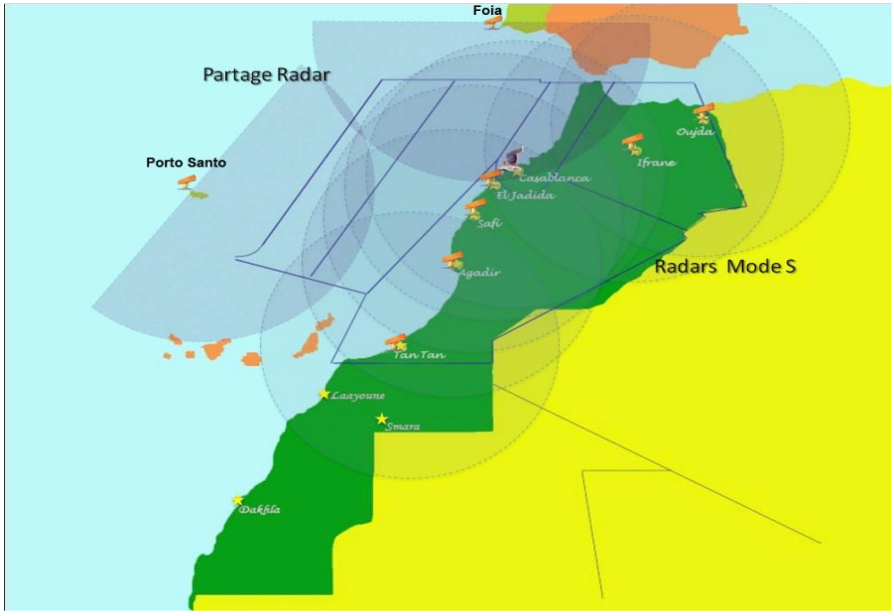


FIGURE 8: COUVERTURE RADAR AU MAROC

partage Foia et Porto santo.

La couverture ADS est assuré par trois stations ADS-B implantées dans les villes

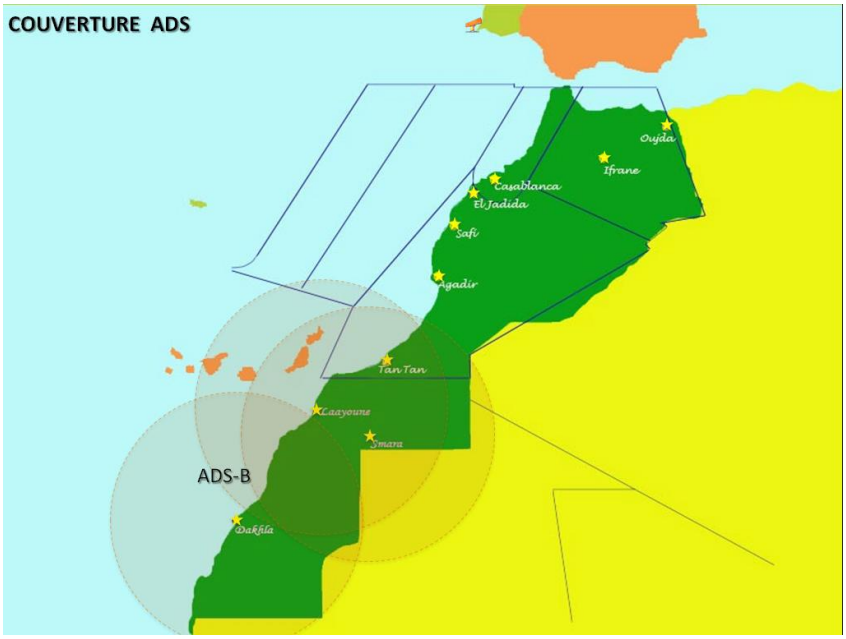


FIGURE 7: COUVERTURE ADS AU MAROC

suivantes: Smara, Dakhla et Laayoune, il est prévu de faire recours à l'ADS-C pour renforcer le contrôle du secteur océanique dans un future proche.

1.4. Format de données radar :

Les messages parvenant de la station Radar sont véhiculés à l'aéroport sous format ASTERIX (All Purpose STructured Eurocontrol Radar Information EXchange). L'expansion des domaines d'application d'ASTERIX a mené à une modification de la signification de l'acronyme ASTERIX, se tenant maintenant pour All Purpose STructured Eurocontrol SuRveillance Information EXchange.

Son but est de permettre un transfert significatif d'information entre deux entités d'application en utilisant une représentation convenable des données pour être échangé.

ASTERIX est un protocole d'application/présentation responsable de la soutenance des données développées pour la surveillance des données transmises et échangées.

Structure générale du message :

En ce qui concerne le standard ASTERIX (ISO 7498), il se réfère aux couches présentation et application comme définit par OSI (Open System Interconnection) le protocole HDLC LAP B étant la couche liaison des données.

Les couches présentation et application définissent le format de données dans l'ASTERIX DATA BLOCK comme il est montré dans le diagramme HDLC FRAME.

Un message Radar ASTERIX est composé de plusieurs pistes auxquelles sont attribuées des plots qui sont en fait les échos captés par le Radar. On suppose dans notre étude que l'association plot piste doit être effectuée correctement c'est-à-dire que les plots correspondants à un message.

En effet un message ASTERIX est divisé en plusieurs blocs contenant les plots captés dans un même secteur.

Un bloc a la forme suivante :

- les deux premiers octets définissent la taille du bloc
- les six suivants sont des octets de padding.

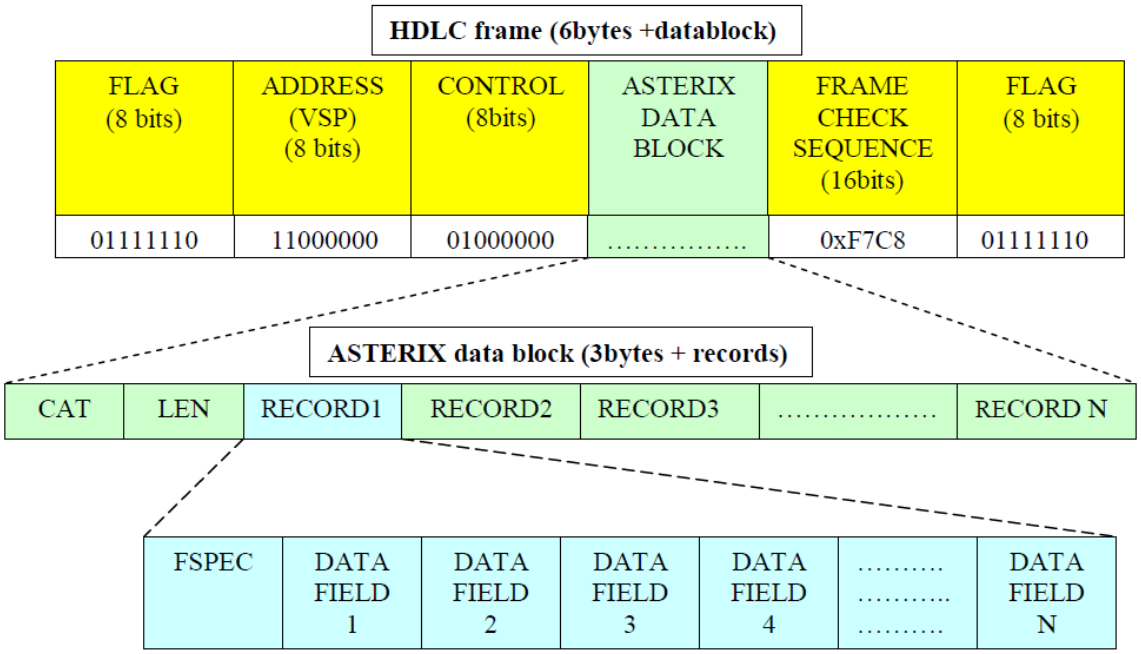


FIGURE 9: TRAME HDLC

1.5. Moyens de transport des données du site de détection vers l'aéroport :

Les données issues du site de détection de Marrakech sont acheminées vers le centre de contrôle d'approche (IFR) de l'aéroport Marrakech Menara via une liaison FH, une image de ses données est acheminée vers le CIR via Fibre optique et vers CNCSA via une liaison E1 à travers le réseau Maroc Telecom. Pour cela, plusieurs techniques de transmission sont utilisées : fibre optique, faisceau hertzien ou ligne spécialisée (LS).

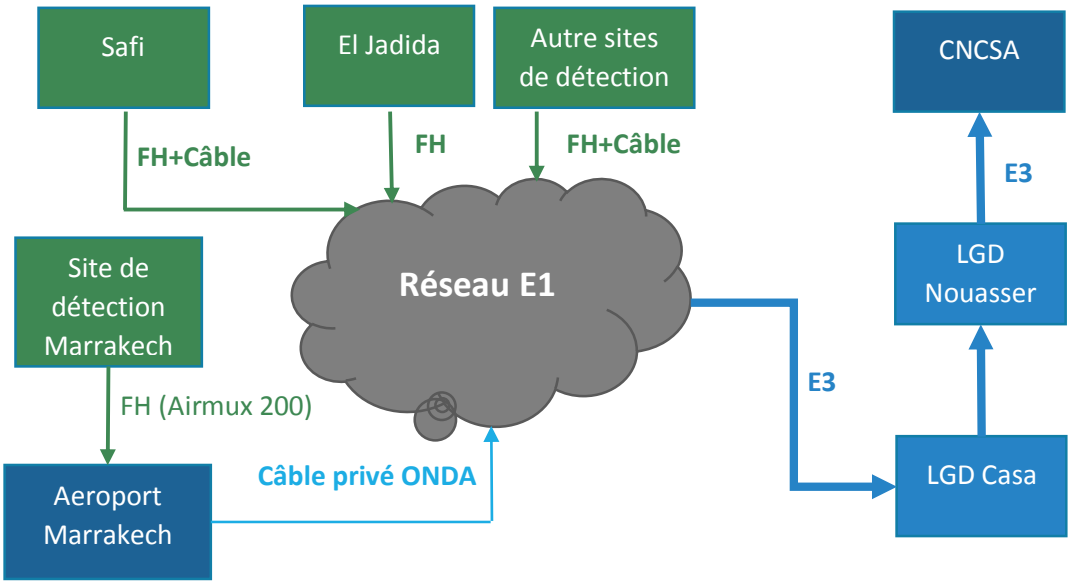


FIGURE 10: MOYENS DE TRANSPORT DES DONNEES RADAR

2.1. Fibre Optique :

C’est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestres et océaniques de données. Elle offre un débit d'informations nettement supérieur à celui des câbles coaxiaux et supporte un réseau « large bande » par lequel peuvent transiter plusieurs données (la télévision, le téléphone, la visioconférence ou les données informatiques)

Avantages de la fibre optique

Les intérêts de ce procédé de transmission par fibre optique, à priori exotique, sont nombreux :

- perte de signal sur une grande distance bien plus faible que lors d'une transmission électrique dans un conducteur métallique,
- vitesses de transmission très élevées,
- poids au mètre faible (c'est important, aussi bien pour réduire le poids qu'exercent les installations complexes dans les bâtiments, que pour réduire la traction des longs câbles à leurs extrémités),
- Insensibilité aux interférences extérieures (proximité d'un néon ou d'un câble à haute tension, par exemple),
- Pas d'échauffement (à haute fréquence le cuivre chauffe, il faut le refroidir pour obtenir des débits très élevés).

Inconvénients de la fibre optique :

- Difficultés d’adaptation avec les transducteurs optoélectroniques
- Exigences micromécaniques importantes (connexions, alignement)
- Coûts d’exploitation encore élevés et personnel spécialisé Pour le déport des données depuis le CNCSA vers LGD Nousasser, deux multiplexeurs de fibre optique de type Alcatel 1521 FL et 1531FL sont utilisés.

2.2. Les Faisceaux Hertziens

Un faisceau hertzien est une liaison radioélectrique point à point ou point à multipoint, bilatérale et permanente (full duplex), à ondes directives, offrant une liaison de bonne qualité et sûre permettant la transmission d'informations en mode multiplex à plus ou moins grande capacité, de 3 à 60 voies. Cependant sa propagation est limitée à l’horizon optique porté de l’ordre de 40km.

Les différents équipements réalisés permettent notamment des transmissions

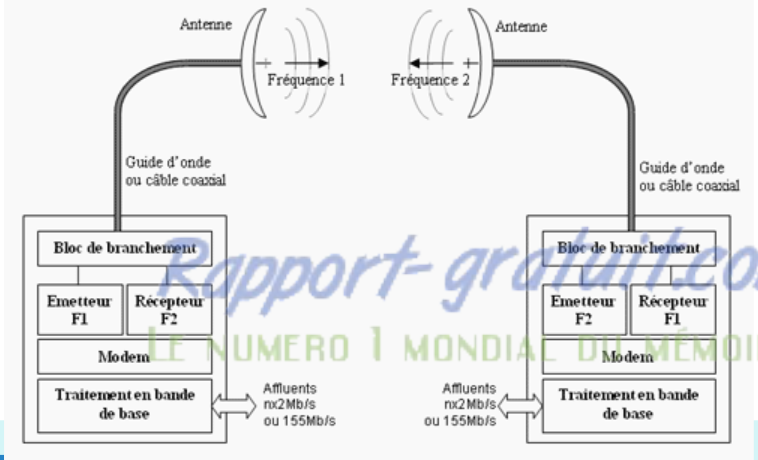


FIGURE 11: LES FAISCEAUX HERTZIENS

numériques aux débits : 2 Mbit/s, 34 Mbit/s, 2*34 Mbit/s et 140Mbit/s

Le faisceau hertzien est destiné à assurer la liaison entre la station radar et le centre LGD (côté urbain) pour le déport des données radar. Il fonctionne en modulation QAM 64 et utilise des fréquences porteuses de 1GHz à 40GHz (domaine des microondes).

Ces ondes sont principalement sensibles aux obstacles (relief, végétation, bâtiments,...), aux précipitations, aux conditions de réfractivité de l'atmosphère et présentent une sensibilité assez forte aux phénomènes de réflexion.

Les faisceaux hertziens utilisés au Maroc sont généralement de type Alcatel 9413UX et Harris Stratex Eclipse, pour le cas d'entre le site de détection et l'aéroport Marrakech sont de type Airmux 200.

La liaison qui relie le site de détection à Douar Soltan à la salle IFR (Système Radar Selex-SI) de l'aéroport Marrakech-Ménara, est une liaison sans-fil composée principalement des faisceaux hertziens.

FIGURE 12: AIRMUX 200

L'Airmux 200 est composée de :

- L'ODU (outdoor unit) est un système radio opérationnel dans la bande des 2.3-2.9 GHz et 4.9-6.0 GHz
- L'IDU (indoor unit) et L'IDU-E (enhanced indoor unit) sont des équipements dotés d'interfaces pour relier les utilisateurs au système radio
- Antenne externe ou intégrée composée d'un panneau ou d'une grille avec simple d'un panneau ou d'une grille avec simple

2.3. Ligne louée :

On appelle lignes "louées" des lignes spécialisées (notées parfois LS) qui permettent la transmission de données à moyens et hauts débits (64 Kbps à 140 Mbps) en liaison point à point ou multipoints (service Transfix).

