N° d'ordre : 030-16/M2/TCO Année Universitaire : 2015 / 2016

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT TELECOMMUNICATION

MEMOIRE

en vue de l'obtention

du DIPLOME de Master

Titre : Ingénieur

Domaine : Sciences de l'Ingénieur

Mention : Télécommunication

Parcours : Ingénierie des Réseaux et Systèmes

par : **ABDOURAMANE ATTOU BOUNOU Nafissa**

DENSIFICATION DE L'ADS-B DANS LA FIR D'ANTANANARIVO

Soutenu le 13 Janvier 2017, devant la Commission d'Examen composée de :

Président :

M. RAKOTOMALALA Mamy Alain

Examinateurs :

M. Boto J.E ANDRIANANDRASANA

M. RANDRIAMITANTSOA Andry Auguste

M. ANDRIAMANALINA Ando

Directeur de mémoire :

M. RAKOTONDRAINA Tahina Ezéchiel

Encadreur professionnel :

M. RAFANAMBINANTSOA Valohery

REMERCIEMENTS

Avant tout, je loue DIEU TOUT PUISSANT, pour toute la grâce, la force, la santé, le temps et tous les bienfaits qu'il m'accorde. C'est par ta grâce Seigneur que j'ai mené à bien mes années d'études à l'Ecole Supérieure Polytechnique d'Antananarivo, et à terme ce mémoire. Gloire à toi mon Dieu.

J'exprime également ma profonde gratitude à :

- Monsieur ANDRIANAHARISON Yvon, Professeur Titulaire, Directeur de l'Ecole Supérieure Polytechnique d'Antananarivo, qui m'a donné l'opportunité de suivre la formation d'ingéniorat au sein de cette école.
- Monsieur RAKOTOMALALA Mamy Alain, Maître de conférences, Chef de Département Télécommunication, qui a daigné présider la soutenance de ce mémoire.

Par ailleurs, je tiens à exprimer mes vifs remerciements et toute ma reconnaissance à mes deux directeur et encadreur de mémoire : Monsieur RAKOTONDRAINA Tahina Ezéchiel, Maître de conférences, et Monsieur RAFANAMBINANTSOA Valohery, Master en informatique spécialité Réseau, Ingénieur Réseaux Systèmes Informatiqies (RSI) à l'ASECNA, pour leur soutien et leur aide précieuse tout au long de la réalisation du présent travail.

Je remercie les membres du jury qui m'ont fait l'honneur d'examiner ce travail et de sacrifier leur temps pour assister à la présentation de ce mémoire, à savoir :

- Monsieur Boto J.E ANDRIANANDRASANA, Assistant d'enseignement et de recherche
- Monsieur RANDRIAMITANTSOA Andry Auguste, Maître de conférences
- Monsieur ANDRIAMANALINA Ando, Maître de conférences

Mes remerciements s'adressent aussi aux membres du corps professoral, ainsi que du corps administratif de l'ESPA, pour la valeur de la formation qui m'a été dispensée durant les années d'études passées au sein de cette école.

J'aimerais également remercier toute l'équipe RSI de la Représentation de l'ASECNA à Madagascar de m'avoir accueilli dans leur loco, et permis d'effectuer mon stage.

Je présente mes sentiments de reconnaissance les plus profonds à mes parents qui m'ont toujours apporté leur soutien moral et financier tout au long de mes études.

Un grand merci à tous les autres membres de ma famille, mes amis, et tous ceux qui de près ou de loin ont contribué à la réalisation de ce travail.

Merci à Tous et que le Ciel vous rende mille fois ce que vous m'avez offert !

Je dédie ce mémoire à mon très cher père Mr ATTOUBOUNOU Abdouramane.

TABLE DES MATIERES

ABREVIATIONS

A	ASECNA	Agence pour la SECurité de la Navigation Aérienne en Afrique et à Madagascar
	AFISNET	AFrican and Indian Ocean Satellite NETwork
	ADS	Automatic Dependent Surveillance
	ATS	Air Traffic Services
	ATC	Air Traffic Controller
	ATN	Aeronautical Telecommunication Network
	ACARS	Aircraft Addressing and Reporting System
	ADS-C	Automatic-Dependent Surveillance Contract
	ADS-B	Automatic-Dependent Surveillance Broadcast
	ADC	Air Data Computer
	ADIRS	Air Data Inertial Reference Unit
	AAC	Airline Administration Communication
	AOC	Airline Operation Communication
	ACARS MU	ACARS Management Unit
	ATSC	ATS Communication
	AMSS	Aeronautical Mobile Satellite System
	AES	Airborne Earth Station
	AIRCOM	Accès Intégrés Réseaux Capillaires Opérateurs Mobiles
	ASAS	Airborne Separation Assurance System
	ACAS	Airborne Collision Avoidance System
	AGDP	Air Ground Data Processing
	ATM	Air Traffic Management
	AMRF	Accès Multiple à Répartition de Fréquence
	AS	Autonomous Systems
	ADSL	Asymmetric Digital Subscriber Line
	ARP	Address Resolution Protocol
	ACL	Access Control List
	AH	Authentification Header
B	BGP	Border Gateway Protocol
C	CSMA/CD	Carrier Sense Medium Access / Collision Detect

	CDTI	Cockpit Display of Traffic Information
	CDMA	Code Division Multiple Access
	CMS-S	Server of Control and Monitoring System
	CA	Contrôleur aérien
	CPDLC	Controller-Pilot Data Link Communication
	CIDR	Classless Inter-Domain Routing
D	DVMRP	Distance Vector Multicast Routing Protocol
E	EADS	European Aeonautic Defence and Space company
	eBGP	external BGP
	EIGRP	Enhanced Interior Gateway Routing Protocol
	ESP	Encapsulating Security Payload
F	FIR	Flight Information Region
	ft	Feet
	FMS	Flight Management System
	FOM	Figure Of Merit
	FDMA	Frequency Division Multiple Access
	FPL	Flight Plan
	FDDI	Fiber Distributed Data Interface
	FCS	Frame Check Sequence
G	GPS	Global Positioning System
	GES	Ground Earth Station
	GNSS	Global Navigation Satellite System
	GSM	Global System for Mobile Communications
	GRE	Generic Routing Encapsulation
H	HFDL	HF Data Link
	HDLC	Hight Data Level Control
I	IRS	Inertial Reference System
	INS	Inertial Navigation
	IHM	Interface Homme Machine
	INTELSAT	International TELecommunications SATellite organization
	ISO	International Standardisation Organization
	IP	Internet Protocol
	IPsec	IP Security
	iBGP	internal BGP

	IBUC	Intelligent Block Upconverter
	INMARSAT	INternational MARitime SATellite
	IANA	Internet Assigned Numbers Authority
	IGMP	Internet Group Management Protocol
	ICV	Intégrity Check Value
	IKE	Internet Key Exchange
	ISAKMP	Internet Security Association and Key Management Protocol
L	LCMS	Local Controlling and Monitoring System
	LAN	Local Area Network
	L2F	Layer Two Forwardin
	L2TP	Layer 2 Tunneling Protocol
	LCP	Link Control Protocol
	LAC	L2TP Access Concentrator
	LNS	L2TP Network Server
M	MSK	Minimum Shift Keying
	MCDU	Multifunction Control Display Unit
	MSSR	Monopulse SSR
	MMI	Multi Media Interface
	MAC	Media Access Control
	MSDP	Multicast Source Discovery Protocol
	MBGP	Multicast Source Discovery Protocol
	MCPC	Multiple Channel Per Carrier
	MPPC	Microsoft Point to Point Compression
	MPPE	Microsoft Point-to-Point Encryption
N	NM	Nautical Mile
	NIC	Navigation Integrity Category
	NUC	Navigation Uncertainty Category
	NAC	Navigation Availability Category
	NAS	Network Access Server
	NCP	Network Control Protocol
O	OACI	Organisation de l'Aviation Civile Internationale
	OSI	Open System Interconnection
	OSPF	Open Shortest Path First
P	PSR	Primary Surveillance Radar

	PGI	Progiciel de Gestion Intégrée
	PIM	Protocol-Independent Multicast
	PIM-DM	PIM Dense Mode
	PIM-SM	PIM Sparce Mode
	PIM SDM	PIM-Sparce Dense Mode
	PIM-SSM	PIM Source-Specific Multicast
	PPP	Point to Point Protocol
	PAP	Password Authentification Protocol
R	RSI	Réseaux Systèmes Informatiques
	RADAR	Radio Detection And Ranging
	RF	Radio Fréquence
	RCMS	Remote Controlling and Monitoring System
	RFC	Requests For Comments
	RNIS	Réseau Numérique à Intégration de Services
	RPV	Réseau Privé Virtuel
	RIP	Routing Information Protocol
	RP	Rendez-vous Point
	RPT	Rendez-vous Point Tree
	RTP	Real Time Transport Protocol
	RTC	Réseau téléphonique commute
S	SSR	Secondary Surveillance Radar
	SDU	Satellite Data Unit
	SITA	Société Internationale de Télécommunication Aéronautique
	STDMA	Self Organise TDMA
	SIL	Surveillance Integrity Limit
	SFS	Service fixe par satellite
	SMS	Service mobile par satellite
	SRS	Service de radiodiffusion par satellite
	SCPC	Single Channel Per Carrier
	SSL	Secure Socket Layer
	SPT	Shortest Path Tree
	SA	Security Association
	SPI	Security Parameter Index
	SAD	Security Association Database

	SPD	Security Policy Database
	SPT	Spanning Tree Protocol
T	TDMA	Time Division Multiple Access
	TCAS	Traffic Collision And Alerting System
	TDMA	Time Division Multiple Access
	TCP	Transmission Control Protocol
	TTL	Time To Live
U	UTC	Temps Universel Coordonné
	UAT	Universal Access Transponder
	UIT	Union Internationale des Télécommunications
	UDP	User Datagram Protocol
V	VHF	Very High Frequency
	VDL	VHF Data Link
	VSAT	Very Small Aperture Terminal
	VPN	Virtual Private Network
W	WAN	Wide Area Network

INTRODUCTION GENERALE

Depuis la fin de la deuxième guerre mondiale l'aviation civile a connu un essor extraordinaire car les efforts fournis pour développer l'aviation militaire ont été réorientés pour le développement du transport aérien civil. On assiste alors à un accroissement du trafic mondial.

Face à cet accroissement du trafic les espaces aériens se trouvent de plus en plus encombrés. Il fallait donc trouver des moyens pour le rendre sûr avec une régularité maximale pour les avions. Deux possibilités s'offrent alors à l'aviation civile internationale, en plus de la réglementation de la circulation aérienne uniformisée au niveau de tous les états signataires de la convention de Chicago, l'une consiste à un développement des moyens de navigation de plus en plus précis à bord des aéronefs et l'autre à l'installation des moyens de navigations et de surveillance basés au sol. Ces moyens au sol doivent être d'une fiabilité et d'une intégrité absolue.

Afin de résoudre efficacement le problème de la surveillance des aéronefs trois moyens sont utilisés en général : le RADAR, l'ADS-C, et l'ADS-B. Pour des organismes comme l'ASECNA ou « Agence pour la Sécurité de la Navigation Aérienne en Afrique et à Madagascar », assurant la gestion du trafic aérien dans ses dix-huit Etats membres, la sécurité est d'une priorité absolue, d'où le choix d'implantation de ces trois types d'équipements en fonction de la zone géographique et de la densité du trafic.

Face au coût très élevé du RADAR et à la discontinuité de l'information fournit par l'ADS-C, l'ADS-B semble être le moyen le plus adéquat pour compléter la surveillance de toute la FIR d'Antananarivo. Actuellement, une seule station ADS-B est implanté à Diego, d'où le but du présent travail qui est la densification de l'ADS-B dans la FIR d'Antananarivo.

En effet, l'ADS-B est un système dans lequel l'avion envoie régulièrement sa position et d'autres informations par une diffusion radio à tous les utilisateurs intéressés. Une station au sol capte ces informations, puis ces dernières sont acheminées vers le centre de Contrôle aérien. On propose alors dans ce projet deux supports de transmissions pour l'acheminement de ces données, les VSAT, déjà utilisées par l'ASECNA, et l'Internet qui sera utilisé comme back up. Les transmissions se feront en multicast, et afin de sécuriser les données nous allons créer des tunnels VPN.

Afin de mieux comprendre comment nous allons procéder pour effectuer cette densification, il s'avère nécessaire d'adopter le plan suivant : le premier chapitre parlera des généralités sur les moyens de surveillance aéronautiques, dans le second nous allons faire une analyse de l'existant dans la FIR d'Antananarivo, ensuite nous allons parler des supports de transmission proposés. Et enfin, le travail se terminera par une simulation sous le logiciel GNS3 dans le dernier chapitre.

CHAPITRE 1 :
GENERALITES SUR LES MOYENS DE SURVEILLANCE AERONAUTIQUE

L'ADS-B étant au cœur de ce mémoire, dans ce chapitre nous allons voir en détail la technologie ADS-B afin de mieux comprendre son principe. Mais avant cela nous allons parler des autres moyens de surveillances aéronautiques qui ont existé bien avant l'ADS-B.

1.1 RADARS

Les radars de contrôle aérien appelés en anglais **Radio Detection And Ranging** sont des appareils utilisés dans la télédétection, afin de pouvoir repérer, pister et guider les aéronefs volant dans l'espace aérien autour d'un aérodrome ou des zones plus étendues. Les antennes sont souvent implantées dans les aérodromes. On distingue 2 types de radar utilisés pour le contrôle aérien civil : le radar primaire et le radar secondaire. [1]

1.1.1 *Radar primaire*

Le radar primaire ou **Primary Surveillance Radar** abrévié **PSR** est un type de radar pouvant couvrir une large portion d'espace défini. Il émet des ondes électromagnétiques qui sont réfléchies par les objets fixes ou mobiles (aéronefs, immeubles, oiseaux, …) se trouvant dans cet espace et qui peuvent réfléchir l'onde électromagnétique. Un radar primaire détecte ainsi tous les avions sans exception, indépendamment du fait qu'ils possèdent ou pas de transpondeur.

Pour éliminer les échos provenant des cibles fixes, on utilise l'effet de la vitesse de la cible sur l'écho. Les échos qui n'ont pas subi d'effet Doppler sont considérés fixes et éliminés.
Le radar primaire émet une onde électromagnétique sous forme d'impulsions de forte puissance, qui se réfléchissent sur la cible et dont on récupère les échos. La position de la cible est déterminée par :

- Le temps d'aller-retour de l'onde, donnant la distance de la cible à la station.
- Le pointage de l'antenne en azimut. Le diagramme d'antenne étant très directif, la cible est supposée se trouver dans l'axe de celui-ci.

Le radar primaire détecte tous les mobiles qui se trouvent dans l'espace qu'il couvre. La détection est dépendante de l'écho sur la cible. [1]

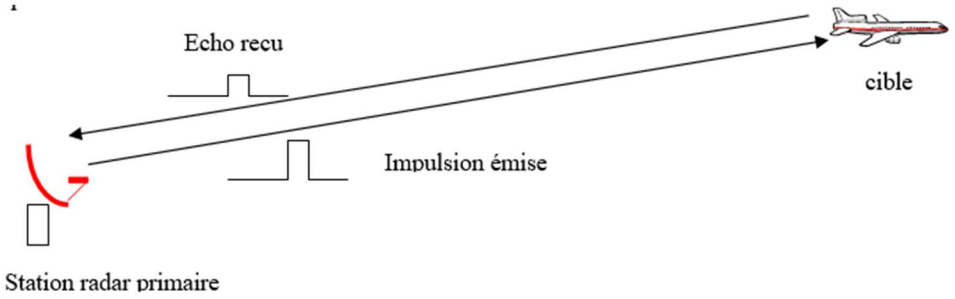

Figure 1.01 : *Principe du radar primaire*

1.1.1.1 Antenne

Comme il a été défini précédemment le radar primaire mesure en distance et en azimut la position de la cible. L'antenne est en général constituée d'un réflecteur parabolique éclairé par des cornets en émission et en réception. Elle est montée sur un support tournant afin de balayer les 360° d'azimut. Un codeur, monté avec le mécanisme d'entraînement de l'antenne, enregistre à chaque instant la position de l'axe de l'antenne (actuellement tous les 0,022°).

Le principe est d'avoir un diagramme en azimut comprenant un lobe principal de très grand gain et contenu dans un angle très faible en azimut (1,4° pour le STAR 2000). Les autres lobes doivent être très atténués. Cela permet de capter les cibles, à un instant donné, uniquement dans une plage d'azimuts étroite.

Le diagramme en site est large, afin de capter toutes les cibles situées sous des angles allant du sol jusqu'à 50° par rapport à l'horizontale. Les cibles ne sont donc pas différenciées en altitude. On ne sélectionne qu'une plage d'azimuts à la fois.

Figure 1.02 : *Antenne radar primaire partie en rouge*

a. Diagramme en azimut

Il est constitué d'un lobe principal à très grand gain et très directif :

- Gain>30Db
- Largeur à -3dB : 1,5 à 2,5°

- Largeur vers –40dB : environs 4°

Et de plusieurs lobes secondaires largement atténués : Le premier lobe secondaire sera vers –30dB.

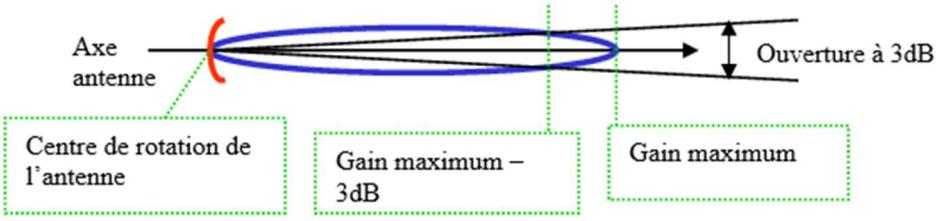

Figure 1.03 : *Diagramme d'antenne en azimut (dans le plan horizontal)*

b. Diagramme en site

Le diagramme doit couvrir les angles de site allant du sol à plus de 50°.

Les cibles lointaines seront vues par la partie basse du diagramme et les cibles proches par la partie haute.

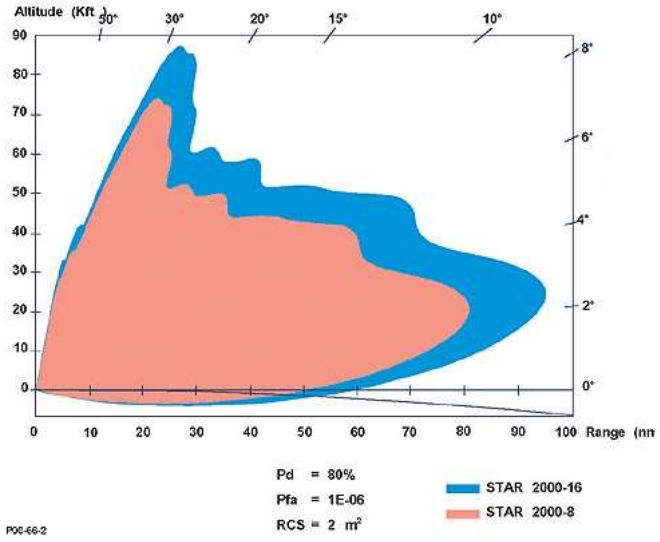

Figure 1.04 : *Diagramme d'antenne en site*

Le diagramme en site n'est pas directif, on ne peut donc pas caractériser deux cibles par leur différence de hauteur par rapport au sol. Ceci implique que le radar est incapable de faire une mesure d'altitude.

1.1.1.2 Mesure d'azimut

a. Repérage de la position d'antenne

Des repères suffisamment fins sont tracés sur le support tournant de l'antenne. Un lecteur, généralement optique, détecte ces repères et incrémente un compteur, dont la valeur représente la position de l'antenne en azimut. La précision est de l'ordre de 0,022°, pour nos radars. Les codeurs renvoient une information de position sur 14 bits, codée de 0 à 3FFFh (16384 repères). L'azimut 0 correspond au Nord géographique, qu'il est possible de recaler sur la baie électronique.

b. Principe du calcul de l'azimut de la cible

On suppose que la vitesse de la cible est négligeable par rapport à la vitesse de balayage du faisceau qui l'éclaire. En principe, la cible n'est éclairée que lorsqu'elle est en regard du lobe principal de l'antenne et les échos ne sont reçus que pendant cette période. En dehors de cette période, les échos sont trop faibles pour pouvoir être vus par le radar.

La fréquence de répétition des impulsions permet d'envoyer un certain nombre d'impulsions vers la cible et de recevoir un certain nombre d'échos, pendant le temps où la cible est éclairée par le lobe principal.

La position de l'antenne étant repérée à chaque instant de manière précise, on fait une moyenne avec les positions enregistrées des échos provenant d'une même cible.

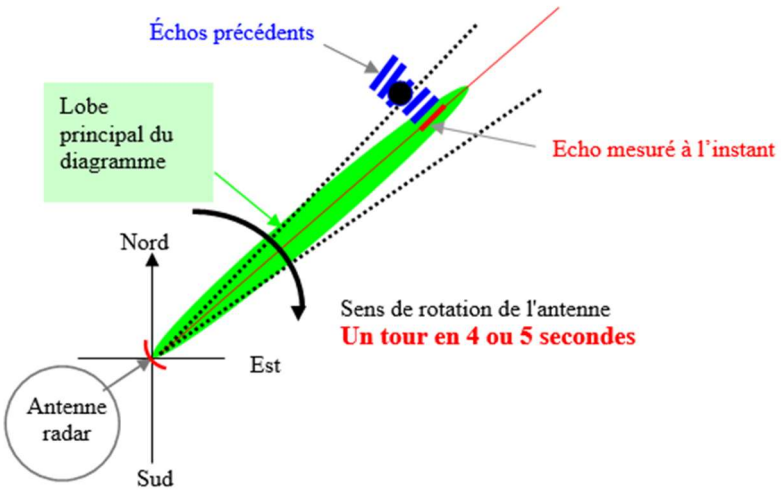

Figure 1.05 : *Principe de calcul d'azimut*

1.1.1.3 Ordre de grandeur du nombre d'échos reçus

Une impulsion est envoyée toutes les millisecondes environ. Sur un tour d'antenne, les échos sont reçus sur un petit secteur azimutal, correspondant au moment où la cible est balayée par le lobe principal de l'antenne.

Les vitesses de rotation des antennes, pour les radars d'approche, sont principalement 4 secondes ou 5 secondes.

Les radars sol tournent à 1 seconde.

Dans le cas d'un radar primaire d'approche, on reçoit environ une vingtaine d'échos, pour une cible. Le nombre d'échos peut varier suivant l'éloignement et la taille de la cible.

1.1.1.4 Paramètres influençant le nombre d'échos reçus en radar primaire

A l'entrée du récepteur, il existe un seuil au-dessous duquel on considère les signaux comme du bruit. C'est le seuil de sensibilité. Les signaux d'amplitude inférieure à ce seuil sont bloqués.

L'amplitude des échos dépend aussi de la capacité de la cible à réfléchir les ondes.

La taille de la cible et son éloignement influencent aussi cette amplitude. Une petite cible éloignée fournit moins d'échos d'amplitude suffisante qu'une grosse cible proche. Le nombre d'échos reçus est donc moins important pour la petite cible que pour la grosse.

1.1.1.5 Mesure de distance (oblique)

La distance est mesurée en convertissant le temps d'aller-retour de l'impulsion :

Distance= c.t/2, avec c vitesse de propagation (~3.10^8 m/s) et t temps d'aller-retour.

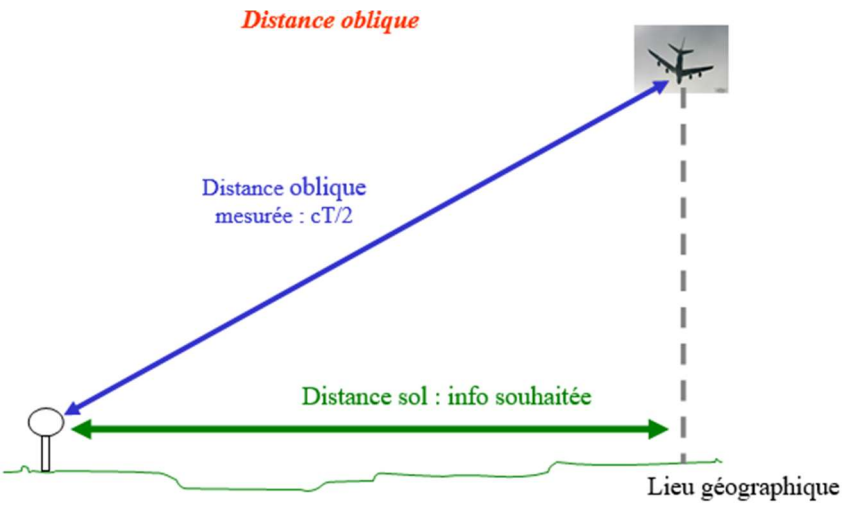

Figure 1.06 : *Mesure de distance oblique*

1.1.1.6 Précision du PSR

Les radars primaires doivent avoir une précision en distance inférieure à 60m, et en azimut inférieure à 0,15°. Dans 100% des cas, le radar situe l'avion à l'intérieur d'un cercle de rayon de 600m autour de sa position réelle.

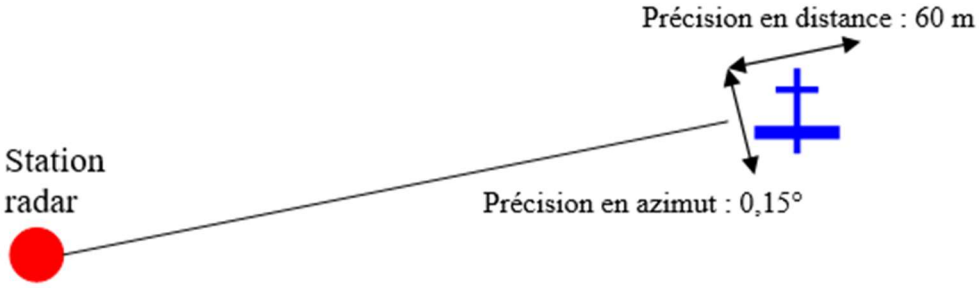

Figure 1.07 : *Précision d'un PSR*

1.1.1.7 Bandes de fréquence

Les bandes de fréquence, utilisées en radar primaire, sont en bande S (2 à 4 GHz) comprises entre 2,7 et 2,9GHz et en bande L (1 à 2 GHz) comprises entre 1,215 et 1,35GHz. Les radars sol utilisent la bande KU (12 à 18 GHz) entre 16 et 18GHz et la bande X (8 à 12 GHz) entre 9 et 11GHz.

La bande L est moins sensible aux perturbations atmosphériques, elle est donc plus performante pour la détection longue portée.

La bande S, du fait de la longueur d'onde plus petite, permet une meilleure précision et une taille des équipements plus petite. Mais, elle est plus sensible aux perturbations atmosphériques.

La taille de l'antenne, en bande L, est de l'ordre de 9x5m et, en bande S, de l'ordre de 5x3m. La structure, utilisée pour la bande L, est donc plus lourde que pour la bande S.

1.1.1.8 Portée

Pour un radar d'approche, on souhaite avoir une portée allant de 60 à 80 NM (Nautical Mile ou en français Mille Marin, 1NM = 1852 m). Par contre, le radar sol porte entre 4 et 8 NM.

Le signal est émis sous forme d'une porteuse UHF modulée en impulsions. Les impulsions se réfléchissent sur la cible et reviennent fortement atténuées au récepteur.

Notons que l'atténuation du signal radar primaire est fonction de la distance : La puissance émise doit faire un aller-retour entre l'antenne et la cible. Si la distance séparant les deux est notée R, la puissance qui revient à l'antenne est atténuée suivant un facteur en $1/R^4$.

De par la forte atténuation subit, on doit envoyer un signal fort vers la cible, pour espérer récupérer un petit signal exploitable. Les puissances d'émission sont de l'ordre de 10 à 50 Kilowatt, et le signal reçu autour de –105dBm.

1.1.1.9 Avantages et inconvénients du radar primaire

a. Avantages

- Le radar primaire n'a pas besoin que l'aéronef ait un équipement spécial à bord ou fasse une action spécifique pour être détecté. Il suffit que l'aéronef soit en portée du radar.
- Pour les radars utilisés en approche, la période de rotation de l'antenne est courte (4 à 5 secondes). Ceci permet d'avoir une image souvent réactualisée.

b. Inconvénients

- Le signal reçu étant faible, il peut être facilement perturbé. La précision de localisation des cibles s'en ressent.
- Le radar primaire ne peut pas fournir d'autres renseignements en dehors de la position en azimut et de la distance.
- Le traitement du signal est complexe.
- Le radar primaire nécessite l'utilisation de fortes puissances, donc un prix de revient cher.

1.1.2 ***Radar secondaire***

SSR ou **Secondary Surveillance RADAR** est le deuxième type de radar utilisé dans la surveillance aéronautique. Contrairement au PSR, le SSR ne détecte que les aéronefs équipés de transpondeur. Le système de surveillance radar secondaire est donc composé de deux éléments : une station sol interrogatrice et un transpondeur embarqué dans l'avion. La localisation se fait de manière analogue au radar primaire :

- La distance est donnée par l'écart de temps entre l'envoi de l'interrogation et la réception de la réponse.
- La position en azimut est donnée par le repérage du pointage de l'antenne en azimut

De même le diagramme d'antenne du radar secondaire marche selon un principe analogue à celui du radar primaire :

- Forte directivité en azimut
- Large lobe en site.

Les réponses reçues sont identifiées par un code et peuvent contenir l'altitude de l'aéronef. On peut donc disposer de trois informations sur la position de l'aéronef, au lieu de deux, ainsi que de l'identification. [1]
Remarquons que tous les radars secondaires actuels utilisent la technique Monopulse qui permet de calculer l'azimut d'un aéronef sur une seule réponse.

1.1.2.1 Principe de fonctionnement

Le signal est émis par le radar sous forme de paires d'impulsions dont l'espacement correspond au type d'interrogation. Ce sont les impulsions d'interrogation.
Celles-ci sont reçues par un équipement à bord de l'aéronef (le transpondeur) qui émet une réponse contenant le code souhaité.
Le transpondeur de l'aéronef émet ses réponses sous forme de trains d'impulsions.

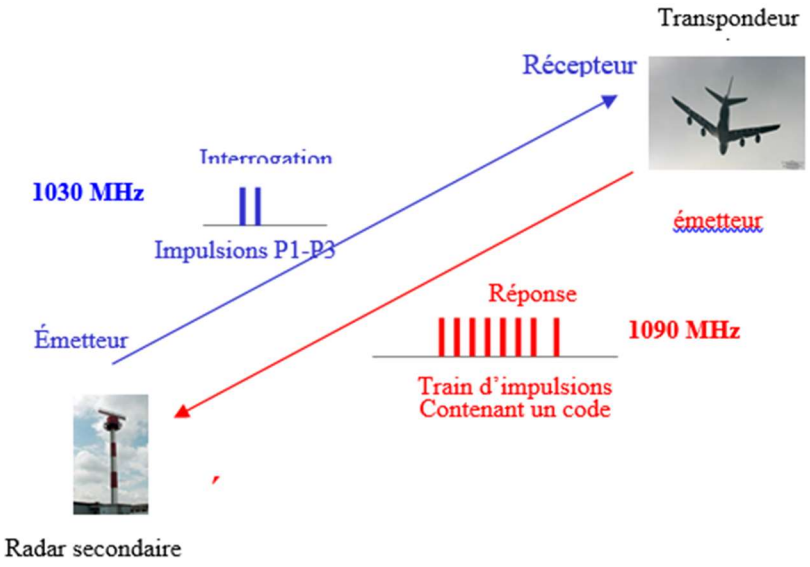

Figure 1.08 : *Mode de fonctionnement d'un SSR*

1.1.2.2 Signal émis par le radar

Les impulsions émises par le radar secondaire sont appelées P1 et P3 :

Figure 1.09 : *Largeur et espacement des impulsions en SSR*

La largeur fait 0,8µs. L'espacement peut prendre plusieurs valeurs dont deux valeurs pour les radars civils :

- **Mode A**, interrogation sur le code identificateur de l'avion : 8 µs
- **Mode C**, interrogation sur l'altitude de l'avion : 21 µs

Les paires d'impulsions sont émises alternativement en mode A et C. La fréquence d'émission des interrogations est d'environ 250Hz (toutes les 4 ms environ).

1.1.2.3 Fréquences et puissances

A l'émission, la fréquence porteuse sur laquelle on module les impulsions est unique et elle est de **1030MHz** quel que soit le radar secondaire**.** Et la puissance crête est de **1600 ou 2600Watts**.
A la réception la fréquence porteuse est de **1090MHz,** quel que soit le transpondeur. La puissance crête varie de **125 à 500Watts**.
Après émission, le transpondeur est bloqué pendant 125 µs.

1.1.2.4 Portée

Elle dépend de la période de répétition des interrogations. Il faut que la réponse revienne avant une nouvelle interrogation, sinon il y a un doute sur la distance.
Le radar secondaire interroge à 250Hz. La période de répétition est de 4ms. Avec 1µs correspondant à 150m, on obtient une portée théorique de 324NM. Elle est donc supérieure à la portée dont on a besoin (200 à 250 NM).

1.1.2.5 Précision du radar

Les radars secondaires doivent avoir une précision en distance inférieure à 70m, et en azimut inférieure à 0,08°.
Les radars secondaires ont en moyenne 100% de probabilité de voir l'avion dans un rayon de 240m autour de sa position réelle.

1.1.2.6 Avantages et inconvénients

a. Avantages

- La puissance nécessaire est moindre. Les signaux ne font qu'une fois le trajet entre le transpondeur et le radar.

- Le signal revenant de l'aéronef étant codé, le traitement de celui-ci par le radar est moins complexe que pour le primaire. L'aéronef est détecté plus facilement.
- L'information de niveau de vol peut être fournie au radar, par l'aéronef. On connaît donc l'altitude de l'aéronef.
- Le radar monopulse a une bonne précision de localisation.

b. Inconvénients

- L'aéronef doit posséder un transpondeur spécifique pour être détecté. Sinon, quoi qu'il fasse, il ne peut pas être vu.
- Le transpondeur de l'aéronef doit être allumé et en état de fonctionner. En cas de panne de transpondeur ou s'il est éteint, le contrôleur ne peut plus voir l'aéronef.
- Risque de Garbling ou enchevêtrement de réponses lorsque deux avions sont situés dans un azimut proche l'un de l'autre et que leurs distances à l'antenne radar diffèrent de moins de 3km
- Blocage du transpondeur suite aux nombreuses interrogations venant de plusieurs radars à proximité.

1.1.2.7 Radar mode S

a. Problèmes à résoudre

Le radar mode S est un radar secondaire qui permet de limiter les inconvénients tels que :

- La pénurie de code A, sur les routes IFR très fréquentées.
- Les risques de garbling dû au grand nombre d'aéronefs évoluant à la fois,
- Les transpondeurs se retrouvant bloqués par les nombreuses interrogations venant de plusieurs radars à proximité.

b. Fonctionnalités supplémentaires

Il permet une plus grande précision de l'information de niveau de vol : 25ft (Feet ou en français Pieds, **1ft = 0.3048 m**) au lieu de 100ft.
Enfin, il permet de passer un certain nombre d'informations supplémentaires sur le vol ou des informations techniques de l'avion.
Il doit rester compatible avec les transpondeurs de bord qui ne sont pas mode S.

c. Différents niveaux de surveillance

Le radar mode S peut être exploité suivant différents niveaux :

- La surveillance élémentaire : On récupère uniquement le code mode A et le code mode C, et on mesure la distance et l'azimut.
- La surveillance enrichie : L'avion dispose, à son bord, de bases de données normalisées interrogeables par le radar. Il existe 256 bases de données, appelées BDS. On peut obtenir le numéro de vol, le cap, l'altitude sélectionnée par les pilotes, etc….

Remarque : L'ASECNA Madagascar utilise pour la surveillance un système radar type MSSR ou Monopulse SSR. Il s'agit d'un radar secondaire fonctionnant en mode S implanté à l'aéroport d'Ivato.

Figure 1.10 : *Monopulse Secondary Surveillance Radar (MSSR)*

1.2 ADS ou Automatic Dependent Surveillance

1.2.1 *Définition OACI*

La Surveillance Dépendante Automatique est une application destinée aux services ATS (Air Traffic Services) (**surveillance**), dans laquelle les aéronefs transmettent automatiquement (**automatique**), sur une liaison de données air/sol, des données de position obtenues à l 'aide des systèmes embarqués de navigation (**dépendante**) et de relevé de position. [2]

Ces données comprennent au minimum l'identification de l'aéronef et une indication de position en trois dimensions. Des données supplémentaires peuvent être fournies selon les besoins.

Le système repose alors sur une idée simple : l'avion équipé de système de navigation moderne doit pouvoir envoyer automatiquement et régulièrement sa position aux services au sol. Les messages arrivent par le réseau ATN ou ACARS (voir paragraphe 1.2.2.3) au centre de contrôle où un calculateur très simple place sur une carte le plot représentant l'avion.

De plus, l'ADS donne une souplesse extraordinaire à la gestion du trafic et délivre le pilote et le contrôleur d'échanges routiniers. Il permet une surveillance authentique visant à obtenir au sol une image de la circulation aérienne permettant d'augmenter la capacité de l'espace aérien et la fluidité du trafic. Il s'avère particulièrement intéressant parce qu'il permet une révolution de la gestion du trafic dans tous les espaces où la couverture radar est impossible, inexistante ou insuffisante.

Il existe actuellement 2 types de technologie ADS :

- ADS-C (Automatic-Dependent Surveillance Contract)
- ADS-B (Automatic-Dependent Surveillance Broadcast)

Nous les détaillerons dans les prochains paragraphes.

1.2.2 *Eléments constitutifs de l'ADS*

Le système ADS est basé sur l'échange de données entre deux calculateurs : un à bord de l'aéronef et l'autre au sol. Ces calculateurs sont reliés au moins par un support de communication. Le système est donc constitué de trois segments :

- Segment bord
- Segment sol
- Segment de communication. [2]

1.2.2.1 Segment bord

Le système ADS bord est constitué des éléments suivants :

- Une avionique ADS composée de plusieurs modules qui sont connectés à d'autres systèmes pour répondre aux besoins bord de l'ADS ;
- Un système de gestion de vol (FMS ou Flight Management System) permettant de collecter les informations issues des équipements embarqués nécessaires à l'élaboration du contenu des messages. Ces informations peuvent être :
    - Les intentions avion issues du FMS

- Les paramètres de référence sol de position avion issus du GPS (Global Positioning System) ou de l'IRS (Inertial Reference System) ou INS (Inertial Navigation System)
- Les paramètres de référence air issus de l'ADC (Air Data Computer)

(Ou simplement des paramètres issus des ADIRS (Air Data Inertial Reference Unit))

- Une interface homme machine (IHM) permettant au pilote de recevoir et d'émettre des messages.
- Un support de communication pour acheminer et recevoir des données (réseau ATN ou ACARS).
- Un package intégrant les applications de connexions initiales (package : ensemble complet de programmes conçus par différents utilisateurs et destinés à un même type d'applications ou de fonctions)
- Une source de temps externe à la fonction ADS, référencée par rapport à l'heure UTC qui permet de dater les reports de position (la tolérance d'écart par rapport à l'heure UTC ne doit pas excéder 2 secondes).

1.2.2.2 Segment sol

Le système ADS sol est constitué des éléments suivants :

- Un système de traitement des données de vol, qui est le serveur de l'application ADS au sol capable de répondre aux besoins opérationnels du système ATC ;
- Un support de communication pour acheminer et recevoir des données (réseau ATN ou ACARS) ;
- Un système de visualisation (IHM) composé d'un écran, d'un clavier, d'une souris et d'une imprimante permettant au contrôleur :
  - de visualiser le trafic aérien à travers les trajectoires des avions,
  - de recevoir et transmettre des messages sur liaison de données,
  - d'être averti de l'existence d'un conflit potentiel par des alarmes sonores et visuelles.
- Une application logicielle pour l'exécution du contrat rempli par l'ADS (cas de l'ADS-C) selon les besoins opérationnels du système sol.

1.2.2.3 Segment de communication

Le segment de communication est le support de communication qui permet une liaison bidirectionnelle entre le calculateur bord et le calculateur sol. Deux réseaux de communication se présentent pour répondre aux besoins de l'ADS en matière de communication. Il s'agit du :

- Réseau ACARS qui utilise le Satellite et la VHF ;
- Réseau ATN normalisé par l'OACI, et constitué des sous réseaux Satellite, Mode S, VDL (VHF Data Link) et HFDL (HF Data Link).

a. Réseau ACARS

Le réseau ACARS **(Aircraft Addressing and Reporting System)** est un système de communication, d'adressage et de compte rendu introduit en 1976. Il était initialement utilisé par les compagnies aériennes pour l'acheminement des messages AAC (Airline Administration Communication) et AOC (Airline Operation Communication) par liaison de données. De nos jours, il est utilisé pour les besoins de l'ADS. [2]

Pour assurer une liaison de données, il est nécessaire d'avoir :

- A bord de l'avion, une avionique ACARS MU (ACARS Management Unit) qui inclut deux modems : le SDU (Satellite Data Unit), interface de communication pour le satellite, et le modem MSK (Minimum Shift Keying) connecté à une radio embarquée pour accéder au canal VHF.

  Par ailleurs, il est connecté à une unité écran/clavier (MCDU) et une imprimante pour l'interface pilote.
- Au sol, une station VHF et une station terrienne GES (Ground Earth Station) connectée à un réseau de fournisseur de service de télécommunication pour l'acheminement des messages aux différents utilisateurs potentiels.

L'ACARS n'offre pas une fonctionnalité assurant le contrôle d'intégrité et la surveillance de la disponibilité de la communication de bout en bout. Il y a toujours un risque de perte de message et le débit est limité à **2400 bits/s**. En effet, le mode d'accès est aléatoire : Quand une station veut transmettre un message, elle « écoute » d'abord la ligne pour déterminer si une autre station est en train de transmettre. Si la liaison est libre, la station transmet. Si deux ou plusieurs stations transmettent simultanément, leurs messages vont entrer en collision. Dès qu'une station détecte une collision, elle cesse l'émission, surveille le réseau et recommence à transmettre.

b. Réseau ATN

Jusqu'à ces dernières années, l'ACARS était le seul moyen de communication de liaison de données numériques air-sol disponible pour la communauté aéronautique. La mise sur le marché de système de communication par satellite, de transpondeur Mode S et de VDL, offre de nouvelles possibilités de communication air-sol numérique.

Afin d'éviter la coexistence d'une multitude de modes de communication numérique air-sol (Mode S, satellite, VDL), l'OACI a normalisé un nouveau concept nommé ATN **(Aeronautical Telecommunication Network).** Il est le réseau fédérateur de tous les sous réseaux (bord, air-sol, sol) intervenant dans la mise en place d'une liaison de données air - sol.

L'ATN a comme objectif l'interconnexion des différents sous réseaux. Cela, en définissant un plan d'adressage global permettant d'atteindre chaque système. Un routeur ATN permettra de choisir le moyen le plus approprié en fonction de la disponibilité et de la qualité de service requise, dans le cadre du modèle OSI (Open System Interconnection) de l'ISO (International Standardisation Organization).

❖ **Le sous réseau satellite : AMSS**

Le système INMARSAT (INternational MARitime SATellite), dont la vocation initiale était de fournir des liaisons de données par satellite au trafic maritime, est jusqu'à présent le seul fournisseur de communication par satellite pour l'aéronautique.

Les normes associées au système INMARSAT ont été modifiées et adoptées par l'OACI pour l'ATSC (ATS Communication) sous le sigle de AMSS (Aeronautical Mobile Satellite System). Ce système permet d'échanger de la voix numérisée et des données.

Le sous réseau air-sol de l'AMSS est constitué de trois entités :

- L'AES (Airborne Earth Station),
- Le GES (Ground Earth Station)
- Le satellite lui-même.

L'AES établit la connexion entre les différents réseaux embarqués. Le satellite relaie une liaison bidirectionnelle de communication entre l'AES et le GES. Le GES, implantée au sol, est reliée aux différents réseaux sol comme le réseau SITA (Société Internationale de Télécommunication Aéronautique).

La liaison par satellite permet d'avoir une couverture quasi mondiale. Cependant, des inconvénients majeurs subsistent tels que le coût des équipements, la facturation par un opérateur de télécommunication, les délais d'acheminement des messages.

❖ **Le sous réseau Mode S**

Le mode S du radar secondaire de dernière génération a été conçu pour s'affranchir des limitations techniques des radars secondaires traditionnels. Il assure la surveillance en interrogeant de manière sélective les transpondeurs à bord grâce à un code d'adressage individuel de l'avion (code sur 24 bits).

Outre cette fonction de surveillance, le mode S offre une possibilité de communication numérique. Il propose trois fonctions de liaison de données :

- ADS-B
- Service spécifique ou surveillance enrichie
- Service interopérabilité.

Ce mode S offre de nombreux avantages : il présente un haut niveau de sécurité et de performance, et sur la base de ce qui précède diminue la charge de travail du contrôleur. Il a aussi l'avantage de ne pas dépendre d'un opérateur de télécommunication privé (comme le réseau SITA/AIRCOM).

Malgré ses avantages multiples, il présente toutefois quelques faiblesses. Conçu au départ pour les besoins du radar secondaire de surveillance (SSR), certaines de ses caractéristiques telles que le format de message, la puissance de l'émetteur et les fréquences utilisées avaient déjà fait l'objet d'un consensus mondial. Modifier ces facteurs dans l'optique de l'ADS semble difficile mais pas impossible. Par ailleurs, le coût des équipements et les délais d'acheminement des messages constituent des inconvénients.

❖ **Le sous réseau VDL (VHF Data Link)**

Ce système réutilise une partie des canaux de la VHF analogique et de l'infrastructure au sol. Plusieurs technologies de liaison de données sont actuellement à l'étude pour permettre une transition du système ACARS, dont les performances sont limitées, à un système complètement adapté aux besoins ATSC et AOC/AAC.

- **VDL1** : Il s'agit d'une légère modification de l'ACARS pour le rendre compatible à l'architecture OSI de l'ISO. Elle a des limitations techniques qui lui sont reprochées (manque de fiabilité, performance incertaine en situation de trafic dense), le débit est

assez faible (**600bits/s**) et le mode d'accès au canal, qui est le **CSMA/CD** (Carrier Sense Medium Access / Collision Detect), est peu performant. Les nouvelles générations de VDL affichent de meilleures performances que le VDL1. Ce mode, bien que normalisé par l'OACI, ne sera probablement pas utilisé comme sous réseau ATN.

- **VDL2** : c'est un développement de VDL1 utilisant les mêmes bandes de fréquences et le même type d'accès au canal (**CSMA/CD**). Cependant, elle utilise une compression des données pour obtenir un débit plus élevé (**31500bits/s**) dans les canaux de 25 KHz de largeur dans la bande VHF.
- **VDL3** : le débit est le même, mais le mode d'accès au canal est de type **TDMA** (Time Division Multiple Access) avec synchronisation par la station sol. Ce qui permet d'assurer des temps d'accès précis et non plus aléatoires. La VDL3 permet d'avoir aussi des communications vocales.
- **VDL4** : Elle utilise toujours les mêmes bandes de fréquences et offre le même débit (**31500bits/s**) mais prévoit l'utilisation de **STDMA** (Self Organise TDMA). La VDL4 synchronise elle-même la porteuse et permet donc des communications air-air en l'absence de la station sol.

Actuellement, les aviations civiles européennes penchent plutôt pour la VDL2. Les Etats unis et le Royaume Uni sont intéressés par la VDL3 et la Suède par la VDL4. Cela, non pas pour ses applications en tant que sous réseau ATN mais pour ses fonctions de surveillance.

❖ **Le sous réseau HFDL (HF Data Link)**

Ce système réutilise une partie des canaux de la HF analogique et de l'infrastructure sol. Il prévoit la conversion de l'équipement HF pour la communication vocale en communication data Link et ceci, à faible coût.

Des études ont montré que la liaison de données HFDL peut être intéressante comme moyen de communication de liaison de données par satellite. En effet, compte tenu des effets d'atténuations liées aux scintillations ionosphériques, on estime que la disponibilité d'un système comprenant un satellite géostationnaire est de 99,40%. L'ajout d'un deuxième satellite géostationnaire ne fait gagner que peu de chose (disponibilité de 99,46%), alors qu'un système mixte (satellite et HF) atteint 99,94%.

1.2.3 *Teneur des comptes rendus ADS*

Les comptes rendus ADS seront composés des données suivantes : [2]

❖ **Identification de l'aéronef**

❖ **Bloc ADS de base**

- Position de l'aéronef en trois dimensions : latitude, longitude, et altitude/niveau
- L'heure
- Indice de qualité (FOM : Figure Of Merite) : indication de la précision des données de position.

❖ **Informations ADS facultatives**

En plus du bloc ADS de base, un message ADS peut comprendre l'une ou toutes les informations suivantes :

- Vecteur sol : route, vitesse sol, vitesse verticale de montée ou de descente
- Vecteur air : cap, vitesse indiquée ou nombre de Mach, vitesse verticale de montée ou de descente
- Profil projeté : prochain Waypoint, niveau prévu au prochain Waypoint, heure prévue au prochain Waypoint, prochain Waypoint +1, altitude prévue au prochain Waypoint+1, heure prévue au prochain Waypoint+1
- Renseignements météorologiques : vitesse du vent, direction du vent, température, turbulence
- Intention à court terme : prochaine position (latitude, longitude) et l'heure prévue
- Intention à moyen terme : Si un changement de niveau, de trajectoire ou de vitesse est prévu entre la position actuelle et la position projetée.
- Intention profil projeté étendu : Prochain Waypoint et jusqu'à 128 Waypoints prévus sur la route de l'aéronef.

1.2.4 *ADS-C*

L'ADS-C ou ADS à contrat, est un système pour lequel les messages sont générés automatiquement (sans intervention du pilote) par le système bord et envoyés au système sol dans le cadre d'un contrat. Les données contenues dans le contrat sont élaborées par des senseurs embarqués. L'ADS-C fonctionne donc en mode connecté. Le contrat est établi avec un destinataire unique identifié pour les besoins de Surveillance. Et un aéronef donné ne peut

supporter simultanément que **cinq contrats** : un avec sa compagnie (AOC) et quatre avec quatre centres de service du trafic aérien (ATS : Air Traffic Services). [3]

Les informations sont transmises en utilisant comme support de données la VHF, la HF, ou le satellite. Avec ce dernier il est possible de positionner les avions au-dessus des océans, ce qui est impossible avec les radars. Mais comme les liaisons par satellite sont couteuses, la cadence d'émission des informations est généralement faible **(5 à 30 minutes).**

Notons qu'avec l'ADS-C il est aussi possible du faire du CPDLC (Controller-Pilot Data Link Communication), qui est une communication pilote-contrôleur par liaison de donnée (un peu comme le chat).

1.2.4.1 Notion de contrat ADS-C et différents types

Un contrat ADS est un agrément entre le sol et le bord sur l'information à transmettre au sol, qui spécifie les conditions dans lesquelles les comptes rendus ADS débuteront ainsi que les données qu'ils contiendront. [3]
Il existe trois types de contrat ADS – C :

- Contrat sur demande
- Contrat périodique
- Contrat sur événement

a. Contrat sur demande

Le contrat sur demande permet au système sol de demander un seul compte rendu à un aéronef en spécifiant les données ADS facultatives requises en plus du compte rendu ADS de base.
Un contrat sur demande comprend :

- Le groupe ADS de base
- Le groupe additionnel.

N'importe quel nombre de contrats à la demande peuvent être établis séquentiellement avec l'aéronef. Si l'avionique peut se conformer au contrat sur demande, elle envoie le compte rendu demandé.

b. Contrat périodique

Ce contrat permet au système sol de demander des comptes rendus périodiques à un avion.
Un contrat périodique comprend :

- Le groupe ADS de base,
- Les informations facultatives requises,
- La fréquence T à laquelle les infos doivent être transmises,
- Le groupe additionnel avec une périodicité multiple de T

Il ne peut exister qu'un seul contrat ADS périodique à la fois entre un système sol et un aéronef donnés. Un nouveau contrat périodique remplace tout contrat périodique existant.

c. Contrat sur évènement

Un contrat sur événement permet au système sol de demander à l'avionique d'envoyer des comptes rendus ADS lorsque les évènements spécifiés se produisent.
Un contrat sur événement indique les types d'événement qui doivent déclencher les comptes rendus et les valeurs de seuil qui délimitent les types d'événement.

Un compte rendu d'événement ADS comprend :

- Le groupe ADS de base,
- Toute information supplémentaire requise par l'événement déclencheur
- Un accusé de réception positif

Il ne peut exister qu'un seul contrat événement à la fois entre un système sol et un avion, mais il peut contenir divers types d'événements. Ainsi, un nouveau contrat événement remplace tout contrat événement existant, et si plusieurs événements se produisent au même moment, l'avionique envoie des comptes rendus ADS séparés pour chaque événement.

Les types d'événements suivants ont été définis pour l'ADS :

- Changement de vitesse verticale,
- Changement de point de cheminement,
- Changement d'écart latéral,
- Changement de niveau,
- Ecart par rapport à la gamme de niveaux,
- Changement de vitesse anémométrique,
- Changement de vitesse sol,
- Changement de cap,
- Changement de profil projeté étendu,
- Changement d'indice de qualité (FOM= Figure Of Merit),
- Changement d'angle de route.

1.2.4.2 Mode d'urgence

L'établissement et le fonctionnement du mode d'urgence est une fonction qui permet à l'avionique d'amorcer le mode d'urgence sur instruction du pilote ou automatiquement. Le mode d'urgence est établi entre l'aéronef et tous les systèmes sol avec qui cet aéronef détient des contrats périodiques ou des contrats événement.

Les situations suivantes font l'objet d'un compte rendu d'urgence ADS :

- Urgence absolue,
- Panne des communications,
- Intervention illicite,
- Carburant minimal,
- Urgence médicale,

Tant que le mode d'urgence est en vigueur, les contrats périodiques existants sont suspendus. Les contrats événement et les contrats sur demande restent inchangés.

Un compte rendu d'urgence ADS comprend :

- Position (latitude, longitude, altitude)
- Heure
- Indice de qualité (FOM)
- Identification de l'aéronef (facultatif)
- Vecteur sol (facultatif)

Un compte rendu d'urgence ADS peut être annulé par le pilote lorsque la situation qui l'a provoqué n'existe plus. Dans ce cas, tout contrat périodique en vigueur avant la déclaration du mode d'urgence est rétabli.

1.2.4.3 Avantages et inconvénients

a. Avantages

- Utilisation pour la surveillance des zones sans couverture radar
- Amélioration de la détection et de la résolution de conflits (exemple : contrat sur événement pour surveiller les dépassements d'altitude/de vitesse autorisées)
- Transmission de l'information route « prévue »
- Liaison de données air/sol (comme pour le Mode S et l'ADS-B VDL mode 4).

b. Inconvénients

- Dépend entièrement de l'avion et de la véracité des données qu'il transmet.
- Plus coûteuse si liaison par satellite.
- Faible cadence d'émission des informations

1.2.5 ***ADS-B***

1.2.5.1 Principe de fonctionnement

Le principe de l'ADS–B (Broadcast) ou ADS par diffusion, est de transmettre automatiquement *(*sans commande du pilote*)* différents paramètres à intervalles réguliers, telles que l'identification de l'avion, sa position, sa route, sa vitesse… élaborés par des équipements embarqués (**Dépendance**), pour des applications de surveillance. Ces messages seront diffusés (**Broadcast**) par le biais d'une liaison de données vers des destinataires non désignés qui peuvent être d'autres avions, des stations sol, des véhicules sol… [3]

L'ADS-B fonctionnant en mode diffusion, il n'y a donc pas d'établissement de connexion. L'avion envoie régulièrement sa position et d'autres informations par une diffusion radio dite « **ADS-B out** » à tous les utilisateurs intéressés. Et pour pouvoir capter les informations émises en broadcast, le système de contrôle au sol doit aussi être muni d'un récepteur (antenne **ADSB in**). Comme pour un radar, on peut afficher les aéronefs sur un écran, avec l'altitude, le numéro de vol, etc…

Le taux de rafraîchissement proposé est de **10 secondes** pour les zones en route, **5 secondes** pour les zones terminales et **1 seconde** pour les opérations en surface. Ce taux de rafraîchissement permet de fournir des services de surveillance équivalents au radar (pseudo radar).

L'ADS-B peut être utilisé dans les environnements suivants :

- En zone de couverture radar pour compléter les données disponibles, améliorer la surveillance à bord et envisager d'éventuelles délégations de responsabilités du sol vers le bord,
- En zone désertique ou océanique où l'ADS-B permettrait d'améliorer la sécurité en fournissant à l'ATC et aux aéronefs équipés une image de l'environnement.

Un des avantages de l'ADS-B est que, puisque les avions émettent régulièrement leur position de manière omnidirectionnelle, il n'y a plus besoin de radar : une antenne radio au sol peut recevoir ces messages (station mode S), bien moins coûteuse qu'un radar. Pour cette raison, le déploiement de l'ADS-B est une alternative très intéressante dans les régions non équipées de radar. Dans ce cas bien sûr, pour que le contrôle au sol puisse connaître tous les avions, il doit y avoir une obligation d'emport d'un équipement ADS-B dans les espaces contrôlés.

a. Architecture embarquée : ADS-B Out

L'architecture ADS-B Out, disponible aujourd'hui sur de nombreux aéronefs, permet uniquement de transmettre les messages vers les utilisateurs équipés de récepteurs.
Sur la figure ci-dessous sont présentés :

- A gauche, les différentes sources où seront récupérés les données à bord de l'avion
- Au milieu, le bloc où seront générés les messages ainsi que les équipements de transmission
- Et enfin, à droite, les messages seront diffusés via la liaison de données.

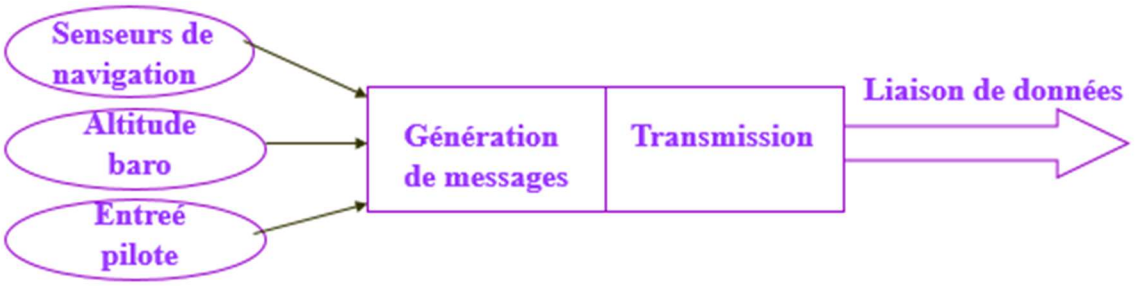

Figure 1.11 : *Architecture ADS-B Out*

b. Architecture embarquée : ADS-B In

L'architecture ADS-B In permet l'implémentation des applications air-air (ASAS : Airborne Separation Assurance System). Plus onéreuse que l'ADS-B Out, elle requiert, selon le type d'applications envisagées, un affichage de trafic (CDTI : Cockpit Display of Traffic Information), de nouvelles alertes, éventuellement un lien avec le pilote automatique.

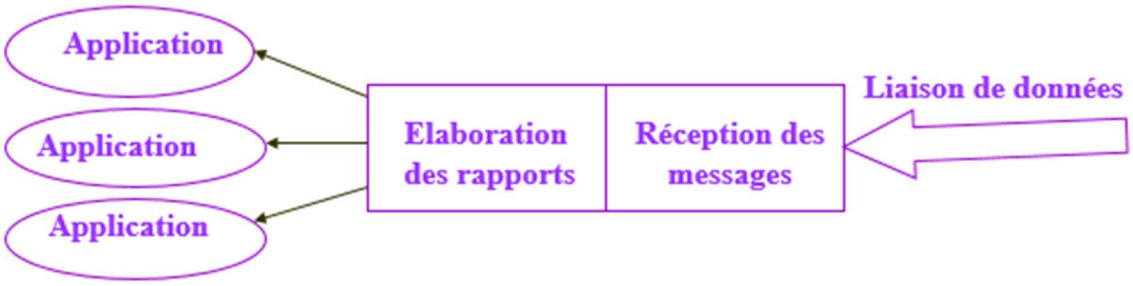

Figure 1.12 : *Architecture ADS-B In*

c. Architecture sol ADS-B

Selon le type de liaison de données utilisé, les messages ADS-B reçus au sol nécessitent plus ou moins de traitement avant d'être envoyés vers l'ATC, suivant le format spécifié (ASTERIX 21). Ces messages peuvent être ensuite fusionnés avec les autres moyens de surveillance disponibles (radar, ADS-C, plan de vol…) avant d'être affichés au contrôleur.

Figure 1.13 : *Architecture sol ADS-B*

Figure 1.14 : *Antenne ADS-B sol*

1.2.5.2 Message ADS-B

Un message ADS-B comprend les informations principales suivantes :

- La datation,
- L'identification de l'aéronef,
- La taille des aéronefs (largeur, longueur)
- La position (du point de référence de l'aéronef)
- La vitesse (vitesse sol/air, vitesse verticale)
- Le cap
- Les messages d'urgence ou de priorité,
- L'indicateurs de qualité

1.2.5.3 Indice de qualité : FOM (Figure Of Merit)

Le FOM est une indication de la précision des données ADS actuelles. En tant que moyen dépendant, la fiabilité des informations transmises est l'un des principaux avantages/inconvénients de l'ADS.

- Avantage car la qualité de l'information est la même quelle que soit la distance à la station de réception.
- Inconvénient car une piètre qualité des données de navigation peut induire des situations dangereuses.

L'information FOM ADS-B comprend :

- Une indication de la précision de la position de l'aéronef **(NIC :** Navigation Integrity Category**),**
- Une indication d'incertitude de la position de l'aéronef **(NUC :** Navigation Uncertainty Category**)**
- Une indication de la présence du système ACAS à bord **(SIL :** Surveillance Integrity Limit**),**
- Une indication de la présence de plusieurs systèmes de navigation à bord **(NAC :** Navigation Availability Category**)**

1.2.5.4 Différents types d'applications ADS-B

a. Applications air-air

Lors de la réception des données ADS-B, le pilote a la possibilité de voir les autres avions à proximité. Ce CDTI (Affichage cockpit d'informations sur la circulation aérienne) est la technologie de base qui permet au pilote de « voir et d'éviter » électroniquement les autres avions en mode largement passif. Indépendamment du radar au sol, le CDTI améliore considérablement la perception situationnelle du pilote et conduit à des opérations plus sûres et plus efficaces dans l'espace aérien. La technique ADS-B permettra également à l'avenir d'améliorer les systèmes de prévention des collisions.

b. Applications air-sol

L'ADS-B permet de fournir des données de surveillance aux contrôleurs du trafic aérien. Un avion en vol indique sa position, son altitude, son identification, ainsi que d'autres informations importantes, aux stations sols qui retransmettent alors ces données au centre de contrôle de trafic aérien. Ces informations permettent d'établir, de manière efficace, une surveillance à distance ou d'étendre voire de remplacer les capacités de surveillance actuelles. L'ADS-B air-sol permet d'assister les contrôleurs en matière de gestion de l'espace aérien.

c. Applications sol-sol

L'ADS-B indique la position précise et l'identification des avions et des autres véhicules équipés pour la surveillance de la surface aéroportuaire. Les avions et les véhicules, si correctement équipés, transmettent des informations concernant la position, la vitesse, le cap et l'identification, aux stations sols situées autour de l'aéroport. Ces informations sont transmises aux contrôleurs de la circulation aérienne et aux bureaux de gestion des aéroports.
La surveillance de la surface aéroportuaire améliorée via l'application de liaison de données ADS-B conduit à des opérations plus sûres et plus efficaces de la surface aéroportuaire, quelles que soient les conditions météorologiques.

1.2.5.5 Support de transmission de données de l'avion vers la station sol

Les données peuvent être transmises par trois types de support :

- Le 1090ES ("1090 MHz Extended Squitter")
- La VDL mode 4 ("VHF Data Link Mode 4")

- L’UAT ("Universal Access Transponder", sur 978 MHz)

L’OACI a recommandé l’utilisation de la liaison de donnée 1090 ES comme technologie de liaison de données mondiale aux fins de l’ADS-B. Les deux autres liaisons de données sont uniquement considérées pour des applications régionales. [1] [2]

a. Le 1090 ES

C’est une extension des transpondeurs radar mode S, qui émettent à 1090 MHz. Sur les avions équipés mode S et TCAS (Traffic Collision And Alerting System), ces transpondeurs permettent déjà d'envoyer et recevoir des messages de 56 bits, utilisés par le TCAS. La modification leur permet d'envoyer des messages de 112 bits sous le format DF17, suffisants pour l'ADS-B "out", et éventuellement de les recevoir (ADS-B "in").

Au sol, les informations ADS-B peuvent être reçues soit par un radar mode S, soit par une simple antenne omnidirectionnelle, bien moins coûteuse. Comme les avions commerciaux sont presque tous déjà équipés du TCAS, le 1090ES est une solution relativement peu coûteuse pour ces avions. Il n'en est pas de même pour les autres avions, en particulier les petits avions privés, pour lesquels l'installation ADS-B en 1090ES "à partir de rien" est très coûteuse.

Les informations transmises sont :

- La position de l’avion en vol toutes les 0,5 secondes
- La position de l’avion au sol toutes les 0,5 secondes si l’avion est en mouvement, sinon toutes les 5 secondes,
- L’identification et le type d’avion toutes les 5 secondes
- La vitesse toutes les 0,5 secondes,
- L’état de l’avion incluant le cap, toutes les 1.25 secondes
- Les messages d’urgence toutes les 0,8 seconde si nécessaire.

Le 1090 ES a une portée de **200 à 250 NM**, et peut supporter jusqu’à environ 475 avions. Il est totalement normalisé par l’OACI.

b. La VDL 4

C’est un système basé sur le STDMA (Self-organising Time Division Multiple Access) consistant à diviser une fréquence de communication en une multitude de créneaux correspondant à une opportunité pour un utilisateur équipé d’émetteur de diffuser son message.

Chaque aéronef réserve alors des créneaux où il émettra son message ADS, par le biais d'un protocole spécifique, lors d'une précédente transmission. Les utilisateurs ont accès au planning de réservation. Soixante-quinze (75) créneaux sont disponibles par seconde et par fréquence avec une taille de 256 bits.
Le taux de transmission est de 10 secondes en route, 5 secondes en zone terminale et 1 seconde au sol.
La VDL mode 4 a une portée de **140 à 200NM** et elle est totalement normalisée par l'OACI.

c. L'UAT (Universal Access Transponder)

Le principe de l'UAT est identique à celui de la VDL mode 4, sauf qu'il n'y a pas de protocole de réservation de créneaux. Plus de 3200 créneaux sont disponibles pour émettre un message ADS-B. C'est un système américain visant à réduire le coût d'implémentation d'un transpondeur ADS-B aux petits avions privés. Il permet la transmission d'un message incluant toutes les informations.
L'UAT opère dans la bande DME (**978 Mhz**), et il est en cours de normalisation par l'OACI.

1.2.5.6 Incidence opérationnelle

Si le GPS d'un avion calcule sa position avec une erreur, la position relative de cet avion par rapport aux autres sera fausse. Or Lorsqu'un radar calcule avec une erreur, celle-ci est la même pour tous les aéronefs. Leur position relative est donc juste.
De plus les messages envoyés par les transpondeurs n'ont pas de datation. Ce sont les récepteurs qui datent les messages. Le temps, entre la mesure de la position et l'envoi du message par l'avion, peut aller jusqu'à une seconde et diffère entre chaque avion.
Par conséquent, l'ADS-B est mieux adapté pour des régions à faible trafic, où l'installation d'un radar serait trop onéreuse. Il peut aussi combler un trou de couverture sur une approche. Dans ce cas, il vient en complément du radar.

1.2.5.7 Avantages et inconvénients

a. Avantages

- Amélioration de la sécurité des vols, grâce à la possibilité d'assurer la surveillance des aéronefs évoluant hors des zones de couverture des radars (zone désertique – zone océanique)

- Diminution de la charge de travail pilote et contrôleur en remplaçant les reports vocaux de position par des reports ADS
- Encombrement réduit
- Réduction des séparations latérales et longitudinales (par rapport aux séparations procédures)
- Amélioration de la détection et de la résolution de conflit
- Réduction des retards de taxi/décollage
- Détection opportune des erreurs d'insertion des points de cheminement et mesures correctrices associées
- Amélioration de la notification des situations de détresse en apportant une précision améliorée de la position de l'aéronef pour sauvetage plus rapide
- Complément au radar : basses altitudes, panne de radar
- Contrôle du respect du plan de vol en vigueur et détection opportune des écarts par rapport à la route autorisée et mesures correctrices associées
- Les données ADS-B sont bien plus précises que celles des radars, puisque leur précision est celle du GNSS (Global Navigation Satellite System)
- Taux de rafraichissement élevé
- Parce qu'il véhicule des informations plus précises que le TCAS, l'ADS-B pourrait également être utilisé pour améliorer ce dernier, et même pour concevoir un nouveau système anticollision embarqué.
- Réduction des coûts

b. Inconvénients

- Dépend entièrement de l'avion et de la véracité des données qu'il transmet
- Les séparations autorisées sont meilleures pour le radar (5 à 8 NM) que pour l'ADS (30NM)

1.2.6 *Tableau comparatif entre l'ADS-B et l'ADS-C*

Voici un tableau comparatif entre les 2 types de technologie ADS :

	ADS-C	ADS-B
Mode de transmission	Point à point	Broadcast
Acquittement	Oui	Non
Liaison de données	Lien ACARS, SATCOM, VDL2, VDL4	1090ES, UAT, VDL4
Périodicité	64 sec à plusieurs minutes	½ sec
Coût des com. air-sol	Oui (SITA et ARINC)	Non
Limitation des utilisateurs sol	Oui (5 max)	Non
Zones géographiques	Océanique, continentale	Continentale (portée station 200 NM)
Applications air-air	Non	Oui
Services associés	CPDLC	TIS-B, FIS-B

Tableau 1.01: *Comparaison entre l'ADS-B et l'ADS-C*

1.3 **Conclusion**

Ce chapitre nous a permis de comprendre le principe des trois moyens de surveillance qui sont utilisés dans les espaces gérés par l'ASECNA. Chacun a ses avantages et ses inconvénients mais l'ADS-B est de loin le moins coûteux et le plus facile à mettre en œuvre, tout en offrant une bonne précision des informations reçues.

CHAPITRE 2 :
ANALYSE DE L'EXISTANT

Voyons maintenant le rapport de l'existant sur le réseau de la représentation de l'ASECNA à Madagascar.

2.1 Topologie générale et nationale du réseau

L'ASECNA utilise la liaison par VSAT (Very Small Aperture Terminal) pour interconnecter les différentes représentations de l'agence dans toute l'Afrique, ce réseau satellite se nomme **AFISNET** ou **AFrican and Indian Ocean Satellite NETwork**. L'interconnexion est réalisée par la location d'une bande de fréquence sur le satellite géostationnaire 10 02 d'INTELSAT (voir paragraphe 3.1.1.3). [4]

Voici une portion de ce réseau pour la représentation de Madagascar.

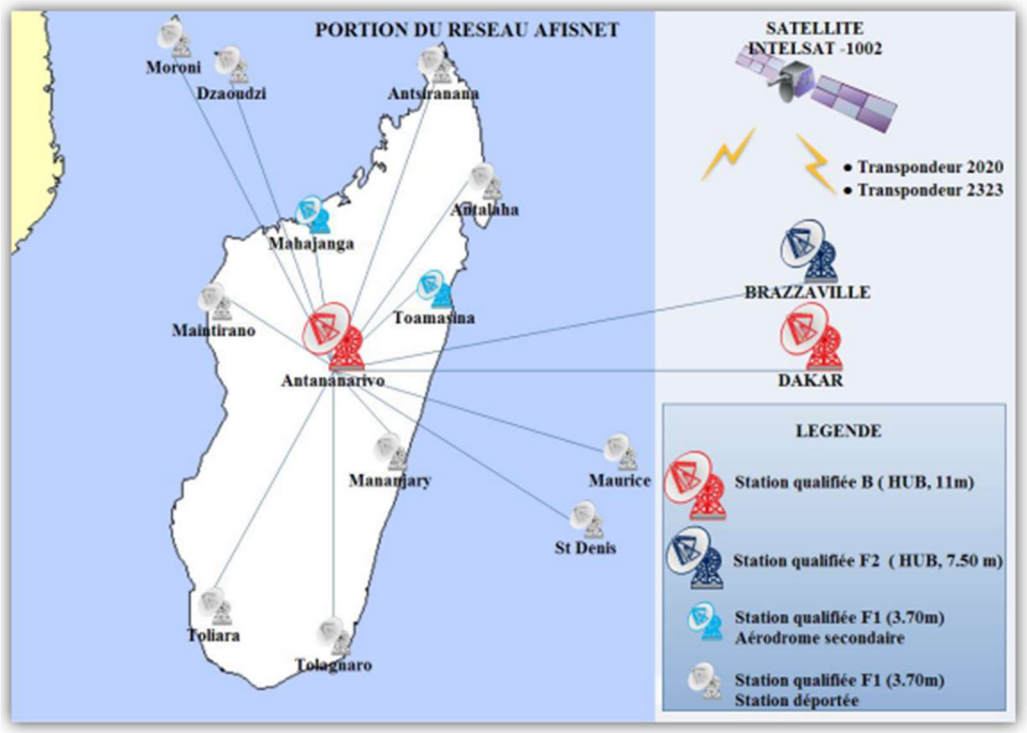

Figure 2.01 : *Portion du réseau AFISNET pour la représentation de Madagascar*

Comme la Figure 2.01 le montre, la topologie du réseau satellite de l'ASECNA possède une structure hybride, soit à la fois maillée et en étoile (voir paragraphe 3.1.2.2). En étoile pour l'interconnexion locale au sein d'une représentation et maillée pour l'interconnexion inter représentations. Dans le cas de Madagascar, le HUB du réseau VSAT se trouve à Ivato. Pour

que les stations VSAT déportées puissent communiquer entre elles, toutes les informations devront être relayées par ce HUB avant d'être envoyées vers le site destinataire.
La Figure 2.02 illustre ce relai.