En Europe, on distingue cinq types de lignes selon leurs débits alors qu'aux Etats-Unis seulement quatre types existent.

Norme Européenne	Norme Américaine
E0 (64Kbps)	
E1 = 32 lignes E0 (2Mbps)	T1 (1.544 Mbps)
E2 = 128 lignes E0 (8Mbps)	T2 = 4 lignes T1 (6 Mbps)
E3 = 16 lignes E1 (34Mbps)	T3 = 28 lignes T1 (45 Mbps).
E4 = 64 lignes E1 (140Mbps)	T4 = 168 lignes T1 (275 Mbps).

Pour les stations nationales, le service choisi est E1, qui est une liaison dédiée à cette application (LS 2Mbps).

Ces moyens sont secourus par une liaison satellitaire alors que pour les sites de partage les données sont principalement transportées par satellite (VSAT).

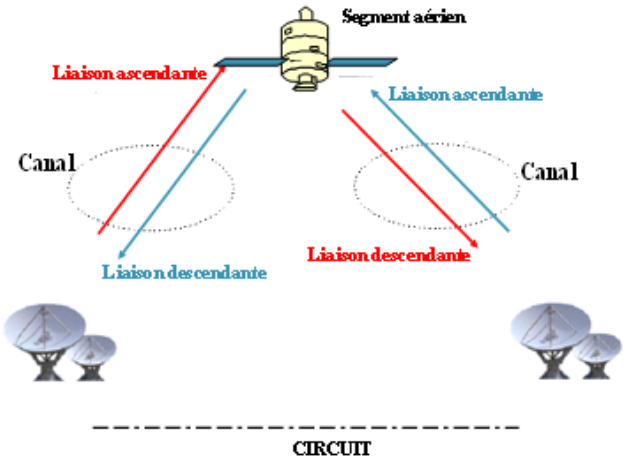
2.4. V-SAT (Very Small Aperture Terminal)

La communication par satellite consiste en l'utilisation d'une station relai dans l'espace (le satellite) servant à relier deux stations émetteurs/récepteurs hertziens au sol.

La notion « VSAT » ou « terminaux à très petite ouverture » est destinée pour désigner les petites stations terrestres équipées d'antennes dont la taille est comprise en général entre 0,96 m et 2,4 m de diamètre.

La technologie VSAT est une alternative économique aux systèmes de communications basés sur le satellite et est employée dans de nombreuses applications de télécommunications, telles que la voix, les données et la vidéo.

Le bon fonctionnement d'un satellite dépend de plusieurs conditions depuis la phase d'installation telle l'orientation de l'antenne voire les conditions de l'environnement (le vent par exemple).



Les services de télécommunications par satellite utilisent une partie étroite de la capacité totale du satellite grâce à un terminal d'émission-réception de petite dimension permettant l'échange d'informations à bas ou moyen débit.

On distingue deux réseaux VSAT au niveau de notre territoire :

- Réseau VSAT national
- Réseau VSAT international : CAFSAT

B) RESEAU V-SAT NATIONAL :

Le réseau VSAT nationale assure le déport des données Radar autant que secours pour l'ensemble des sites nationaux, en outre c'est la liaison principale utilisé pour le déport des données depuis les Radars de partage (FOI et PORTO SANTO).

Ce réseau VSAT est utilisé également pour les autres applications de données et de voix Le réseau national englobe 10 stations déportées, le nœud de réseau étant le centre CNCSA du Casablanca qui assure la coordination entre les autres stations.

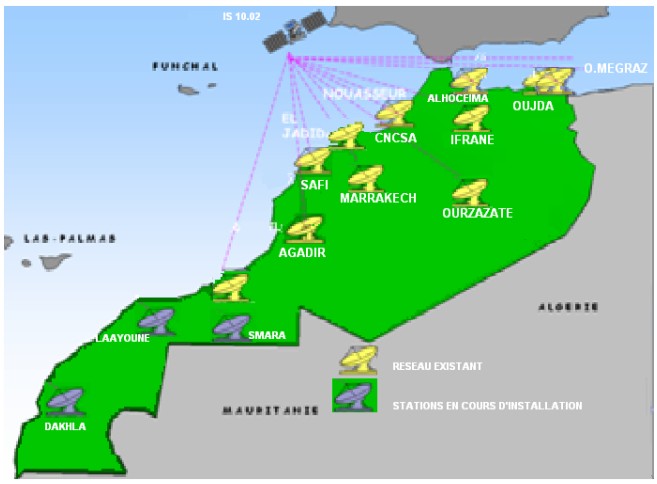


FIGURE 13: RESEAU DES STATIONS NATIONALES DEPORTEES

2. Les Données AFTN/AMHS :

Les données de vols sont issue de Casablanca vu que le Centre Com de Casablanca est la Division Traitement de l'Information qui est qui est un centre de commutation automatique de messages considéré comme une porte d'entrée/sortie Afrique/Europe d'un Réseau mondial d'usage général pour transmettre et recevoir des messages **AFTN–AMHS**.

Des informations sont échangées entre sites ou entités d'un même ou plusieurs pays. Ces messages échangés et normalisés par l'OACI sont :

1. Message de détresse.
2. Messages d'urgence.
3. Messages intéressants la sécurité des vols.
4. Messages NOTAM (Notice To Air Men).
5. Messages administratifs aéronautiques.
6. Messages météorologiques.
7. Messages de service.
8. Messages de location de places.
9. Messages généraux d'exploitation d'aéronefs.
10. Messages intéressant la régularité des vols.

On distingue alors 2 réseaux assurant l'acheminement de ces informations :

- Réseau AFTN
- Réseau AMHS

2.1. Système AFTN :

Le RSFTA est un réseau mondial de circuits fixes aéronautiques destiné, dans le cadre du service fixe aéronautique, à L'échange de messages et/ou de données numériques entre stations fixes aéronautiques ayant des caractéristiques de communication identiques ou compatibles.

Historiquement le RSFTA a été spécifié pour être traité par des procédures manuelles, néanmoins ces procédures ont pu être automatisées et adaptées à l'informatisation.

Les messages échangés sur le RSFTA sont affectés d'un indicateur de priorité qui détermine la priorité de transmission. Ces indicateurs sont, du plus prioritaire au moins prioritaire :

- SS : Trafic de détresse et d'urgence.
- DD : Messages nécessitant un acheminement spécial.
- FF : Messages intéressant la sécurité des vols.
- GG : Messages météo, messages de service et administratif, Messages intéressant la régularité des vols.
- KK : Utilise par les exploitants

a) Mode d'échange et codage de données

Le mode d'échange des données dans le réseau RSFTA est le mode asynchrone.

L'Annexe 10 de l'OACI, définit 2 types de codages qui peuvent être utilisés :

- ITA-2 où chaque caractère est codé sur 5 bits
- IA5 où chaque caractère est codé sur 7 bits (IA5 est très peu différent de l'ASCII qui est l'implémentation américaine de l'IA5).

b) Format

En fonction du code utilisé, le format de message est différent. Principalement, les différences sont : le début du message, le début du texte et la fin d'un message. Ainsi en ITA-2 le début d'un message est la suite de caractères « ZCZC» et en IA-5 c'est la combinaison «SOH».

c) Composition d'un message

Le contenu d'un message RSFTA contient un entête et une information utile.

- L'entête possède comme éléments: la référence de la ligne sur laquelle le message est reçu ou envoyé, le numéro de message dans la journée en cours sur cette ligne donnée, la priorité du message, les adresses destinataires, le numéro du jour dans le mois en cours, le temps et l'adresse origine.
- l'information utile contient le message texte dont la longueur ne doit pas dépasser 1800 caractères donc la longueur du message (entête + texte) ne dépasse pas 2100.

d) Adressage RSFTA

Les adresses sont codées sur 8 caractères exactement. Les adresses destinataires sont au nombre de 21 au maximum.

2.2. Système AMHS :

L'AMHS défini par l'OACI pour l'échange de messages à travers le réseau aéronautique avec le protocole de transport **TCP/IP**.

Le système **AMHS** permet la commutation, la réception, le routage et l'archivage des messages aéronautiques.

L'AMHS est basé sur les standards internationaux X.400 ISO : technologies fiables et matures. Ce système offre les avantages suivants :

- Vitesse et capacité augmentée
- Fiabilité et sécurité des communications
- Riche fonctionnalité (par exemple : la possibilité de joindre des fichiers)

a) Composants du modèle X400

Le X400 est un modèle de messagerie normalisée, il repose sur des modules indépendants :

- MTA: agent de transfert des messages : correspond à un serveur e-mail et permet le stockage et l'acheminement des messages et la communication des MTAs, MSs et UAs, il permet également la collecte et la distribution du courier.
- MS : message store, il assure la connexion entre un MTA à un UA et permet de stocker les messages.
- UA : agent utilisateur (client e-mail), c'est l'interface qui interagit avec le MTS pour soumettre et recevoir les messages et assure la connexion de MTA et MS.

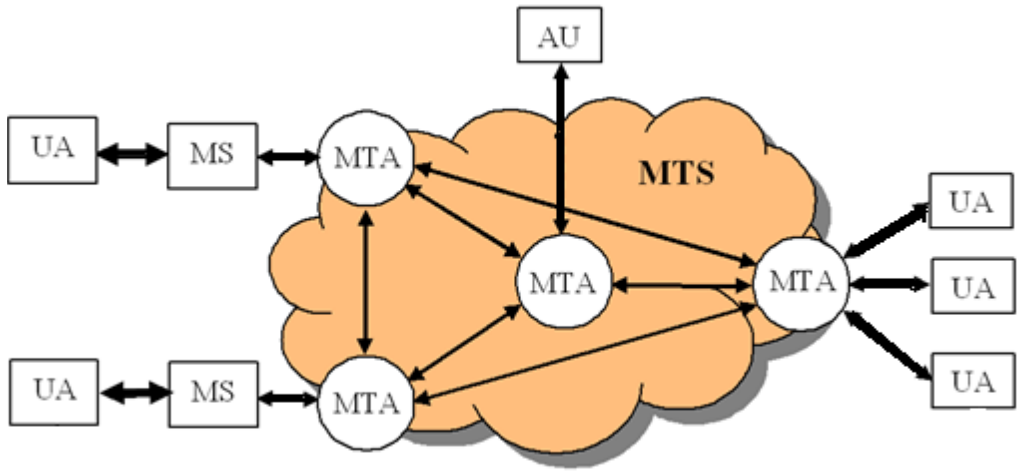


FIGURE 14: RESEAU X400

On note que le MTS (Message Transfert System) est le système de transfert de message reliant plusieurs MTAs, le AU (Access Unit) fonctionne comme une passerelle de message entre différent réseaux.

Pour assurer le fonctionnement du modèle, les recommandations X400 définissent différents protocoles de communication pour le routage des messages :

P1 : assure la communication MTA<-->MTA

P2 : pour la communication UA<-->UA

P3 : permet la communication UA<-->MTA ou MS<-->MTA

P7 : pour qu'un UA communique avec un MS

b) Positions AMHS

- La position OWP : (Operator Working Position) à partir de cette position, on peut créer des messages AFTN, des messages AFTN de test et des messages AMHS.
- La position CADAS : (Comsoft Aeronautical Data Acces System) permet d'échanger procéder et visualiser des messages ATS, il comprend un serveur cluster CADAS installé à la salle technique (MTA), et des terminaux CADAS placé dans les aéroports (UA).
- La position ESMS :(Enhanced System Managment Station), c'est un système de contrôle et de surveillance par l'intermédiaire du protocole SNMP

c) Adressage:

Une adresse AMHS permet d'identifier un utilisateur AMHS dans le réseau et montre la position de l'adresse dans une structure hiérarchique.

L'adresse AMHS se caractérise par plusieurs attributs et la conversion d'adresse

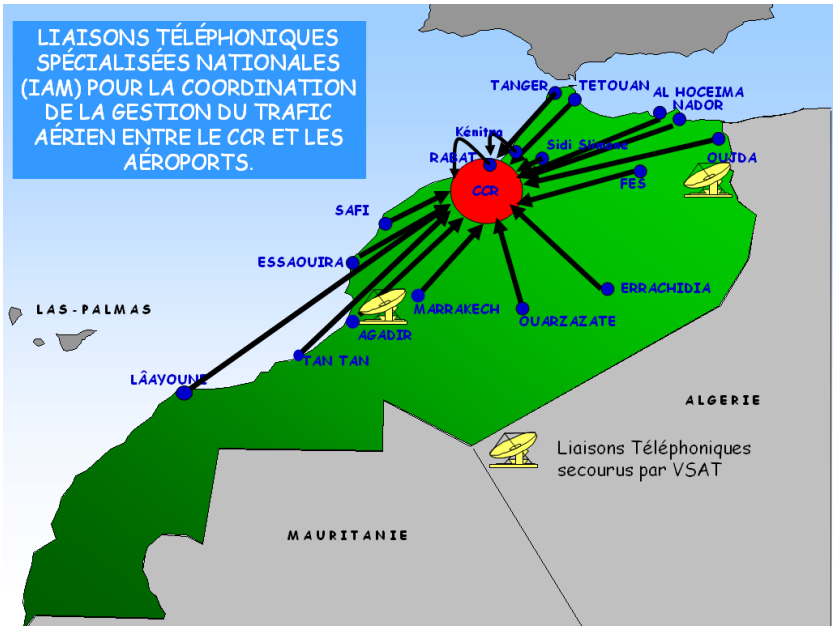
AFTN en adresse AMHS se fait en utilisant un tableau look up générique ou utilisateur (tableau contenant les correspondances AFTN-AMHS).

3. Données vocales :

L'aéroport de Marrakech reçoit des données vocales du contrôle des avions, issue du CNCSA sous forme de message sol-sol, par une interface E&M.

L'interface E&M qui désigne les méthodes de signalisation permettant d'initier et de gérer des connexions vocales sur un lien analogique à 4 fils. Ear (E) désigne la signalisation reçue et Mouth (M) la signalisation émise.

Le CNCSA est relié à l'ensemble des aéroports/sites radars du Maroc, formant le



réseau téléphonique national pour le contrôle et la gestion du trafic aérien.

III. Expression du besoin :

Vu que le système actuel de communications de données Radar, données de vol et voix est basé sur des liaisons de transmission point à point, certes efficaces mais plus couteuses et moins adaptables aux nouvelles applications CNS/ATM et puisque l'ensemble des applications ATS sont dans des sites éloignés géographiquement les uns des autres, à savoir stations, aéroports et centres, la mise en place d'un réseau capable de répondre aux besoins de connectivité et de performances pour l'ensemble des applications s'avère nécessaire.

Face à ces exigences il a été jugé souhaitable de s'orienter vers une architecture réseau basé sur le modèle TCP/IP totalement sécurisé et permettant des communications point-multipoint tout en gardant l'ensemble des installations et systèmes de surveillance, données de vol et communications vocales existantes.

En effet on peut résumer les différentes exigences qu'il faut satisfaire lors de l'établissement du réseau reliant les sites du Maroc sous IP dans les points suivants :

- Les données à acheminer sont données Radar, messages de vol (AFTN/AMHS) et la voix.
- Le réseau doit supporter voix et données analogiques et numériques.
- Il faut prendre en considération d'intégrer l'infrastructure de télécommunications existante (stations satellite, faisceaux hertziens et fibre optique) dans la conception du réseau de l'aéroport sous IP.