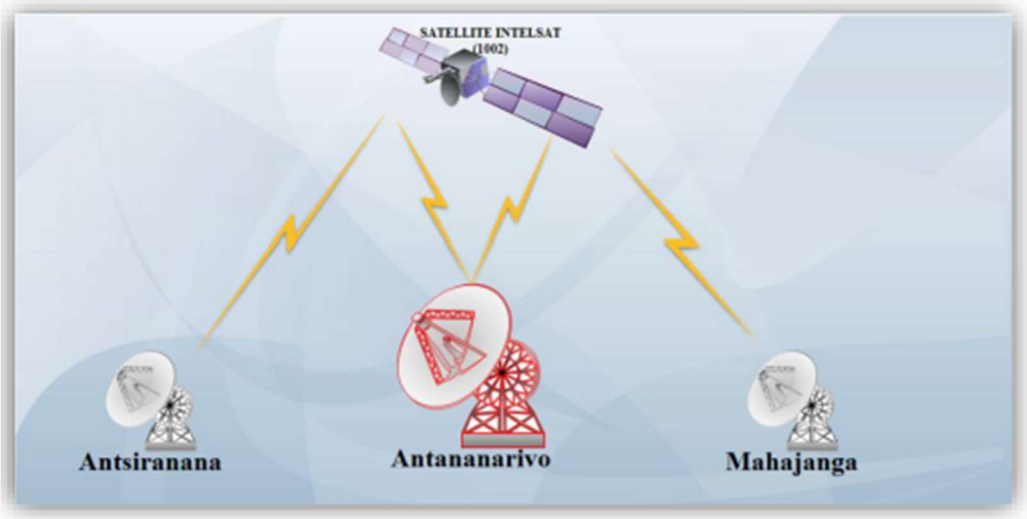

Figure 2.02 : *Relai d'information via le HUB d'Antananarivo*

La location de bande de fréquence sur INTELSAT est effectuée sur 2 transpondeurs en bande C, le **transpondeur 20 20 en mode d'accès FDMA** pour la transition des données opérationnelles (données ADS-B, communications vocaux entre Pilote et contrôleur aériens via les antennes VHF sur les stations déportées) et le **transpondeur 2323 en mode d'accès TDMA** (bande de 30 Mhz) pour la transition des données Internet et « Corporates » dont :

- 10 Mhz pour l'Internet,
- 20 Mhz : pour les applications «Corporates » soient : Mails, PGI, Paie, etc.

Figure 2.03 : *Antenne VSAT, HUB d'Ivato (11 mètres)*

2.2 Interconnexions nationales et internationales

L'agence utilise pour les liaisons nationales et internationales le réseau VSAT AFISNET. Comme la station d'Ivato est le HUB, soit le centre du réseau pour la représentation de Madagascar, toutes les liaisons seront donc ramenées vers celui-ci. Pour que les données puissent être acheminées via le réseau AFISNET, elles doivent passer par divers équipements.

Le **multiplexeur** est un équipement ou circuit permettant en émission de concentrer sur une même voie de transmission différents types de liaisons (voix, IP, asynchrone, …) vers une même et unique sortie numérique ; en réception, il effectue l'opération inverse soit le démultiplexage. Un **modem satellite** (modulateur-démodulateur) quant à lui, sert en émission à convertir les données numériques multiplexées en signal modulé (en bande L) ou signal analogique afin que les données puissent être acheminées sur le réseau VSAT, et inversement en réception. Chaque modem représente une liaison unique vers un site, ainsi sur chaque site distant, un modem parallèle doit exister pour que la démodulation puisse être effectuée. On utilise ensuite les **« combiner »** et **« splitter »** pour combiner les câbles coaxiaux en émission (**TX**) ou les distribuer en réception (**RX**) afin que tous les modems puissent utiliser une antenne unique pour envoyer ou recevoir les données. La dernière partie à passer est le circuit RF ou Radio Fréquence utilisant la technologie IBUC pour l'ASECNA permettant de convertir en émission la fréquence en bande L, utilisée en locale, en bande C pour accéder au satellite et inversement en réception. La Figure 2.04 illustre l'interconnexion des équipements.

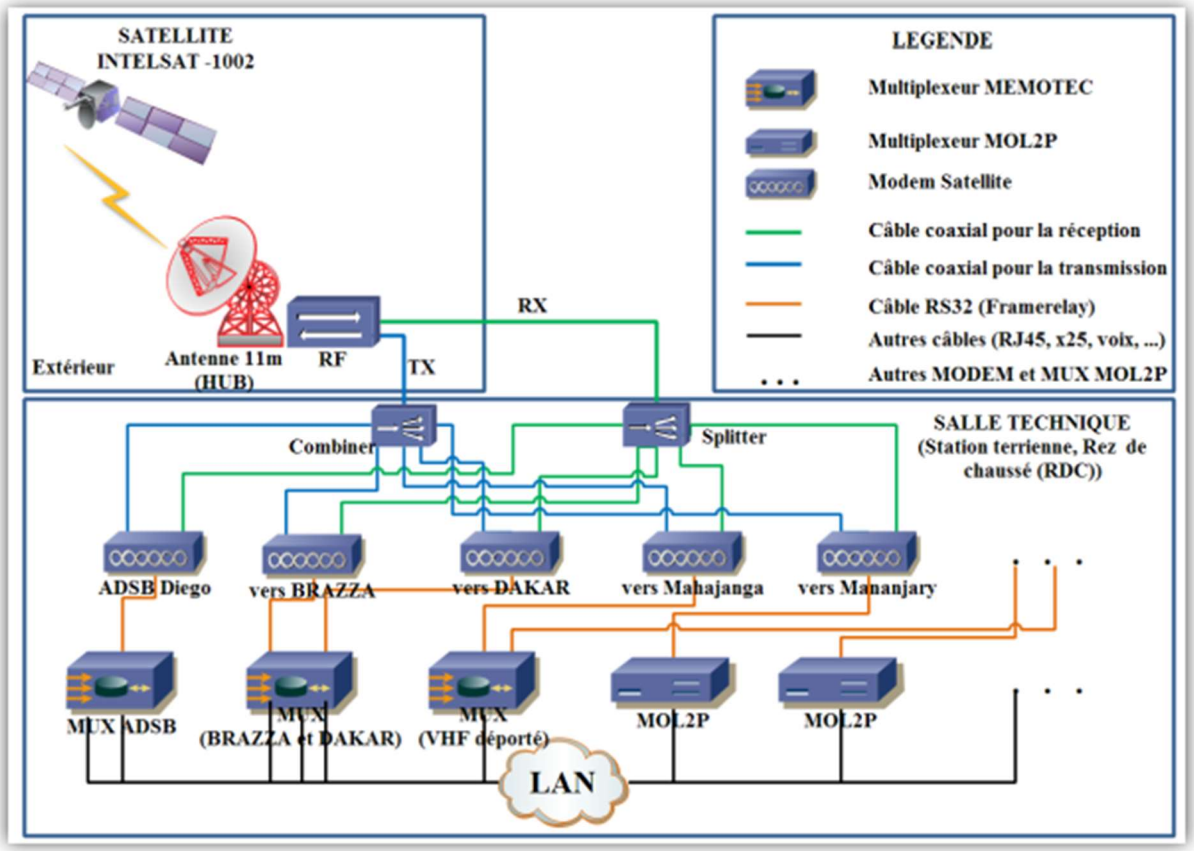

Figure 2.04 : *Interconnexion des modems et multiplexeurs du site d'Ivato*

Nb	Type		Caractéristiques	Utilisation
2	Modems satellite	i-Direct	Support IP (pas besoin de MUX)	Internet Données Corporates
2		COMTECH	Support IP	Deport Radar vers Moroni
20		DATUM	RS32 Frame Relay	Liaisons vers les stations déportées et FIR adjacentes (Maurice, Réunion)
3	Multiplexeurs	MEMOTEC CX950E	Support voix, IP, asynchrone, X25, RS32 Frame Relay	**Report ADS-B Réunion et Antsiranana**
				VHF déporté
				Liaison Brazza et Dakar
9		MOL2P	Support voix, asynchrone, X25, RS32 Frame Relay	Voix, messages RSFTA, supervision stations déportées, messages SMT

Tableau 2.01: *Equipements d'interconnexion nationales et internationales*

La Figure 2.04 ne présente qu'une partie de l'interconnexion des équipements, mais le Tableau 2.01 liste les effectifs et les rôles des multiplexeurs et modems utilisés sur le site d'Ivato afin d'assurer la liaison VSAT sur le réseau AFISNET.

La Figure 2.05 illustre l'emplacement de ces équipements dans la Station Terrienne d'Ivato.

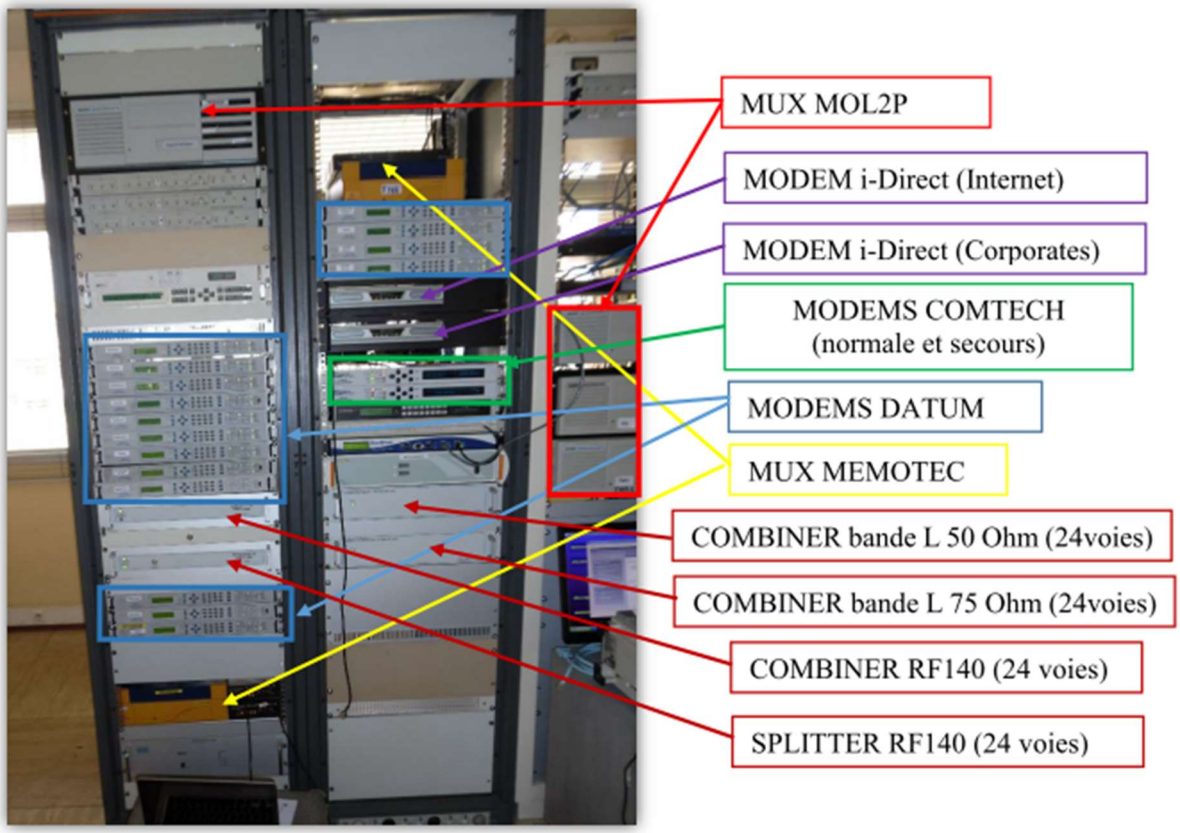

Figure 2.05 : *Partie de la baie contenant les équipements d'interconnexion satellites*

2.3 **Routage**

En ce qui concerne le routage, l'ASECNA utilise encore un routage statique dans chaque représentation, aucun routage dynamique n'est encore implémenté. Mais vu l'étendue du réseau qui est déjà assez vaste, l'utilisation d'un routage dynamique serait intéressant.

2.4 Les différents moyens de surveillance existants dans la FIR d'Antananarivo

2.4.1 *Topologie des moyens de surveillance existants dans la FIR Tana*

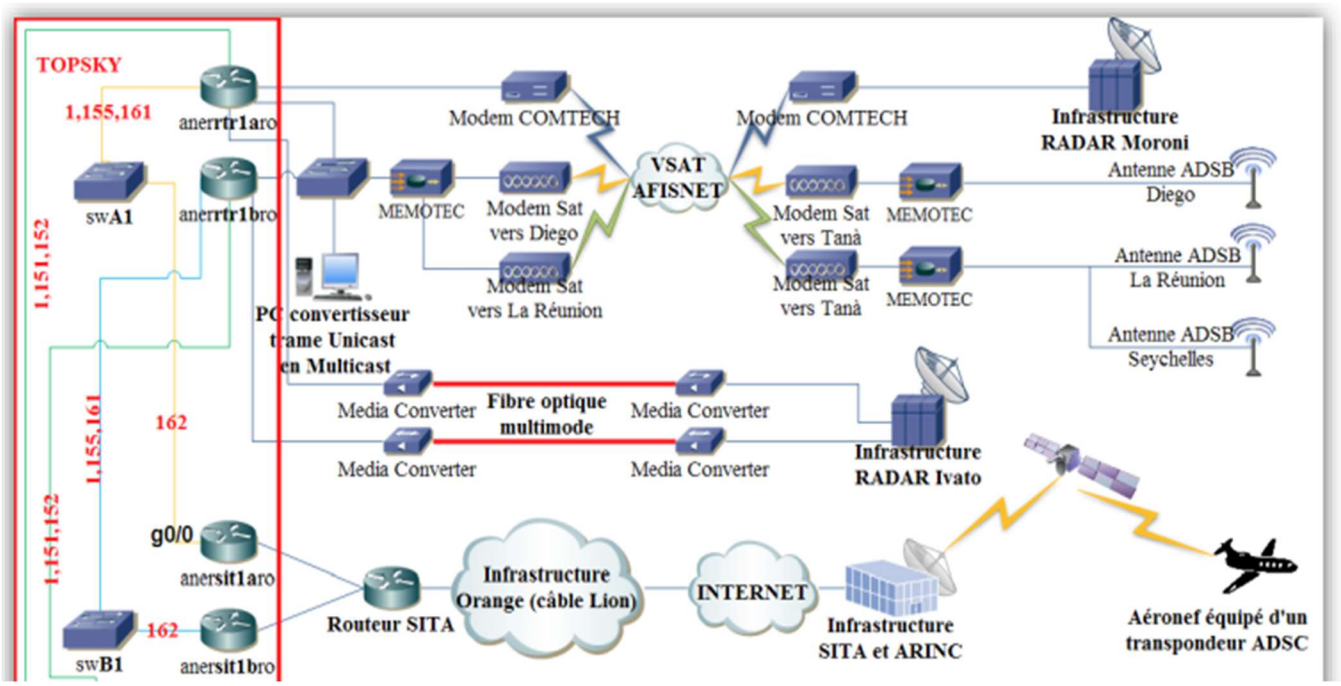

Figure 2.06 : *Les différents moyens de surveillance dans la FIR Tana*

Remarquons que La Réunion et Seychelles ne font pas parti de la FIR Tana, mais pour des besoins opérationnels, afin d'élargir la zone de couverture ADS-B, l'ASECNA a effectué un contrat avec eux pour que les données captées par les antennes ADS-B La Réunion et Seychelles soient acheminées vers Ivato.

2.4.2 *Radar mode S*

Le premier moyen de surveillance utilisé par la représentation de Madagascar est le Radar. Il est aussi utilisé par les Contrôleurs de la circulation aérienne pour offrir une assistance aux aéronefs. Ce radar était en phase d'expérimentation depuis Août 2014, mais il a été rendu opérationnel en Septembre 2016. C'est un radar de type MSSR ou Monopulse SSR (voir paragraphe 1.1.2.7 page 11) fonctionnant en **mode S** et implémenté à l'aéroport d'Ivato. Ainsi, sa fréquence de transmission est de **1030 MHz**, et sa fréquence de réception est de **1090 MHz**. L'antenne a une fréquence de rotation de **11 tour/min**. Le radar couvre un rayon de **250 nautiques**, et sa puissance d'émission est de **64,8 dBm soit 3kWatt**. Il envoie les données de type ASTERIX en multicast vers TopSky, plus précisément vers le serveur **MEDISIS**, via une liaison par fibre optique. Ce serveur a pour rôle de traiter les informations obtenues depuis ce type de senseur.

Tout appareil volant équipé d'un transpondeur Radar allumé et évoluant dans la zone de couverture de l'antenne Radar sera donc détecté et affiché sur le MMI (Multi Media Interface) représenté par un plot ou trace radar. Afin d'avoir une zone de couverture radar plus large, les informations radars captées par le Radar de Moroni sont reportées vers Tana par un tunnel créé via le modem COMTECH passant par le réseau VSAT AFISNET (voir Figure 2.01). Ainsi le système TopSky d'Ivato (voir paragraphe 2.4.5) reçoit des données radar via deux SSR.

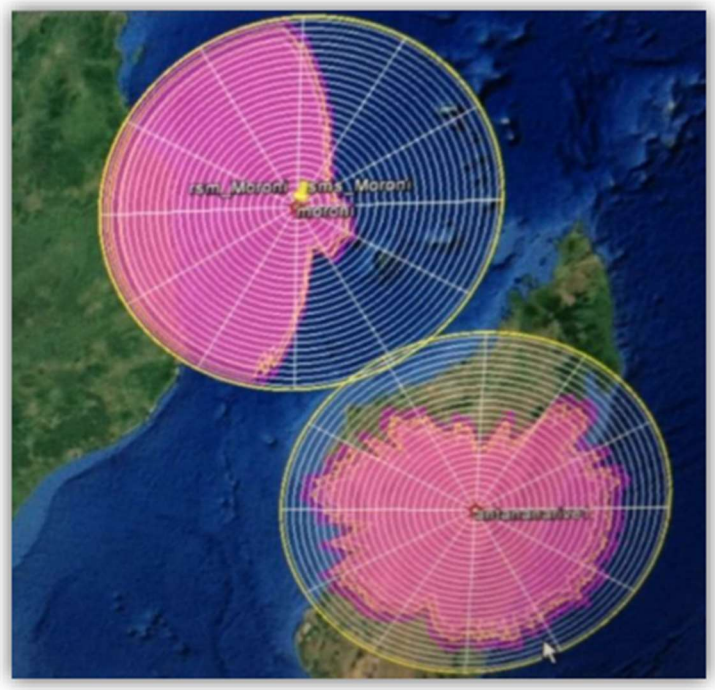

Figure 2.07 : *Couverture Radar d'Ivato et de Moroni*

2.4.3 ***Station ADS-B Diego***

2.4.3.1 Présentation

Afin de compléter la couverture Radar dans la FIR d'Antananarivo, l'ASECNA a implanté une station ADS-B à Antsiranana (Diego) en Mai 2012. Cette station est encore en phase d'expérimentation jusqu'à ce jour.

La station ADS-B Diego est un senseur de la gamme RX ADS-B : Récepteur ADS-B AX 680 de type 1090 MHz Extended Squitter (voir paragraphe 1.2.5.5 page 27). Il couvre un rayon d'environ **250 nautiques**, soit entre 400 et 500 km sans obstacle. Ce senseur reçoit les informations envoyées par tout aéronef en survol de la zone de couverture. Puis les données sont reportées à Ivato en unicast via le réseau AFISNET (transpondeur 2020 en mode d'accès FDMA sur le satellite Intelsat 10 02) vers le PC convertisseur de trame unicast-multicast (voir Figure 2.06 page 36) puis renvoyées par celui-ci en Multicast vers le serveur **MEDISIS** qui se

trouve dans le système TopSky. Les données ADS-B sont en effet bien plus précises que celles des radars, puisque leur précision est celle du GNSS. Comme pour les radars, afin d'élargir les zones couvertes, les données ADS-B de la Réunion et de Seychelles sont aussi reporté de la même façon vers Ivato. Les aéronefs détectés via le système ADS-B sont représenté sur le MMI par ce qu'on appelle plot ADS-B.

La Figure 2.08 ci-dessous montre en cercle rouge les zones couvertes ADS-B.

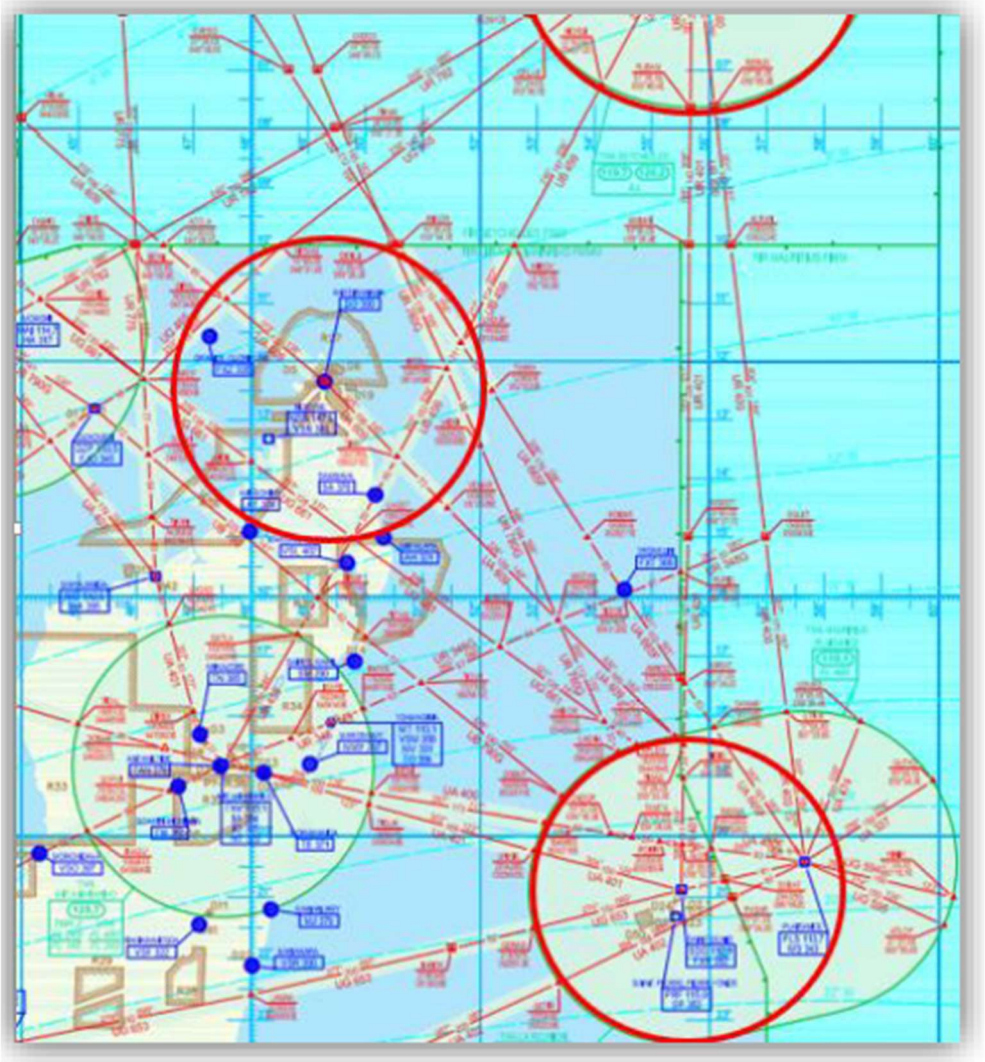

Figure 2.08 : *Couverture ADS-B Diego*

2.4.3.2 Composants du système

Un système ADS-B complet comprend 3 modules principaux :

- **AX 680 SPU** : Il s'agit du module de base à installer sur les sites distants comme station sol. Il est complété par des périphériques, comme par exemple : antennes, dispositif de surveillance du site, etc…

- **RCMS** : Le système de surveillance et de commande à distance centralisé (RCMS) permet de surveiller, configurer, et contrôler une station sol ADS-B
- Equipements de maintenance (en option) : **LCMS** (Système de surveillance et de contrôle local : ordinateur portable), un ensemble de pièces de rechange.

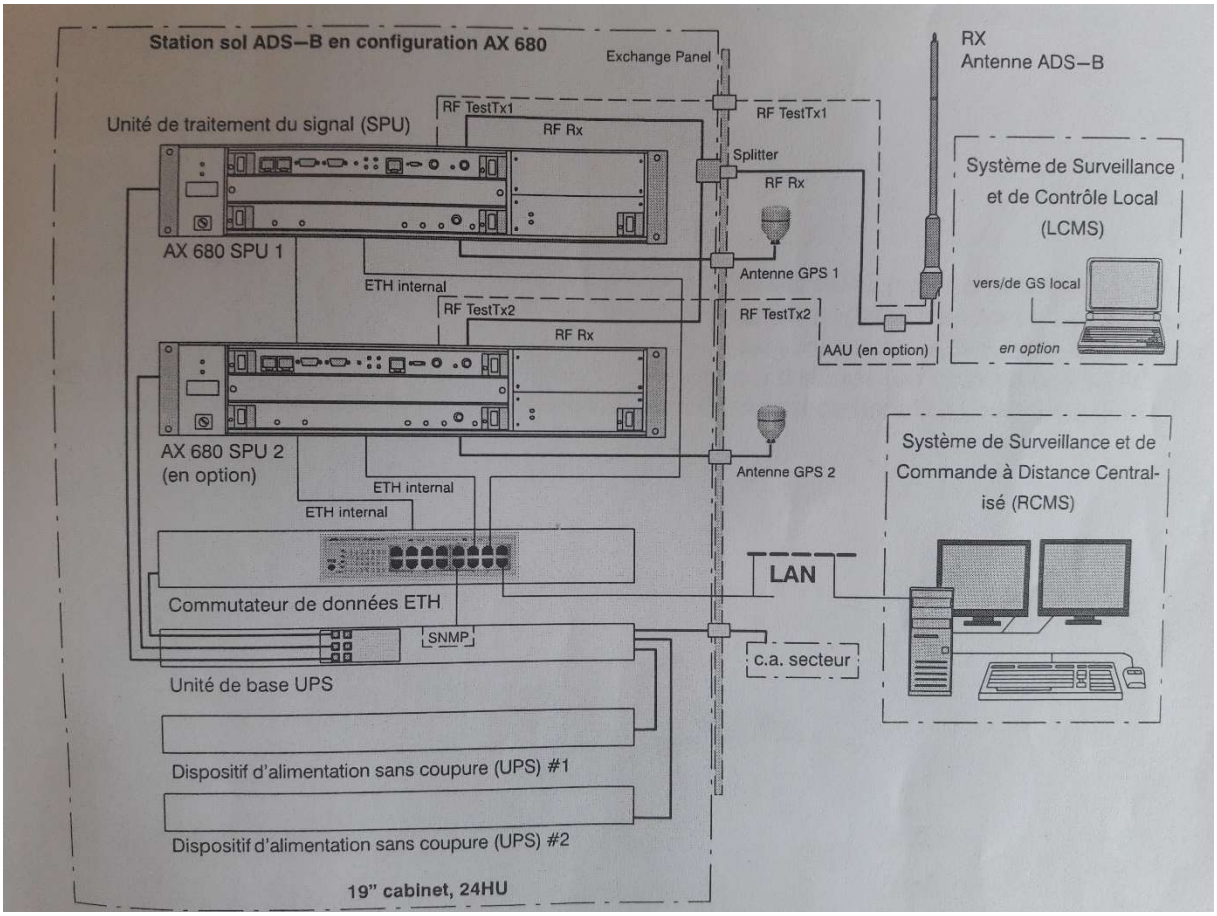

Figure 2.09 : *Composants du système ADS-B sol*

c. Unité de traitement du signal AX 680 SPU

Le système AX 680 SPU comprend les principaux sous-groupes suivants :

- Carte de traitement du signal (SPB3)
- Alimentation, AC/DC et/ou DC/DC (en option)
- Ventilateur avec filtre à poussière
- Récepteur GPS (carte PTM) (en option)

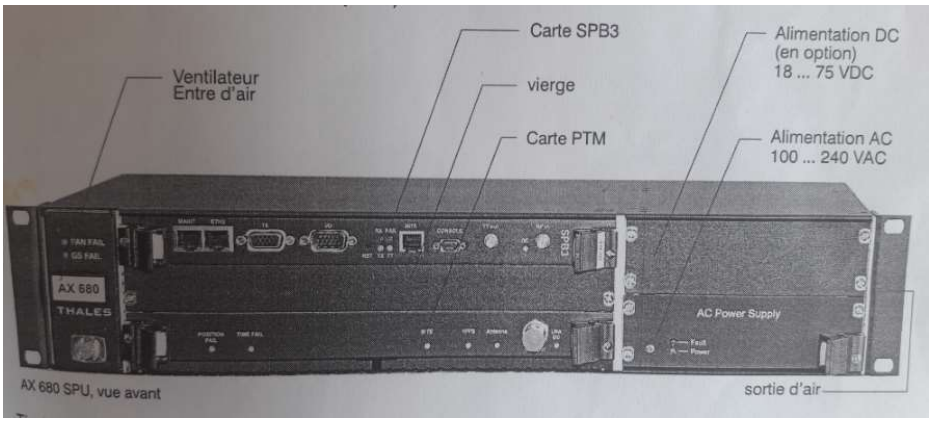

Figure 2.10 : *AX 680 SPU*

La principale fonction de l'AX 680 SPU est de recevoir et traiter les messages ADS sur 1090 MHz, et de sortir directement des données de rapport de cible cohérentes et décodées vers une application ATC à l'aide de la norme internationale ASTERIX, catégorie 21. Pour pouvoir établir des rapports ASTERIX complets, les données de différents rapports ADS-B (messages de squitter long) de la même cible sont collectées (exemple : position, vitesse, etc.).

d. RCMS

Le système de surveillance et de contrôle à distance (RCMS) est l'interface au CMS-S (Serveur de Surveillance et de Commande Centralisé) et permet la configuration de tous les paramètres du système et des dispositifs. Le RCMS fournit un ensemble d'outils pour la consignation de l'état, l'enregistrement et la reproduction des données. Il dispose également des outils ADS-B spécifiques utilisés dans les systèmes ADS-B pour l'enregistrement, la reproduction, et l'affichage de la situation technique.

e. LCMS et équipement de maintenance

Il est possible d'utiliser un système local de gestion et de surveillance (c'est-à-dire l'ordinateur portable de maintenance) pour procéder au réglage et à la maintenance sur site, c'est-à-dire à l'endroit où se trouvent les stations ADS-B.

f. Station de traitement centrale

Le CMS-S est un sous-système de l'équipement central ATC. Le CMS constitue le contrôleur principal du système ADS-B tout entier. Le CMS-S (ou Serveur CMS) se compose d'un système à moyenne portée constitué d'une station de travail de serveur PC avec au maximum 8 disques durs échangeables (SATA, par exemple, 250 GB), une interface Ethernet dual 1000Base-T, un DVD, etc. Le type sélectionné fournit une solution industrielle avec de

nombreuses fonctions utiles pour une prise en charge et une gestion pratiques, sans compromettre la robustesse.
Le système d'exploitation est un système basé sur Linux. Le CMS-S est connecté via Ethernet aux différentes stations sol et, via le réseau local ADS-B, au RCMS.

2.4.4 *ADS-C*

Comme on a pu le constater, les senseurs radars et ADS-B ont une portée limitée (200 à 250 NM). Donc les aéronefs en évolution dans les zones non couvertes (Radar ou ADS-B) ne seront prisent en charge que par les données FPL (Flight Plan ou en français Plan de vol) , soit seulement représenté approximativement sur le MMI par un Track FPL. C'est pourquoi l'ASECNA à compléter son système de surveillance avec la technologie ADS-C (voir paragraphe 1.2.4 page 19). Bien que très coûteuse, cette technologie est indispensable afin d'avoir un système de Tracking complet.

Pour cela, l'Agence s'est abonné auprès d'un fournisseur, SITA qui se charge de communiquer via satellite à l'aide du réseau ACARS (voir paragraphe 1.2.2.3) avec le transpondeur ADS-C de l'aéronef. Comme c'est un système par contrat, pour l'ASECNA, les informations sont envoyées toutes les **10 minutes**. Bien sûr les CA (Contrôleurs aériens) peuvent actualiser à tout instant les informations en cas de besoin, mais ce sera un frais supplémentaire auprès du fournisseur. Les données sont véhiculées via le support de la société Orange. Ces données ADS-C sont traitées par le **serveur AGDP (Air Ground Data Processing)** et représentées sur le MMI par des plots ADS-C. En plus d'être précise, la technologie ADS-C permet de faire des chats CPDLC entre le pilote et le CA. Le chat CPDLC est privilégié par rapport à la communication vocale (via HF ou VHF déportée).

Figure 2.11 : *Routeur Radar mode S, Routeur vers SITA, serveur AGDP, serveur Radar mode S*

2.4.5 ***Le système TOPSKY***

Pour pouvoir effectuer la surveillance aéronautique de la FIR malgache, la représentation de l'ASECNA à Madagascar utilise plusieurs technologies de surveillance comme le Radar, l'ADS-B, l'ADS-C, qui se concentrent sur un système de gestion de trafic aérien dénommé TOPSKY. Ce dernier étant le plus important puisqu'il assure l'interopérabilité de tous ces systèmes de surveillance.

En quelques mots, TopSky est un « ATM System » (Air Traffic Management System) ou système de gestion automatisé du trafic aérien, ayant pour but d'aider le contrôleur aérien à remplir sa mission de contrôle. C'est un système composé de plusieurs sous-systèmes électroniques et informatiques interconnectés. La solution TopSky ATC s'est imposée comme la norme mondiale car il s'agit d'un système modulaire servant à contrôler le trafic continental en route, l'approche terminale ainsi que l'espace aérien transcontinental et océanique.

Anciennement sous l'appellation, SAMAD en 1999, puis EurocatX en 2012, et enfin TopSky de nos jours, c'est un produit évalué autour de 50 millions d'euros et qui est développé par la grande firme nommée « Thales », spécialiste dans le domaine de la surveillance aéronautique mondiale.

On sait que chaque type de senseur a sa précision et son intégrité. Il est aussi possible qu'un aéronef soit en même temps détecté par deux ou plusieurs senseurs (ADSB-ADSC ou radar-ADS-C, etc.) à la fois, donc plusieurs plots seraient générés pour un même et unique avion. Heureusement, c'est le rôle des serveurs AGDP et MEDISIS, qui se trouve dans Topsky, de calculer et traiter les données afin qu'un seul et unique plot soit généré sur le MMI pour un même et unique avion même si celui-ci a été localisé par plusieurs senseurs. Ainsi ces calculateurs sont chargés de fusionner les plots afin d'en obtenir un seul, c'est à eux de voir quel type de piste (plot) affiché pour un aéronef donné. Toutefois des règles de priorité peuvent généralement être appliquées.

Priorité	Type de plot	Représentation sur le MMI
1	ADS-C	
2	ADS-B	
3	Radar	
4	FPL	

Tableau 2.02: *Priorité d'affichage des plots*

La Figure 2.12 montre l'interface du MMI où les différents plots sont affichés, chaque plot représente un aéronef en évolution dans la FIR.

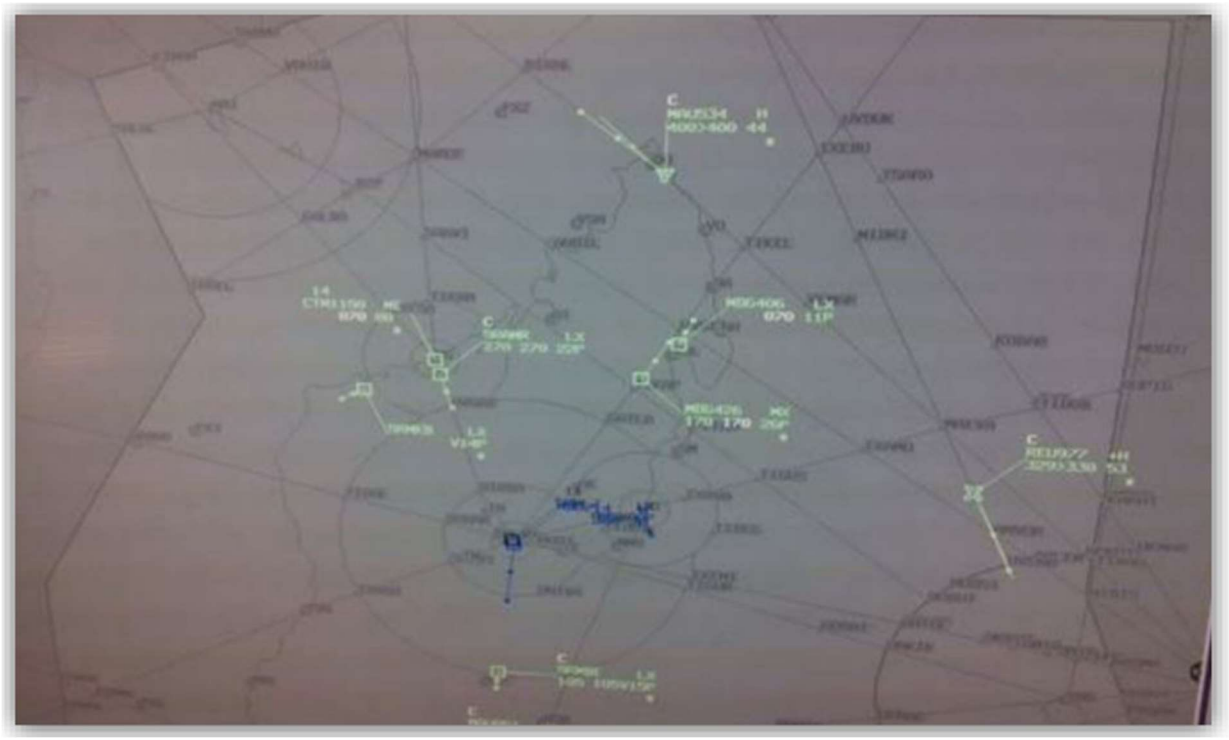

Figure 2.12 : *Copie d'écran du MMI*

2.5 **Conclusion**

Afin d'interconnecter ses différentes représentations l'ASECNA a constitué un réseau satellite appelé AFISNET en louant une bande de fréquence sur le satellite géostationnaire 10 02 d'INTELSAT. La topologie du réseau a une structure hybride, soit à la fois maillée et en étoile. Par ailleurs, le routage utilisé est jusqu'à ce jour un routage statique. Afin d'assurer la surveillance des aéronefs qui survole la FIR d'Antananarivo, l'ASECNA a implanté un Radar mode S, une station ADS-B à Diego, et elle utilise aussi la technologie ADS-C. Mais cela est insuffisant pour avoir une vue sur tous les avions qui survols la FIR.

CHAPITRE 3 :
SUPPORTS DE TRANSMISSION

Une fois les données captées par les différentes station ADS-B elles devront être acheminées vers le centre d'Ivato afin d'être traitées et utilisées par les Contrôleurs de la circulations aériennes intéressés. Pour cela on propose deux supports de transmission, les VSAT et l'internet. Ce dernier sera utilisé comme backup en cas de problème des liaisons VSAT.
Les données qui arrivent dans le serveur MEDISIS devant être en multicast, nous allons utiliser le mode de transmission multicast via le protocole PIM dense mode, et afin de sécuriser les données qui transitent dans le réseau nous allons créer des tunnels GRE et le protocole IPsec pour l'authentification et la confidentialité.

3.1 **Support VSAT**

3.1.1 ***Satellites***

3.1.1.1 Historique

Historiquement, le concept de satellite a vu le jour en 1945 par l'intermédiaire d'un britannique nommé Arthur C. Clarke qui a été le premier à introduire le concept de communication par satellite. En octobre 1957, l'Union Soviétique lance le premier satellite artificiel qui porta le nom de **Spoutnik 1**. C'était une simple sphère métallique d'un diamètre de 58 cm équipée d'un simple émetteur radio.
Les premiers satellites furent d'abord passifs, c'est-à-dire qu'ils réfléchissaient seulement les signaux émis par les stations terrestres. En 1960, les Américains mettent en orbite leur premier satellite en mode passif : **Echo 1**. Ce satellite était un ballon de plastique aluminé de 30 mètres de diamètre. Ensuite, les satellites actifs apparurent, ils possédaient leur propre système de réception et d'émission. **Teslar 1** fut le premier satellite américain mis en orbite deux (02) ans après Echo 1. Ce satellite disposait d'un enregistreur à bande qui enregistrait les données lors de son passage au-dessus d'une station émettrice et les diffusait lorsqu'il se situait au-dessus d'une station réceptrice. En 1965 on commença l'exploitation commerciale de ce type de satellite.

3.1.1.2 Notions sur les satellites

a. Définition

Un satellite de télécommunication est une sorte de relais hertzien. Il ne s'occupe pas de la compréhension des données, il se comporte simplement si on peut le dire comme un miroir. Sa mission est de régénérer le signal reçu puis le retransmettre amplifié en fréquence vers la station réceptrice. Le satellite possède également une capacité de diffusion, c'est-à-dire la retransmission des signaux captés depuis la terre vers plusieurs stations, et inversement. Il est également possible d'établir des liaisons directes entre satellites.

Ainsi un satellite est un élément spatial qui a pour rôle de relayer des données vers des multiples récepteurs terrestres. L'avantage principal des solutions satellites est la mobilité des stations terrestres puisqu'elles ne dépendent plus des infrastructures terrestres qui existent à travers le monde.
De plus les transmissions satellites permettent de mettre en œuvre plus facilement (par rapport aux structures câblées) les principes de diffusion et ceci de façon économique (en bande), puisqu'à partir d'un satellite, une même information peut être envoyé à de nombreuses stations ou à l'inverse relayer depuis un satellite la synthèse de multiples sources terrestres ou spatiales.

b. Orbites

Pour pouvoir maintenir une position déterminée de la Terre, les satellites exploitent la force gravitationnelle de celle-ci. Ainsi il est possible de définir à tout moment les caractéristiques d'un satellite pour établir des transmissions. Il existe quatre (04) types d'orbites utilisées par les satellites : [5]

- **L'orbite géostationnaire** : Aujourd'hui c'est l'orbite la plus répandue, le satellite se déplace en même temps que la terre ; il fait donc le tour de la terre en 24h et paraît ainsi immobile. Le satellite est placé à 35786 Km d'altitude et peut ainsi couvrir une large superficie pouvant atteindre un hémisphère. L'avantage de ces satellites, c'est que l'on peut utiliser des antennes fixes au sol.

- **L'orbite circulaire polaire** : les satellites sur ces orbites passent au-dessus des deux pôles, et peuvent au bout d'un certain temps couvrir toute la surface du globe. Leur domaine d'application se situe surtout dans l'observation ou la communication différée.

- **L'orbite circulaire inclinée** : ce type d'orbite ne permet pas aux satellites de couvrir en totalité toute la surface du globe, car la plus haute latitude desservie correspond à l'inclinaison du plan orbital.

- **Les orbites elliptiques** : Les satellites en orbite elliptique ont une vitesse très variable en fonction de l'endroit où ils se placent sur l'ellipse. Ils n'occupent donc pas une position fixe par rapport à la terre, ce qui suppose d'utiliser des antennes terrestres mobiles pour suivre ces satellites, contrairement aux satellites géostationnaires.

c. Bandes de fréquences

Dans le but d'éviter le chaos total dans le ciel, une réglementation internationale spécifique et stricte a été mise en place par l'Union Internationale des Télécommunications (UIT) concernant la répartition des fréquences ; elle fait partie intégrante du règlement international des radiocommunications. Cette réglementation définit notamment la position orbitale des satellites et les bandes de fréquences qu'ils doivent utiliser et respecter. Plusieurs types de services de communications par satellites sont définis dans la réglementation : le **service fixe par satellite (SFS)**, le **service mobile par satellite (SMS)**, qui comporte un service mobile terrestre et un service mobile maritime, le **service de radiodiffusion par satellite (SRS)**.

Il existe également une répartition géographique en trois (03) régions :

- La région 1 (Europe, Afrique, Moyen-Orient et l'Union Soviétique).
- La région 2 (Asie, Océanie)
- La région 3 (Amérique)

Bande		Sens Montant/descendant	Largeur de gamme
Services fixes	Bande C	6/4 GHz	1100 MHz
	Bande X	8/7 GHz	500 MHz
	Bande Ku	14/11 GHz	1000 MHz
	Bande Ku	14/12 GHz	250 MHz
	Bande Ka	30/20 GHz	2500 MHz
Services mobiles	Bande L	1,6/1,5 GHz	29 MHz
Services de radiodiffusion	Bande K	17/12 GHz	800 MHz

Tableau 3.01: *Fréquences des services satellites dans la région 1(Europe, Afrique et Asie du Nord)*

Voici l'utilisation de chaque bande :

- **Bande C** : c'est une bande fortement encombrée. Elle est divisée en deux sous bandes; la plus basse, pour les flux descendants (satellite/terre) et la plus haute, pour les flux montants (terre/satellite). Dans le cas d'une communication full duplex, il est nécessaire de disposer de deux canaux par connexion dans chaque plage de fréquences. Cette bande est surtout utilisée par les opérateurs pour leurs liaisons intercontinentales.
- **Bande X** : est une bande réservée aux applications militaires
- **Bande Ku** : elle est surtout utilisée pour les SFS et exclusivement pour les SRS dans les bandes 12/11 GHz. C'est une bande très sensible aux orages ; les signaux sont absorbés par l'eau de pluie.
- **Bande Ka** : Cette bande est surtout utilisée par les terminaux mobiles de type GSM car elle permet l'utilisation d'antennes encore plus petites.
- **Bande L** : définie pour le service mobile par satellite, elle est principalement destinée aux satellites en orbite basse.

d. Contraintes des solutions satellites

Les principales contraintes des solutions satellites sont :

- La couverture
- La gestion de la bande passante
- Le délai

3.1.1.3 INTELSAT

International TELecommunications SATellite organization abrévié INTELSAT est une coopérative à but non lucratif comprenant 136 pays. Les interconnexions des pays dans le monde ne sont pas tous forcement des fibres optiques, mais la plupart ont une liaison via les satellites d'INTELSAT. Cette organisation prend en charge les satellites internationaux fonctionnant dans la bande de radiofréquences réservée aux « satellites fixes ». Des dizaines de milliers de conversations téléphoniques sont transmises simultanément par les satellites d'INTELSAT. [6]

Remarque : L'ASECNA est liée à INTELSAT par un contrat de location de bande de fréquences sur le satellite 10-02 appelée **IS 10-02**. L'IS 10-02 @359°E a été conçu et fabriqué en Europe par EADS Astrium pour le compte de cet opérateur international (INTELSAT). IS 10-02 est un **satellite géostationnaire**. Offrant une couverture, de premier ordre, de l'Europe, de l'Afrique et du Moyen-Orient, et une couverture complète s'étendant à l'Est depuis l'Asie (Inde) jusqu'à l'ouest (Amérique du Sud), c'est l'un des plus gros satellites de communication jamais construits et le plus puissant d'INTELSAT. En **bande C**, il comprend jusqu'à 70 transpondeurs, espacés de 36 MHz.

3.1.2 *Technologie VSAT*

3.1.2.1 Présentation

La VSAT est un système basé sur le principe d'un site principal (le hub) et d'une multitude de points distants appelés stations VSAT. Les stations VSAT permettent de connecter un ensemble de ressources au réseau. Tout est géré par le hub, point central du réseau. Les points distants ne prennent aucune décision sur le réseau. Ce qui permet de réaliser des matériels relativement petits et peu coûteux. Une station VSAT n'est donc pas un investissement important et l'implantation d'un nouveau point dans le réseau ne demande quasiment aucune modification du réseau existant.

3.1.2.2 Topologie

Les topologies des réseaux VSAT ont été conçues pour pouvoir répondre aux exigences de certaines techniques de transmission :

- Les liaisons fixes (de type point à point) : Il s'agit des liaisons montantes vers un satellite. Dans ce cas, le point d'émission et le point de réception sont parfaitement connus géographiquement, et le trajet de l'information est parfaitement défini.

- Les liaisons en diffusion hertzienne (de type point à multipoint) : Le point émetteur est parfaitement connu. Mais la réception se fait sur une zone généralement large dans laquelle les récepteurs sont fixes ou mobiles. Il s'agit, notamment, des émissions de radio ou de télévision reçues par voie hertzienne à partir d'un satellite.

Ainsi, trois types de topologie s'imposent aux réseaux VSAT : la **topologie en étoile**, la **topologie maillée** et la **topologie hybride**.

a. Topologie en étoile

L'architecture d'un réseau en étoile comporte deux éléments : le Hub et les stations distantes. Les stations distantes n'étant pas à mesure de communiquer entre elles, il importe donc de doter le Hub d'une antenne à fort gain pour amplifier et relier le trafic d'un VSAT à un autre. Le choix de cette topologie augmente le délai de transmission et réduit le coût des équipements VSAT.

b. Topologie maillée

Ici, deux VSAT quelconques pris dans le réseau sont interactifs. Cependant, lorsqu'il existe un Hub, il joue normalement son rôle. Aussi, l'absence du Hub à gain élevé fait que le délai de transmission est court par rapport à celui de la topologie en étoile. La topologie maillée est donc appropriée pour la transmission de données qui ne supporte pas les longs délais de transmission.

c. Topologie hybride

Une topologie hybride est l'association des deux topologies précédentes au sein d'un même réseau. Dans un tel type de topologie, on peut catégoriser deux types d'usagers qui sont : les usagers à faible trafic et les usagers à fort trafic dont les VSAT interagissent entre elles en configuration maillée.

3.1.2.3 Techniques d'accès au réseau VSAT

Dans un souci d'optimisation de l'utilisation des ressources réseau (largeur de bande du satellite, voies entrantes, voies sortantes...), il est nécessaire d'avoir une technique d'allocation. C'est l'objet même des différents protocoles d'accès mis en œuvre sur les réseaux VSAT. Ces techniques décrivent la façon dont les VSAT se partagent la largeur de bande du satellite.

a. FDMA

Le FDMA ou **Frequency Division Multiple Access** est une technique qui consiste à diviser la largeur de bande du récepteur en un certain nombre de sous-bande. Chaque sous-bande est occupée par une porteuse monovoie (SCPC) ou multivoie (MCPC).
Le niveau de puissance de l'ensemble des porteuses ne doit pas dépasser une certaine valeur. La configuration d'un réseau en mode AMRF (Accès Multiple à Répartition de Fréquence) est très simple dans la mesure où elle ne requiert pas de système de synchronisation. [7]

b. TDMA

Dans la technique **Time Division Multiple Access**, la largeur de bande du satellite est partagée entre les stations VSAT selon un découpage temporel donné. En effet, lorsqu'une station émet un paquet d'informations, elle occupe la totalité du récepteur pendant le temps qui lui est attribué. Une fois ce temps écoulé, elle cède le canal à une autre station prête à transmettre. [7]

c. CDMA

Avec le **Code Division Multiple Access**, la totalité de la bande passante du canal satellite est occupée par chaque station quel que soit l'instant où se manifeste le besoin de transmettre des informations ou paquets vers une autre station. Cela est possible grâce au principe d'étalement de spectre qui consiste à étaler la puissance du signal au moyen d'un code à l'émission. Lorsqu'il y a collision des paquets, les signaux étalés s'ajoutent linéairement. Le code d'émission est unique et représente le numéro pour l'identification de chaque station.
Dans le cas où une station désire émettre vers une autre station, les deux stations se synchronisent à l'aide de leur code et la relation entre les deux codes d'étalement permet l'extraction de l'information ou du signal utile et les autres signaux étalés sont perçus comme un bruit. [7]

3.1.2.4 Applications du VSAT

La technologie VSAT est un système prévu pour la mise en place des réseaux de données. Mais depuis son apparition, les constructeurs ne cessent d'apporter de plus en plus d'améliorations à ce système en augmentant considérablement le nombre d'applications possible avec un réseau de ce type.

Les terminaux VSAT de nos jours possèdent des Slots pouvant accueillir des cartes de différents types:

- Cartes réseaux : X25, Frame Relay, ATM, Ethernet, …
- Cartes multimédia : Visioconférence, Streaming vidéo
- Cartes de communication : lignes analogiques, lignes numériques, ports séries

Il est à noter que ces différentes technologies peuvent fonctionner en même temps ce qui accroît encore plus la modularité du système.

3.2 **Support Internet**

Comme deuxième support de transmission pour acheminer les données des différentes stations ADS-B sol vers le centre Ivato, nous allons utiliser l'Internet. Ce dernier sera utilisé comme back up au support VSAT. Les débits offerts par l'opérateur téléphonique TELMA Madagascar figurant parmi les meilleurs, on a alors opté de le choisir comme fournisseur d'accès internet.

Pour ce projet on aura besoin d'un débit garanti de **19.2 Kbps**, ainsi Telma nous a proposé d'utiliser la liaison ADSL vu que cette dernière aboutie aux différents points où on veut placer nos stations ADS-B sol et elle offre de très bon débit pour le transport des données.

3.2.1 Définition

L'INTERconnected NETwork est un réseau informatique mondial, plus spécifiquement un réseau de réseaux s'appuyant sur des technologies et des protocoles standardisés pour que tous les ordinateurs connectés puissent communiquer entre eux. Il est constitué d'un ensemble de réseaux nationaux, régionaux et privés utilisant le protocole de communication IP, et s'appuie sur le protocole de routage BGP.

3.2.2 Protocole BGP

Border Gateway Protocol (**BGP**) est un protocole d'échange de route utilisé notamment sur le réseau Internet. Son objectif est d'échanger des informations de routage et d'accessibilité de réseaux (appelés préfixes) entre systèmes autonomes (AS pour Autonomous Systems).

Contrairement aux protocoles de routage interne, BGP n'utilise pas de métrique classique mais fonde les décisions de routage sur les chemins parcourus, les attributs des préfixes et un

ensemble de règles de sélection définies par l'administrateur de l'AS. On le qualifie de protocole à vecteur de chemins (path vector protocol). Il prend en charge le routage sans classe et utilise l'agrégation de routes afin de limiter la taille de la table de routage. Ses spécifications sont décrites dans la RFC 4271.

Les connexions entre deux voisins BGP (neighbors ou peers) sont configurées explicitement entre deux routeurs. Ils communiquent alors entre eux via une session TCP sur le port 179 initiée par l'un des deux routeurs. BGP est le seul protocole de routage à utiliser TCP comme protocole de transport.

On peut distinguer deux types de dialogue BGP :

- Entre deux routeurs de bordure de deux AS différents, dénommé eBGP (external BGP)
- Entre les routeurs d'un même AS dénommé iBGP (internal BGP)

3.2.3 ADSL

ADSL ou **Asymmetric Digital Subscriber Line** est une technique de communication permettant l'utilisation d'une ligne téléphonique ou RNIS afin de transmettre et recevoir des données numériques de manière indépendante du service téléphonique. [8]

L'intérêt de cette technologie est qu'elle tire partie des bandes de fréquence non utilisées par le téléphone. Ainsi, alors que la voix est transportée sur une bande de fréquence allant de 300 à 3400Hz (rappelons que la bande de fréquence audible va de 20Hz à 20kHz), le signal ADSL est transmis sur les plages de fréquences hautes, inaudibles, de **25,875kHz à 1,104MHz**. L'utilisation de cette bande très large permet de transporter des données à des débits pouvant atteindre **8Mbit/s** au maximum en réception et **768Kbit/s** en émission (d'où le A de ADSL qui signifie asymétrique).

Ainsi, dans le cadre de notre projet, les avantages d'utiliser l'ADSL comme support de transmission de données sont :

- Transport des données à des débits élevés
- Partage des connexions : avec un tel débit, l'ADSL permet à plusieurs stations d'utiliser la même ligne, tout en conservant de bonnes performances.
- Ligne dédiée : l'ADSL offre une ligne dédiée à chaque utilisateur. De ce fait, la sécurité est nettement supérieure. Le critère de sécurité étant fondamental dans le domaine aéronautique.

3.3 Routage multicast

3.3.1 *Introduction*

Dans les réseaux IP traditionnels, il existe principalement deux modes d'acheminement des données : l'unicast et le broadcast. Le terme unicast définit une connexion réseau point à point, c'est-à-dire d'un hôte vers un (seul) autre hôte. Tandis que le broadcast est l'envoi d'un paquet d'un hôte vers tous les autres hôtes appartenant au même sous réseau.

Lorsque plusieurs hôtes non seulement interne mais aussi externe au domaine de broadcast sont intéressés par le même contenu simultanément, les données devront être envoyées en unicast une fois vers chaque hôte comme le montre l'exemple de la Figure 3.01 ; ce qui n'est pas très efficace et nécessite de la part de l'hôte émetteur une puissance et une bande passante proportionnel au nombre de client.

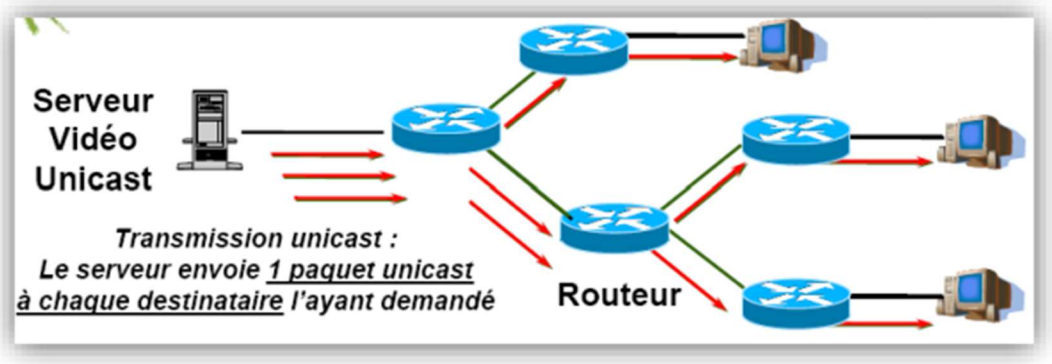

Figure 3.01 : *Envoie de donnée en Unicast*

En mode broadcast, l'hôte émetteur n'a qu'à envoyer les données une seule fois et économise ainsi ses ressources. Par contre, avec ce mode, tous les hôtes du réseau cible internes au domaine de broadcast reçoivent les données, même ceux qui ne le désirent pas, ce qui entraîne une consommation des ressources de ces hôtes pour traiter ces données. D'ailleurs, en pratique, le broadcast est inutilisable au-delà du réseau local donc toute émission externe via ce mode ne sera pas possible.

TCP (Transmission Control Protocol) est par nature orienté unicast tandis qu'UDP (User Datagram Protocol) est déclinable selon plusieurs modes de transmission.

3.3.2 *Présentation du routage multicast*

Le multicast est une solution alliant le meilleur des deux autres modes énoncés précédemment mais sans les inconvénients. Dans ce mode, les données ne sont émises qu'une seule fois

(comme en broadcast) par l'hôte émetteur et c'est au réseau d'acheminer les données seulement vers les hôtes intéressés comme le montre la Figure 3.02. Ce mode assure donc une meilleure utilisation des ressources car les données ne sont acheminées qu'une seule fois sur chaque lien et ne sont reçues uniquement que par les hôtes abonnés. [9]

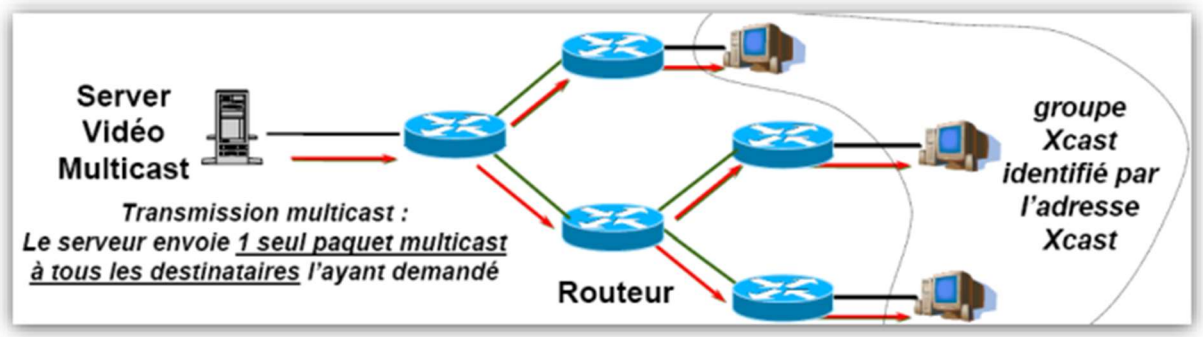

Figure 3.02 : *Emission de donnée en multicast*

Voici quelques avantages de l'utilisation du multicast :

- Optimisation des performances : tout trafic redondant est éliminé.
- Communication et transmission efficace : réduction de la charge CPU et réseau
- Autorisation de vraies applications distribuées multipoint
- Groupe multicast non limité au réseau local.

D'après ces avantages, le multicast répond aux besoins de certaines applications, comme les applications temps réel interactives (ex : visioconférence à plusieurs intervenants distants), la distribution multimédia (ex : diffusions radios et satellite), ou encore la distribution de documents et de données (ex: Données ADSB et Radar de TopSky). Le multicast s'appuie sur l'UDP pour transmettre les données, effectivement il fonctionne en mode non connecté. D'ailleurs, l'utilisation de TCP entraînerait rapidement la saturation de l'émetteur avec les paquets d'acquittement reçus depuis les hôtes récepteurs, ainsi c'est l'UDP qui a été adopté.

3.3.3 *Adressage multicast*

3.3.3.1 Plage d'adresse IP multicast (couche 3 modèle OSI)

Pour pouvoir effectuer la transmission de donnée, le multicast se base sur le principe de groupe. Le groupe est caractérisé par une adresse IP et chaque hôte qui souhaite recevoir le trafic doit s'abonner à ce groupe. Ainsi, en multicast, les données ne sont plus envoyées directement à l'adresse de chaque hôte mais plutôt à l'adresse IP du groupe dont les membres

sont dynamiques. L'attribution de ces adresses IP utilise un plan d'adressage spécifique. On sait qu'auparavant les adresses IP ont été découpées en plusieurs classes et c'est la **classe D** qui a été réservée aux groupes multicast, cette classe prend actuellement dans la norme CIDR (Classless Inter-Domain Routing) le préfixe 224.0.0.0. Les adresses y appartenant sont caractérisées par les quatre bits de poids forts positionnés à 1 1 1 0, ce qui correspond à la plage d'adresse **224.0.0.0 à 239.255.255.255**.

Dans cette plage d'adresse, il y a quelques règles d'utilisation imposées par l'autorité d'assignation des numéros Internet, l'IANA (Internet Assigned Numbers Authority), afin de normaliser et standardiser l'affectation d'adresse multicast. L'ensemble des assignations est accessible sur leur site Internet. Cependant, on peut en citer quelques-unes de ces différentes règles d'assignation : [10]

- **224.0.0.0 –224.0.0.255** : les adresses de cette plage sont strictement réservées pour la diffusion sur le LAN, ce sont des adresses fixes et attribuées par l'IANA, transmises avec une portée locale (soit TTL=1).

  Voici quelques exemples :

  - 224.0.0.1 : tous les systèmes multicast
  - 224.0.0.2 : tous les routeurs multicast
  - 224.0.0.4 : tous les routeurs DVMRP
  - 224.0.0.5 : tous les routeurs OSPF
  - 224.0.0.9 : tous les routeurs RIP v2
  - 224.0.0.13 : tous les routeurs PIM v2
- **232.0.0.0/8** : réservées pour PIM Source-Specific Multicast
- **233.0.0.0/8** : Adressage GLOP (RFC 27707) qui permet à un fournisseur de contenu de disposer de ses propres adresses. Les octets 2 et 3 représentent un numéro d'AS (Security Association) public
- **239.0.0.0/8 (239.0.0.0 –239.255.255.255)** : sont réservées pour des usages privés.

3.3.3.2 Plan d'adressage au niveau 2

Dans le multicast il est nécessaire aussi de pouvoir adresser une même trame à un ensemble de client au niveau de la couche liaison du modèle OSI. Pour cela, l'utilisation du mécanisme utilisé pour l'unicast, ARP (Address Resolution Protocol), ne répond pas à ce besoin. On utilise donc un autre mode d'acheminement pour le multicast qui consiste à faire correspondre les

adresses multicast IP avec des adresses multicast MAC dans le cas d'Ethernet (d'autres mécanismes sont utilisés pour Token Ring ou FDDI). Les 23 bits de poids faible de l'adresse IP sont extraits puis combinés à un préfixe fixe : **0x01 005e** (voir Figure 3.03). Les clients intéressés par un groupe multicast doivent ensuite configurer leur carte réseau pour écouter ces adresses MAC supplémentaires.

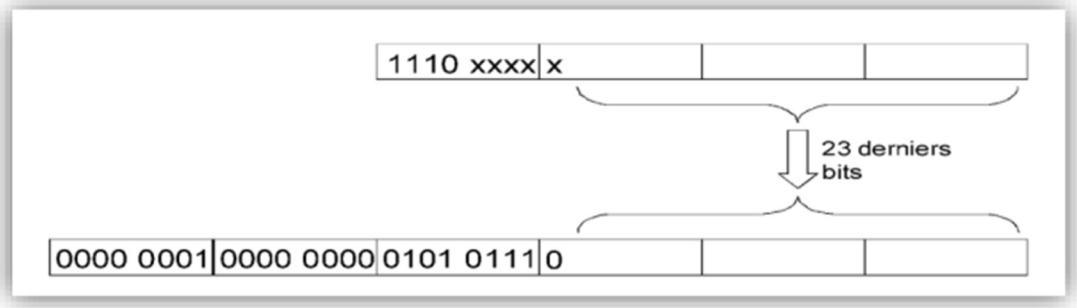

Figure 3.03 : *Plan d'adressage niveau 2*

Il est quand même possible que plusieurs adresses de niveau 3 peuvent correspondre à la même adresse de niveau 2 (comme 224.1 .1 .1 et 225.1 .1 .1). Ce type de collision sera résolu par la couche IP.

3.3.4 ***Protocoles***

Un groupe multicast se compose d'un ensemble de machines. Il est entièrement dynamique (une station peut rejoindre ou quitter le groupe à tout moment), et ouvert (sans restriction des sources à priori) ; une station peut même émettre un paquet dans un groupe sans en faire partie. Des protocoles ont été mis en œuvre pour permettre aux routeurs de gérer et véhiculer correctement les trames multicast vers les hôtes destinataires.

3.3.4.1 IGMP

Le protocole **IGMP (Internet Group Management Protocol)** est le protocole qui permet aux routeurs de gérer les groupes multicast. Ce protocole de gestion des groupes Internet assure la communication directe avec les hôtes clients afin de déterminer les groupes multicast dont le trafic doit être acheminé. Ce protocole existe actuellement en 3 versions.

Version	Particularités
IGMP v1	• Définit par la RFC 1112 • Il fournit un mécanisme de base pour la gestion de groupe par l'envoie régulier de requête sur le LAN pour déterminer les abonnements aux divers groupes multicast.
IGMP v2	• Définit par la RFC 2236 • Possibilité pour un hôte de se désabonner explicitement pour réduire les temps de latence avant la disparition d'un groupe. • Permet aussi au routeur d'émettre des requêtes spécifiques à un groupe pour lui permettre de vérifier qu'il n'y a plus d'hôte intéressé avant de cesser l'envoie des données.
IGMP v3	• Définit dans la RFC 3376 • Possibilité pour un hôte client de définir un filtre sur les sources pour un groupe donné : mode « include » si l'hôte définit les sources qu'il désire recevoir pour un groupe ; et mode « exclude » s'il définit les sources qu'il ne désire pas recevoir pour un groupe • Opération exploitée par PIM-SSM (Source-Specific Multicast)

Tableau 3.02: *Les différentes versions d'IGMP*

Remarque : Certains commutateurs reçoivent puis traitent le trafic multicast comme inconnu ou comme broadcast et envoie la trame sur tous les ports, ceci implique que toutes les stations (même non intéressées) reçoivent la trame d'où l'inondation du réseau. L'implémentation de l'**IGMP Snooping** au niveau du switch permet de palier à ce problème. Elle donne au commutateur le supportant une capacité de niveau 3, donc d'analyser la trame et de ne l'envoyer que sur le/les port(s) intéressé(s) seulement. IGMP Snooping optimise ainsi le routage multicast. Une autre alternative à l'IGMP Snooping est le protocole propriétaire Cisco CGMP.

3.3.4.2 Protocole de routage multicast

IGMP est un protocole qui permet la distribution des datagrammes multicast sur le LAN, mais pour pouvoir acheminer ces paquets hors du LAN il est nécessaire d'utiliser des protocoles de routage multicast, ces protocoles sont différents des protocoles utilisés en unicast (RIP, OSPF, EIGRP, BGP, …). Il existe 2 familles de protocoles de routage multicast, les protocoles **intra-**

domaine (ex : PIM, DVMRP) et les protocoles **inter-domaine** (ex : MSDP et MBGP). On ne verra dans ce document que les protocoles intra domaine.

a. Différents modes de diffusion des protocoles intra domaine

Il existe 2 modes de diffusion des paquets multicast en intra domaine :

- Le **mode dense** : ce mode part de l'hypothèse que les clients sont concentrés dans le domaine de diffusion des données. Il utilise alors un modèle **inondation – élagage** (Flooding - Pruning). Le routeur qui reçoit des données d'une source diffuse l'information à tous les autres routeurs auxquels il est relié et ceux-ci diffusent à leur tour vers leurs voisins excepté vers les routeurs qui remontent vers la source. Lorsqu'un routeur n'a aucun client ou routeur à qui envoyé l'information, il effectue un élagage de l'arbre de distribution en informant le routeur montant qu'il ne désire plus recevoir cette source. Très facile à mettre en œuvre, ce mode est suggéré pour la diffusion dans un domaine restreint tel qu'une partie d'un réseau d'entreprise.

- **Mode épars (Sparse mode**) : au contraire du précédent, ce mode part de l'hypothèse que les clients sont disséminés dans le domaine de diffusion. Ce mode utilise un modèle d'adhésion explicite (**greffe – élagage**) c'est-à-dire que l'information n'est acheminée que vers les routeurs qui l'on explicitement demandés. Il utilise des arbres de distribution basés sur un point de rendez-vous. Lorsqu'un hôte client désire rejoindre un groupe, le routeur directement connecté à ce client rejoint l'arbre de distribution en envoyant une demande d'adhésion au point de rendez-vous (RP). Ce mode peut être utilisé sur des domaines de diffusion large comme Internet.

Dense mode	Sparse mode
• Flood + Prune : très inefficace si large domaine de diffudion • Peut provoquer des problèmes dans certaines Topologies (congruence). • Création d'un état (S, G) dans chaque routeur même s'il n'y a aucun récepteur pour ces données • Optimisation du trafic pratiquement impossible	• Impose de configurer un RP • Très efficace car : o L'abonnement est explicite o Trafic va seulement là où c'est nécessaire o Les états ({*, S}, G) sont seulement créés sur les chemins. • Traffic engineering possible • Utilise des arbres partagés dont différents RP peuvent être l'origine
Les protocoles qui utilisent ce mode : **DVMRP, PIM-DM et MOSPF**	Les protocoles qui utilisent ce mode : **PIM-SM, CBT, OCBT, QOSMIC**

Tableau 3.03: *Tableau comparatif entre le mode dense et le mode épars*

b. Arbre de diffusion multicast

Les protocoles de routage génèrent deux types d'arbre qui décrivent comment atteindre les membres des différents groupes de diffusion répartis sur tout un domaine, afin d'acheminer les données:

- Les arbres de plus court chemin, **SPT** (**S**hortest Path **T**ree), qui ont leur base à la source et définissent le plus court chemin vers les destinataires. Ils nécessitent la construction d'un arbre par source de trame multicast. Ces arbres se caractérise par l'état (S, G) avec S comme adresse source et G l'adresse du groupe destinataire.

- Les arbres basés sur un point de rendez-vous, **RPT** (**R**endez-vous **P**oint **T**ree), dite aussi arbre partagé, quant à eux utilisent une base unique, le point de rendez-vous ou cœur, utilisé par toutes les sources, qui est représenté par l'état (*, G) (l'étoile représente toutes les sources). Les données sont acheminées vers le point de rendez-vous dans un premier temps puis parcourent l'arbre ensuite.