- Le réseau de l'aéroport sous IP doit être sécurisé et à l'abri de toute attaque ou intrusion.
- L'architecture du réseau proposé doit permettre la communication entre les différents sites de la DNA (connexion any to any, au cas de généralisation de la solution pour toutes les plateformes de la DNA) et doit supporter toute extension future et intégration de nouveaux systèmes.
- Comme une absence de données est intolérable, alors il faut prévoir une solution alternative pour acheminer les données en cas d'anomalies affectant le réseau (voie de secours).
- La solution réseau doit supporter des mécanismes pour faire face à des situations de congestion du réseau et un éventuel système d'attribution de priorités pour le trafic acheminé.

La deuxième partie de ce rapport présentera la solution que j'ai apportée pour concevoir un réseau de télécommunications aéronautiques de l'aéroport Marrakech-Ménara sous IP.

Chapitre 4

Technologies WAN et services opérateur

Chapitre 4 : Technologies WAN et Solutions opérateurs

I- Technologies WAN :

Les architectures qu'on va présenter ici définissent des modes de communication dont chacun de ces modes modélise un service opérateur. Ces services peuvent être classés selon leurs modes de transport en 3 types :

- Services Point à point
- Services de commutation de circuits
- Services de commutation de paquets

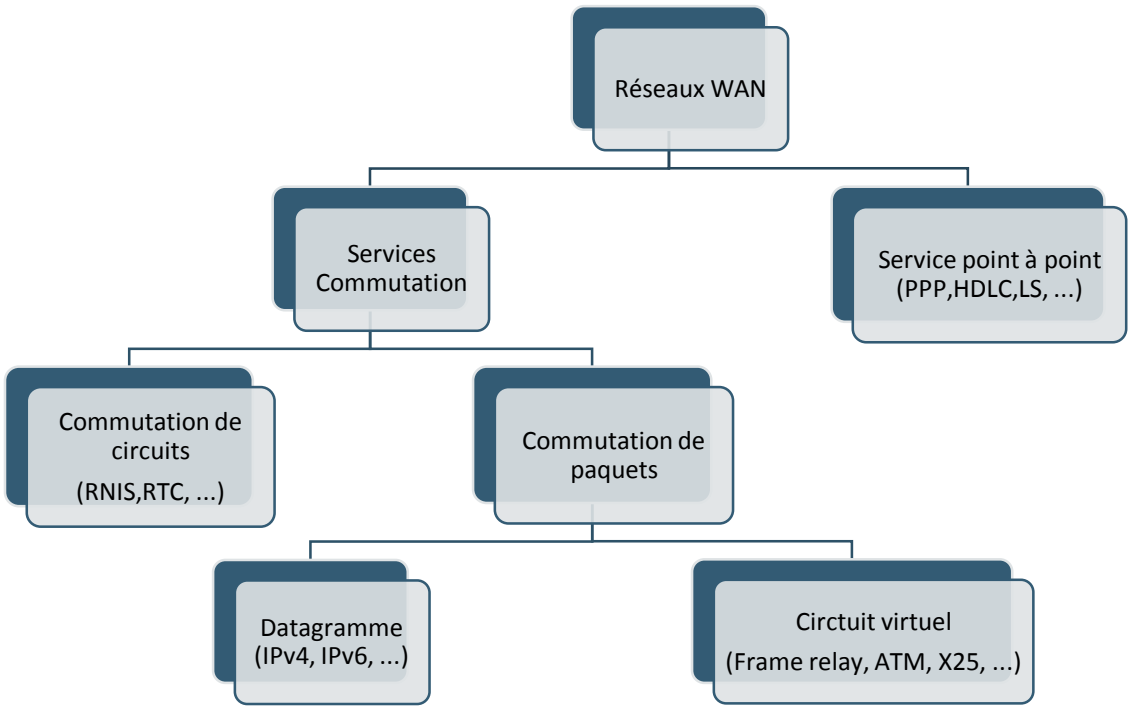


FIGURE 15: MODES DE COMMUNICATIONS DES RESEAUX WAN

1. Services point-à-point

Les liaisons point-à-point sont généralement utilisé sous-forme de liaisons louées. En effet une liaison point-à-point est un lien préétablie, à travers le réseau du fournisseur, allant d'un site vers un autre distant.

La liaison point-à-point n'est pas conçue pour être utilisée initialement dans un réseau, vu que la notion native d'adresse réseau des deux hôtes, ni de contrôle avancé du

flux n'existe pas. Par contre des protocoles comme le PPP, HDLC et SLIP sont utilisé pour pallier les limitations de cette liaison et l'utilisé dans un réseau. Les liaisons Point-à-Point sont facturées à base de la distance entre sites et la bande passante souhaitée, ce qui la rend plus couteuse que les services partagées.

Parmi les inconvénients que cette liaison présente, est quand un équipement A veut communiquer avec un autre équipement B auquel il n'est pas relié directement, il faut soit recourir à l'aide de l'équipement centrale C ou bien de substituer une éventuelle liaison entre les deux, et c'est le cas pour le reste de chaque équipement avec un autre.

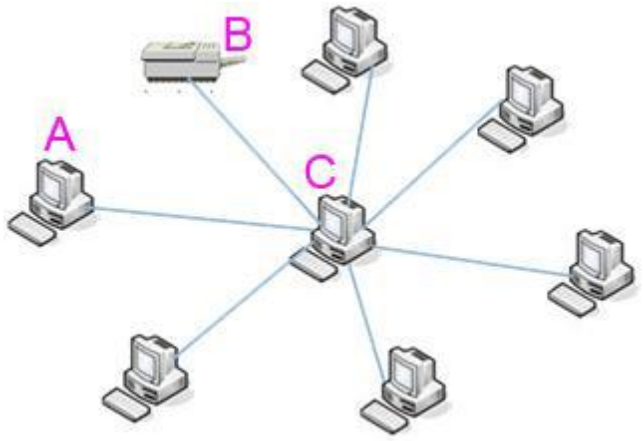


FIGURE 16: TOPOLOGIE D'UNE LIAISON POINT-A-POINT

2. commutation de circuits

Elle consiste à établir un branchement matériel de lignes joignant des terminaux. Les informations échangées parcourent toujours le même chemin au sein du réseau durant le temps de la session. On peut considérer cette méthode de transfert de données avec réservation de ressources, vu qu'un maintien de canal physique doit être maintenu durant toute la communication, ce qui implique la possibilité du **gaspillage de la bande passante**. Cette méthode est souvent utilisée dans le RTC et le RNIS(ISDN).

Ce service est orienté communication, et on distingue trois étapes :

- Etablissement de la connexion (réservation d'un chemin)
- Transfert de l'information

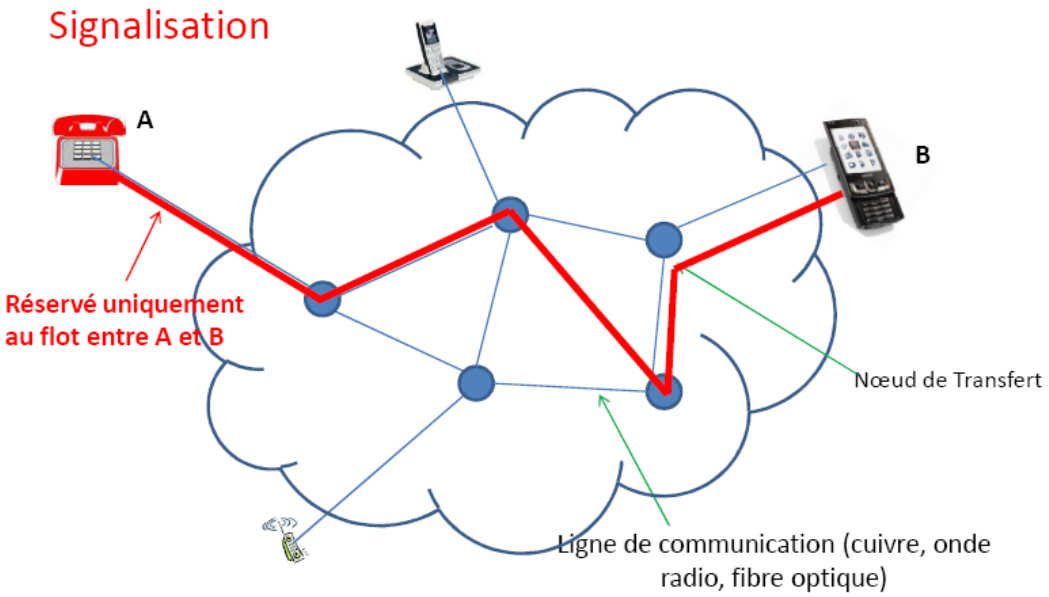


FIGURE 17 : COMMUTATION DE CIRCUIT

- Libération du canal (chemin)

3. commutation des paquets

La commutation des paquets et une technologie WAN permettant aux utilisateurs de partager le ressources (Bandes passantes) et gère d'une manière efficace les infrastructures du réseau, quant au cout pour le client est beaucoup plus optimal que les

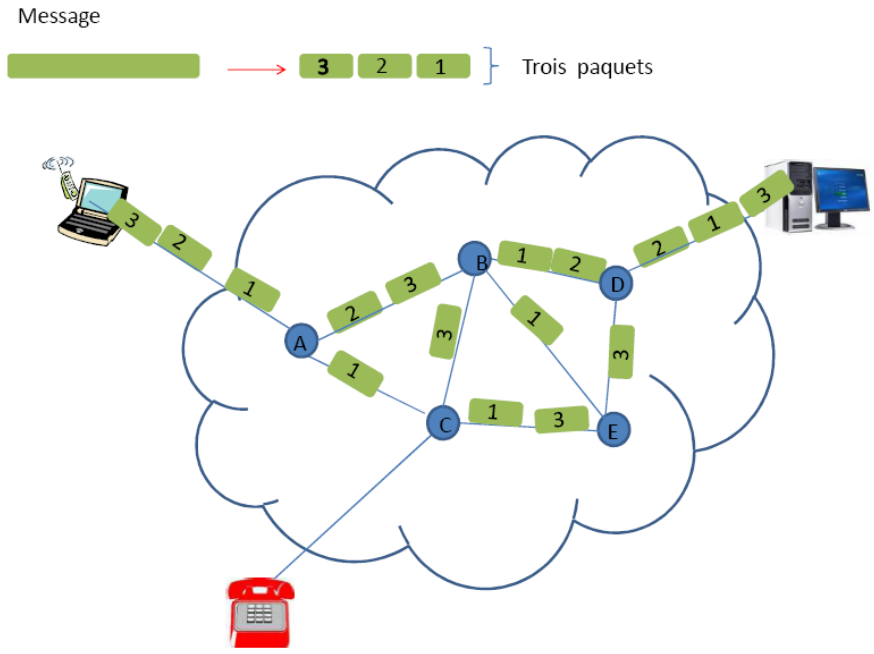


FIGURE 18: RESEAU A COMMUTATION DE PAQUETS

lignes point à point.

Lors de la transmission des données en commutation de paquets, les données sont découpées en plusieurs paquets envoyés séparément.

On distingue deux modes de commutations de paquets Datagramme et Circuit virtuel.

- Mode Circuit virtuel

Un circuit virtuel est une sorte de circuit logique établie dans un réseau partagé entre deux équipements réseau. Dans ce mode un chemin logique au travers du réseau est choisi entre l'origine et la destination. Une fois le chemin logique et établie dans des conditions normales, les données le parcourent. En cas de défaillance un autre chemin et sélectionné.

- Mode Datagramme

Dans ce mode les nœuds du réseau déterminent le chemin de chaque paquet individuellement, selon leur table de routage.

Les paquets arrivent en désodre

4. réseaux IP

Un réseau IP est indépendant par rapport au matériel, il permet aussi d'établir une connexion entre deux équipements chacun appartenant à un réseau différent.

Un réseau IP se caractérise par une architecture logique indépendante de tout réseau particulier, tout en interconnectant ses réseaux entre eux afin que les machines et ordinateurs puissent communiquer sans savoir quel réseau ils utilisent ou comment l'information circule dans ce dernier.

Le fait que les réseaux IP soient « des réseaux non orienté connexion » et à commutation de paquets constitue certainement une caractéristique distinctive présentant ses avantages et inconvénients, mais celle-ci est surement moins importante que les deux caractéristiques l'intelligence aux bords en plus du routage dynamique.

Protocole IP :

Le protocole IP détermine l'adresse du destinataire à l'aide de trois champs :

- Champ adresse IP : adresse de la machine
- Le champ masque de sous-réseau : un masque de réseau permet au protocole d'identifier la partie de l'adresse propre au réseau
- Le champ passerelle par défaut (default Gateway) : permet au protocole IP de reconnaitre la machine à laquelle il doit transmettre le paquet au cas où l'adresse de destination ne figure pas sur le réseau local.

Les données qui circulent sur internet sont sous-forme de datagrammes qui sont

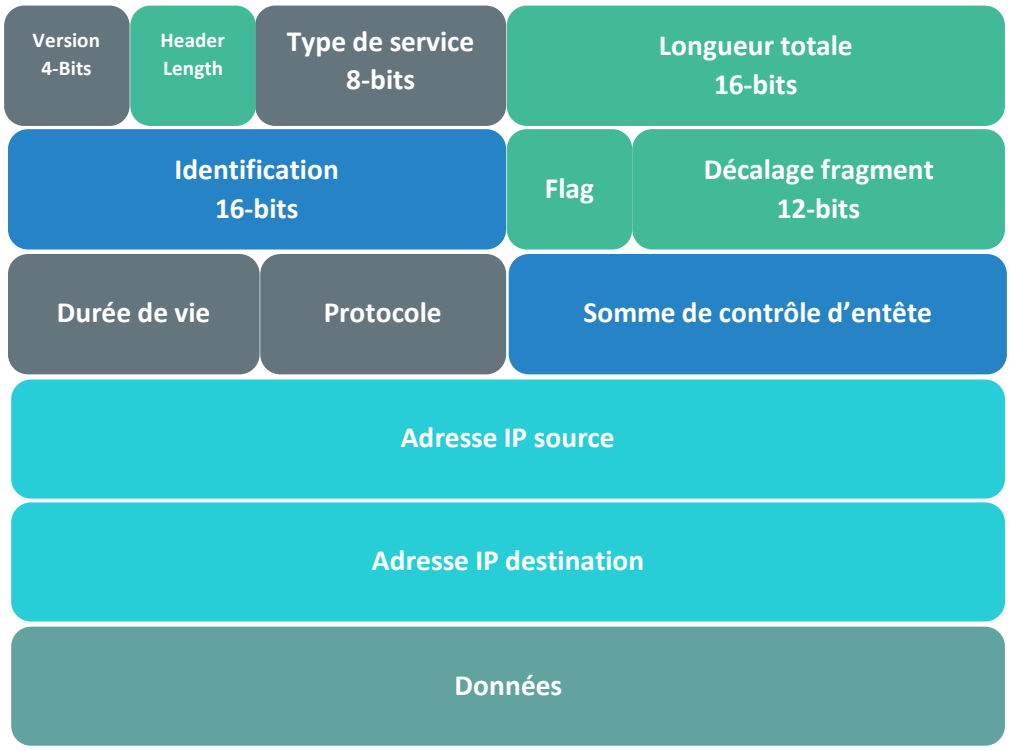


FIGURE 19 : ENTETE IPV4

vérifiés au niveau des routeurs avant de permettre leur transit.

Signification des champs :

Version (4 bits) : il s'agit de la version du protocole IP qu'on utilise IPv4 (utilisé actuellement) ou IPv6 (en cours de développement) afin de vérifier la validité du datagramme.

Longueur d'en-tête, ou **IHL** pour Internet Header Length **(4 bits) :** il s'agit du nombre de mots de 32 bits constituant l'en-tête.

Type de service (8 bits) : ce champ joue un rôle très important dans l'acheminement des informations en VPN, il indique la façon selon laquelle le datagramme doit être traité ce qui sera utile dans la définition des classes de services des applications. En affectant des numéros désignant la priorité, en cas de congestion le routeur traitera davantage les paquets ayant la priorité la plus élevée.

Longueur totale (16 bits): il indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.

Identification, drapeaux (flags) et déplacement de fragment sont des champs qui permettent la fragmentation des datagrammes.

Durée de vie appelée aussi **TTL**, pour Time To Live **(8 bits) :** ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce

champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus.

Protocole (8 bits) : ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme (par exemple ICMP : 1, IGMP : 2, TCP : 6 et UDP : 17).

Somme de contrôle de l'en-tête, ou **header checksum (16 bits) :** ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission.

Adresse IP source (32 bits) : Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre

Adresse IP destination (32 bits) : adresse IP du destinataire du message

4-2) Les vulnérabilités du protocole IP:

La famille des protocoles IP présente des failles de sécurité intrinsèques, car ils n'ont pas été conçus dans une optique de sécurité, mais plutôt dans une optique de résilience et de performance il n'y a notamment :

- aucun chiffrement des données (les données et souvent les mots de passe circulent en clair)
- aucun contrôle d'intégrité (les données peuvent être modifiées par un tiers)
- aucune authentification de l'émetteur (n'importe qui peut émettre des données en se faisant passer pour un autre)

Les paragraphes suivants décrivent quelques-uns des réseaux qui comblent l'inconvénient majeur des réseaux IP qui est l'absence de tout mécanisme de sécurité, On parle ainsi du réseau **VPN** et de la technologie **MPLS**.

5. VPN

Un VPN (Virtual Private Network) ou quelque fois RPV (réseau privé virtuel) est un système permettant de créer un lien direct entre des ordinateurs/réseaux distants. On utilise notamment ce terme dans le travail à distance notamment, ainsi que pour l'accès à des structures de type cloud computing. Le réseau VPN permet d'émuler un réseau privé en empruntant les voies publiques et interconnectant les sites par le biais d'une méthode dite de « tunnel ».

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.

Le VPN est concept : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs protocoles de tunnelisation, par exemple : **PPTP, L2TP, L2F, MPLS, IPsec**,…etc., Néanmoins, il est possible de distinguer deux rivaux sortant leurs épingles du jeu, à savoir IPsec et MPLS. Mais la prise en charge de la qualité de service (QOS) offerte par le MPLS lui rend plus répondus chez

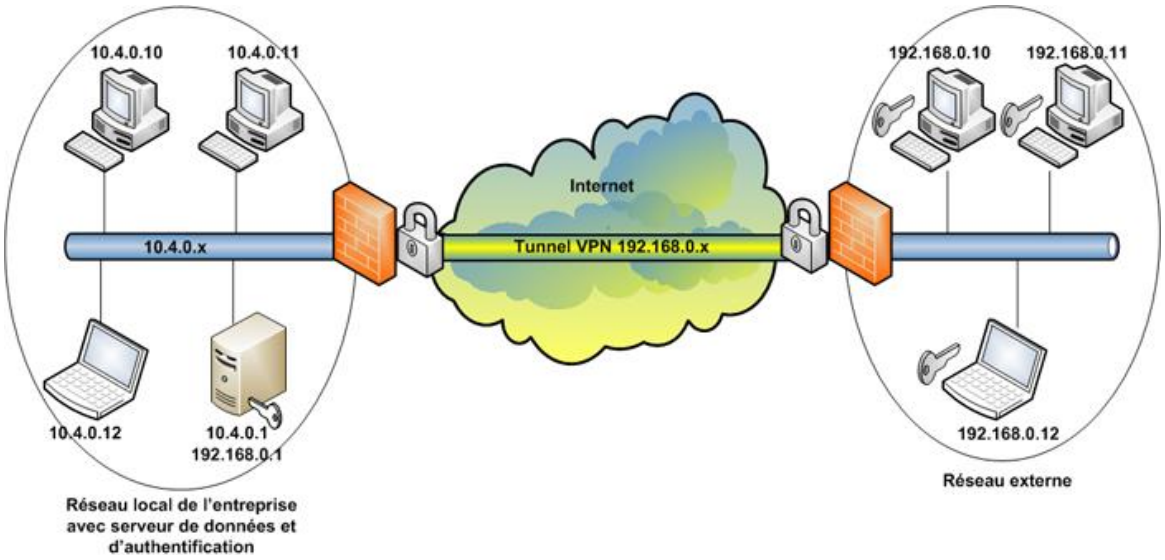


FIGURE 20 : PRINCIPE VPN

la plupart des opérateurs de télécommunication.

Intérêt :

Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local. On peut ainsi avoir un accès au réseau interne (réseau d'entreprise, par exemple).

Un VPN dispose généralement aussi d'une passerelle permettant d'accéder à l'extérieur, ce qui permet de changer l'adresse IP source apparente de ses connexions. Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service. Cependant, l'infrastructure de VPN (généralement un serveur) dispose des informations permettant d'identifier l'utilisateur. Cela permet aussi de contourner les restrictions géographiques de certains services proposés sur Internet.

Le VPN permet également de construire des réseaux overlay, en construisant un réseau logique sur un réseau sous-jacent, faisant ainsi abstraction de la topologie de ce dernier.

L'utilisation de VPN n'est généralement pas légalement restreinte.

6. MPLS

La technologie MPLS se présente comme une solution aux problèmes de routage des datagrammes véhiculés sur un réseau IP.

En effet le routage sur Internet repose sur des tables dites ''tables de routage''. Pour chaque paquet les routeurs, afin de déterminer le prochain saut, doivent analyser l'adresse de destination du paquet contenu dans l'entête de niveau 3. Puis il consulte sa table de routage pour déterminer sur quelle interface doit envoyer le paquet. Ce mécanisme de recherche dans la table de routage est consommateur de temps et ressources (processeur) et avec la croissance de la taille des réseaux ces dernières années, les tables de routage des routeurs ont constamment augmenté.

MPLS permet donc d'améliorer le routage en combinant les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2 grâce à un mécanisme de permutation des étiquettes, ce qui rend le flux MPLS vu comme un flux de niveau 2.5 appartenant à la fois au niveau 2 et niveau 3 du modèle de l'OSI.

La permutation d'étiquette est réalisée en analysant une étiquette entrante, qui est ensuite permutée avec l'étiquette sortante et finalement envoyée au saut suivant.

Les routeurs MPLS situés à la périphérie du réseau (Edge LSR), qui possèdent à la fois des interfaces IP traditionnelles et des interfaces connectées au backbone MPLS, sont chargés d'imposer ou de retirer les labels des paquets IP qui les traversent. Les routeurs d'entrée, qui imposent les labels, sont appelés Ingress LSR, tandis que les routeurs de

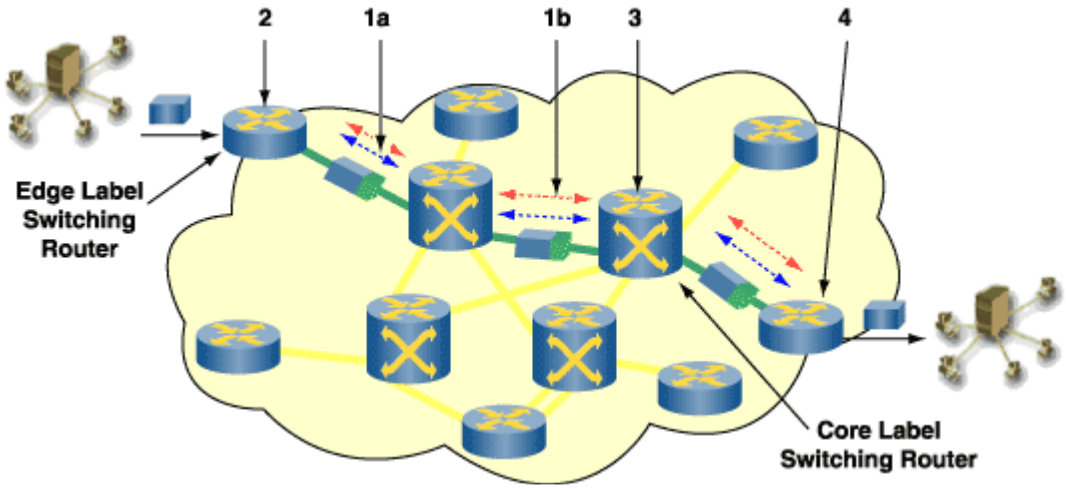


FIGURE 21: RESEAU MPLS

sortie, qui retirent les labels, sont appelés Egress LSR.

1a: Protocoles de routage existants (plus court chemin ouvert en premier (OSPF), système intermédiaire à système intermédiaire (IS-IS)) établissent l'accessibilité des réseaux de destination.

1b: LDP (Label distribution protocol) : Protocole de distribution de labels est le protocole de signalisation qui permet d'affecter des labels à un chemin au sein d'un réseau. Cependant, LDP ne contient pas de paramètres permettant de formuler une demande de ressources à l'établissement d'un LSP (Label Switched Path)

2: Ingress edge Label Switching Router

3: Label Switching Router (LSR)

4: Egress edge LSR

II- Solutions opérateurs :

Les opérateurs offrent aux clients comme solution, l'utilisation du réseau de l'opérateur en leur dédiant les ressources nécessaires (Bande passante) et le niveau de service d'exploitation, on définit ainsi 3 niveaux :

	Niveau de prestation	Description technique	Service fourni	exemples
Niveau 1 (solution privée)	Fourniture du transport de transmission brut	Liaisons (Souvent point à point) pour créer un réseau privé	Support Client de la liaison	Lignes spécialisées, liaison V-SAT
Niveau 2	Réseau fédérateur	Création d'un réseau privé au-dessus du réseau opérateur (souvent multipoint)	Réseau fourni et exploité par l'opérateur + support client	Réseau ATM, Frame Relay, accès à internet
Niveau 3	Service à valeur ajoutée	Support de transmission + réseau fédérateur + équipements (routeurs, téléphones, ..)	Réseau bout à bout (jusqu'au site client) fourni et exploité par l'opérateur	RTC, RNIS, Ligne à grande distance (Interconnexion entre LANs), accès à internet, MPLS

En effet pour concevoir le réseau de transport de données, on peut choisir entre deux solutions :

- **Solution privée :** reposant sur le niveau 1 – l'entreprise construit son réseau étendu (incluant les liaisons des sites de détection adjacents)
- **Solution opérateur :** reposant sur les niveaux 2 et 3 – l'entreprise confie une partie ou tout l'ensemble de son réseau à un opérateur.

1- Solution privée :

L'ONDA investie dans la création d'un réseau qui lui est propre, reliant tous les

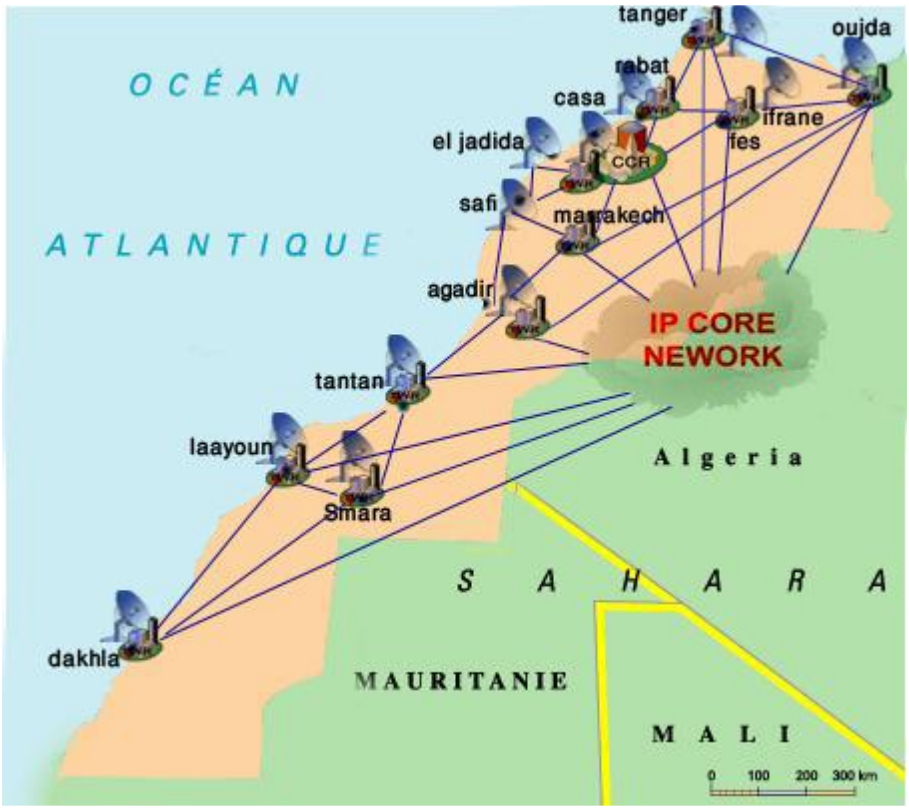


FIGURE 22: RESEAU PRIVEE ONDA (EN COURS D'IMPLEMENTATION)

sites, centres et aéroports, à bases de liaisons point-à-point :

Avantages de la conception d'un tel réseau

- C'est une solution sécurisée et fiable dont le trafic sera acheminé indépendamment.
- Une qualité de service garantie

Inconvénients

- Coût d'installations trop élevé
- Des investissements supplémentaires dans le personnels qualifié réseau

2- Solution opérateur :

Cette solution repose sur le réseau public d'un opérateur télécom, en effet la tendance actuelle des grands organismes et entreprises, à l'échelle mondiale, est d'externaliser la gestion de leurs réseaux télécoms.

Choisir l'externalisation, est le moyen qui permettra à l'ONDA de se consacrer pleinement à ses activités et son savoir-faire. Un choix qui s'inscrit dans une logique de partenariat technologique qui leur permettra de bénéficier des meilleures technologies et de faire face aux besoins croissants et urgents de compétitivité et d'efficacité.

Dans cette solution l'opérateur s'engage toujours pour offrir une qualité de service suffisamment adéquate à l'application correspondante.

3- QOS :

La qualité de service (QDS) ou quality of service (QoS) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets…

La qualité de service est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau (en management du système d'information) ou d'un processus (en logistique) et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par applications (ou activités) suivant les protocoles mis en œuvre au niveau de la structure.

En outre une priorité peut être accordée à ces données ainsi que les applications critiques.