3.3.4.3 PIM

Dans les tous premiers pas du multicast, on avait utilisé comme protocole de routage le DVMRP, ou **D**istance **V**ector **M**ulticast **R**outing **P**rotocol, similairement au RIP, ce protocole mode dense utilisait un mécanisme de calcul des routes de type vecteur de distance. Ainsi chaque routeur participant au routage multicast devait avoir une table de routage distinct de celui de l'unicast pour pouvoir transiter une trame multicast. Le protocole n'a pas pu être généralisé faute de consommation non négligeable des ressources du routeur.
Cisco System propose alors une solution avec le protocole **PIM (Protocol-Independent Multicast)**. C'est un protocole qui peut utiliser les tables générées par n'importe quel protocole du routage unicast tel que RIP, OSPF, EIGRP ou BGP, pour acheminer les trames multicast. Cela ne signifie quand même pas qu'il ne fonctionnera pas sans eux. Il existe deux (02) versions de PIM (PIM v1 et PIM v2) mais actuellement on n'utilise plus la version 1. PIM est actuellement le protocole de routage multicast le plus utilisé, et le seul encouragé par Cisco. [9]

a. PIM-Dense Mode

Ressemblant à DVMRP mais n'utilisant pas des tables de routage spécifiques, PIM-DM fonctionne en mode dense, il consiste pour un routeur à flooder sur toutes ses interfaces un flux multicast dans le cas où il ne connait pas de clients. Les routeurs recevant ce flux et n'ayant pas à le recevoir car ils n'ont pas de clients, le signalent au routeur émettant ce flux. On a alors le traditionnel fonctionnement flooding - stop - flooding - stop, et ainsi de suite. Etant très facile à mettre en œuvre, c'est ce mode que nous allons configurer dans les routeurs utilisés pour la densification de l'ADS-B.

b. PIM-Sparse Mode

Le protocole aujourd'hui utilisé est PIM Sparse définit par la RFC 2362. Comme son nom l'indique encore une fois, il fonctionne en mode Sparse. Un routeur n'envoie un flux multicast sur une interface que si un autre routeur ou un client le lui a explicitement demandé (Join). Bien sur ce mode est beaucoup plus efficace et également beaucoup plus complexe à implémenter. Puisque PIM-SM fonctionne en mode épars, l'existence d'un Rendez-vous Point (RP) est donc impérative pour pouvoir transiter de la trame multicast dans le réseau. Toutefois il est possible d'utiliser plusieurs RP (pour gérer différents groupes multicast via des ACL par exemple) dans un même réseau multicast, à la seule condition qu'un groupe multicast ne peut être enregistré auprès que d'un seul et unique RP. Le/les routeur(s) RP du réseau peut être indiqué statiquement

ou dynamiquement selon le besoin. Ce RP sera la racine de l'arbre de diffusion multicast partagé (RPT).

La source s'enregistre sur le RP défini en envoyant une requête **Register** vers celui-ci, tandis que pour s'abonner au groupe, le destinataire envoie un **Join** au RP via le routeur qui lui est directement connecté. Le RP envoie ensuite des requêtes **Join** vers la source pour faire passez le trafic sur le RPT ainsi construit et termine avec un **Register-stop** quand le trafic est établi. Lorsque les données arrivent au récepteur, et après consultation de la table de routage unicast si besoin, un **Join** sera ensuite envoyé directement vers la source afin d'obtenir le plus court chemin pour la transition des données et ainsi avoir un SPT. Enfin il y aura envoie d'un **Prune** vers le RP puis vers la source pour arrêter l'envoie du trafic passant par le RP via le RPT.

3.4 Variantes de PIM

PIM-SM est déjà très bien, mais il y a d'autres alternatives ou améliorations qui peuvent être utilisées pour répondre à des besoins spécifiques ou pour mieux couvrir le domaine d'application du multicast :

3.4.1 *PIM-Sparse Dense Mode*

PIM-SDM est un mode qui combine le PIM-DM et le PIM-SM pour en tirer une meilleure partie. C'est un protocole propriétaire Cisco. Lorsqu'il est implémenté sur l'interface d'un routeur, cette interface pourra fonctionner à la fois en mode Dense (si sans RP connu) et en mode Sparse (si un RP est connu) dépendant de chaque groupe multicast. PIM SDM est idéal pour l'implémentation du multicast dans les réseaux où les architectes ne sont pas sûr de la version de PIM, SM ou DM, qui est la plus adapté. C'est un protocole facile à mettre en œuvre et il permet l'implémentation de l'Auto-RP (gestion dynamiquement de(s) RP) dans une topologie multicast.

3.4.2 *Bi-directional PIM et le PIM-SSM*

Le **Bi-directional PIM** est un protocole PIM amélioré qui intègre une méthode permettant d'éviter les boucles dans l'acheminement des paquets multicast. Le **PIM-SMM** ou **PIM Source-Specific Multicast** quant à lui, est un protocole qui permet une implémentation plus facile de PIM dans un réseau multicast très vaste à densité de source et de groupe très grande, dans lequel la gestion des RP devient rapidement un casse- tête. Utilisé avec IGMP v3, PIM SSM donne l'avantage de ne plus passer par un point de rendez-vous (RP) du réseau lorsqu'un client souhaite obtenir un trame multicast mais directement vers la source via un SPT par

construction direct du chemin le plus court ce qui permet d'avoir une convergence rapide. Evidemment, l'application cliente doit supporter IGMP v3 pour pouvoir spécifier directement dans le paramètre du mode « include » la source et le groupe (S, G). Toutefois, il est possible d'utiliser le PIM SSM avec IGMP v2 en utilisant la méthode du SSM Mapping.

3.5 VPN (Virtual Private Network)

Le VPN ou RPV (réseau privé virtuel) en français est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques comme l'internet. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique. Jusqu'à l'avènement des VPN, les sociétés devaient utiliser des liaisons Transpac, ou des lignes louées, dont le coût était très élevé. Les VPN ont permis de démocratiser ce type de liaison. [11]

3.5.1 *Principe de fonctionnement*

Un réseau VPN repose sur un protocole appelé "**protocole de tunneling**". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

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. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme internet.

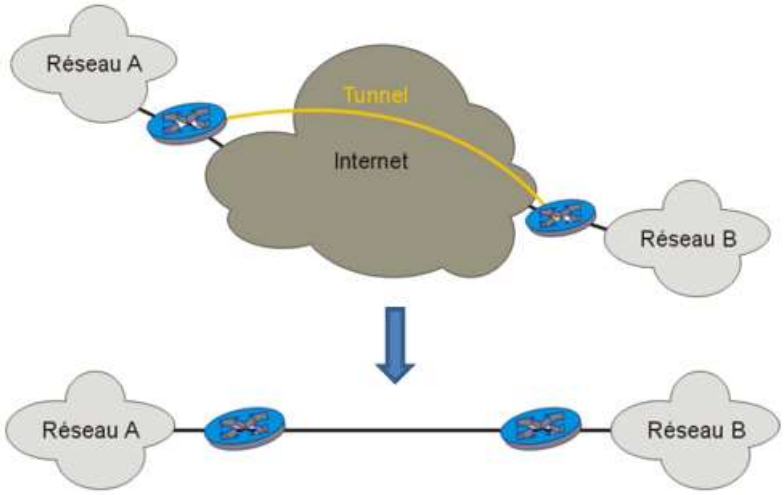

Figure 3.04 : *Principe du tunneling*

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'**encapsulation**, de **transmission** et de **désencapsulation**.
Les principaux avantages d'un VPN sont :

- **La sécurité :** assure des communications sécurisées et chiffrées.
- **La simplicité :** utilise les circuits de télécommunication classiques.
- **L'économie :** utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.

3.5.2 *Les différents types de VPN*

Suivant les besoins, il existe trois (03) types standard d'utilisation des VPN : le VPN d'accès, l'intranet VPN, et l'extranet VPN. [11]

3.5.2.1 VPN d'accès

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée Ce qui peut poser des problèmes de sécurité.
- Sur la deuxième méthode ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Pour pallier ce problème certaines entreprises mettent en place des VPN à base de SSL, technologie implémentée dans la majorité des navigateurs Internet du marché.

Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe", par un algorithme dit "Tokens sécurisés" (utilisation de mots de passe aléatoires) ou par certificats numériques.

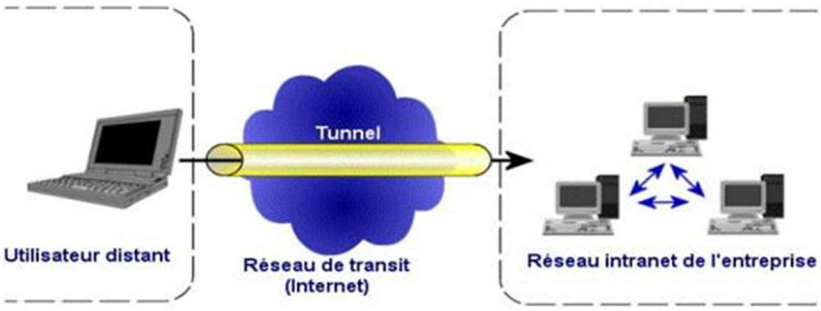

Figure 3.05 : *VPN d'accès*

3.5.2.2 L'intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage "infaillible". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

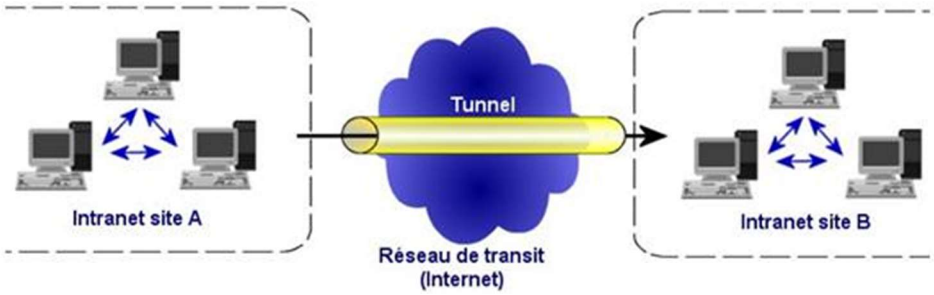

Figure 3.06 : *Intranet VPN*

3.5.2.3 Extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

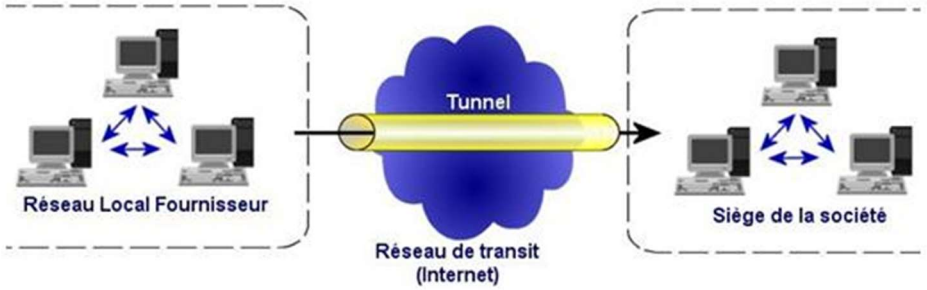

Figure 3.07 : *Extranet VPN*

3.5.3 ***Les contraintes d'un VPN***

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur : Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- Gestion d'adresses : Chaque client sur le réseau doit avoir une adresse privée. Cette adresse doit rester confidentielle. De plus, un nouveau client doit pouvoir se connecter facilement au réseau.

- Cryptage des données : Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- Gestion de clés : Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multi protocole : La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

3.6 **Protocoles utilisés pour réaliser une connexion VPN**

Nous pouvons classer les protocoles que nous allons étudier en trois catégories : [12]

- Les protocoles de niveau 2 comme PPTP et L2tp.
- Les protocoles de niveau 3 comme IPsec.
- Les protocoles de niveau 4 comme SSL.

Il existe en réalité trois protocoles de niveau 2 permettant de réaliser des VPN : PPTP (de Microsoft), L2F (développé par CISCO) et enfin L2tp. Nous n'évoquerons dans cette étude que PPTP et L2tp : le protocole L2F ayant aujourd'hui quasiment disparut. Le protocole PPTP aurait sans doute lui aussi disparut sans le soutien de Microsoft qui continue à l'intégrer à ses systèmes d'exploitation Windows. L2tp est une évolution de PPTP et de L2F, reprenant les avantages des deux protocoles.

Les protocoles de couche 2 dépendent des fonctionnalités spécifiées pour PPP (Point to Point Protocol), c'est pourquoi nous allons tout d'abord rappeler le fonctionnement de ce protocole.

3.6.1 ***Rappels sur PPP***

PPP (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets IP, IPx et Netbeui dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau (NAS). Le protocole PPP est défini dans la **Rfc 1661** appuyé de la **Rfc 2153.**

3.6.1.1 Généralité

PPP est l'un des deux protocoles issus de la standardisation des communications sur liaisons séries (SLIP étant le deuxième). Il permet non seulement l'encapsulation de datagrammes, mais également la résolution de certains problèmes liés aux protocoles réseaux comme l'assignation et la gestion des adresses (IP, X25 et autres).

Une connexion PPP est composée principalement de trois parties :

- Une méthode pour encapsuler les datagrammes sur la liaison série. PPP utilise le format de trame **HDLC (Hight Data Level Control)** de l'ISO.
- Un protocole de contrôle de liaison (**LCP - Link Control Protocol**) pour établir, configurer et tester la connexion de liaison de données.
- Plusieurs protocoles de contrôle de réseaux **(NCPs - Network Control Protocol)** pour établir et configurer les différents protocoles de couche réseau.

3.6.1.2 Format d'une trame PPP

Fanion	Adresse	Contrôle	Protocole	Données	FCS	Fanion
01111110	11111111	00000011	16 bits		16 bits	01111110

Figure 3.08 : *Format d'une trame PPP*

Fanion : séparateur de trame. Un seul drapeau est nécessaire entre 2 trames.

Adresse : Le champ adresse correspond à une adresse HDLC, or PPP ne permet pas un adressage individuel des stations donc ce champ doit être à 0xFF (toutes les stations), toute adresse non reconnue fera que la trame sera détruite.

Contrôle : Le champ contrôle doit être à 0x03, ce qui correspond à une trame HDLC non numérotée. Toute autre valeur fera que la trame sera détruite.

Protocole : La valeur contenue dans ce champ doit être impaire (l'octet de poids fort étant pair). Ce champ identifie le protocole encapsulé dans le champ informations de la trame. Les différentes valeurs utilisables sont définies dans la RFC « assign number » et représentent les différents protocoles supportés par PPP (OSI, IP, Decnet IV, IPx,…), les NCP associés ainsi que les LCP.

Informations : De longueur comprise entre 0 et 1500 octets, ce champ contient le datagramme du protocole supérieur indiqué dans le champ « protocole ». Sa longueur est détectée par le drapeau de fin de trame, moins 2 octets de contrôle.

FCS (Frame Check Sequence) : Ce champ contient la valeur du checksum de la trame. PPP vérifie le contenu du FCS lorsqu'il reçoit un paquet. Le contrôle d'erreur appliqué par PPP est conforme à X25.

3.6.1.3 Les différentes phases d'une connexion PPP

Toute connexion PPP commence et finit par une phase dite de "liaison morte". Dès qu'un événement externe indique que la couche physique est prête, la connexion passe à la phase suivante, à savoir l'établissement de la liaison. Comme PPP doit être supporté par un grand nombre d'environnements, un protocole spécifique a été élaboré et intégré à PPP pour toute la phase de connexion ; il s'agit de LCP (Link Control Protocol). LCP est un protocole utilisé pour établir, configurer, tester, et terminer la connexion PPP. Il permet de manipuler des tailles variables de paquets et effectue un certain nombre de tests sur la configuration. Il permet notamment de détecter un lien bouclé sur lui-même.

La connexion PPP passe ensuite à une phase d'authentification. Cette étape est facultative et doit être spécifiée lors de la phase précédente.

Si l'authentification réussie ou qu'elle n'a pas été demandée, la connexion passe en phase de "Protocole réseau". C'est lors de cette étape que les différents protocoles réseaux sont configurés. Cette configuration s'effectue séparément pour chaque protocole réseau. Elle est assurée par le protocole de contrôle de réseau (NCP) approprié. A Ce moment, le transfert des données est possible. Les NPC peuvent à tout moment ouvrir ou fermer une connexion. PPP peut terminer une liaison à tout moment, parce qu'une authentification a échouée, que la qualité de la ligne est mauvaise ou pour toute autre raison. C'est le LCP qui assure la fermeture de la liaison à l'aide de paquets de terminaison. Les NCP sont alors informés par PPP de la fermeture de la liaison.

3.6.2 *Protocole PPTP*

PPTP (Point-to-point tunneling protocol), définit par la **Rfc 2637**, est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN). Microsoft a

implémenté ses propres algorithmes afin de l'intégrer dans ses versions de windows. Ainsi, PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression. L'authentification se fait grâce au protocole **Ms-Chap** de Microsoft qui, après la cryptanalyse de sa version 1, a révélé publiquement des failles importantes. Microsoft a corrigé ces défaillances et propose aujourd'hui une version 2 de Ms-Chap, plus sûre. La partie chiffrement des données s'effectue grâce au protocole **MPPE (Microsoft Point-to-Point Encryption).**

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole **GRE (Generic Routing Encapsulation)**. Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établie une connexion de type PPP et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP. Tout trafic client conçu pour Internet emprunte la connexion physique normale, alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de PPTP.

Figure 3.09 : *Principe du protocole PPTP*

Plusieurs protocoles peuvent être associés à PPTP afin de sécuriser les données ou de les compresser. On retrouve évidement les protocoles développés par Microsoft et cités précédemment. Ainsi, pour le processus d'identification, il est possible d'utiliser les protocoles PAP (Password Authentification Protocol) ou MsChap. Pour l'encryptage des données, il est possible d'utiliser les fonctions de MPPE. Enfin, une compression de bout en bout peut être réalisée par MPPC (Microsoft Point to Point Compression). Ces divers protocoles permettent

de réaliser une connexion VPN complète, mais les protocoles suivants permettent un niveau de performance et de fiabilité bien meilleur.

3.6.3 *Protocole L2TP*

L2TP (Layer 2 Tunneling Protocol), définit par la **Rfc 2661**, est issu de la convergence des protocoles PPTP et L2F. Il est actuellement développé et évalué conjointement par Cisco Systems, Microsoft, Ascend, 3Com ainsi que d'autres acteurs clés du marché des réseaux. C'est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. L2TP repose sur deux concepts : les concentrateurs d'accès L2TP **(LAC : L2TP Access Concentrator)** et les serveurs réseau L2TP **(LNS : L2TP Network Server)**.

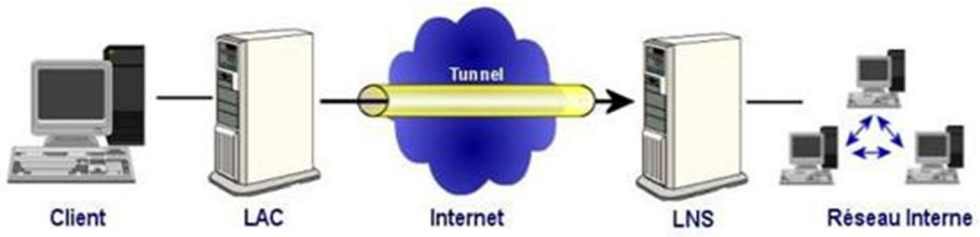

Figure 3.10 : *Concept du L2TP*

L2TP se sert d'une série de messages L2TP pour assurer la maintenance du tunnel et d'UDP pour envoyer les trames PPP dans du L2TP. Il n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'IPsec et L2TP.

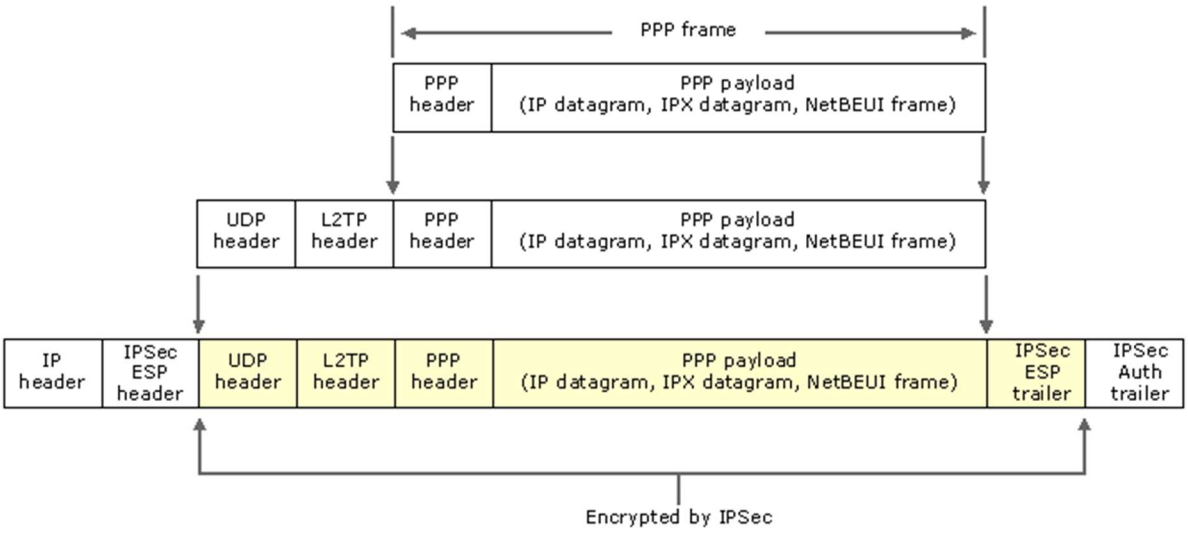

Figure 3.11 : *Format de trame L2TP*

3.6.3.1 Concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator)

Les périphériques LAC peuvent être intégrés à la structure d'un réseau commuté comme le réseau téléphonique commuté (RTC) ou encore associés à un système d'extrémité PPP prenant en charge le protocole L2TP.

Le rôle du concentrateur d'accès LAC se limite à fournir un support physique qui sera utilisé par L2TP pour transférer le trafic vers un ou plusieurs serveurs réseau L2TP (LNS). Il assure le fractionnement en canaux pour tout protocole basé sur PPP. Le LAC est l'émetteur des appels entrants et le destinataire des appels sortants.

3.6.3.2 Serveur réseau L2TP (LNS : L2TP Network Server)

Les serveurs réseau L2TP ou LNS peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP. Le LNS gère le protocole L2TP côté serveur. Le protocole L2TP n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP. C'est pourquoi, les serveurs réseau LNS, ne peuvent avoir qu'une seule interface de réseau local (LAN) ou étendu (WAN). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès LAC : Asynchrone, RNIS, PPP sur ATM ou PPP sur relais de trame. Le LNS est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le LNS qui sera responsable de l'authentification du tunnel.

3.6.4 *Protocole IPsec*

IPsec, définit par la **Rfc 2401**, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration vers IPv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPsec pour **IP Security Protocols**. IPsec est basé sur deux mécanismes. Le premier, **AH**, pour **Authentification Header** vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par ce "protocole" ne sont pas encodées. Le second, **ESP**, pour **Encapsulating Security Payload** peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole **IKE** permet de gérer les échanges ou les associations entre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans IPsec. [11] [13]

3.6.4.1 Vue d'ensemble

Les mécanismes mentionnés ci-dessus font bien sûr appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes de chiffrement, clefs, mécanismes sélectionnés...) sur lesquels les tiers communicants doivent se mettre d'accord. Afin de gérer ces paramètres, IPsec a recours à la notion d'association de sécurité **(Security Association, SA).**

L'association de sécurité IPsec est une connexion qui fournit des services de sécurité au trafic qu'elle transporte. Il s'agit d'une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée. Une SA est unidirectionnelle ; en conséquence, protéger les deux sens d'une communication classique requiert deux associations, une dans chaque sens. Les services de sécurité sont fournis par l'utilisation soit de AH soit de ESP. Le rôle d'une SA est donc de consigner, pour chaque adresse IP avec laquelle l'implémentation IPsec peut communiquer, les informations suivantes :

- Index de la SA appelé SPI (pour Security Parameter Index) choisi par le récepteur
- Un numéro de séquence, indicateur utilisé pour le service d'anti-rejet
- Une fenêtre d'anti-rejet : compteur 32 bits
- Dépassement de séquence

- Paramètres d'authentification (algorithmes et clés)
- Paramètres de chiffrement (idem)
- Temps de vie de la SA
- Mode du protocole IPsec (tunnel ou transport)
- etc…

Chaque association est identifiée de manière unique à l'aide d'un triplet composé de :

- L'adresse de destination des paquets
- L'identifiant du protocole de sécurité (AH ou ESP)
- Le SPI

Pour gérer les associations de sécurités actives, on utilise une "base de données des associations de sécurité" **(Security Association Database, SAD)**. Elle contient tous les paramètres relatifs à chaque SA et sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre. Les protections offertes par IPsec sont basées sur des choix définis dans une "base de données de politique de sécurité" **(Security Policy Database, SPD)**. Cette base de données est établie et maintenue par un utilisateur, un administrateur système ou une application mise en place par ceux-ci. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer ou rejeté.

3.6.4.2 Principe de fonctionnement

Le schéma ci-dessous représente tous les éléments présentés ci-dessus, leurs positions et leurs interactions.

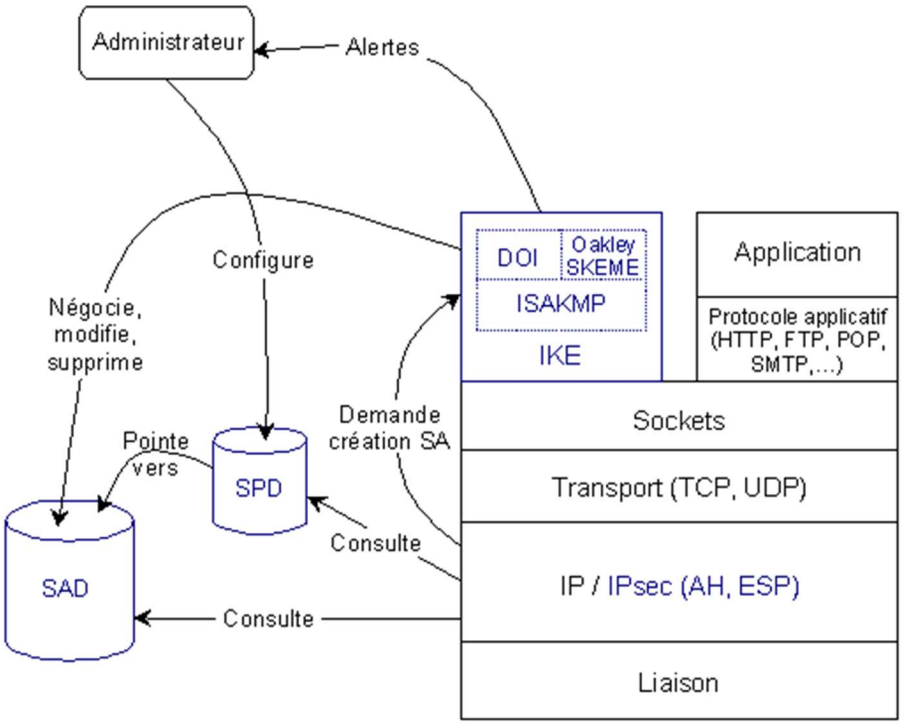

Figure 3.12 : *Les différents éléments de IPsec*

On distingue deux situations :

- Trafic sortant

  Lorsque la "couche" IPsec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPsec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.
- Trafic entrant

  Lorsque la couche IPsec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPsec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la SPD est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité.

Dans le cas où le paquet reçu est un paquet IP classique, la SPD permet de savoir s'il a néanmoins le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont traités par IKE, qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse.

3.6.4.3 Les protocoles à la base d'IPsec

a. AH (authentication header)

AH est le premier et le plus simple des protocoles de protection des données qui font partie de la spécification IPsec. Il est détaillé dans la **Rfc 2402**. Il a pour vocation de garantir :

- L'**authentification** : les datagrammes IP reçus ont effectivement été émis par l'hôte dont l'adresse IP est indiquée comme adresse source dans les en-têtes.
- L'**unicité** (optionnelle, à la discrétion du récepteur) : un datagramme ayant été émis légitimement et enregistré par un attaquant ne peut être réutilisé par ce dernier, les attaques par rejet sont ainsi évitées.
- L'**intégrité** : les champs suivants du datagramme IP n'ont pas été modifiés depuis leur émission : les données (en mode tunnel, ceci comprend la totalité des champs, y compris les en-têtes, du datagramme IP encapsulé dans le datagramme protégé par AH), version (4 en IPv4, 6 en IPv6), longueur de l'en-tête (en IPv4), longueur totale du datagramme (en IPv4), longueur des données (en IPv6), identification, protocole ou en-tête suivant (ce champ vaut 51 pour indiquer qu'il s'agit du protocole AH), adresse IP de l'émetteur, adresse IP du destinataire (sans source routing). [11]

Cependant, notant qu'AH n'assure pas la confidentialité, les données sont signées mais pas chiffrées. Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé "valeur de vérification d'intégrité" (Intégrity Check Value, **ICV**). La protection contre le rejet se fait grâce à un numéro de séquence.

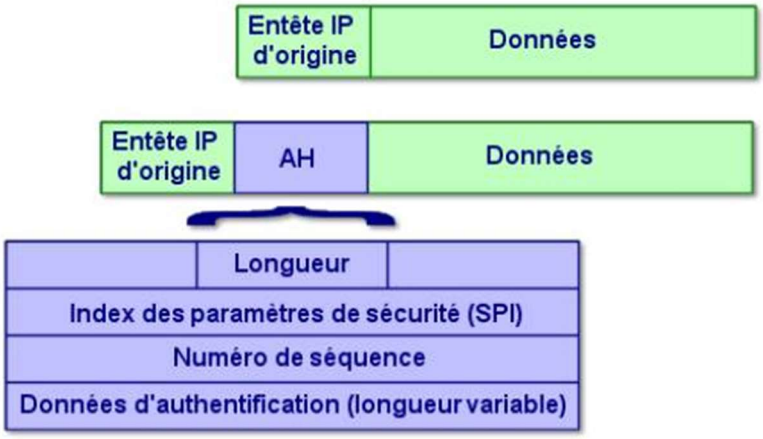

Figure 3.13 : *Principe du AH*

b. ESP (Encapsulating Security Payloasd)

ESP peut assurer au choix, un ou plusieurs des services suivants :

- Confidentialité (confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel).
- Intégrité des données en mode non connecté et authentification de l'origine des données, protection contre le rejet. [11]

La confidentialité peut être sélectionnée indépendamment des autres services, mais son utilisation sans intégrité/authentification (directement dans ESP ou avec AH) rend le trafic vulnérable à certains types d'attaques actives qui pourraient affaiblir le service de confidentialité.

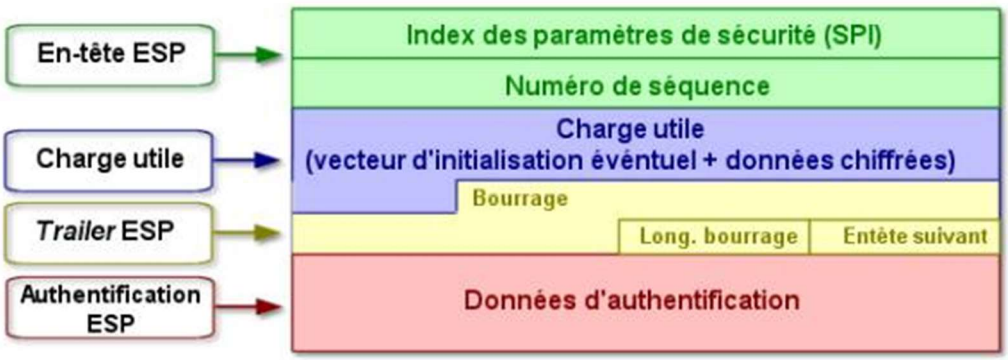

Figure 3.14 : *Principe du ESP*

Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs ou pour aligner le texte chiffré sur une limite de 4 octets ; et les données d'authentification ne sont présentes que si ce service a été sélectionné.

Voyons maintenant comment est appliquée la confidentialité dans ESP. L'expéditeur :

- Encapsule, dans le champ "charge utile" de ESP, les données transportées par le datagramme original et éventuellement l'en-tête IP (mode tunnel).
- Ajoute si nécessaire un bourrage.
- Chiffre le résultat (données, bourrage, champs longueur et en-tête suivant).
- Ajoute éventuellement des données de synchronisation cryptographiques (vecteur d'initialisation) au début du champ "charge utile".

c. La gestion des clefs pour IPsec : IKE ET ISAKMP

Les protocoles sécurisés ont recours à des algorithmes de cryptage, et ont donc besoin de clefs. Un des principaux problèmes dans ce cas est la gestion de ces clefs. Par gestion, on entend la génération, la distribution, le stockage et la suppression de ces clefs. Ces différentes tâches sont dévolues à des protocoles spécifiques de gestion de ces clefs, à savoir :

- **IKE (Internet Key Exchange) :** C'est un système développé spécifiquement pour IPsec qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'Internet. Il est composé de plusieurs éléments : le cadre générique ISAKMP et une partie des protocoles Oakley et SKEME. Lorsqu'il est utilisé pour IPsec, IKE est de plus complété par un "domaine d'interprétation" pour IPsec.
- **ISAKMP (Internet Security Association and Key Management Protocol) :** Il a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clefs (et plus généralement des associations de sécurité).

3.6.5 *Protocole SSL*

SSL **(Secure Socket Layer)** est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application. Il a

deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

SSL est le dernier arrivé dans le monde des VPN, mais il présente un gros avantage dans la mesure où coté client, il ne nécessite qu'un navigateur Internet standard. Ce protocole est celui qui est utilisé en standard pour les transactions sécurisées sur Internet.

L'inconvénient néanmoins de ce type de protocole est qu'il se limite au protocole https, ce qui n'est pas le seul besoin de connexion des entreprises.

3.7 Conclusion

Ce chapitre nous a permis d'étudier les techniques et les technologies proposées pour l'acheminement des données captées par les différentes stations ADS-B vers le centre Ivato. Les VSAT sont de très bon support de transmission. Mais comme tous système et vu les nombreux paramètres qu'on ne maîtrise pas, il peut y avoir des problèmes dans le réseau. Ainsi on se propose d'utiliser l'Internet comme backup. Par ailleurs la transmission multicast sera utilisée pour une meilleurs optimisation des ressources, et des tunnels seront créés pour que les données soient acheminées de manière sûre.

CHAPITRE 4 :
SIMULATION SOUS GNS3

4.1 Introduction

Le but de ce mémoire étant la densification de l'ADS-B dans la FIR d'Antananarivo, nous allons ainsi voir en premier lieu une présentation de la couverture de l'ensemble des stations ADS-B dans cette FIR ainsi que le choix de leurs emplacements. Ensuite, à l'aide d'une simulation sous GNS3 nous allons configurer le routage statique dans les différents routeurs, et mettre en évidence le protocole multicast PIM dense mode, ainsi que la création des réseaux VPN entre les différentes stations ADS-B et le centre Ivato en utilisant le tunnel GRE et le protocole IPsec, et enfin nous allons vérifier l'acheminement des données en temps réel à l'aide du protocole RTP.

4.2 Choix du logiciel

Afin de simuler la partie réseau du projet, nous allons utiliser les logiciels GNS3, VirtualBox et Wireshark.

4.2.1 *GNS3*

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation des réseaux informatiques complexes. Tout comme VMWare et VirtualBox qui permettent d'émuler différents systèmes d'exploitations, comme les différentes versions de Windows ou Ubuntu Linux, dans un environnement virtuel, GNS3 permet de faire le même type d'émulation utilisant des IOSs (Internetwork Operating Systems) Cisco.
GNS3 permet l'émulation des IOSs Cisco sur des ordinateurs tournant sous Windows ou Linux. L'émulation est possible pour une grande variété de routeurs ainsi que des pare-feu PIX. En utilisant une carte EtherSwitch sur un routeur, les plateformes interversibles peuvent aussi être émuler jusqu'à un certain niveau suivant les fonctionnalités supportées par la carte. Ce qui signifie que GNS3 est un outil inestimable pour préparer des certifications Cisco comme CCNA et CCNP. Il y a sur le marché beaucoup de simulateurs de routeur, mais suivant les lignes de commandes que le développeur choisit d'inclure les choix de simulateurs se réduisent. Dans presque la totalité des cas, il y a des commandes ou des paramètres qui ne marchent pas en pratique quand on travaille en laboratoire. Dans ces simulations, on a juste une représentation

du rendu final d'une simulation d'un routeur. La précision de la représentation ne dépend que du développeur. En utilisant GNS3, nous sommes sur un système IOS Cisco, donc nous pouvons voir le rendu du système et nous pouvons avoir accès à chaque commande ou paramètre supporté par le système. De plus, GNS3 est un open source, donc un programme gratuit, cependant dû aux restrictions au niveau de la licence, nous allons devoir trouver nos propre IOSs Cisco à utiliser sous GNS3. Ce dernier nous donnera un débit de près de 1000 paquets par seconde dans un environnement virtuel. Un routeur normal donnera un débit entre cent à mille fois plus élevé. Ainsi, GNS3 ne peut pas se substituer à un routeur réel, mais il est désigné pour être un outil pour apprendre et tester dans un laboratoire.