Pour assurer la QoS, plusieurs mécanismes sont mis en place pour le marquage et la priorisation des paquets, et des algorithmes intelligents au niveau de la file d'attente qui prennent en charge le réseau quand il est encombré. Pour Chaque type d'application on peut attribuer une priorité relative sur le réseau. Par exemple, la Voix doit avoir une priorité relativement élevée, contrairement à la navigation Web à laquelle on affectera une priorité faible.

La QoS permet généralement de traiter les paquets au niveau des commutateurs de réseau selon l'algorithme ‘’premier entré premier sorti ‘’(FIFO), en cas de concurrence pour les ressources réseau, (cas de congestion), la QoS s'engage à fournir une stratégie de file d'attente plus intelligente afin de protéger le niveau de service des applications de plus haute- priorité, tout en demandant aux applications avec une priorité inférieure d'attendre.

La qualité de service se traduit par plusieurs facteurs définissant les marges tolérables pour la livraison des données d'une application considérée :

- **Loss (perte) :** la différence entre le nombre de paquets envoyés et reçus les pertes sont généralement une fonction de la disponibilité. Le taux de disponibilité est autant élevé que les pertes sont faibles.
- **Delay (latence) :** la durée entre l'envoi d'un paquet et sa réception.
- **Jitter (variation du délai) :** la différence de retard entre deux paquets. Par exemple, si un paquet nécessite 100 ms pour parcourir le réseau de la source à la destination, et un second paquet nécessitant 125 ms pour faire le même trajet, la variation du délai est de 25 ms.

- **Taux d'erreur :** valeur maximale toléré pour les erreurs de transmission (par exemple pour la transmission des données de vol ce taux doit être moins de 10-6)

Notons que chaque application possède ses propres caractéristiques selon sa nature concernant la tolérance de latence, la gigue, le taux d'erreurs et les pertes.

Classes de services opérateur

L'opérateur garantie une QOS sous forme de services répartis en différentes classes.

Un opérateur national présente les classes de ses services correspondants aux types d'applications suivants :

Classe de service	Types d'application
Multimédia plus	Application utilisant intensivement la voix ou la vidéo
Multimédia	Applications qui nécessitent des délais de transit court (voix…)
Business critique	Applications de données extrêmement critiques et sensibles (transactionnels, client serveurs sensible au temps de latence)
Business	Application de données critique (Base des données)
Standard	Application et flux standard (messagerie, ftp,..)

III- Choix du moyen de transport :

Après consultation des trois opérateurs nationaux (IAM, Méditel, INWI), je peux dire que tous les trois offrent le service du 3éme niveau : **VPN-MPLS,** qui est une solution clé offrant les équipements terminaux, les supports de transmission en plus de la gestion de réseau en contrepartie.

Le choix du réseau offre un gain de cout considérable par rapport à l'architecture réseau déjà existante.

Le tableau suivant présente une comparaison de cout des liaisons des données radars point à point avec celle envisagées (ie comparaison entre service 1 et 3) :

Station 1	Station 2	Frais d'abonnement pour accès au réseau par LS 2Mbps (DH HT)	Frais d'abonnement d'une LS 2Mbps (DH HT)
Marrakech	CNCSA	20 100.00	**44 060.40**
Safi	Marrakech	20 100.00	**40 814.40**
El Jadida	Marrakech	20 100.00	**33 914.40**
Oujda	CNCSA	20 100.00	**44 060.40**

TABLEAU 2: COMPARAISON ENTRE SERVICE 1 ET 3

On remarque que la liaison spécialisé 2Mbps liant un site Radar à l'Aéroport Marrakech ou le CNSCA coûte beaucoup plus voire même le double des frais d'accès au réseau par liaison spécialisé au même débit (2Mbps), sachant que cette dernière permet de substituer 3 réseau de données (Radar, messages de vol et voix).

Le trafic des données sera donc acheminé dans le backbone propre à l'un des opérateurs, j'ai procédé par la distinction des données selon leurs natures en trois flux transmis séparément en définissant ainsi trois QoS.

Chaque VPN modélise le niveau de qualité de service (QOS) mis en jeu dans le déploiement d'une liaison.

Par défaut, un réseau IP se contente d'acheminer les paquets au mieux de ses possibilités (Best effort), et sans distinction. Tant que la bande passante (c'est-à-dire le débit) est suffisante, il n'y a pas de problème. Mais, en cas de saturation, les routeurs sont obligés de rejeter les paquets, invitant tous les émetteurs à réduire leur flux.

La notion de qualité de service introduit la possibilité de partager le plus équitablement possible une ressource utilisée par un grand nombre de flux applicatifs qui peuvent interférFIGURE 23: MODEL DU RESEAU VPN CHOISI ossibilité de déterminer différents niveaux de service en fonction de la nature de ce flux (donnée synchrone, donnée asynchrone, voix …).

IV- Contraintes

Dans le but d'élaborer un réseau IP (VPN) commun pour acheminer les données de la surveillance, données de vol et de la voix ; des données de différents types. Le mieux serait de préciser les spécifications et les qualités de service de chaque type d'application.

1. Données radars :

Pour les données de surveillance où la notion de délai est un facteur décisif dont l'OACI exige les spécifications ci-dessous

	spécifications	valeur	Référence
Délai	Délai de la transmission (temps de transit + temps de traitement multi-radar)	< 0.25s	Document 8071 Volume 3 page 42 (vérification des systèmes radars de surveillance).

TABLEAU 3: EXIGENCES DES DONNEES RADARS

En plus de ces exigences de délai on note la nécessité primordiale d'une livraison dans le bon ordre des paquets lors de la réception.

Il est évident que le protocole IP ne répond pas à ces attentes ce qui pousse à utiliser un protocole pour combler les lacunes à ce stade, le problème rencontré est le suivant :

Le protocole de transport à utiliser est le **TCP** vue la garantie qu'il offre au niveau du flux et des données (par le contrôle de flux et l'acquittement de réception) ce qui introduit un délai qui le rend inconvenable.

La solution alternative est le protocole **UDP**, cependant ce dernier n'offre aucune garantie en matière de livraison des paquets, et leurs arrivées dans le bon ordre. La sécurité du contrôle aérien consiste surtout à la disponibilité de la donnée au bon moment, ce qui incite à se baser sur le protocole UDP, et chercher éventuellement un mécanisme pour lui assurer la **fiabilité**.

2. les données de vols :

Pour les données de vol, le type de données est de nature messagerie ce sont surtout des contraintes d'intégrité qui s'opposent, donc l'élément le plus important à prendre en compte est le taux d'erreur.

	spécifications	valeur	Référence
Taux d'erreur	Le taux d'erreur de 10^{-6} dans 1000 octets	< 10^{-6}	DOC9896 Ed 2 VM2 page 26 (Manual for the ATN using IPS Standards and Protocols).
Délai	Délai de transmission	< 5s	DOC9896 Ed 2 VM2 page 26 (Manual for the ATN using IPS Standards and Protocols).

TABLEAU 4: EXIGENCES DES DONNEES DE VOLS

L'utilisation d'un protocole qui garantit la fiabilité et le contrôle d'erreurs est donc nécessaire.

3. la communication vocale :

La communication vocale est une application temps réel, elle impose-t-ainsi des contraintes au réseau en matière de gigue et de délai, contrairement aux autres applications (données de vol).

Les spécifications requises dans une transmission de la voix sont :

- **Délai de transmission** (temps de latence) : il faut que le temps de transport des données entre l'émetteur et le récepteur soit faible
- **La perte de paquets** : la voix supporte bien les pertes de paquets par rapport aux données radar.
- **La gigue** : c'est une variation du délai de transmission de l'information. Elle provient de la variation de la charge du réseau, elle ne doit pas être trop importante

	spécifications	valeur	Référence
Délai de latence	Temps de transit	< 0.1s	DOC9896 Ed 2 VM2 page 26 (Manual for the ATN using IPS Standards and Protocols).
La gigue	La variance du délai de transmission	< 0.015s	DOC9896 Ed 2 VM2 page 26 (Manual for the ATN using IPS Standards and Protocols).

TABLEAU 5: EXIGENCES DES DONNEES DE LA VOIX

L'utilisation d'un protocole de transport de la voix sous IP est évidente, afin de répondre aux contraintes de celle-ci.

V- Conclusion :

Jusqu'à ce point se termine ma collecte d'informations et contraintes nécessaires pour concevoir une solution sous forme d'un réseau IP VPN-MPLS. Bien sûre dans le chapitre qui suit j'entamerais la conception de ce réseau tout en se basant sur les choix que j'ai mentionnés dans ce quatrième chapitre, aussi tout en respectant les contraintes spécifiées.

Chapitre 5

Conception du réseau (solution)

Chapitre 5 : Conception du réseau

Le **modèle hiérarchique** est une approche hiérarchique relative à la conception du réseau local qui a été définie afin de pallier les problèmes que l'évolution de la technologie avait rencontré ces 30 années en informatique, plus particulièrement quand on parle des réseaux.

I. Modèle hiérarchique :

Plus généralement nommé par sa version anglaise, «tree-layers hierarchical internetworking design/model », ce modèle a été inventé et diffusé par Cisco. Il s'agit d'une approche préconisant le découpage du réseau en trois grandes parties s'inspirant du modèle OSI et permettant ainsi d'augmenter la performance du réseau, faciliter son évolutivité et sa maintenance. Ces trois couches sont :

- La couche core (cœur du réseau)
- La couche distribution

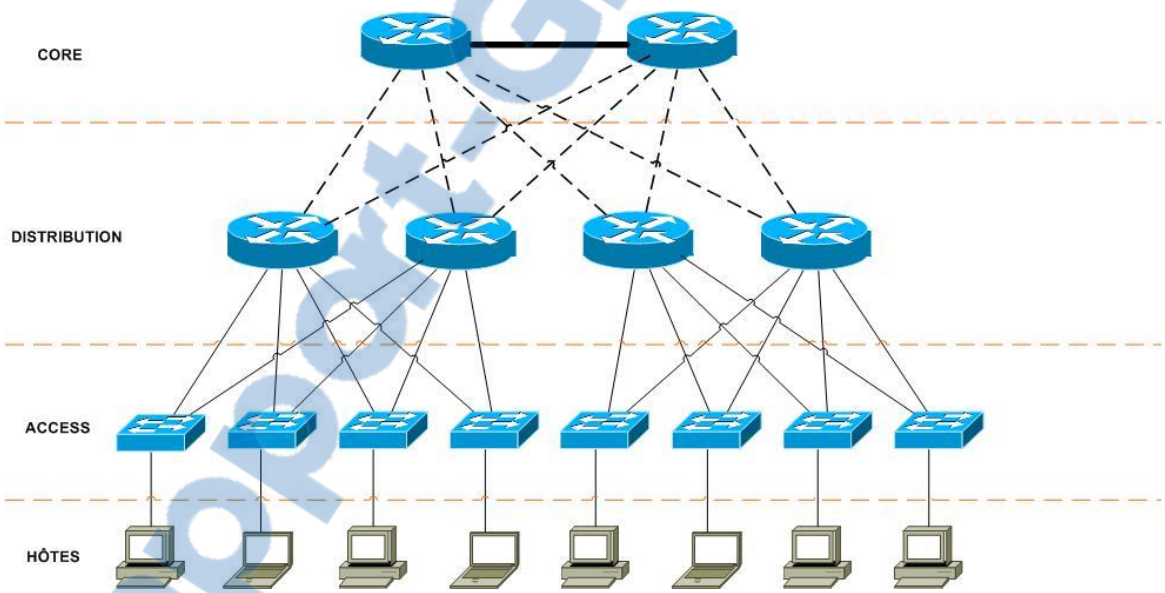


FIGURE 24: MODELE HIERARCHIQUE

- La couche access

1. Couche core :

C'est la couche supérieure. Son rôle est simple : relier entre eux les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société. Elle représente le noyau l'artère centrale du réseau de l'entreprise, elle est appelée aussi **backbone**, et permet de garantir l'équilibre, la stabilité et l'évolutivité du réseau.

2. couche distribution :

Cette couche qui se situe entre la couche core et la couche access, a pour rôle de filtrer, router, autoriser ou non les paquets, elle permet l'agrégation des connexions réseaux et l'application de la politique de sécurité adoptée. Il faut noter bien qu'ici, on commence à diviser le réseau en segment, en ajoutant plusieurs routeurs/switchs de distribution, chacun étant connecté au Core d'un côté, et à la couche Access de l'autre. Selon la taille et les moyens de l'entreprise, on devra choisir entre routeur et switch.

3. couche access :

C'est la dernière couche de ce modèle. Son rôle est très important : connecter les périphériques « end-users » au réseau, aussi d'assurer la sécurité. C'est à ce niveau que l'accès d'un utilisateur au réseau de l'entreprise est autorisé ou refusé, ainsi là où la qualité de service est appliquée.

II. Application du modèle hiérarchique au cas de l'ONDA :

Pour appliquer le modèle hiérarchique, il faut d'abord choisir parmi une des topologies design campus, et puisque l'aéroport de marrakech ainsi que les deux sites de détection Safi et El Jadida ne nécessitent pas au dela de 200 ports, j'opte pour la topologie d'un campus de petite taille.

La configuration de la topologie adoptée :

- Couche access :
  - Des switch L3 (Routage IP)
  - Des passerelles et des concentrateurs VoIP
  - Des routeurs voice
  - Des routeurs avec des passerelles pour passer du protocole asynchrone/synchrone(HDLC) vers l'IP.
- La couche Core :
  - Des routeurs multi-services

Cette configuration offre :

- La communication A-G (Air Ground) et G-G (Ground Groun) over IP
- L'émulation des lignes E&M à travers à travers un réseau IP
- Le transport des données synchrone et asynchrone sous IP
- Les applications LAN to LAN sous IP
- Les mécanismes de la QoS pour le trafic réseau, notamment engendrés par les applications radar, radio et AMHS.
- La sécurisation des données via des algorithmes de cryptage

Les applications concernées, sont classées comme suit :

- Données vocales (radio, telephonie)
- Données synchrone (radar) et asynchrone (AFTN)
- Données LAN (radar, AMHS)

On envisage donc de transmettre les données Radar, les données de vol ainsi que les communications vocales (A/G et G/G) via un réseau IP/VPN, la technologie MPLS nous garantit la sécurité, l'intégrité et la fiabilité des données.

1. les données vocales :

La solution envisagée est d'utiliser le protocole **RTP** basé sur le protocole UDP en plus d'un protocole de signalisation **SIP** basé sur TCP.

- **RTP** est un protocole qui a été développé par l'IETF afin de faciliter le transport à temps réel de bout en bout des flots de données sur les réseaux de paquets. RTP est un protocole qui se situe entre la couche **application** et la couche de **transport** UDP qui lui permet d'atteindre plus facilement la livraison temps réel.
- **SIP** est un protocole de signalisation appartenant à la couche **application** du modèle OSI. Son rôle est d'ouvrir, modifier et libérer les sessions, il peut aussi inviter des participants à des sessions déjà existantes. Des supports peuvent être ajoutés (et retirés) à une session existante.

SIP étant indépendant de la transmission des données, tous types de données et de protocoles peuvent être supportés dans l'échange. Il prend en charge cinq fonctions de l'établissement et de la terminaison de communications multimédia

- Localisation de l'utilisateur **(User location)**: détermination du système terminal à utiliser pour la communication
- Disponibilité de l'utilisateur **(User availability)**: détermination de la volonté de l'appelé à s'engager dans une communication
- Capacités de l'utilisateur **(User capabilities)**: détermination du support et des paramètres de support à utiliser
- Etablissement de session **(Call setup/ringing)**: "sonnerie", établissement des paramètres de session à la fois chez l'appelant et l'appelé
- Gestion de session **(Call handling)**: comprend le transfert et la terminaison des sessions, la modification des paramètres de session, et l'invocation des services

Le protocole SIP permet l'ouverture de la session pour tracer le chemin que va suivre les paquets par la suite, donc on peut dire qu'il joue le rôle de signalisation afin d'établir la connexion

Une fois la session est ouverte, la communication s'effectue à travers le protocole RTP qui assure la livraison dans un délai tolérable.

Pour **l'implémentation** on utilisera des passerelles VoIP pour émuler les signalisations E&M analogiques à travers un réseau IP (Voice Gateway). Ces passerelles permettent de concentrer plusieurs canaux VoIP dans des liaisons E1 pour les transmettre

vers les ‘routeurs voice’ qui vont leurs affecter la QoS requise pour les données vocales et ensuite les acheminer vers les routeurs multiservices de la ‘couche Core’.

2. les données synchrones (Radar) :

Pour les systèmes de surveillance, les informations véhiculées sont des données temps réel c’est à dire qu’elles doivent être affichées à un délai minimal après leurs détections.

La solution qu’on propose, et qui est adaptée à ce type de données est la suivante :

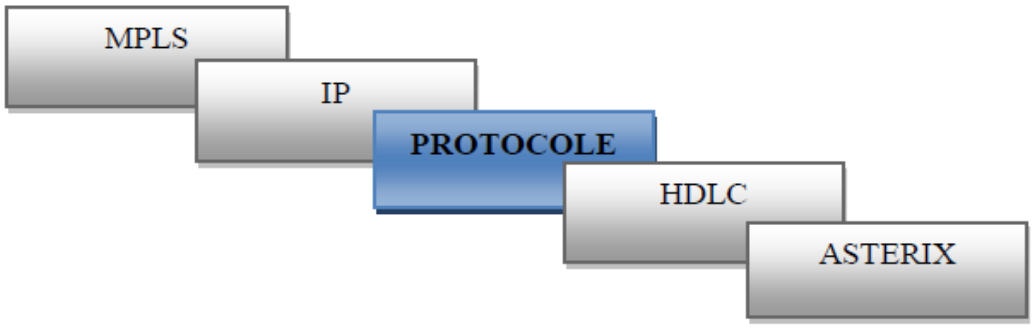


FIGURE 25: PROTOCOLE SOLUTION

Le **PROTOCOLE** (en bleu) doit offrir le transport temps réel aussi bien que la fiabilité des données, on peut donc se baser sur le protocole de transport **UDP** qui garantit le **délai minimal** souhaité en plus d’un protocole dont le rôle principal est d’éviter le problème de **séquencement des paquets** (possibilité d’arriver dans un ordre différent).

Le protocole que l’on va ajouter à l’UDP permettra de tracer un chemin virtuel au sein d’une infrastructure partagée. or que le réseau est sous le protocole IP fonctionnant en best effort, c’est la tunnelisation déjà abordé dans la partie VPN (on cite notamment le protocole L2TP et IPSEC).

Le tunneling par l’intermédiaire du protocole **IPSEC** consiste à encapsuler les paquets IP à l'intérieur d'un autre paquet IP, c’est un assemblage de plusieurs protocoles et mécanismes ce qui le rend techniquement très complexe.

Le protocole optimal et le plus répondu en ce sens est le protocole **L2TP**, donc le **PROTOCOLE** proposé n’est d’autre que le protocole L2TP over UDP.

Pour **l’implémentation** on utilisera des passerelles pour passer du protocole synchrone (HDLC) vers le protocole IP. Ces passerelles vont encapsuler les données de surveillance qui sont sous format Asterix dans les protocoles L2TP, UDP et IP. Ces passerelles sont des cartes séries enfichées dans des routeurs dont le rôle est d'affecter la QoS requise pour les données Radar et ensuite acheminer ces données vers les routeurs multiservices de la couche Core.

3. Les données asynchrones (AFTN/AMHS) :

AFTN et AMHS sont considérés comme des services de messagerie, ce qui implique l'utilisation du TCP, un protocole de transfert de données n'exigeant pas le transfert en temps réel.

Pour **l'implémentation** on utilisera des passerelles pour passer du protocole asynchrone vers le protocole IP. Ces passerelles vont encapsuler les données AFTN dans des trames TCP et ensuite dans des paquets IP. De même Ces passerelles sont des cartes séries enfichées dans des routeurs dont le rôle est d'affecter la QoS requise pour les données AFTN et ensuite acheminer ces données vers les routeurs multiservices de la 'couche core'.

4. les données LAN :

Ces données sont des données natives IP qui n'ont pas besoin de passerelles IP. Donc ces données sont branchées dans des commutateurs de niveau 3 (Switch L3) qui vont les séparer en VLANs et leur affecter la QoS requise pour les données de surveillance et AMHS avant de les acheminer vers les routeurs multiservices de 'la couche core'.

III. Topologie du réseau IP :

La topologie du design campus que l'on va adopté est celle d'un campus de petite taille vu que le nombre des ports utilisateurs dans les cas de l'aéroport de Marrakech Menara et les sites radar Safi et EL Jadida ne dépassent pas les 200 ports.

1. Topologie du réseau IP l'aéroport de Marrakech Menara :

Vue que le réseau se constitue de 3 sites, la topologie que l'on propose est basée sur:

- Deux routeurs multiservices qui assurent les fonctions de la couche Core
- 2 Switch niveau 2/3 pour les applications LAN, assurant les fonctions la couche accès

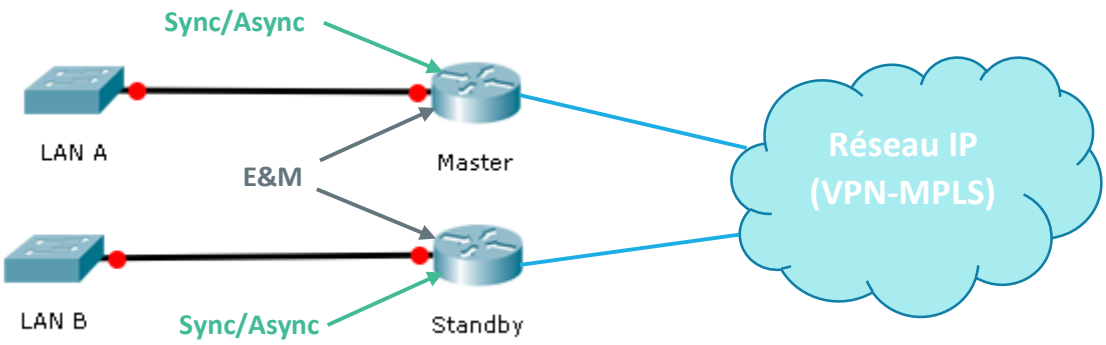


FIGURE 26: TOPOLOGIE DE L'AEROPORT

2. Topologie du réseau IP des sites radars :

Ces sites assurent essentiellement les applications/services opérationnels et meilleurs degré d'importance une topologie redondante est exigée.

Généralement il n'y a pas de trafic LAN to LAN donc les Switch locaux peuvent être éliminés de cette topologie, sauf si il y a des exigences particulières pour la gestion des différents équipements dans ce cas il est fortement recommandé d'utiliser une topologie similaire à celle des principaux aéroports.

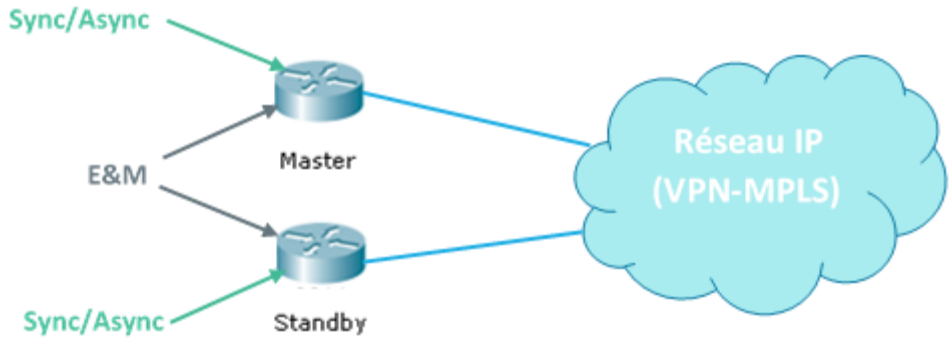


FIGURE 27: TOPOLOGIE DES SITES RADARS

3. Proposition d'une topologie du réseau IP couvrant l'ensemble de l'ONDA :

3.1. CNCSA :

Le CNCSA est considéré comme un site très important vu son rôle primordial dans le contrôle de la sécurité de la navigation aérienne au Maroc. La topologie du réseau IP du CNCSA est la suivante avec une configuration des couches accès et core complètement redondante.

- La couche Core : 2 routeurs multiservice (hot/standby)
- La couche accès:
- application de la voix : 2 routeurs voix, 2 concentrateurs
- application série synchrone/asynchrone : 2 routeurs serie
- application LAN to LAN : 2 commutateurs niveau 3 pour l'accès hôte et deux dispositifs de pare-feu pour sécuriser les LAN.

Dans cette topologie j'ai a respecté les spécifications suivantes :

- Les deux routeurs voix n'ont pas de lien IP entre eux de façon à éviter que le 2ème routeur soit affecté si le 1èr l'est.
- Chaque concentrateur a deux liaisons E1 connectées au deux routeurs, et c'est au concentrateur de choisir l'E1 qui sera active.
- Si on a besoins de plus de 30 canaux, plusieurs concentrateurs seront installés
- Les deux routeurs SYN/ ASYN n'ont pas de lien IP entre eux, les connexions séries doivent être attachées séparément sur ces deux routeurs.
- Les applications LAN IP seront reliées à deux commutateurs niveau 3 et tout le trafic montant de ces commutateurs ne sera pas propagé à l'extérieur de la zone LAN.

- Les deux pare-feu sont pour filtrer le trafic et donc protéger les routeurs de coeur

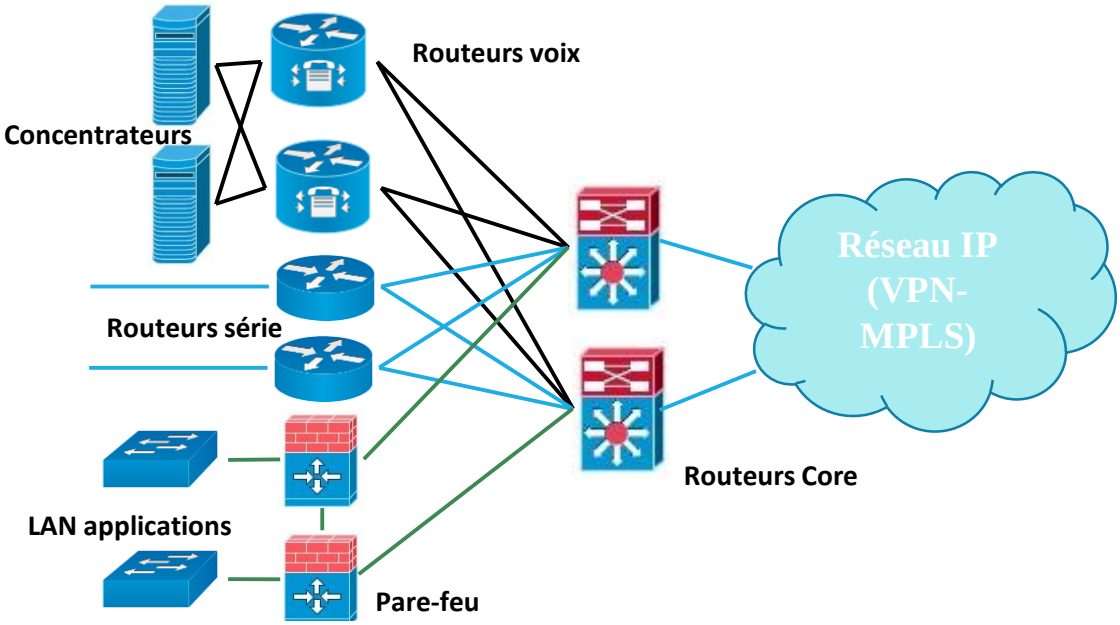


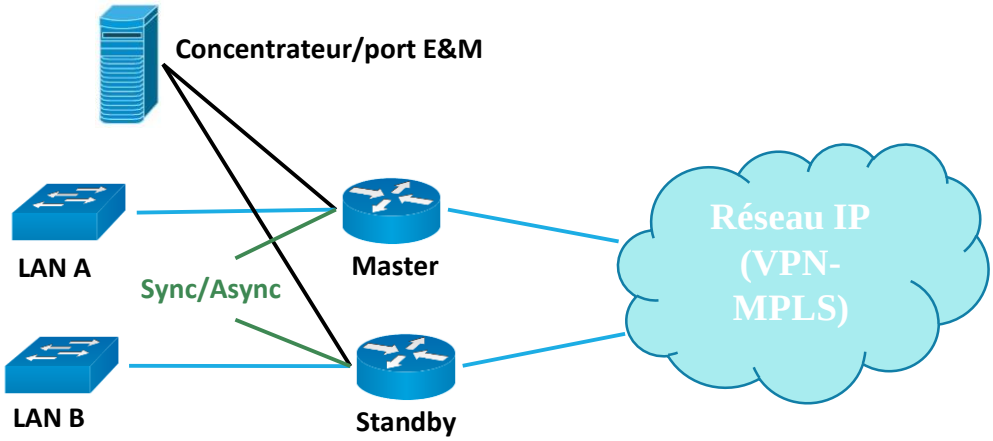
FIGURE 28: TOPOLOGIE DU CNCSA

ainsi que définir les permissions et les droits d'accès aux données.

3.2. Aéroports principaux

Pour les aéroports principaux la topologie proposée est basée sur:

- Deux routeurs multiservices qui assurent les fonctions de la couche accès et Core



- 2 Switch niveau 2/3 pour les applications LAN

Selon le nombre de canaux de communication vocale requis sur chaque aéroports on envisage deux modèles de site (avec ou sans concentrateurs de la voix)

3.3. Aéroports secondaires

L'architecture envisagée pour les aéroports secondaires dépend du niveau de sécurité requis. On peut toujours utiliser la même topologie comme dans les principaux aéroports mais on peut aussi utiliser une topologie moins sécurisée en utilisant la

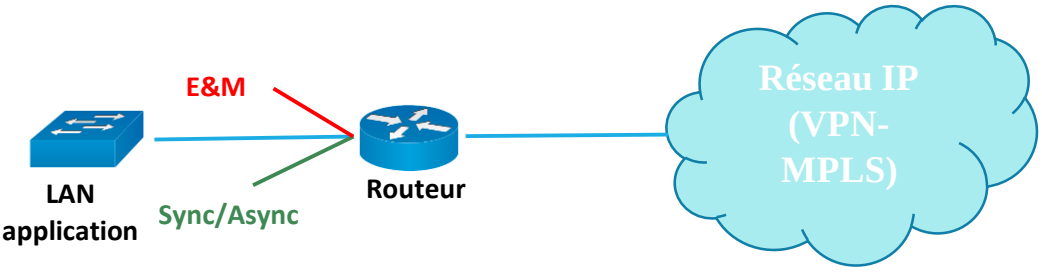


FIGURE 30: TOPOLOGIE DES AEROPORTS SECONDAIRES

3.4. Sites Radars et sites Radio

L'architecture et la meme que celle de FIGURE 27: TOPOLOGIE DES SITES RADARS.