Figure 4.01 : *Logo de GNS3*

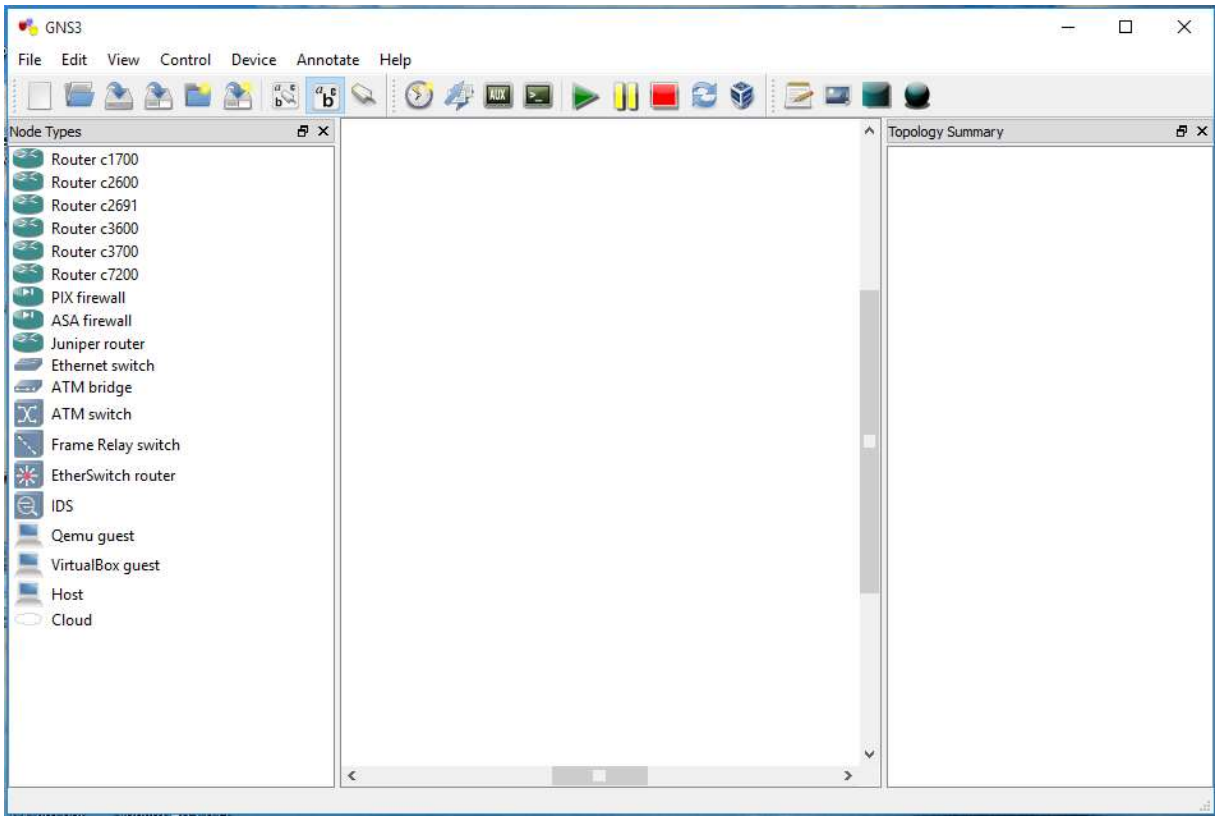

Figure 4.02 : *Interface graphique de GNS3*

Dans le cas de notre simulation, nous utiliserons des machines virtuelles à l'aide du logiciel VirtualBox. Ainsi, voyons dans le paragraphe qui suit une présentation de ce dernier.

4.2.2 *VirtualBox*

Comme nous l'avons dit plus haut, VirtualBox permet d'émuler n'importe quel système d'exploitation grand public. Par exemple, VirtualBox permet de démarrer un Windows dans une fenêtre d'un ordinateur sous GNU/Linux (ou inversement), il permet également de démarrer toutes les versions de Windows, MacOS X, GNU/Linux Debian/Ubuntu ... Il est donc utile aux utilisateurs de Windows qui veulent tester un Linux sans redémarrer leur machine, et aux utilisateurs de Linux qui ne peuvent se débarrasser d'un logiciel tournant sous Windows.
Avec VirtualBox, des interfaces graphiques nous guident dans la configuration des machines virtuelles, du choix du système installable au nombre de carte réseau à simuler, en passant par la taille du disque dur, les fonctionnalités du micro-processeur, la quantité de mémoire RAM vampirisée à la machine physique et la présence de lecteurs (disquette, CD-ROM).
Pour démarrer une machine virtuelle, il suffit de double-cliquer sur son icône dans la liste des machines virtuelles configurées dans notre VirtualBox. Une fois démarrée, elle se comporte comme un ordinateur à part entière, et si nous positionnons sa fenêtre en plein écran l'illusion sera parfaite. Il sera également possible d'en lancer plusieurs en même temps si nous disposons d'une machine suffisamment puissante et nous pourrons alors faire fonctionner un serveur, comme dans notre cas celui d'une station ADS-B et aller consulter ce dernier vers le client Ivato.
Les principaux concurrents de VirtualBox sont VMware et VirtualPC pour les non-libres et Qemu voire Xen et KVM pour les libres, mais ces deux derniers sont dépourvus d'interfaces graphiques.
Nous avons choisi VirtualBox car c'est un logiciel libre et qui compte parmi les plus performants et les plus conviviaux de sa catégorie. C'est un logiciel puissant qui permet de tester et débloquer bien des situations, mais qui nécessite une machine tout aussi puissante tant du point de vue de la mémoire RAM (>1Go), que du processeur (>2GHz) et bien sûr suffisamment de place sur son disque dur pour installer plusieurs systèmes dessus.

Figure 4.03 : *Interface graphique du logiciel VirtualBox*

4.2.3 ***Wireshark***

Wireshark est un logiciel d'analyse réseau (sniffer) qui permet de visualiser l'ensemble des données transitant sur les interfaces, au choix, d'une quelconque machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP (Packet Capture), puis regroupés en blocs d'informations et analysés par le logiciel.

Wireshark permet d'analyser un trafic enregistré dans un fichier annexe, mais également et surtout le trafic en direct sur des interfaces réseau. Cette seconde fonction nécessite de posséder les droits administrateurs, ou d'appartenir à un groupe possédant ces droits.

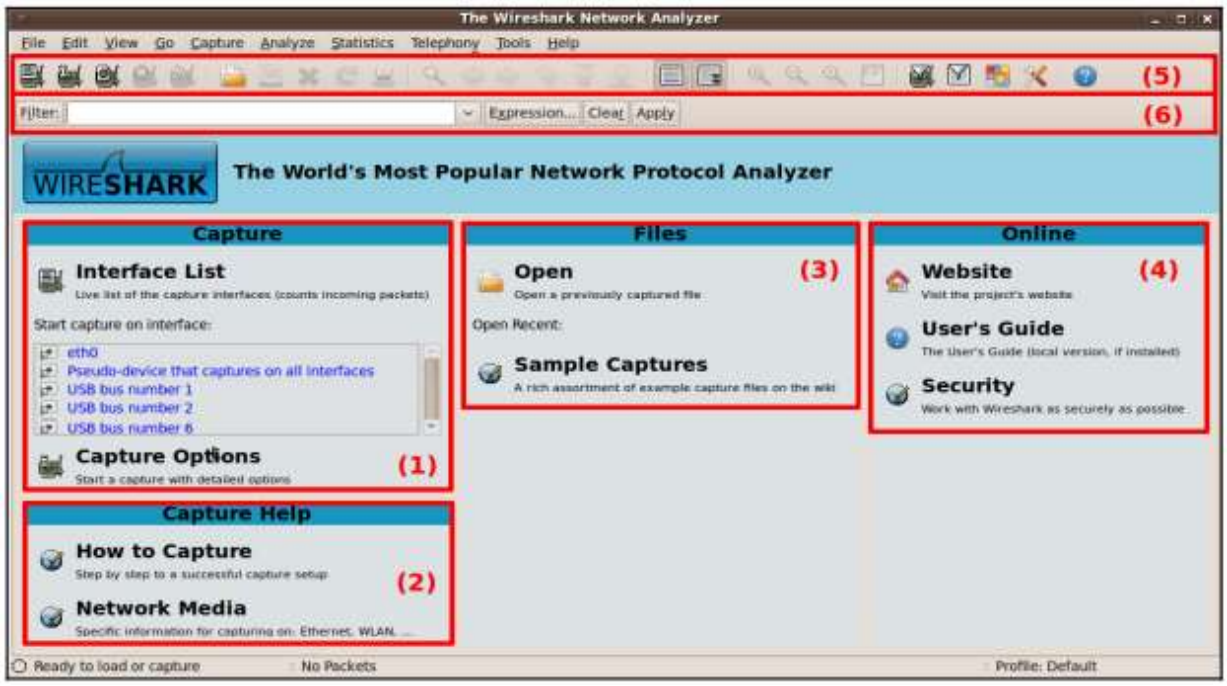

Figure 4.04 : *Fenêtre d'ouverture de Wireshark*

L'utilitaire s'ouvre sur l'interface présentée en Figure 4.03 découpé en quatre zones :

(1) liste des interfaces et lancement rapide d'une capture

(2) Aide sur la capture de paquets

(3) Analyse d'une capture précédente enregistrée sur fichier

(4) Aide online et manuel utilisateur

Une fois lancée, la capture peut être interrompue, et lorsqu'elle est active, le logiciel présente l'interface de l'analyseur comme sur la Figure 5.04. Cette interface reste ensuite visible lorsque la capture est arrêtée.

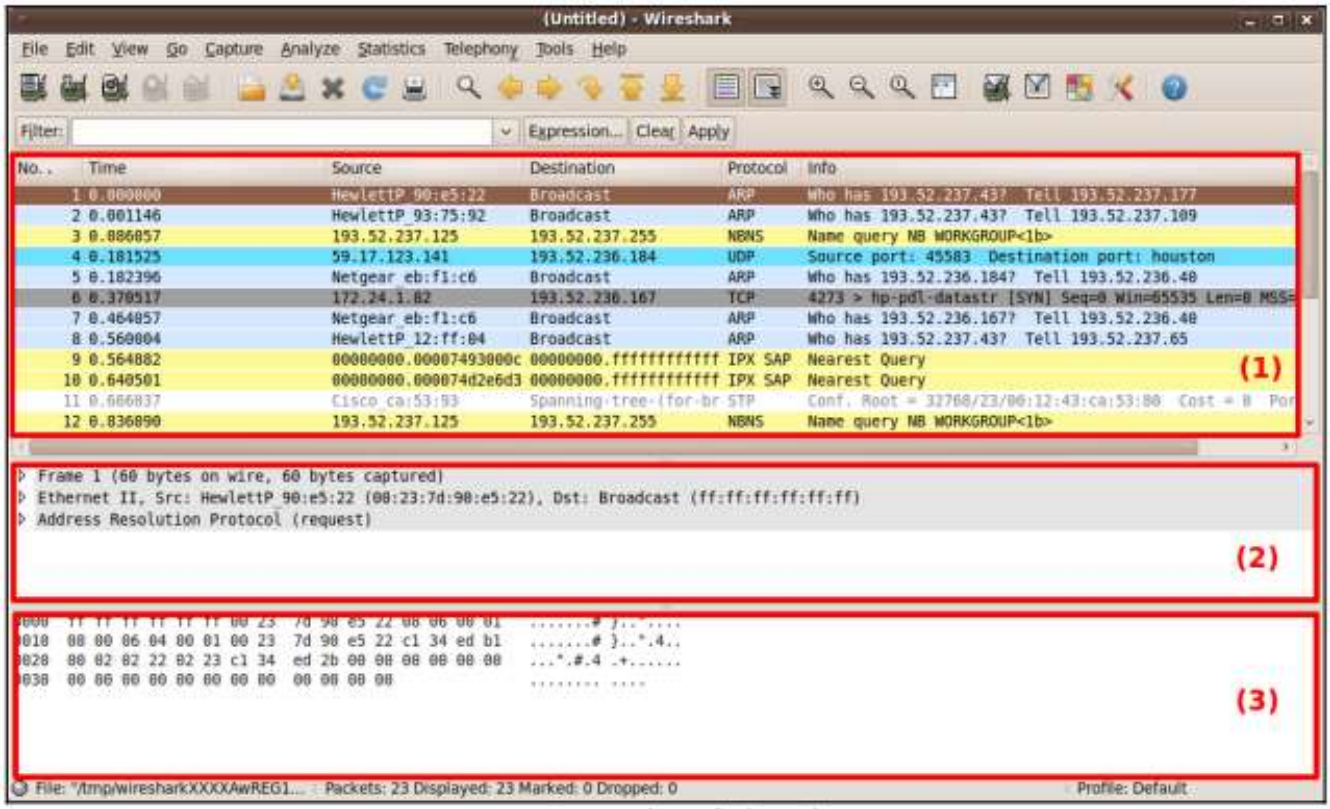

Figure 4.05 : *Interface de l'analyseur*

L'interface de l'analyseur est découpée en trois zone :

- Zone supérieure, numérotée (1) : liste l'ensemble des paquets capturés
- Zone centrale, numérotée (2) : affiche le détail d'un paquet sélectionné dans la liste des paquets de la zone supérieure. Les informations présentées y sont de loin les plus pertinentes, puisqu'il est possible de visualiser aisément les différents en-têtes résultant de l'encapsulation d'un message.
- Zone inférieure, numérotée (3) : présente l'ensemble du paquet sous forme octale et ASCII. Ces octets contiennent les en-têtes des différentes couches de l'architecture TCP/IP ainsi que les données transmises par le processus à l'origine du message.

Notant qu'il est souvent utile de filtrer les paquets à capturer, afin de pouvoir visualiser correctement un certain type de paquets seulement. Wireshark permet de filtrer les paquets à capturer en fonction des informations des différentes couches d'encapsulation.

La mise en place d'un filtre s'effectue par le biais d'une règle de filtre à définir dans la zone « filtre » de l'analyseur. Une règle de filtre est constituée d'un ensemble de tests d'expressions impliquant des noms de champs et des valeurs. Un paquet n'est alors listé qu'à la condition qu'il satisfasse les conditions du filtre. L'ensemble des champs utilisables dans l'établissement des

règles est listé dans la fenêtre pop-up accessible en cliquant sur le bouton « expression ». Les règles peuvent être élaborées en sélectionnant les champs à partir de cette fenêtre, ou en les écrivant directement dans la zone de filtre. Un ensemble de filtres pré-définis est accessible en cliquant sur le bouton « filter ». Cette liste de filtres peut être complétée d'entrées enregistrées. Une fois le filtre défini, il ne faut pas oublier de l'appliquer avec le bouton « Apply ».

4.3 **Présentation de la couverture**

Comme nous l'avons vu dans le chapitre 2, il n'existe actuellement qu'une seule station ADS-B (dans le cadre d'une expérimentation) dans la FIR d'Antananarivo qui a une couverture de 250 NM. Pourtant cette unique station ne permet pas de compléter la couverture Radar dans toute la FIR. L'implantation de l'ADS-B étant bien moins couteuse que celle d'un Radar, on se propose alors d'installer des stations ADS-B sol sur des points stratégiques.

Dans la FIR d'Antananarivo, l'ASECNA a placé des stations déportées, afin que les Contrôleurs aériens puissent garder la communication voix avec les Pilotes, dans les régions suivantes : Antalaha, Antsiranana, Maintirano, Mananjary, Mahajanga, Toamasina, Tolagnaro, Toliary, Moroni. Le choix de ces emplacements est surtout dû au flux du trafic aérien qui est dense dans ces zones.

Ainsi, afin de densifier la couverture ADS-B, nous avons choisi de faire cohabiter avec ces stations VHF déportées les stations ADS-B sol. La couverture de ces deux stations étant la même (250NM) dans le cas de Madagascar, nous avons utilisé la couverture de ces stations déportées pour présenter la couverture ADS-B après densification.

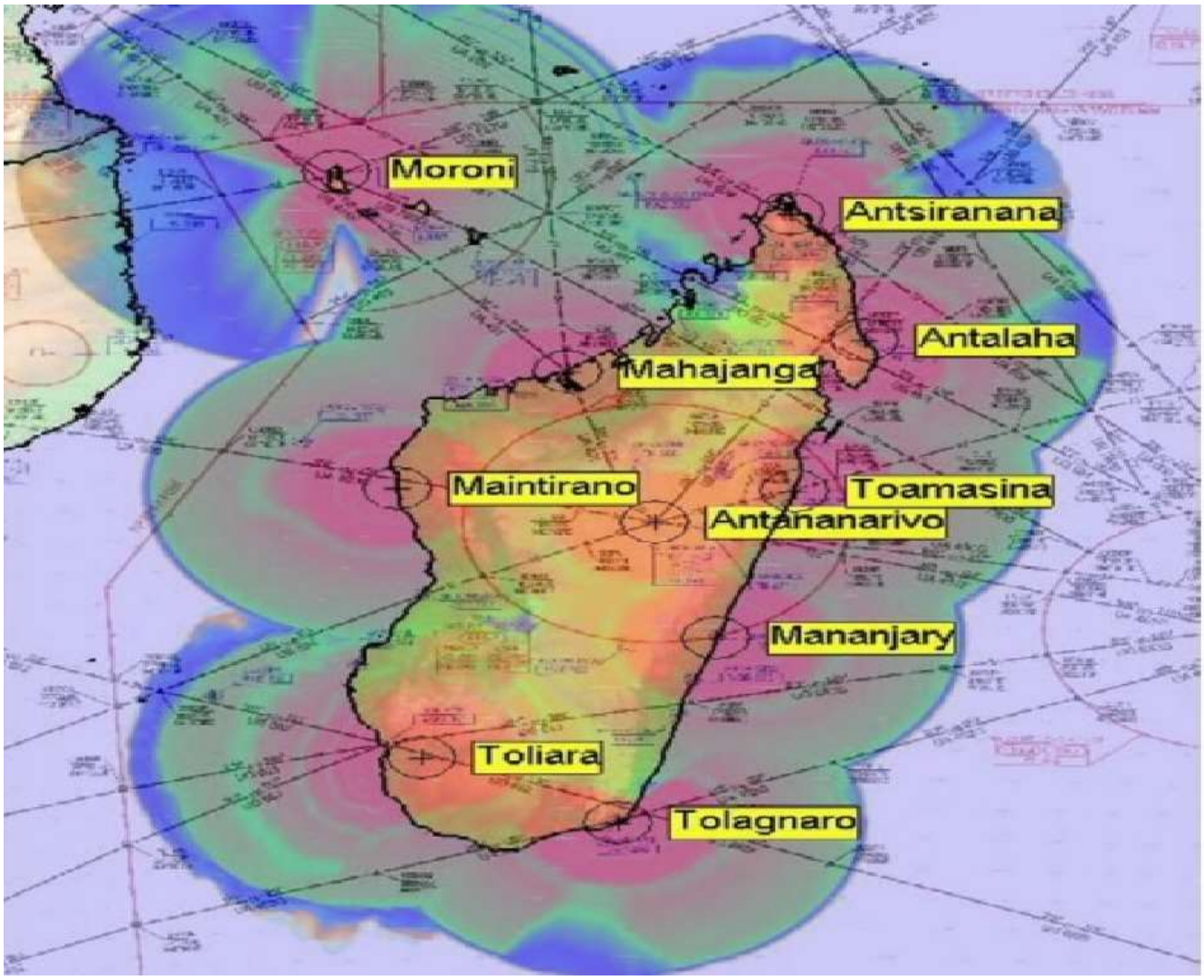

Figure 4.06 : *Couverture ADS-B après densification*

4.4 **Présentation de la simulation sous GNS3**

4.4.1 ***Topologie du réseau***

Comme nous l'avons dit précédemment, nous allons placer les stations ADS-B à Antalaha, Antsiranana, Maintirano, Mananjary, Mahajanga, Toamasina, Tolagnaro, Toliary, Moroni. Afin de simuler le réseau, nous allons représenter ces stations (serveurs) ainsi que le centre d'Ivato (client) par des machines virtuelles (VirtualBox), et nous aurons besoins de onze (11) routeurs (dont un va représenter le FAI (fournisseur d'accès internet)) et de dix (10) switchs.

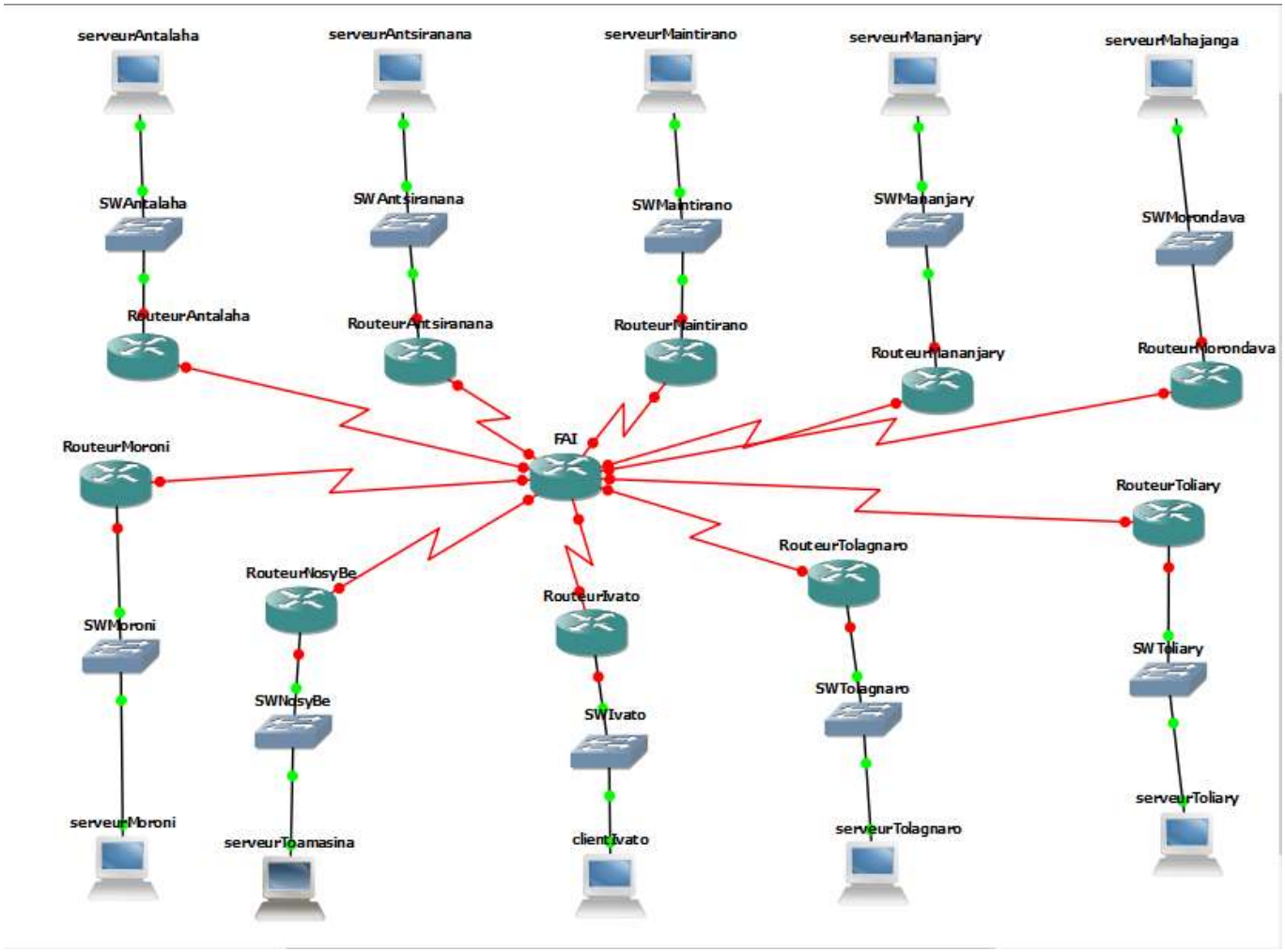

Figure 4.07 : *Topologie générale du réseau*

Comme nous pouvons le voir il nous faut un grand nombre de machines virtuelles et de routeurs pour réaliser cette simulation. Pour cela il nous faut une machine très puissante tant du point de vue de la mémoire que du processeur, et bien sûr de l'espace suffisant dans le disque dur. Malheureusement la machine que nous avons à notre disposition a une RAM de 8 Go, et un processeur Intel Core I5, et cela ne permet pas de simuler le réseau entier. Ainsi, nous allons juste nous limiter à trois machines virtuelles qui vont représenter le serveur d'Antsiranana (Diego), le serveur de Mahajanga (Majunga), et le client Ivato, quatre routeurs et trois switchs.

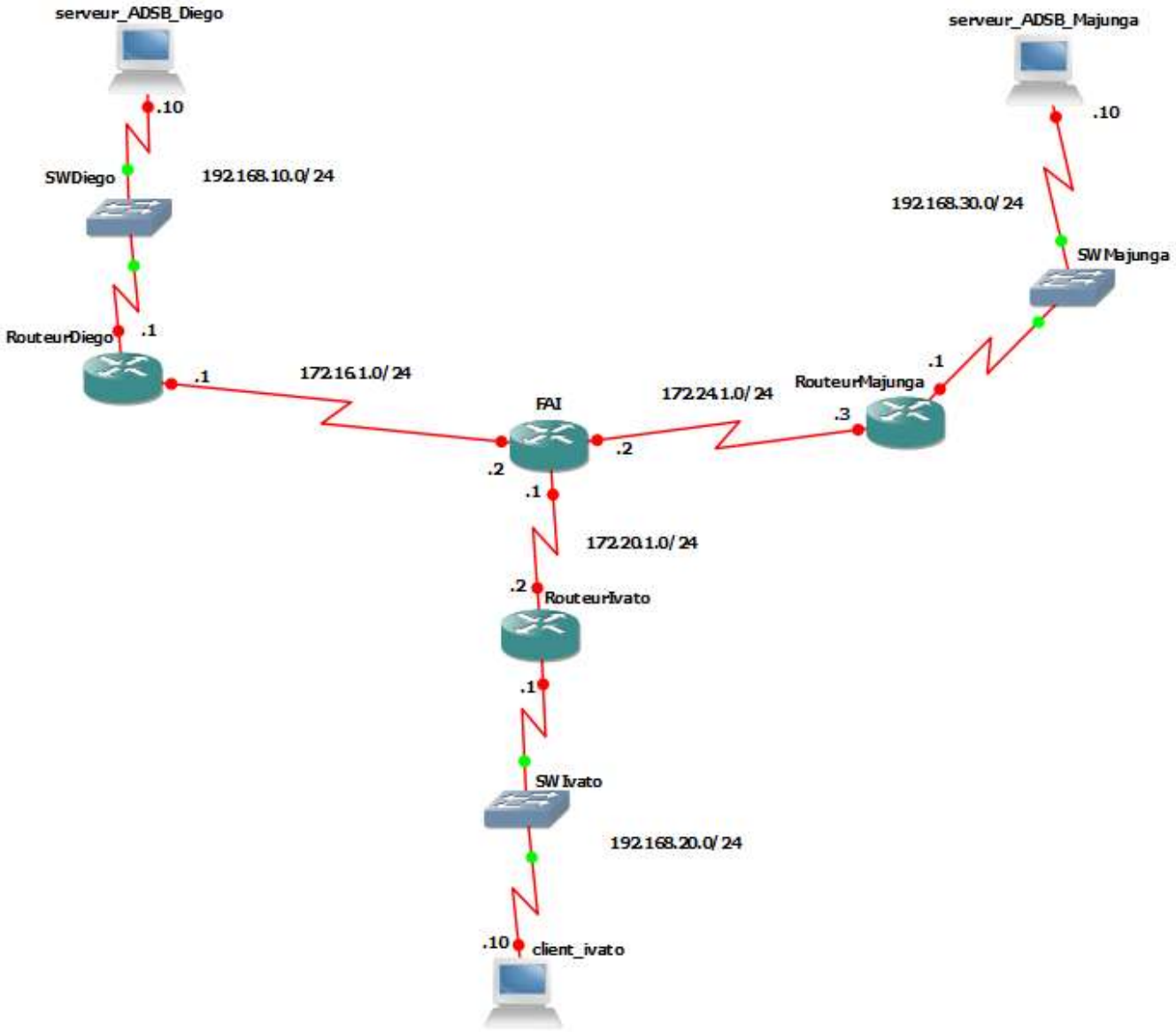

Figure 4.08 : *Topologie utilisée pour la simulation*

Les équipements utilisés sont :

- Routeurs de type **c3700** avec l'IOS « c3725-adventerprisek9-mz.124-15.T5.bin »
- Switchs de type Ethernet
- Câble série entre les routeurs, et câble FastEthernet entre des équipements différents (Machine virtuelle-switch, switch-routeur).

4.4.2 *Paramétrages des machines virtuelles*

Après avoir installé le logiciel VirtualBox, nous avons créé trois machines virtuelles avec le système d'exploitation Windows 7. Puis, nous avons configuré les cartes réseaux des différentes machines virtuelles. Afin que ces dernières puissent être connectées à un équipement CISCO,

il faut configurer la carte réseau en « Réseau Privé Hôte » et décliquer « câble connecté ». Ensuite, nous devons créer deux cartes réseaux : l'une servira à relier la machine virtuelle à la machine physique, et l'autre pour relier la machine virtuelle à GNS3.

Nous avons aussi attribué aux différentes machines virtuelles des adresses IP privées de classe C :

- Serveur ADS-B Diego : 192.168.10.10/24
- Serveur ADS-B Majunga : 192.168.30.10/24
- Client Ivato : 192.168.20.10/24

Enfin nous avons installé le logiciel VLC dans chaque machine virtuelle : dans celles qui vont servir de serveur, VLC va être utilisé pour diffuser du flux multicast, et dans le client Ivato nous allons lancer VLC afin de récupérer ce flux et le lire.

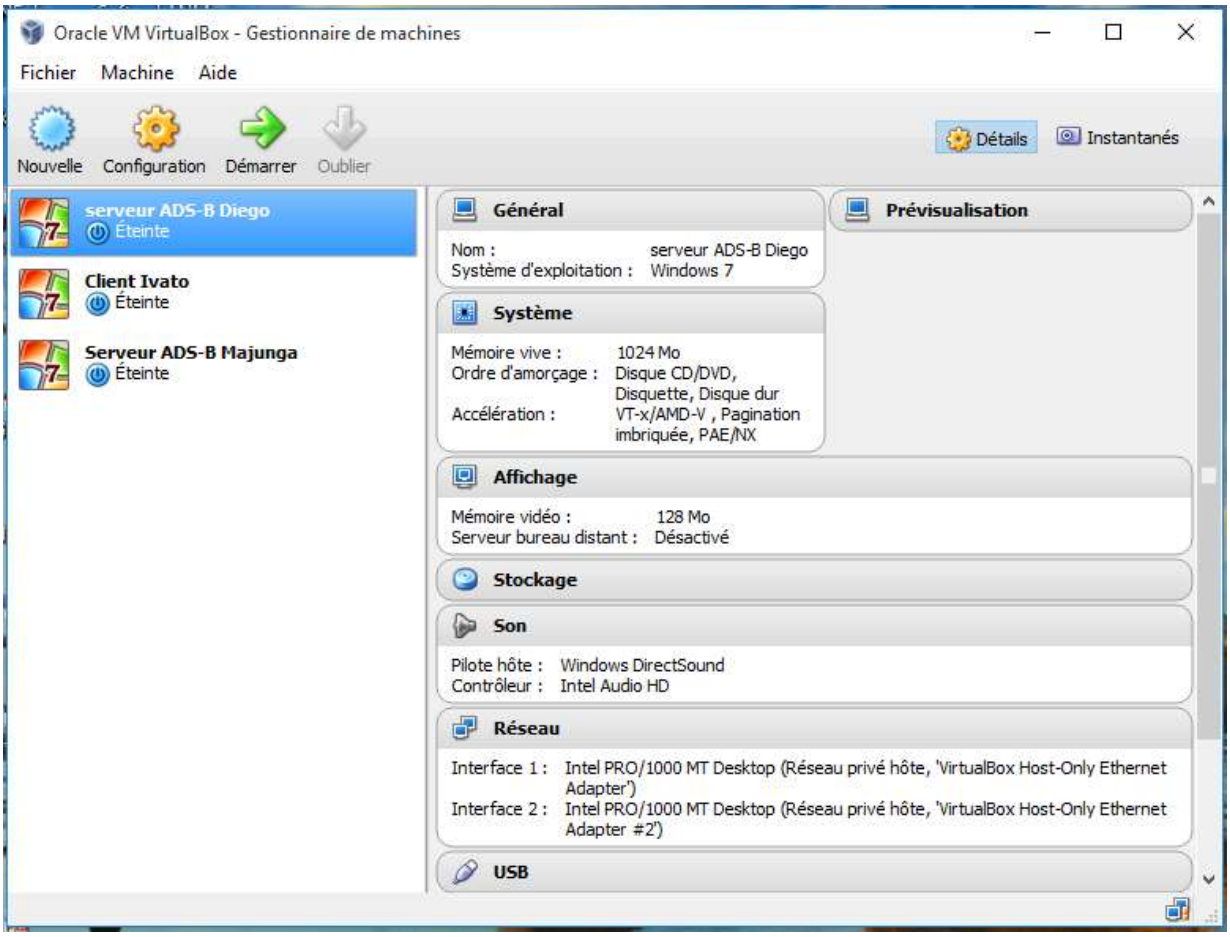

Figure 4.09 : *Interface VBOX avec les 3 machines virtuelles*

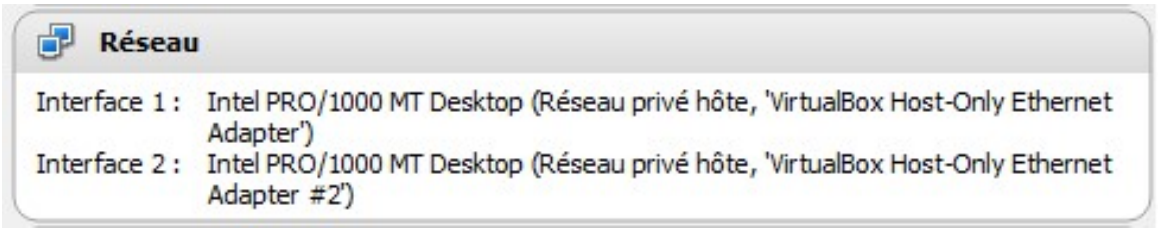

Figure 4.10 : *Paramétrage des deux cartes réseau*

4.4.3 ***Paramétrage des routeurs***

Avant toute chose on a d'abord attribuer des adresses IP à toutes les interfaces des routeurs que nous avons utilisé. Pour se faire, on a tapé les commandes suivantes :

- Dans RouteurDiego :

```
RouteurDiego>en
RouteurDiego#conf t
RouteurDiego(config)#interface FastEthernet0/0
RouteurDiego(config)#ip address 192.168.10.1 255.255.255.0
RouteurDiego(config)#no shutdown
RouteurDiego(config)#interface Serial0/0
RouteurDiego(config)#ip address 172.16.1.1 255.255.255.0
RouteurDiego(config)#no shutdown
```

- On a procédé de la même manière pour les routeurs FAI, RouteurIvato, et RouteurMajunga en se référant aux adresses IP sur la topologie.

Ensuite, nous avons opté de configurer le **routage statique** dans tous nos routeurs vu le nombre peu élevé de routeurs dans notre réseau.