VI. Sécurité :

Avec la libre circulation des informations et la haute disponibilité de nombreuses ressources, on doit connaître toutes les menaces susceptibles de compromettre la sécurité des données, donc Il est important de connaître les points de vulnérabilité du réseau pouvant servir de porte d'entrée à d'éventuels intrus Donc sécuriser les données, c'est garantir :

- La confidentialité : les données communiquées ne peuvent pas être connues d'un tiers non-autorisé.
- L'authenticité : l'identité des acteurs de la communication est vérifiée.
- L'intégrité : les données de la communication n'ont pas été altérées.
- La disponibilité : les acteurs de la communication accèdent aux données dans de bonnes conditions.

D'un point de vue technique, la sécurité recouvre à la fois l'accès aux informations sur les postes ainsi que le réseau de transport des données. Voici quelques-uns parmi les mécanismes proposés :

1. Au niveau du réseau de transport :

- Le chiffrement : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.

Pour les données, on procédera d'un chiffrement symétrique : AES (Advanced Encryption Standard) ou encore 3DES (Digital Encryption Standard).L'algorithme de chiffrement est à configurer au niveau du routeur multiservice.

- Détection d'intrusion : repère les activités anormales ou suspectes sur le réseau surveillé.
- Analyse des vulnérabilités ("security audit") : identification des points de vulnérabilité du système.

2. Au niveau du réseau local :

Le pare-feu : qui est un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quelles sont les communications autorisées ou interdites.

Conclusion générale

La sécurité et la gestion de la navigation aérienne représentent la tâche primordiale de tout aéroport. L'aéroport Marrakech Menara est classé en deuxième place au Maroc. Avec l'augmentation continue de son nombre de vols, cet aéroport voit son troisième terminal en cours de construction. Pour cette raison, les systèmes et mécanismes de sécurité doivent être fortifiés afin de maintenir le même niveau de sécurité après le lancement du nouveau terminal.

L'objectif de ce projet de fin d'études, effectué au sein de l'Office Nationale des Aéroports à l'aéroport Marrakech Menara, a principalement porté sur l'étude du système de contrôle et surveillance de la sécurité du trafic aérien utilisé à l'aéroport et la suggestion d'une solution dans le but de rester dans les standards et normes de sécurité imposés par l'OACI.

Dans le but de réaliser mon projet, j'ai dans un premier temps pris connaissance de la problématique et collecté les informations nécessaires pour dresser l'état de l'existant. Avant de choisir la solution qui se base sur l'utilisation de sources de détection multiples, j'ai dû envisager une solution indépendante qui est l'ADS-B. Cette solution s'avère trop couteuse et limitée à un certain type d'aéronefs.

La solution se basant sur l'utilisation de sources de détection multiples apportera au système un maintien de la continuité du fonctionnement du système, ainsi que l'augmentation de la précision au niveau des résultats de la position des aéronefs détectés.

Cette solution se traduit par la conception d'un réseau IP VPN-MPLS qui se chargera du transport des données radars des sites SAFI et EL Jadida vers l'aéroport Marrakech Menara. Le choix s'est basé sur une étude comparative avec ADS et une étude comparative des solutions possible pour la création de réseau IP.

J'ai aussi suggéré de circuler d'éventuelles informations relatives à la gestion du trafic aérien dans le même réseau.

En perspective, j'ai envisagé de proposer une topologie incluant l'ensemble du réseau de l'ONDA à savoir les aéroports principaux, secondaires, stations de détection et centres de contrôle régionaux. Le présent travail peut être considéré comme une première étape de la mise en œuvre d'un cahier de prescriptions technique ou la réalisation d'un appel d'offre future.

« L'imagination est plus importante que la connaissance. La connaissance est limitée alors que l'imagination englobe le monde entier, stimule le progrès, suscite l'évolution. »

Albert Einsten

Bibliographie

1- Brochure Selex ATCR-33S NG **– *Ch.3 Etude de l'existant***
2- Brochure Selex SIR-S **– *Ch.3 Etude de l'existant***
3- Manual of SSR Systems: ICAO Doc.9684.Ed 2 VM2 **– *Ch.4 Contraintes***
4- Manual on Testing of Radio Navigation Aids: Volume III (Testing of Surveillance Radar Systems): ICAO Doc.8071 **– *Ch.4 Contraintes***

webographie

1- www.onda.ma **– *Ch. 1 Présentation de l'organisme d'accueil***
2- http://www.radartutorial.eu/index.fr.html **- *Ch.2 Contexte théorique***
3- http://www.inwi.ma/entreprises/data/ip-vpn-mpls **- *Annexe 3***
4- http://entreprises.meditel.ma/Data/IPVPN **- *Annexe 3***
5- http://www.iam.ma/entreprise/grandes-entreprises/solutions-reseaux/vpn-ip.aspx **- *Annexe 3***
6- www.icao.int
7- fr.wikipedia.org

Annexe

Annexe A : Le système radar Selex-SI

Comme le montre le schéma ci-dessous le système de SELEX se compose de plusieurs serveurs :

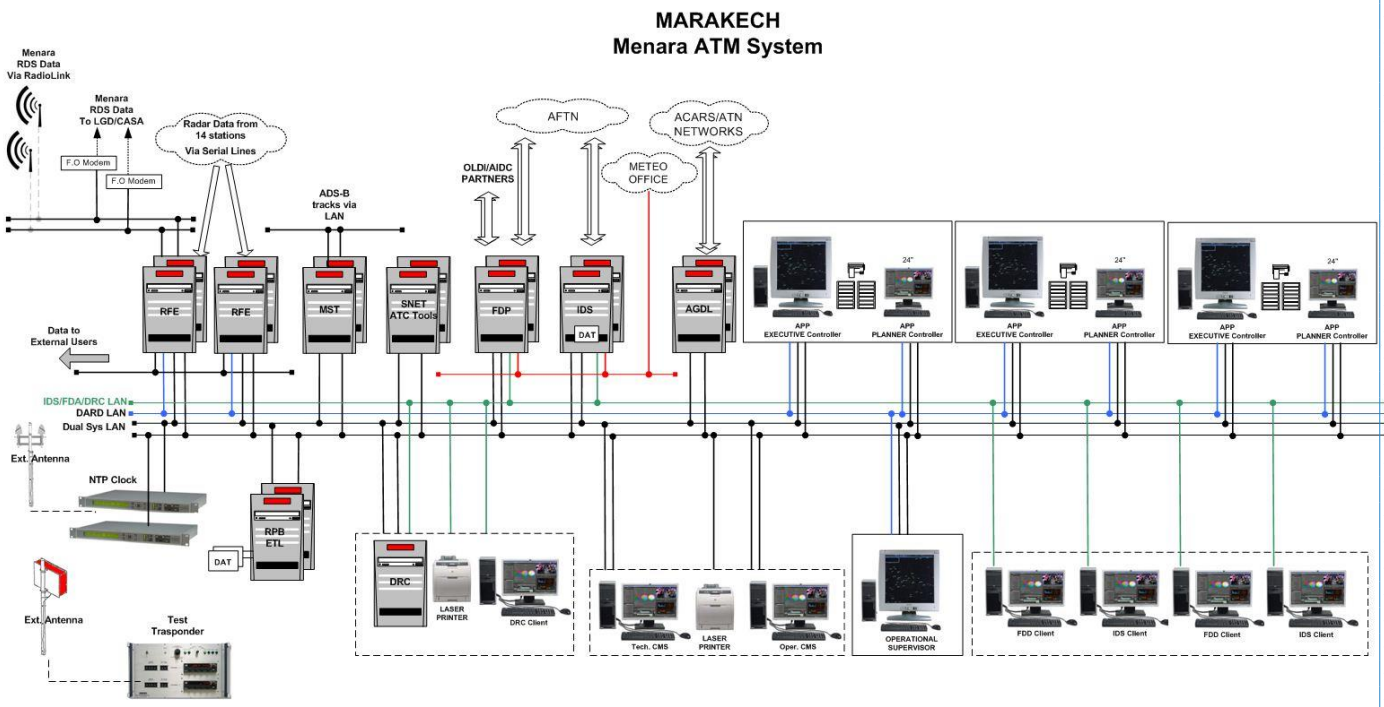


FIGURE 31: ARCHITECTURE DU SYSTEME SATCAS DE L'AEROPORT MARRAKECH MENARA

ATC (Air Traffic Control), est le plus exigeant de tous les systèmes à logiciel prépondérant. Il est sensible à la sécurité, hautement distribué et en temps quasi réel.

SATCAS (Standard Air Traffic Control Automatic System) est la solution SELEX SI-ATM pour le contrôle du trafic aérien. Il répond à un certain nombre des exigences de dimensionnement architectural, par exemple:

Grande disponibilité - haute performance - Modificabilité et évolutivité - ergonomie.

Afin de répondre aux exigences ci-dessus, SATCAS est un système distribué comprenant un certain nombre d'éléments reliés entre eux par des réseaux LAN que l'on détaillera dans ce qui suit.

4.1. Les différents serveurs :

a) RFE (Radar Front End) :

⇨ DESCRIPTION:

Le RFE est un système d'acquisition et de diffusion de données radar en provenance des différents sites radar sous différents formats.

⇨ FONCTIONALITES DU RFE:

Le système RFE reçoit les données radars, sous format de message AMS, SELEX-SI, ASTERIX et CD2, issues de plusieurs sources (« Radar Head Processors » et « multi-radar data producers ») et à travers différents protocoles d'entrée: serial HDLC, UDP/IP. Après la réception des données radar; les messages sont vérifiés, validés puis convertis dans un format commun interne SELEX-SI.

Chaque serveur RFE permet de contrôler et gérer les cartes d'acquisition ainsi que la configuration des ports d'entrée de 7 sites radar.

b) MRT (Multi Radar Tracking) :

La poursuite multi-radar est généralement basée sur une technique de fusion de détections radar ou MPVU, selon l'acronyme pour Multiple Plot - Variable Update. Par cette technique, chaque point, ou "plot", issu de la détection d'un même aéronef est traité le plus rapidement possible, afin de mettre à jour la piste multi-radar correspondante dans les meilleurs délais. Avantage du MRT :

- Réduction de la marge d'erreurs à cause de la compensation faite entre les erreurs des différents radars.
- Pistage continu à proximité des radars limites.
- Une plus grande précision dans l'estimation des paramètres de la piste (position et vitesse), en raison du taux supérieur des données radar à celles en provenance d'un seul radar.
- Probabilité de détection supérieure dans les zones de chevauchement.

c) RDP (Radar Data Processing):

Toutes les fonctions de traitement des données radar (primaire, secondaire, combinés ou ADS) sont réalisées par le serveur RDP. C'est un calculateur qui traite les données radar primaires et secondaires reçues afin d'accomplir une poursuite de tous les avions détectés à l'intérieur de la couverture radar. Il collabore avec les serveurs :

- Poursuite multi-radar.
- Des données des plans de vol.
- ADS (Automatic Dependant Surveillance).

d) SNET (Safety Net) :

Safety Net est un système de la détection et de la gestion des conflits fonctionnant d'une potentiellement dangereuses du trafic. Ce système est basé principalement sur des données de surveillance et les renseignements du plan de vol pour identifier les situations de conflits prévus.

Des algorithmes d'évaluation permettent de protéger les contrôleurs aériens contre les fausses alertes, et de réduire la charge de travail. Le système, en raison de son interface standardisée peut être facilement intégré dans un système ATC.

Deux types de conflits peuvent être détectés par le Safety Net:

- **STCA** (Short Term Conflict Alert) : cette alerte est active lors des violations potentielles des normes de séparation entre deux avions, ce qui permet d'alerter le contrôleur du risque de collision entre deux aéronefs.
- **MSAW** (Minimum Safe Altitude Warning): cette alerte s'active si l'aéronef vol à basse altitude.

e) FDP (Flight Data Process):

C'est un calculateur de traitement des données de vol (plans de vol et Météo) reçues du réseau AFTN (Aeronautical fixed telecommunication network) afin qu'ils soient associés par la suite aux plots détectés par le système de surveillance de Selex. Un plan de vol déposé comportera toutes les informations pertinentes relatives au vol prévu. Ceci inclut: L'identification de l'aéronef (note: c'est à dire l'indicatif d'appel). Les règles et le type de vol.

- Le nombre, le type d'aéronef.
- L'équipement embarqué.
- L'aérodrome de départ.
- L'heure estimée de départ du poste de stationnement.
- La vitesse de croisière.
- Le niveau ou l'altitude de croisière.
- La route suivie.
- L'aérodrome de destination et la durée totale estimée.
- L'aérodrome de dégagement.
- L'autonomie.
- Le nombre total des personnes présentes à bord.
- L'équipement de survie.
- Certains renseignements divers.

a) IDS (Information Display System):

Information display system est un système développé par Selex SI pour fournir un support d'information pour le contrôle radar de l'aéroport Marrakech-Ménara. Le role de l'IDS est de collecter les informations en l'occurrence ceux du AFTN et les distribuer afin d'assurer la sécurité, la régularité et l'efficacité de la circulation aérienne.

b) RPB (Record and Playback)

Un ensemble de données est stocké sur un disque dur partagé déduit à la sauvegarde et au replay.

Ces données sont de différentes natures:

- System tracks.
- Local tracks.
- Données météo.
- Ordres des contrôleurs.
- Ordres de supervision.
- Messages de diagnostic.
- Messages de contrôle (time, date, etc.).
- Données de vol.

Les données qui sont stockées peuvent être rejouées à n'importe quel moment grâce au système RPB qui offre la possibilité du playback.

c) AGDL (Air-Ground DataLink):

L'AGDL est un calculateur qui permet de faire une interface de liaison de donnée afin d'accomplir une poursuite de tous les avions détectés à l'intérieur de la FIR (Flight Information Région).

d) NTP

C'est un équipement redondant composé d'antennes réceptrices GPS NTP1 & NTP2 qui permet la synchronisation du système SELEX. Il distribue l'horloge pour toutes les composantes du système via le réseau local (LAN1 & LAN2).

e) DRC: (Statistics and Billing)

C'est un système qui se charge du traitement des données de vol et des redevances ainsi que des statistiques de la gestion du trafic aérien.

a) Système de contrôle de supervision CMS

Système de supervision et de contrôle des états des équipements SELEX. Il permet :

L'affichage graphique pour la supervision de l'état opérationnel de chacun des éléments du système représenté par sa couleur (vert : opérationnel, orange : en réserve, rouge : non opérationnel)

- Le contrôle des lignes Radar.
- L'initialisation des Applications et système d'exploitation.
- Le contrôle de l'état du réseau.
- La gestion des événements.
- La gestion des statistiques.
- La configuration et le paramétrage en temps réel.