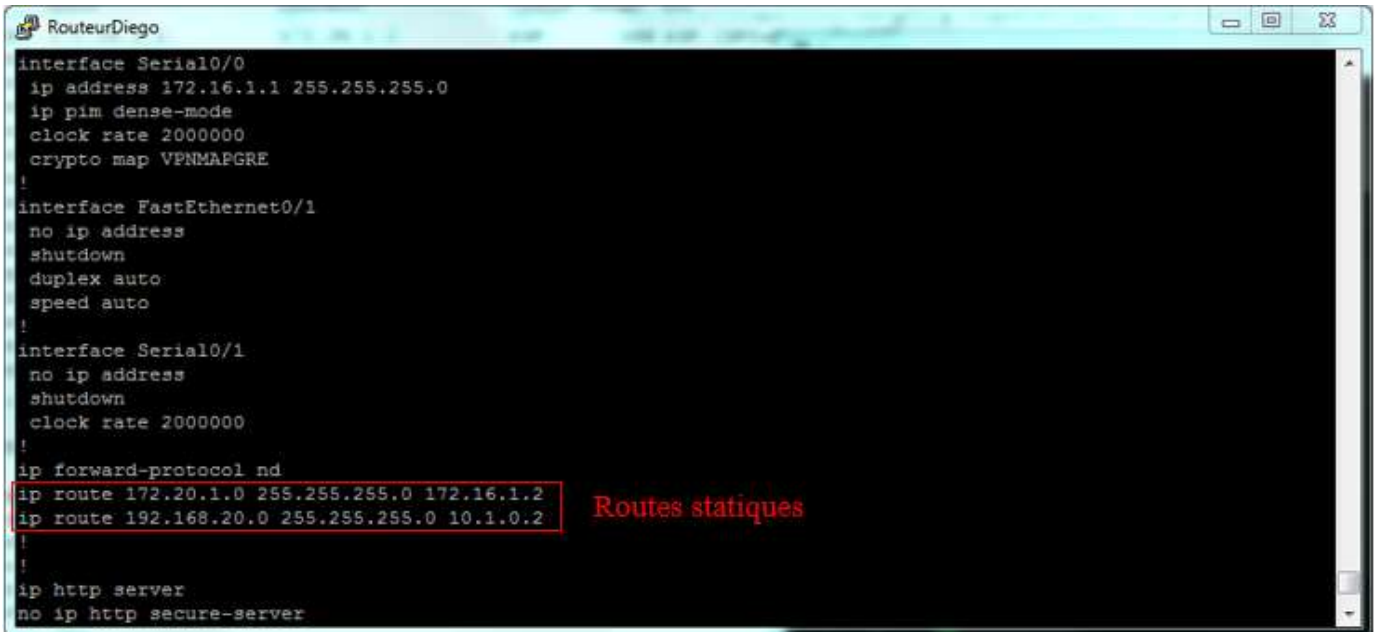

Figure 4.11 : *Routage statique dans RouteurDiego*

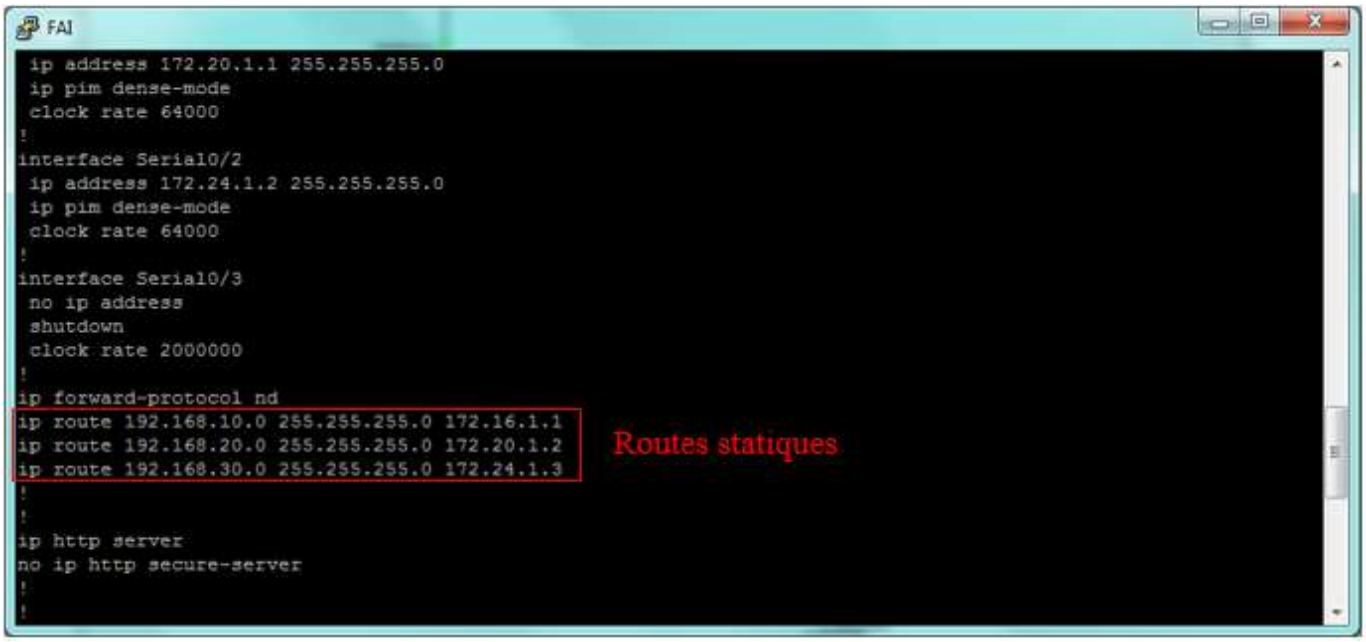

Figure 4.12 : *Routage statique dans Routeur FAI*

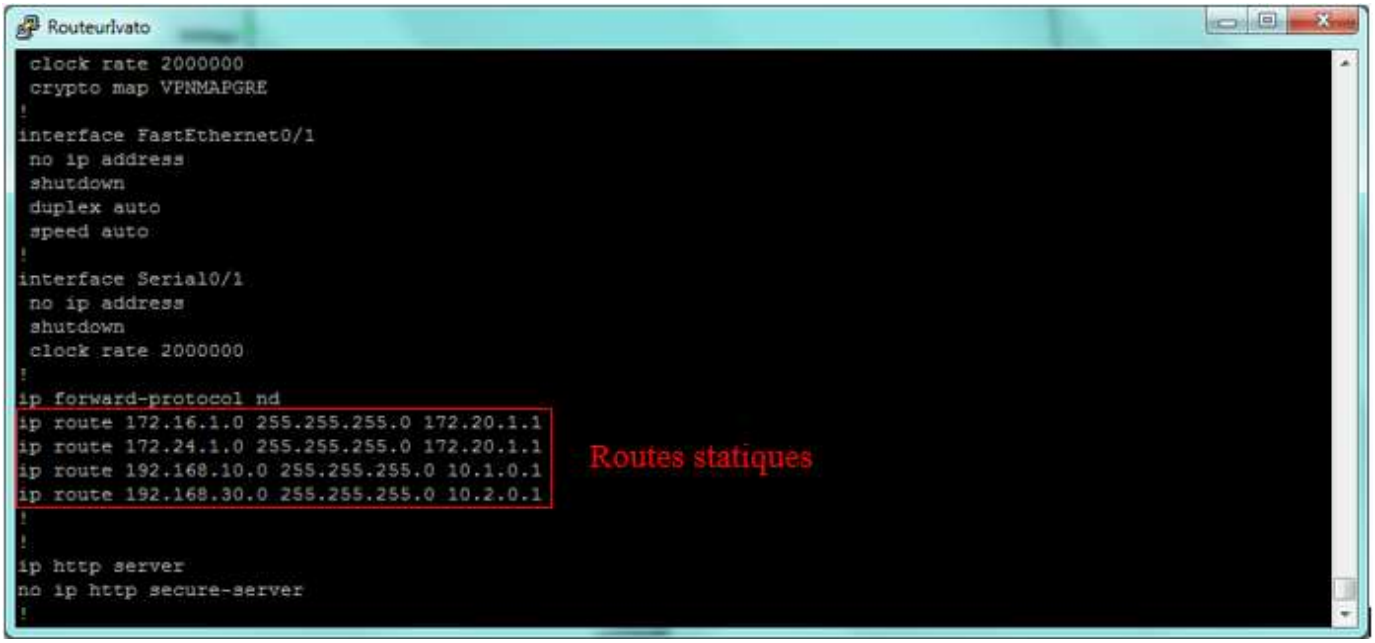

Figure 4.13 : *Routages statiques dans RouteurIvato*

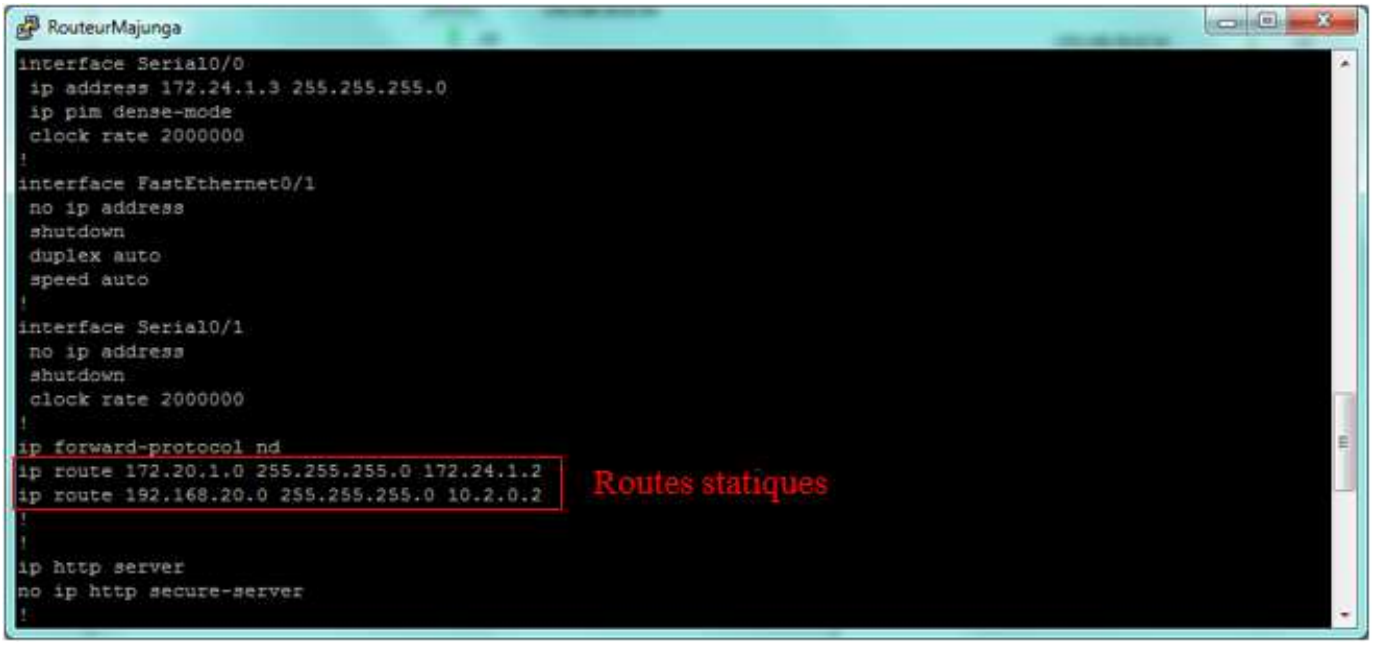

Figure 4.14 : *Routage statique dans Routeur Majunga*

Comme nous l'avons dit dans le chapitre 2 paragraphe 2.4.3.1, dans le réseau ADS-B existant actuellement dans la FIR d'Antananarivo les données de la station ADS-B d'Antsiranana sont reportées vers Ivato en unicast via le réseau AFISNET vers le PC convertisseur de trame unicast-multicast puis renvoyées par celui-ci en multicast vers le système TopSky. Mais cela a un grand inconvénient vu qu'il y a un traitement intermédiaire au niveau du PC convertisseur de trame unicast-multicast ce qui augmente le délai d'acheminement des données. Et en cas de

panne de ce PC les données n'arriveront jamais au niveau du serveur MEDISIS, d'où la rupture de la liaison ADS-B.

Nous proposons alors qu'à partir de toutes les stations que nous allons implanter, les données soient reportées en multicast vers Ivato. Ainsi dans la simulation sous GNS3 nous avons choisi de configurer dans tous les routeurs le protocole multicast PIM Dense mode.

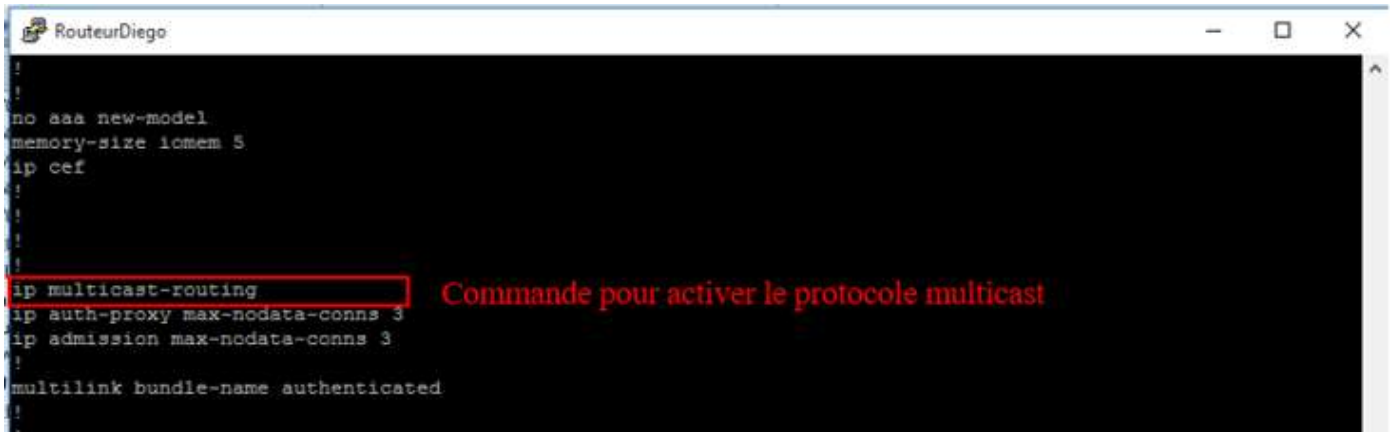

Figure 4.15 : *Activation du protocole multicast dans RouteurDiego*

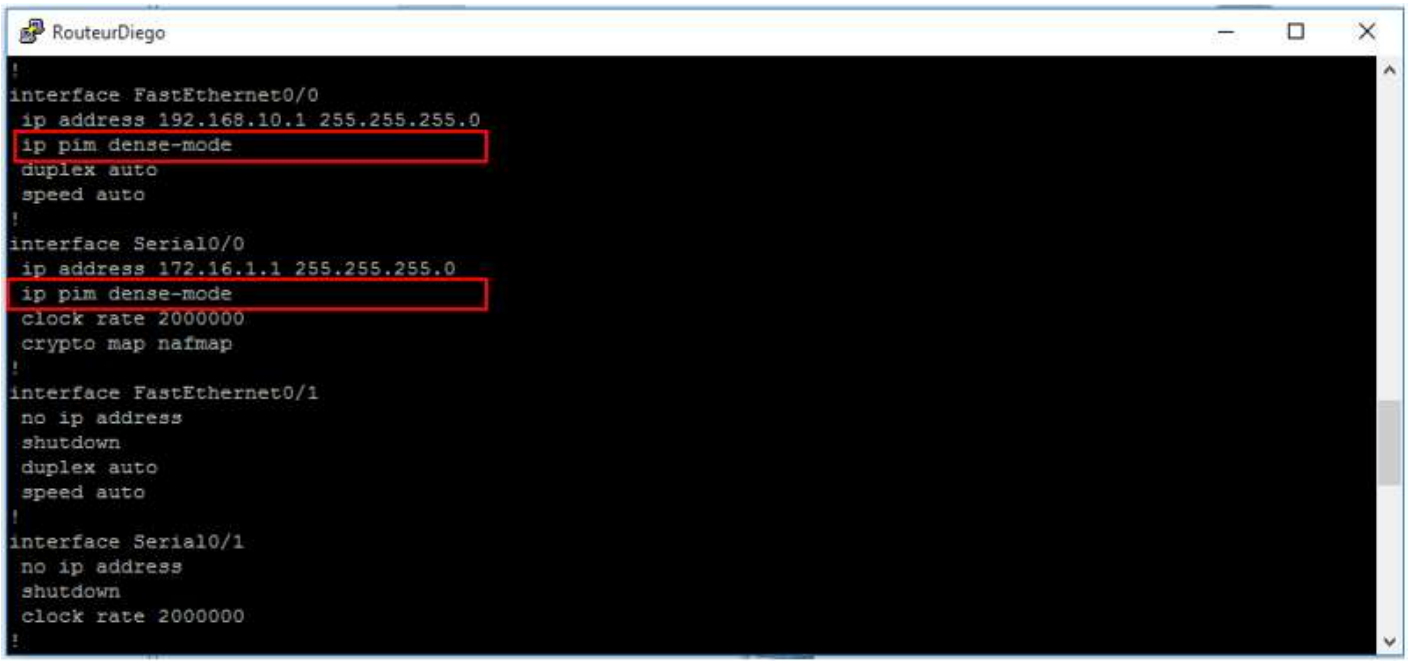

Figure 4.16 : *Configuration de PIM Dense Mode dans chaque interface du RouteurDiego*

On a configuré de la même manière le protocole multicast PIM Dense mode dans les routeurs RouteurIvato, FAI, et RouteurMajunga.

Afin de sécuriser les données acheminées vers le centre d'Ivato, nous avons créé des tunnels VPN à l'aide du protocole GRE et du protocole IPsec. L'étape suivante consiste donc à la

création des VPN entre RouteurDiego et RouteurIvato, puis entre RouteurMajunga et RouteurIvato. Le FAI devient ainsi transparent.

Tout d'abord nous avons créé des tunnels entre ces routeurs à l'aide du protocole GRE. Pour cela nous avons créé deux tunnels :

- Un tunnel entre RouteurDiego et RouteurIvato qu'on a nommé Tunnel10 : les adresses IP des deux interfaces de ce tunnel sont 10.1.0.1/24 et 10.1.0.2/24
- Un tunnel entre RouteurMajunga et RouteurIvato qu'on a nommé Tunnel20 : les adresses IP des deux interfaces de ce tunnel sont 10.2.0.1/24 et 10.2.0.2/24

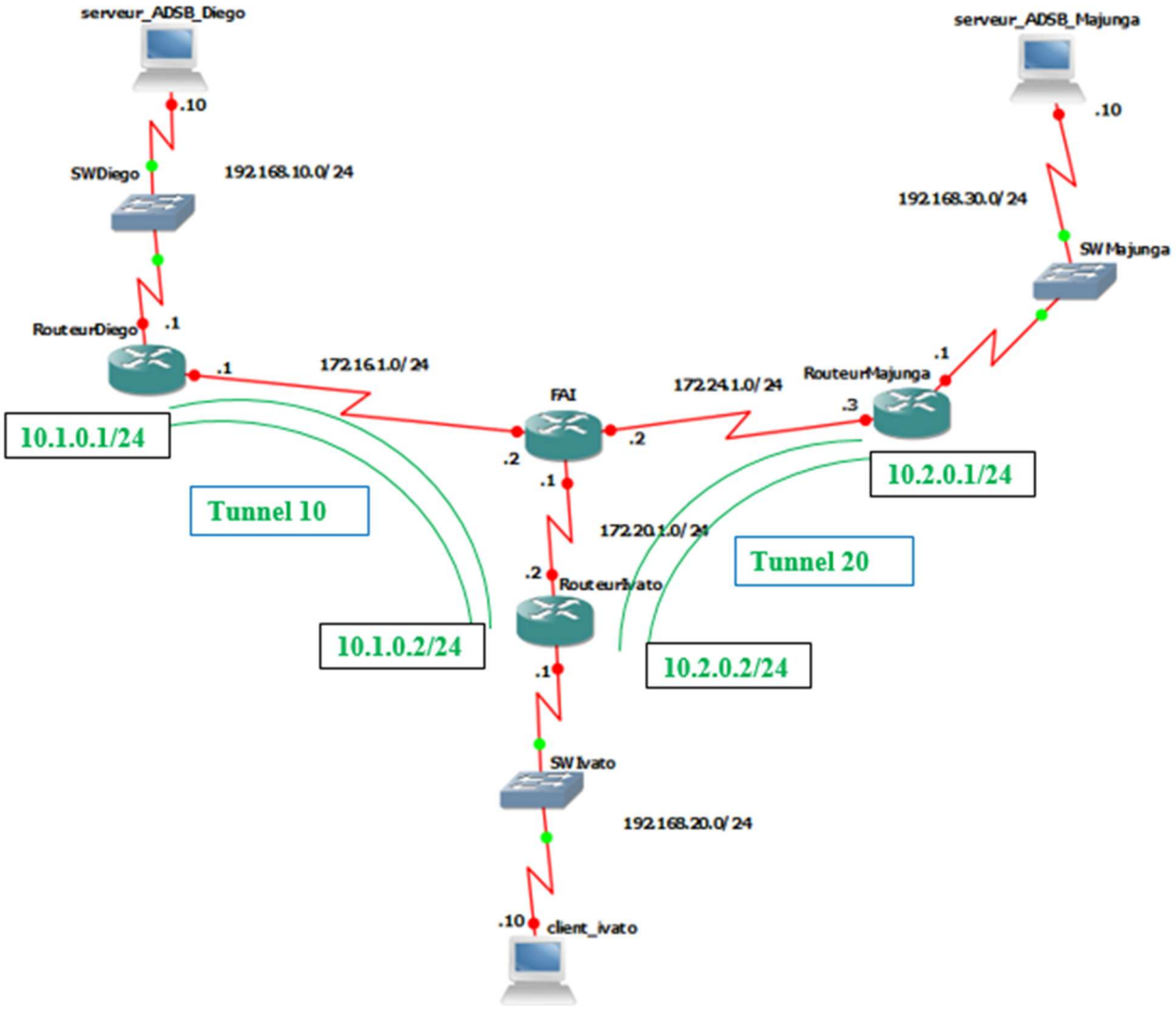

Figure 4.17 : *Topologie des tunnels VPN*

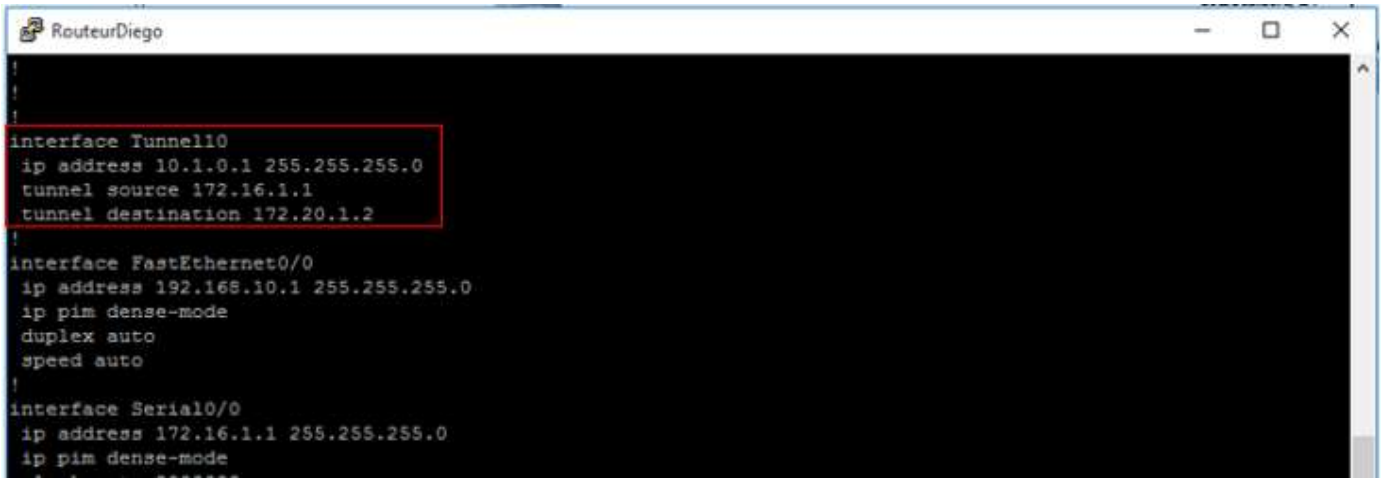

Figure 4.18 : *Création du Tunnel10 dans RouteurDiego*

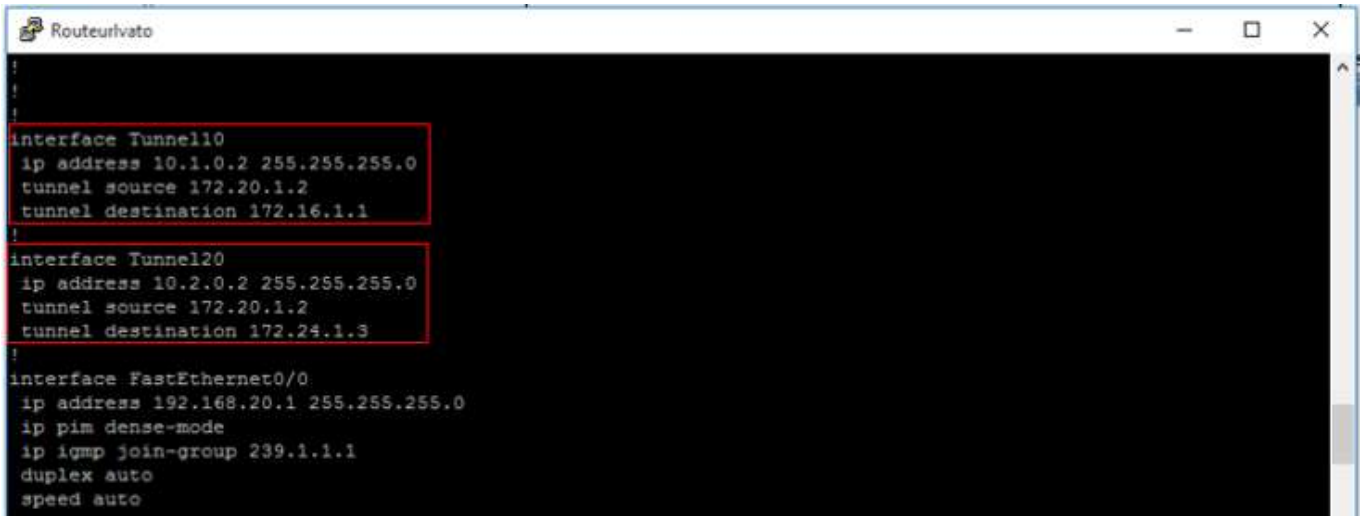

Figure 4.19 : *Création du Tunnel10 et Tunnel20 dans RouteurIvato*

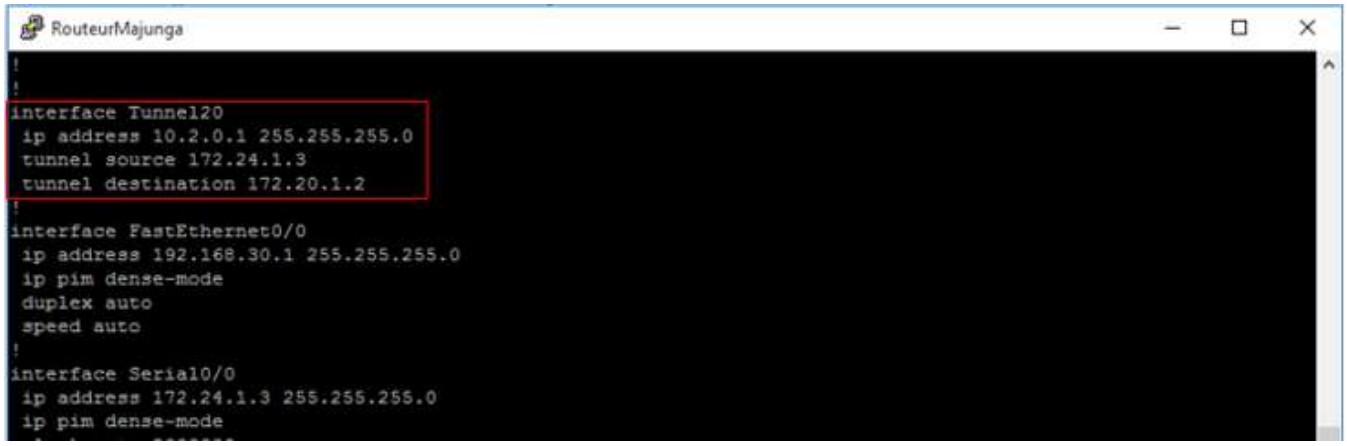

Figure 4.20 : *Création du Tunnel20 dans RouteurMajunga*

Après avoir créé les tunnels, les données qui y transitent ne sont pas encore sécurisés. Afin de fournir l'authentification et la confidentialité des données, nous avons utilisé le protocole IPsec. Pour montrer les configurations que nous avons fait, nous allons prendre le cas du RouteurDiego. Celles des RouteurIvato et RouteurMajunga se feront de la même manière.

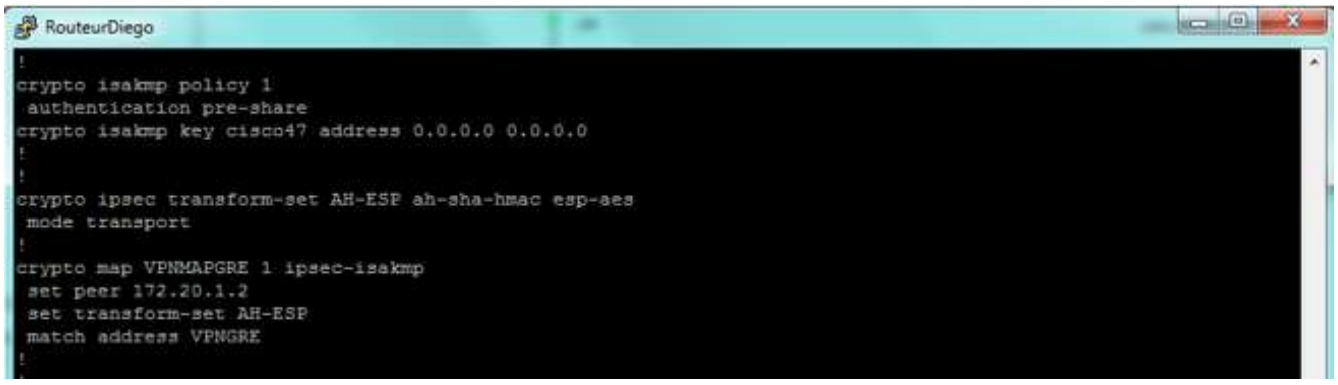

Figure 4.21 : *Configuration IPsec dans RouteurDiego*

Figure 4.22 : *Configuration IPsec dans RouteurDiego (suite)*

Figure 4.23 : *Configuration IPsec dans RouteurDiego (suite)*

Toutes les configurations sont à présent terminées. Nous allons maintenant lancer la simulation en diffusant des flux vidéo à l'aide de VLC.

4.4.4 *Lancement de la simulation*

Rappelons que l'ADS-B est un système qui utilise la transmission multicast. Ainsi afin de simuler le multicasting nous allons diffuser des flux vidéo, à l'aide du logiciel VLC, dans les

deux machines virtuelles qui représentent les serveurs de la station ADS-B Diégo et celle de Majunga. Ensuite nous allons observer l'arrivée des données au niveau du client Ivato toujours en utilisant VLC.

Voici les différentes étapes à suivre pour diffuser un flux vidéo sur VLC (côté serveur) :

- Lancer le logiciel VLC
- Aller dans « Média » et cliquer sur « Ouvrir un flux réseau »
- Aller dans « Fichier », puis ajouter la vidéo à diffuser. Sur la liste déroulante du bouton « Lire », cliquer sur « Diffuser »
- Cliquer sur le bouton « Suivant »
- Dans la fenêtre qui s'ouvre, choisir « RTP/MPEG Transport Stream » puis cliquer sur « Ajouter »
- Saisir l'adresse du groupe multicast, dans notre cas c'est **239.1.1.1**, le port de base (**5004**), et un nom (exemple : fluxDiego)
- Choisir comme profil « Video for Android SD Low)
- Cocher la case « Diffuser tous les flux élémentaires »
- Dans l'accolade, mettre à la fin une valeur de ttl. Choisir une grande valeur pour être sûr que nos paquets arrivent à destination (exemple : ttl=20)
- Enfin cliquer sur flux

Dans le client Ivato, on lance le logiciel VLC, et on suit les étapes suivantes pour recevoir la vidéo provenant des serveurs :

- Aller dans « Média » et cliquer sur « Ouvrir un flux réseau »
- Aller dans « Réseau », et entrer une URL réseau sous la forme suivante : rtp://@230.1.1.1:5004
- Cliquer sur « Lire »

4.4.5 *Résultats et interprétations*

Une fois les vidéos diffusées, nous allons maintenant montrer à l'aide de quelques commandes et du logiciel Wireshark que les différents protocoles que nous avons configurés plus haut ont bien été appliqué à notre réseau.

- #**show ip route** : Cette commande permet d'afficher la table de routage du routeur. Sur les images suivantes nous pouvons voir les routes empruntées par les paquets pour aller d'un nœud à un autre nœud du réseau.

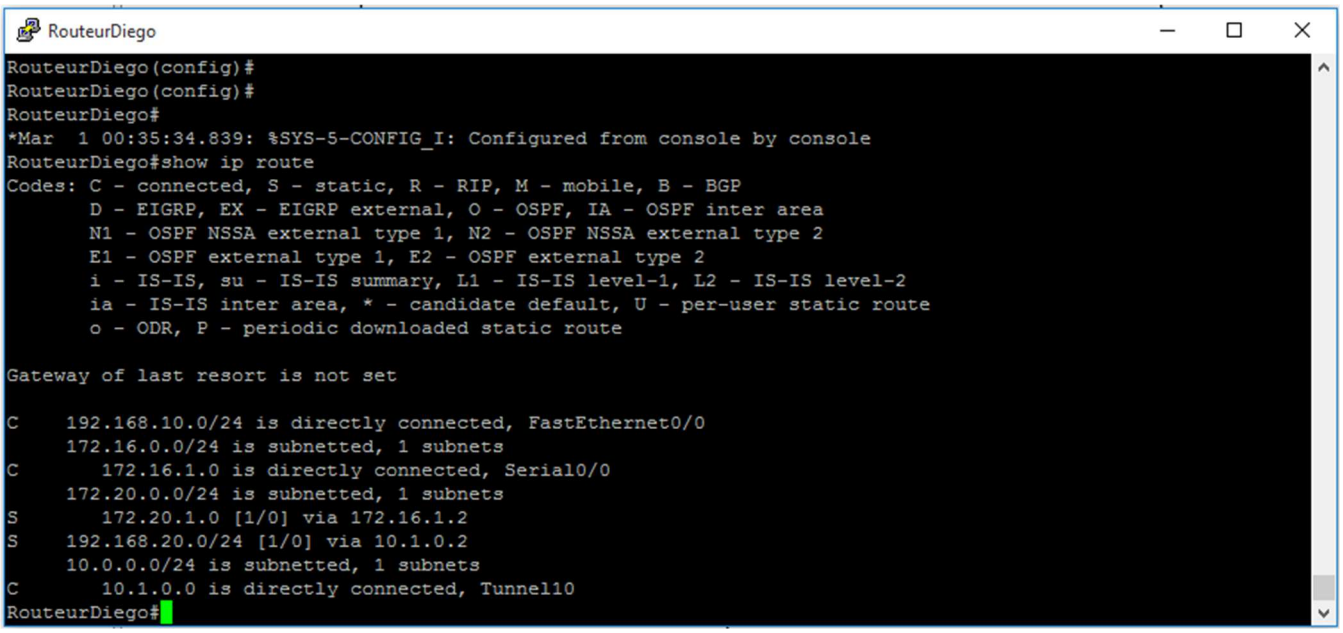

Figure 4.24 : *Table de routage dans RouteurDiego*

La route que nous venons de rajouter pour joindre le réseau 192.168.20.0/24 se fait via l'interface 10.1.0.2 du tunnel10.

Ici, nous n'avons pas besoin de rajouter la route pour joindre le réseau 192.168.10.0/24 puisque le routeur à une interface réseau directement connecté à ce réseau. Il "connaît" donc la route à prendre pour joindre 192.168.10.0/24.