Pour répondre aux besoins de traitement des équipements de pointe ont été mises en place pour assurer une analyse adéquate, un switching efficace et une disponibilité des données.

Annexe B : Aéroports et Stations Radars

On distingue 4 types de stations-Aéroports :

CCR	1ére Catégorie	2éme Catégorie	3éme Catégorie
CNCSA	Casablanca	Tetouan	SR Casablanca
CCR AGADIR	Marrakech	Tit melil	SRd Touaher(Taza)
	Rabat	Hoceima	SRd Tanger
	Tanger	Errachidia	SR/SRd Oujda
	Nador	Tantan	SR Ifrane
	Oujda	Agadir-Inzegan	SRd Errachidia
	Fes	Ben Sliman	SR/SRd Marrakech
	Ouarzazate	Bouarfa	SR Safi
	Dakhla	Oufela	SR El Jadida
	Smara	Essaouira	SR Tantan
	Laayoune	Guelmim	SR/SRd Agadir
	Agadir	Sidi Sliman	CNDA

		Zagora	DAC
			Météo
			Kénitra Air Base
			Meknès Air Base
			Sidi-Sliman Air Base

TABLEAU 6: CLASSEMENTS DES STATIONS ET AEROPORTS AUX MAROC

Les stations de partage de données Radars :

Lieu du site	Caractéristiques
Foia	**portée** = 200NM au FL368 **latitude**= N **371844,89** **longitude**= W **83359,18**
Porto Santo	**portée** = 200NM au FL368 **latitude**= N 330414,5 **longitude**= W – 0162059,4
Casablanca	**Primaire :** • **Portée** = 60NM au FL200 • **Latitude**= N332124,12 • **Longitude**= W0073642, 99 • **Altitude antenne=** 700FT **Secondaire :** • **Portée** = 250NM au FL460 • **Latitude** = N332124,12 • **Longitude** = W0073642,9 • **Altitude antenne** = 700.65FT+30FT
Agadir	**portée** = 250NM au FL460 **latitude**= N301908,96 **longitude** = W0092440,75 **altitude antenne** = 266.76FT + 30FT
Safi	**portée**= 250NM au FL460 **latitude**= N321904,94 **longitude** = W0091347,10 **altitude antenne** = 396.41FT
Ifrane	**portée** = 250NM au FL460 **latitude**= N333152,02 **longitude**= W0050924,06 **altitude antenne** = 5877.14FT
Oujda	**Fonction** : Radar secondaire MSSR / Mode S pour le contrôle aérien en route et d'approche des aéroports Oujda et Nador. **Fréquences** : • Emission : 1030 Mhz • Réception : 1090 Mhz **Puissance** : 800 watts **Portée** : 250 NM ≈ 480 Km de rayon **Altitude Max** : 40 000 pieds ≈ 12 km **Position géographique** : • Latitude : 34°43'43.42 '' N

	• Longitude : 002°04’19.71’’W **Elévation par rapport au niveau de la mer** 995.57m **Hauteur d’antenne** : 20 m
El Jadida	**Fonction :** Radar secondaire MSSR /Mode S pour le contrôle aérien en route. **Fréquences** : • Emission : 1030 Mhz • Réception : 1090 Mhz **Puissance** : 800 watts **Portée** : 250 NM ≈ 480 Km de rayon **Altitude Max** : 40 000 pieds ≈ 12 km **Position géographique** : • Latitude : 32°48’42.90’’N • Longitude : 008°55’06.65’’W **Elévation par rapport au niveau de la mer** : 95 m **Hauteur d’antenne** : 15 m
Tantan	**Fonction :** Radar secondaire MSSR / Mode S pour le contrôle aérien en route. **Fréquences** : • Emission : 1030 Mhz • Réception : 1090 Mhz **Puissance : 800 watts** **Portée** : 250 NM ≈ 480 Km de rayon **Altitude Max** : 40 000 pieds ≈ 12 km **Position géographique** : • Latitude : 28°28’40’’N • Longitude : 011°12’07.7’’W **Elévation par rapport au niveau de la mer :** 190 m **Hauteur d’antenne :** 15 m

TABLEAU 7: CARACTERISTIQUES DES SITES RADAR COUVRANT LE TERRITOIRE DU MAROC

Annexe C : Consultations des Offres des opérateurs

I. Solutions data pour les entreprises offertes par IAM

Parmi les services proposés par l’opérateur MAROC TELECOM on trouve :

- IP connexion
- Liaisons Louées Nationales Plus
- Interconnexion LAN to LAN
- Solution d’Accès Optique
- Frame Relay

On s’intéresse pour la conception de notre réseau au service dit IP connexion.

Principe

La solution proposée par l’opérateur MAROC TELECOM est le VPN IP, ce dernier permet de simplifier la communication entre les différents sites et collaborateurs. Ce réseau privé basé sur la fibre optique garantit performance, sécurité et fiabilité de bout en bout.

IP Connexion offre le choix entre une large gamme d'accès, de 64 Kbps à 34 Mbps :

Permanents : Liaisons Louées ou ADSL avec possibilité de raccorder votre site au réseau via la fibre optique

Commutés : RTC, MARNIS

Nomades : Accès nomade sécurisé via Internet ou GPRS pour une plus grande mobilité

Avantages

Solution simple et intégrée : Cette solution inclut l'accès, la fourniture du routeur, sa gestion et son administration par Maroc Telecom Flexible : Toute modification de l'architecture est prise en charge par les routeurs. Ce qui offre la possibilité d'augmenter, diminuer le nombre de sites ou encore modifier les débits d'accès, sans impact sur l'architecture.

Et le plus important, cette solution prend en charge :

La sécurité : Le protocole MPLS assure :

- L'étanchéité des flux de données
- L'authentification Radius sécurise l'accès des collaborateurs.

La sûreté : Utilisation d'une technologie certifiée MPLS

Disponibilité des sites et rapidité de transmission

Connectivité Any to Any qui permet l'échange de flux de données entre tous les sites sans rebond

Maîtrise : La tarification forfaitaire assure une facture sans surprise

Options :

VPN via ADSL:

En intégrant la technologie ADSL, Maroc Telecom Entreprises rend la solution réseau VPN IP accessible à toutes les entreprises.

Avec des tarifs particulièrement avantageux et une offre sous forme de pack incluant l'accès au service VPN IP, la fourniture et la gestion du routeur, on peut disposer rapidement et simplement d'un accès au VPN IP ADSL avec des débits allant jusqu'à 20 Mbs. Maroc Telecom offre également l'accès VPN ADSL avec un débit minimum garanti.

VPN via LL:

Classe de service	Types d'applications adaptées
Multimédia Plus	Applications utilisant intensivement la voix ou la vidéo
Multimédia	Applications qui nécessitent des délais de transit courts (voix)
Business critique	Applications de données extrêmement critiques et sensibles (transactionnels, client serveur sensible au temps de latence...).
Business	Applications de données critiques (base de données, ERP).
Standard	Applications et flux standard (messagerie, FTP)

TABLEAU 8: SERVICES DE L'OFFRE MAROC TELECOM

On peut choisir parmi cinq classes de services selon la nature des flux traités :

Le client dispose ainsi, quels que soient le volume et la sensibilité des données transférées, du service le mieux adapté aux exigences de qualité de service et de sécurité du client.

Intranet 3G :

L'Intranet 3G est une solution d'accès au VPN de l'entreprise via la technologie 3G Mobile, pour nous, la mobilité n'est pas notre premier soucis donc c'est inutile de détailler cette proposition.

Option de secours : MARNIS, ADSL :

Maroc Telecom permet au client d'améliorer la disponibilité de ses sites à travers son offre Secours Marnis ou ADSL. Le client épargne ainsi l'activité de votre entreprise de conséquences préjudiciables causées par une indisponibilité des sites et réduisez les coûts engendrés par le ralentissement de l'activité.

II. Solutions data pour les entreprises offertes par INWI

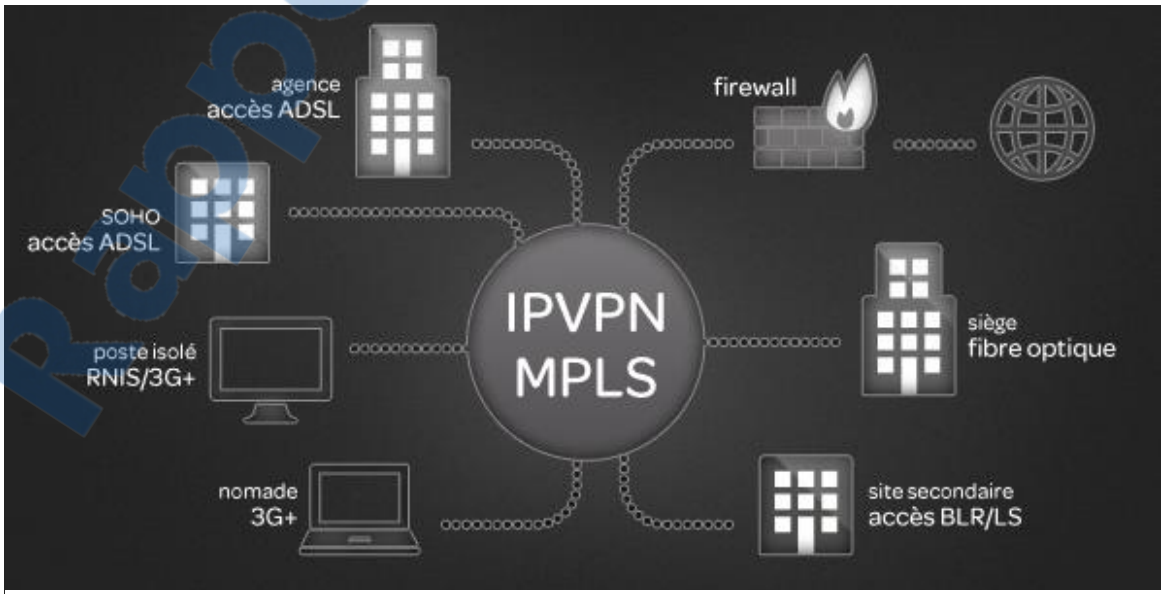


FIGURE 32: OFFRE INWI - ARCHITECTURE

Toujours pour les données, l'opérateur INWI offre les services suivants :

- Service Lan to Lan
- Service IP VPN MPLS
- Service Liaisons Louées Internationales
- Service internet haut débit
- Service internet mobile 3G
- Service extranet

Le service qui repend à mes perspectives est le service IP VPN MPLS. Cette solution offre :

Accès sécurisé au réseau d'entreprise

L'accès et les flux sont entièrement sécurisés et cloisonnés vis-à-vis des autres clients d'inwi.

Haut débit de connexion

Le bénéfice d'interconnexions à haut débit et la possibilité de la mise en place d'une gestion de la qualité de service afin d'optimiser les flux métiers et la bande passante.

Flexibilité

Possibilité de choisir une solution parmi une très large gamme de débits (symétriques ou asymétriques, garantis ou non), de 256 Kbps à 100 Mbps. L'accès peut être différencié par site, qu'il soit ou non permanent.

Services clés en main

inwi réserve une partie de son infrastructure réseau nationale pour votre réseau privé. Les équipements d'accès sont loués et leur maintenance est assurée sur les sites du client. Il bénéficie aussi d'un extranet permettant de suivre en temps réel l'état de son réseau.

Haut niveau de service

La sécurité est assurée par une redondance complète des équipements cœur de réseau et les liens sont sécurisés par un accès de secours.

Dans le cadre de sa qualité de service client, inwi prend les engagements suivants :

- garantie d'un temps de rétablissement minimum
- garantie d'un taux de disponibilité annuel
- garantie de taux de transit et de pertes de paquets
- garantie d'un temps de rétablissement inférieur ou égal à 4 heures
- engagement sur des délais de livraison

III-Solutions pour les entreprises offertes par MEDITEL

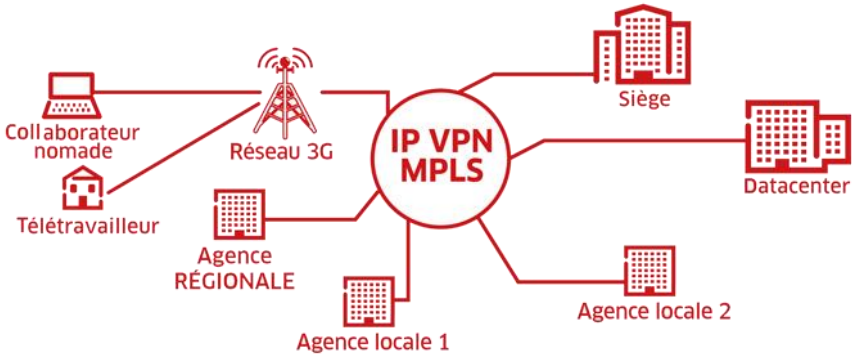


FIGURE 33: OFFRE MEDITEL - ARCHITECTURE

L'offre de connectivité nationale IPVPN de méditel permet de bâtir un réseau privé IP entre les sites, avec un haut niveau de sécurité et de performance.

En confiant la fourniture et la gestion de votre réseau IPVPN aux experts de méditel : routeurs, garanties, tables de routage, et sécurité, ce qui réalise de réels bénéfices en temps et en coûts télécom, l'entreprise peut donc se consacré au développement de ses activités plutôt qu'à la gestion quotidienne de son réseau.

Les avantages :

- **Performance :** Le service IPVPN méditel est basé sur un réseau MPLS (Multi-Protocol Label Switching) exclusivement dédié aux entreprises qui offre un niveau de sécurité extrêmement élevé.
- **Accompagnement :** Le service IPVPN est une solution d'interconnexion multi-sites fournie clés en main par méditel : les routeurs et les accès sont fournis et installés sur chaque site, administrés et supervisés par le Network Operation Center (NOC) de méditel, en heures et jours ouvrés et 7j/7, 24h/24 en option premium.
- **Flexibilité :** Possibilité d'augmenter, diminuer le nombre des sites ou encore modifier les débits d'accès, sans impact sur votre architecture.
- **Engagement :** solides engagements avec les meilleures garanties de performance, de disponibilité et de continuité de service de votre réseau.
- **Extranet de pilotage :** Via une interface Web Sécurisée, le client garde un aperçu en temps réel de la performance de votre réseau.

Options !

Intranet VPN 3G :

Avec le service Intranet VPN 3G méditel, les collaborateurs peuvent accéder en mobilité, à tout moment et en toute sécurité à tous types d'applications métiers de votre entreprise depuis leurs PC, avec tout le confort du haut débit mobile 20 Mbps.

Classes de services :

méditel propose quatre catégories de qualité de service pour distinguer les trafics, à savoir :

- **Gold** pour les applications extrêmement critiques qui nécessitent des délais de transit courts (voix et vidéos) ;
- **Silver** pour les applications de données critiques et sensibles (transactionnels sensibles au temps de latence, etc.) ;
- **Bronze** pour les applications de données type base de données ;
- **Standard** pour les applications et flux standard (messagerie, ftp, etc.).

Secours :

Pour obtenir une meilleure garantie de disponibilité, méditel peut connecter les sites au réseau IP VPN via :

Un lien d'accès redondant (actif/passif ou actif/actif) ;

Un routeur redondant ;

Un lien Backup RNIS.