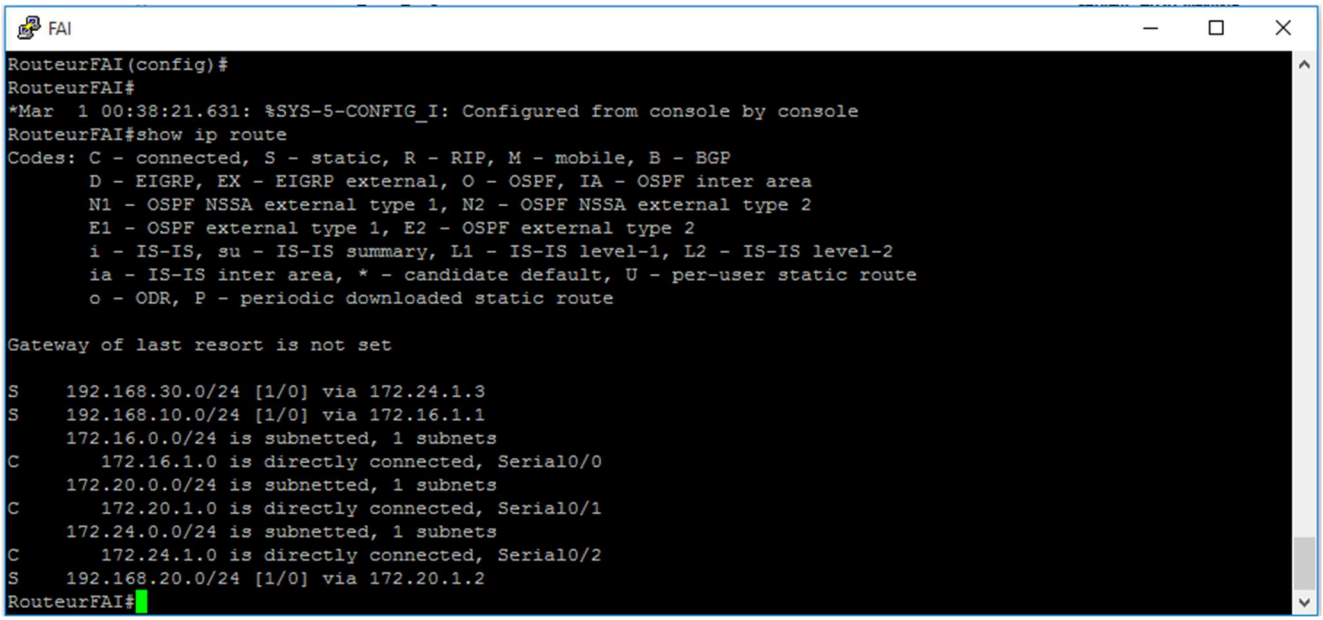

Figure 4.25 : *Table de routage dans RouteurFAI*

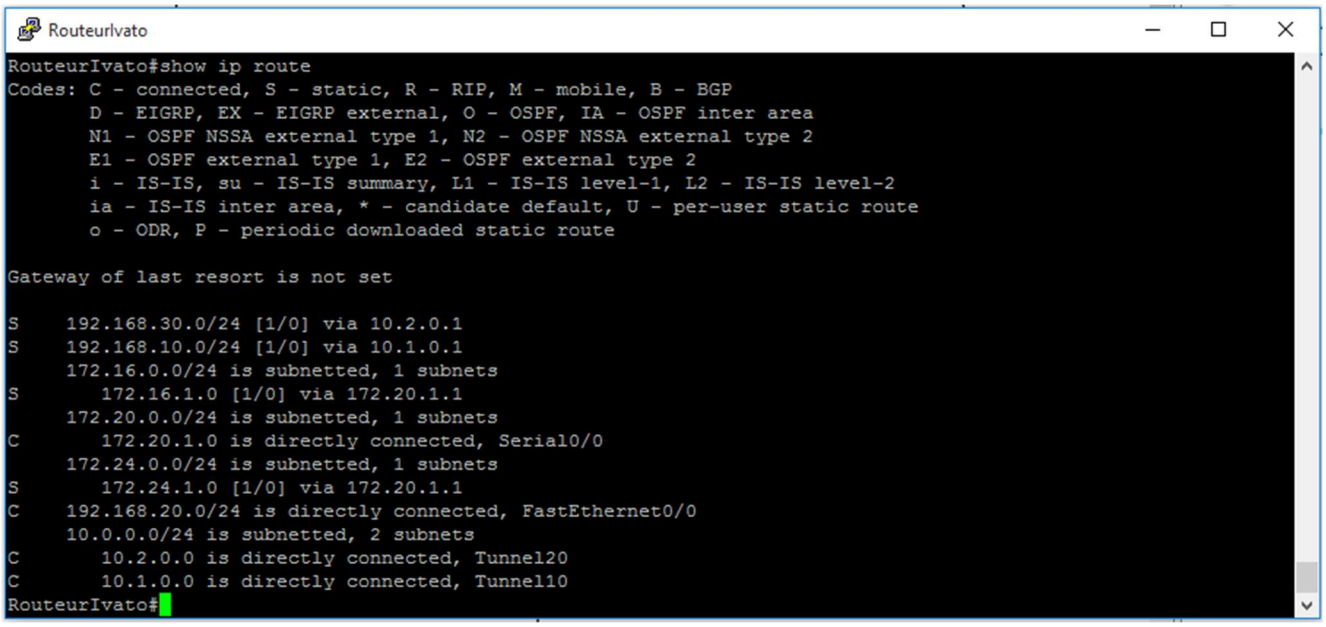

Figure 4.26 : *Table de routage dans RouteurIvato*

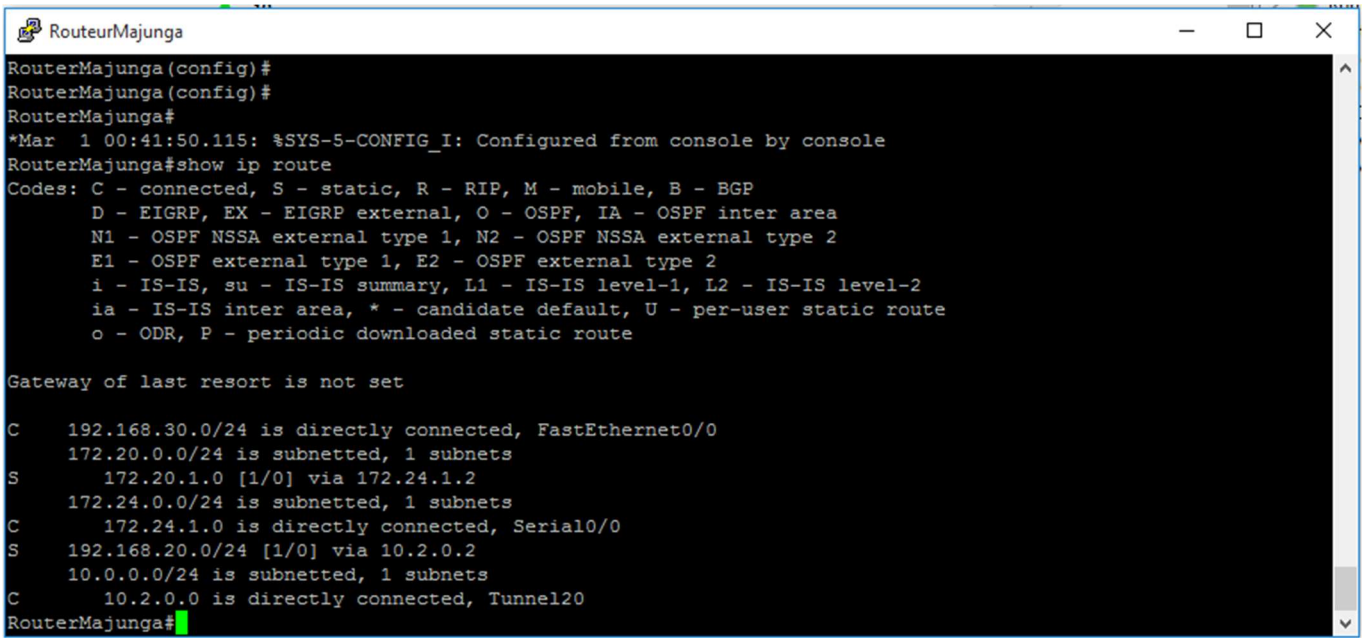

Figure 4.27 : *Table de routage dans RouteurMajunga*

- #**traceroute** 192.168.20.10 : Cette commande permet de déterminer le chemin suivi par les paquets pour arriver au client Ivato. Nous verrons qu'effectivement les paquets passent par le tunnel10 via l'interface 10.1.0.2 pour les paquets venant du serveur ADS-B Diego, et par le tunnel20 via l'interface 10.2.0.2 pour les paquets venant du serveur ADS-B Majunga.

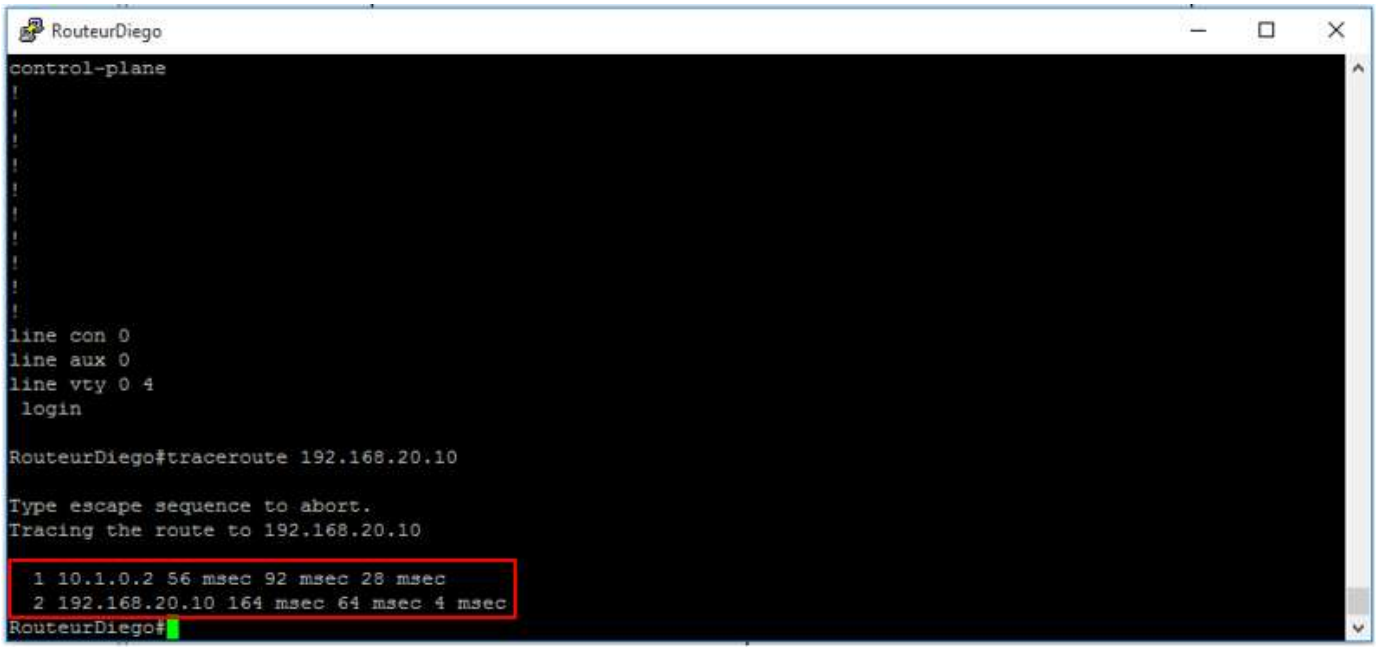

Figure 4.28 : *Chemin suivi par les paquets à partir du serveur ADS-B Diego vers Ivato*

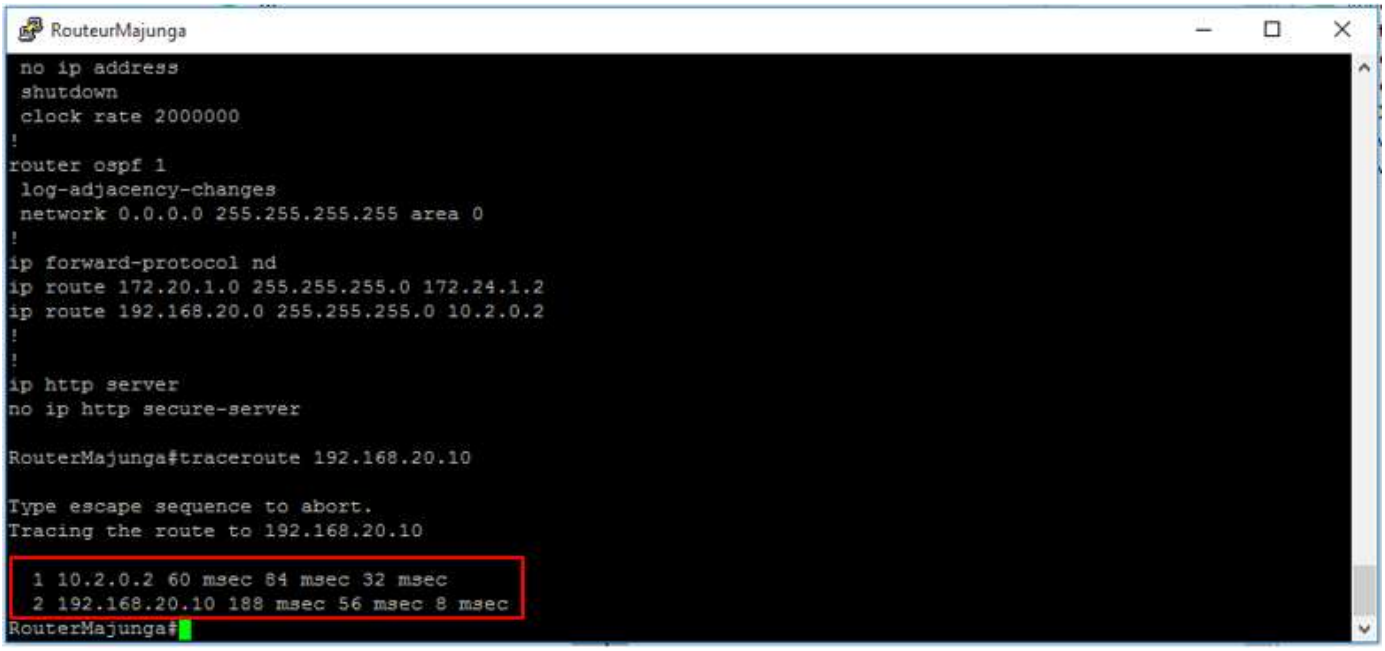

Figure 4.29 : *Chemin suivi par les paquets à partir du serveur ADS-B Majunga vers Ivato*

Vérifions maintenant les opérartions d'IPsec :

- **#show crypto session :** cette commande permet d'afficher les informations d'état des sessions de cryptage actives. Elle nous donnera une liste rapide de toutes les sessions IKE et IPSec SA.

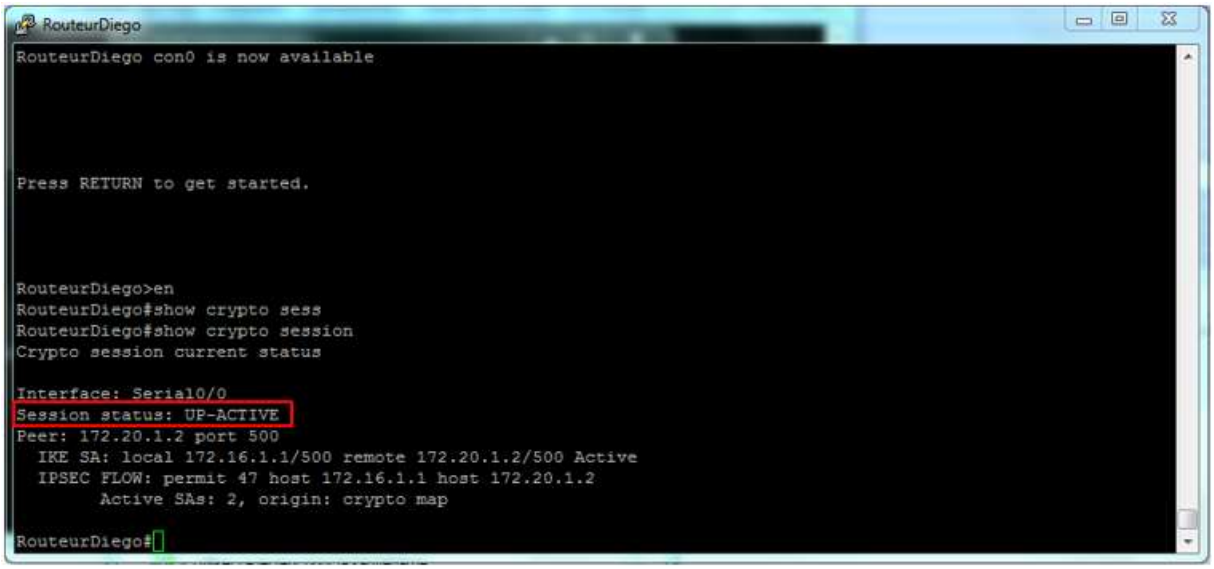

Figure 4.30 : *Statut IPsec dans RouteurDiego*

Session status : UP-ACTIVE veut dire que IPSec SA est actif / activé et transfère des données

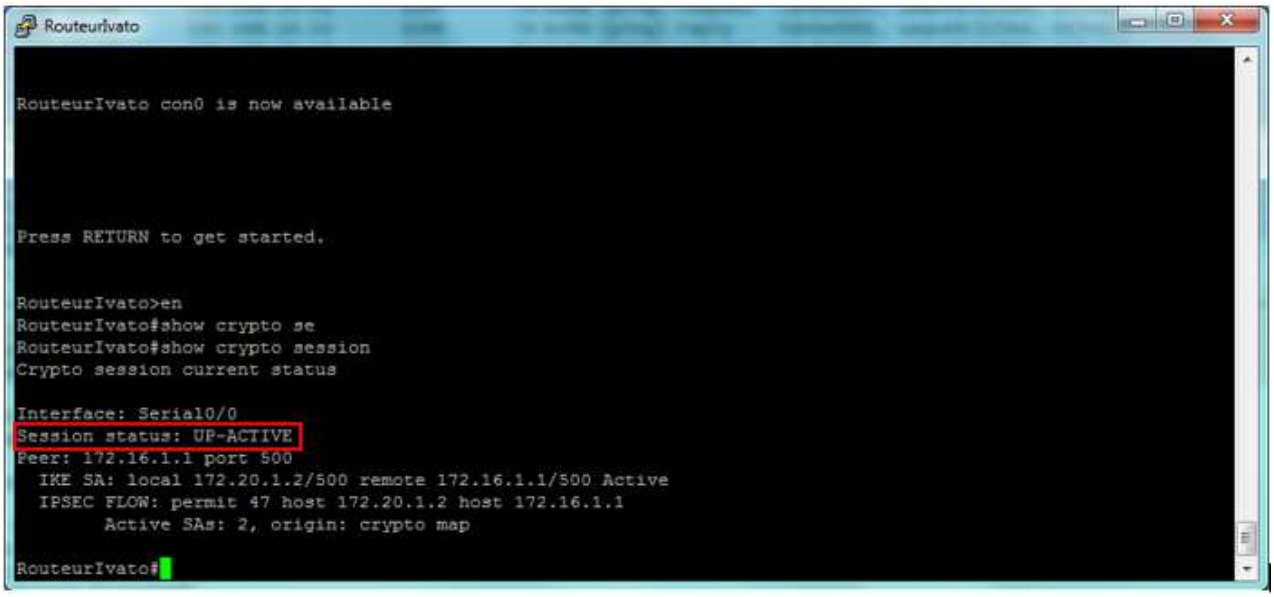

Figure 4.31 : *Statut IPsec dans RouteurIvato*

- # **show crypto isakmp sa :** Cette commande nous indiquera l'état de nos négociations. Dans les figures suivantes nous pouvons voir que le protocole isakmp est activé, et son état au moment où on a tapé la commande est « QM_IDLE », ce qui signifie qu'il n'y a pas de trafic qui transite mais il est authentifié.

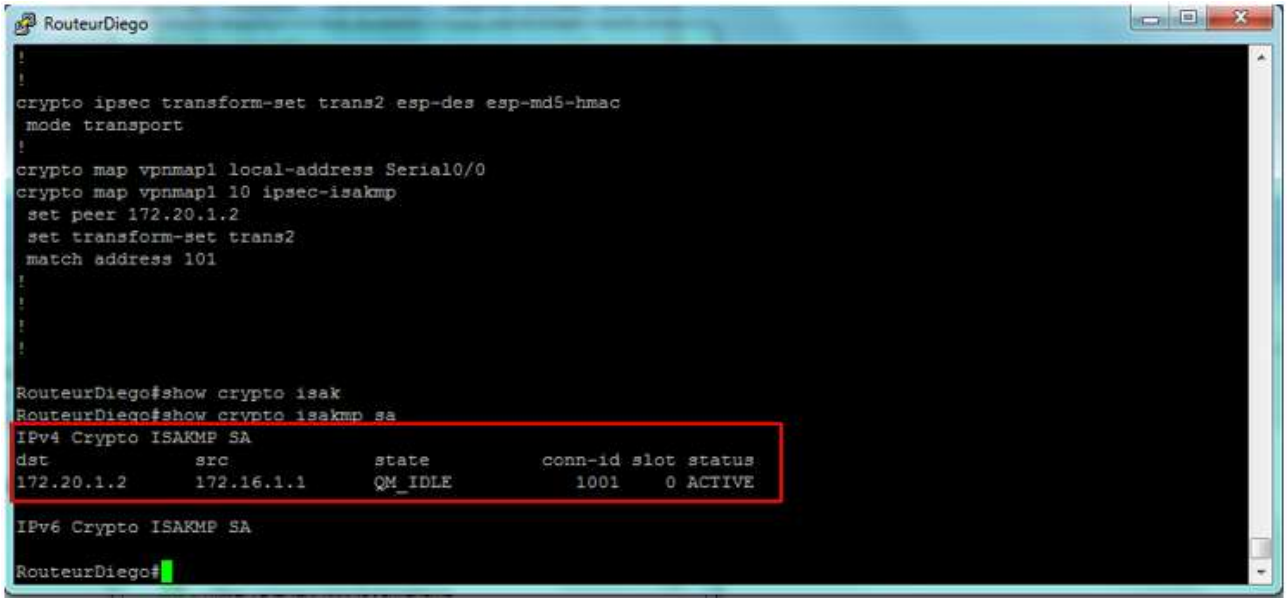

Figure 4.32 : *Protocole isakmp dans RouteurDiego*

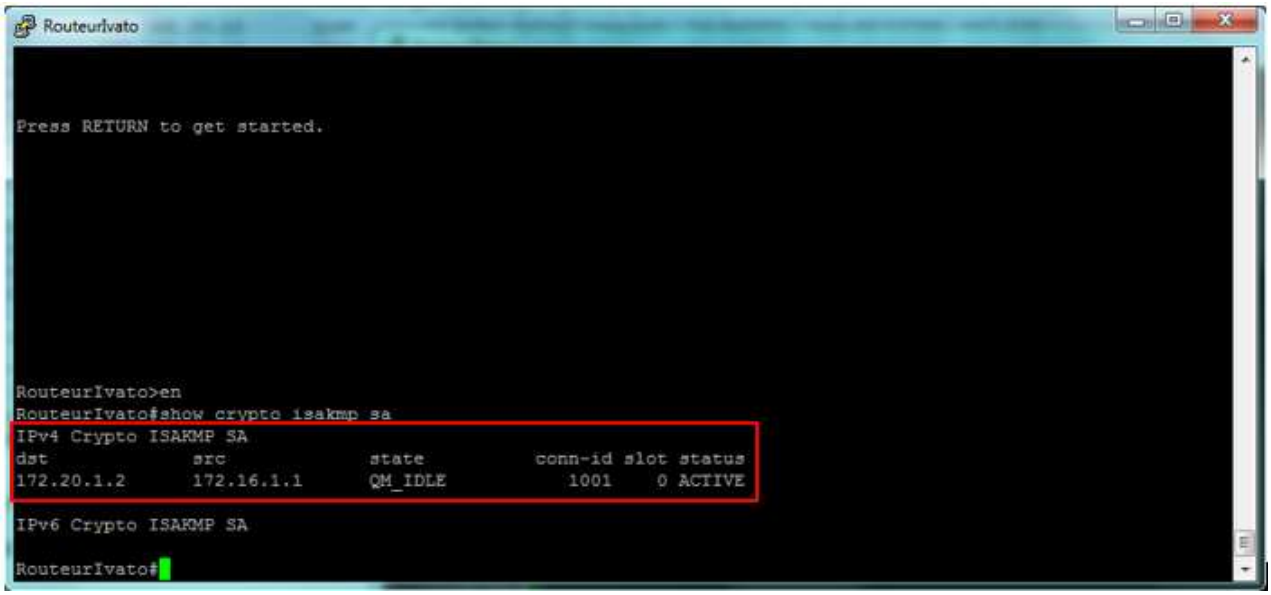

Figure 4.33 : *Protocole isakmp dans RouteurIvato*

- **#show crypto ipsec sa :** Cette commande nous permet de vérifier quelques éléments clefs comme les #pkts encaps / encrypt / decap / decrypt, ces nombres nous indiquent combien de paquets ont réellement traversé le tunnel IPSec et vérifient également que nous recevons du trafic à partir de l'extrémité distante du tunnel VPN. Cela nous indiquera également le SPI local et distant, transform-set, et le mode tunnel pour IPSec SA.

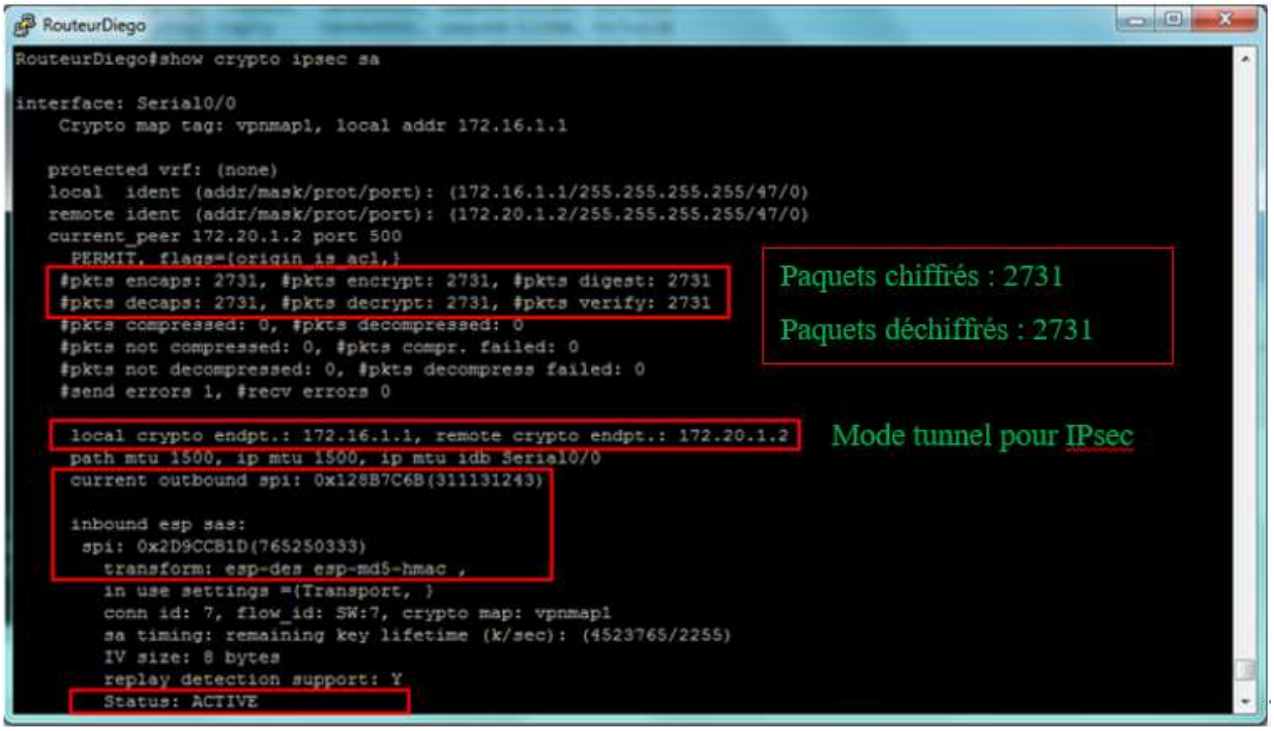

Figure 4.34 : *Vérifications de quelques éléments clefs de IPsec dans RouteurDiego*

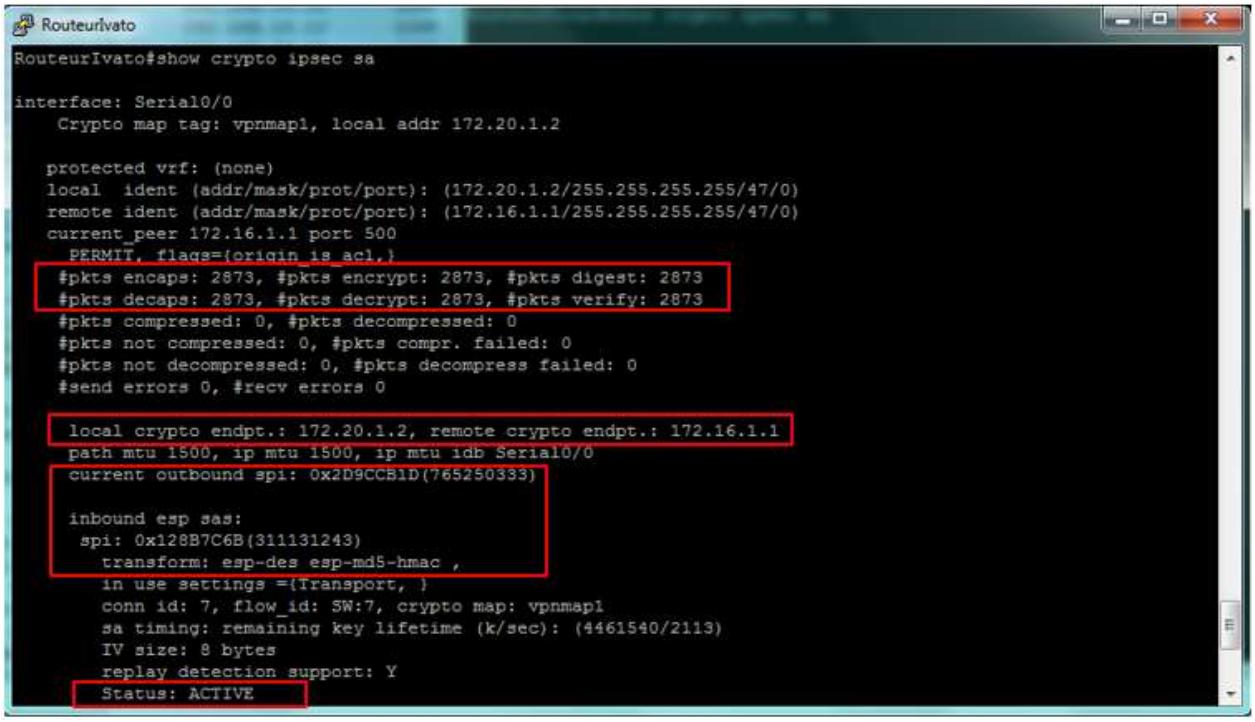

Figure 4.35 : *Vérifications de quelques éléments clefs de IPsec dans RouteurIvato*

- **Capture à l'aide du logiciel Wireshark**

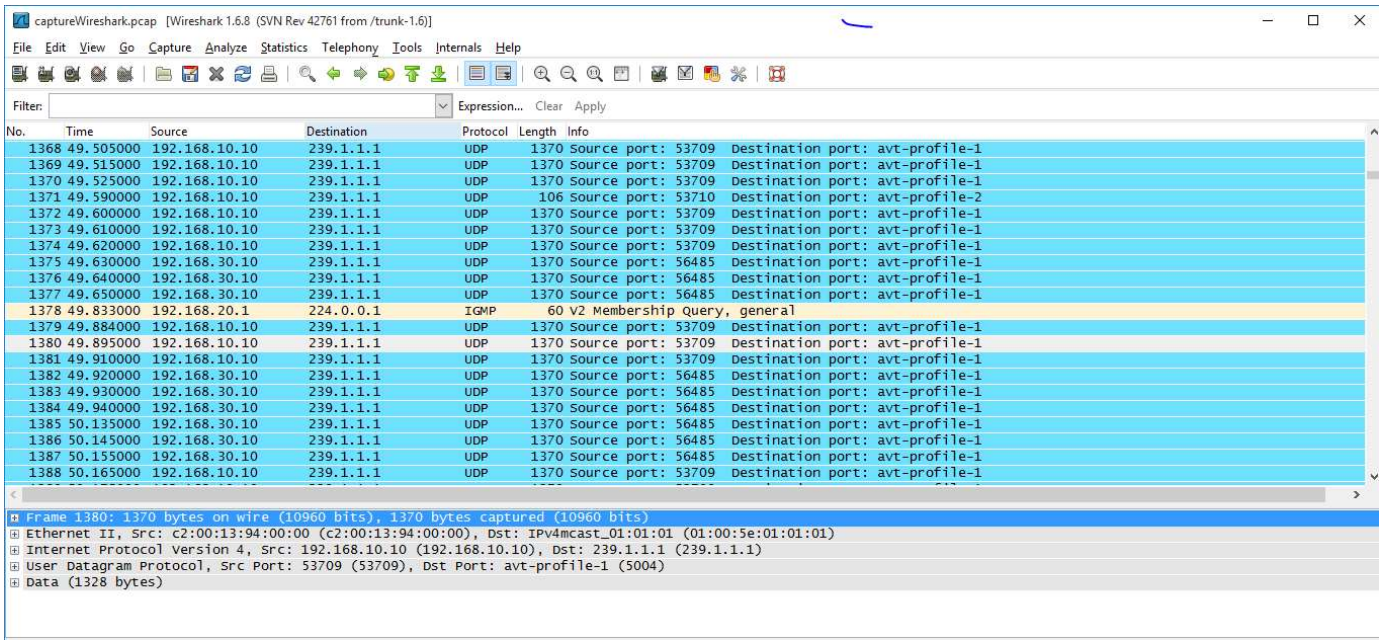

Figure 4.36 : *Capture des données Wireshark*

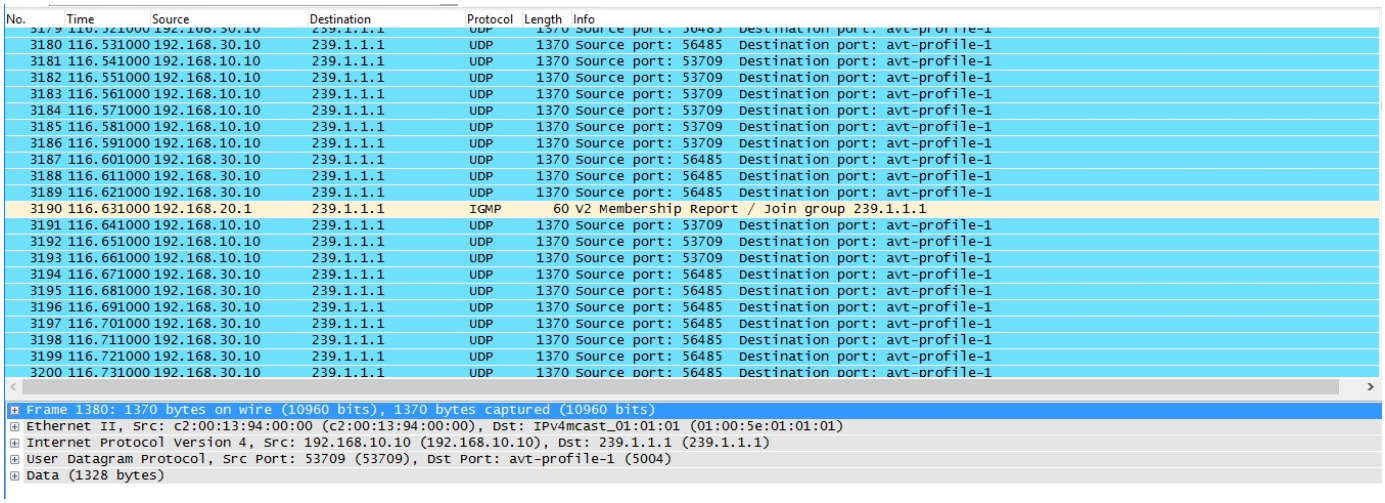

Figure 4.37 : *Capture wireshark (suite)*

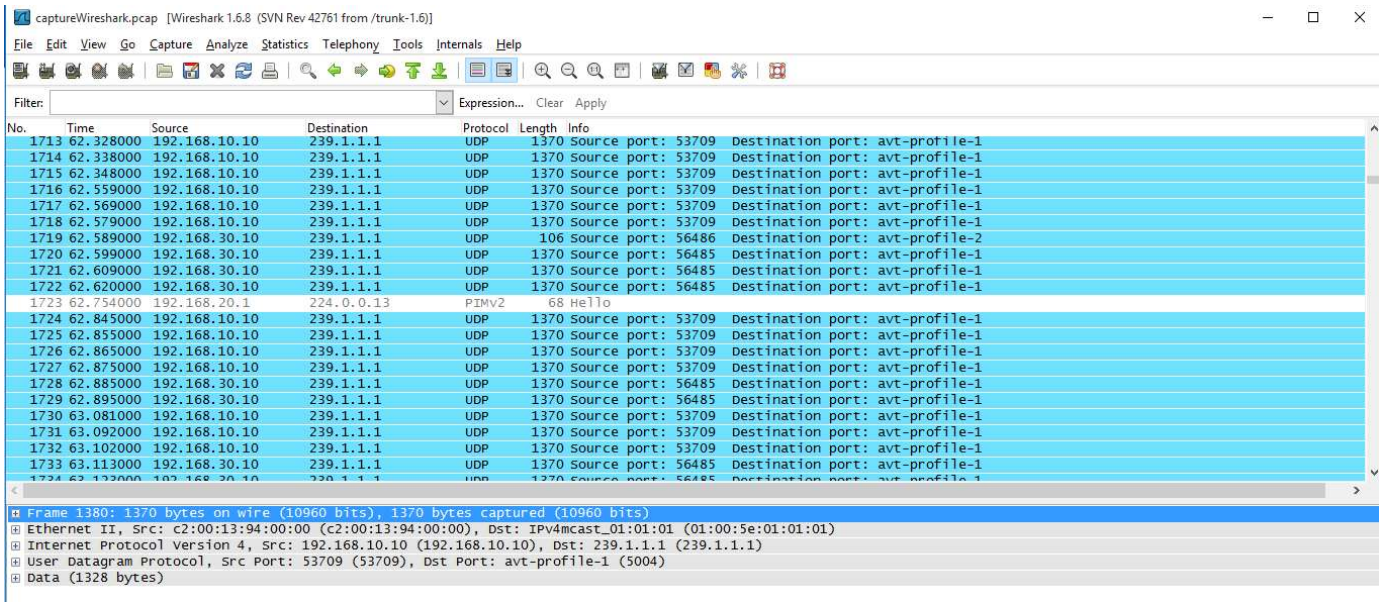

Figure 4.38 : *Capture Wireshark (suite)*

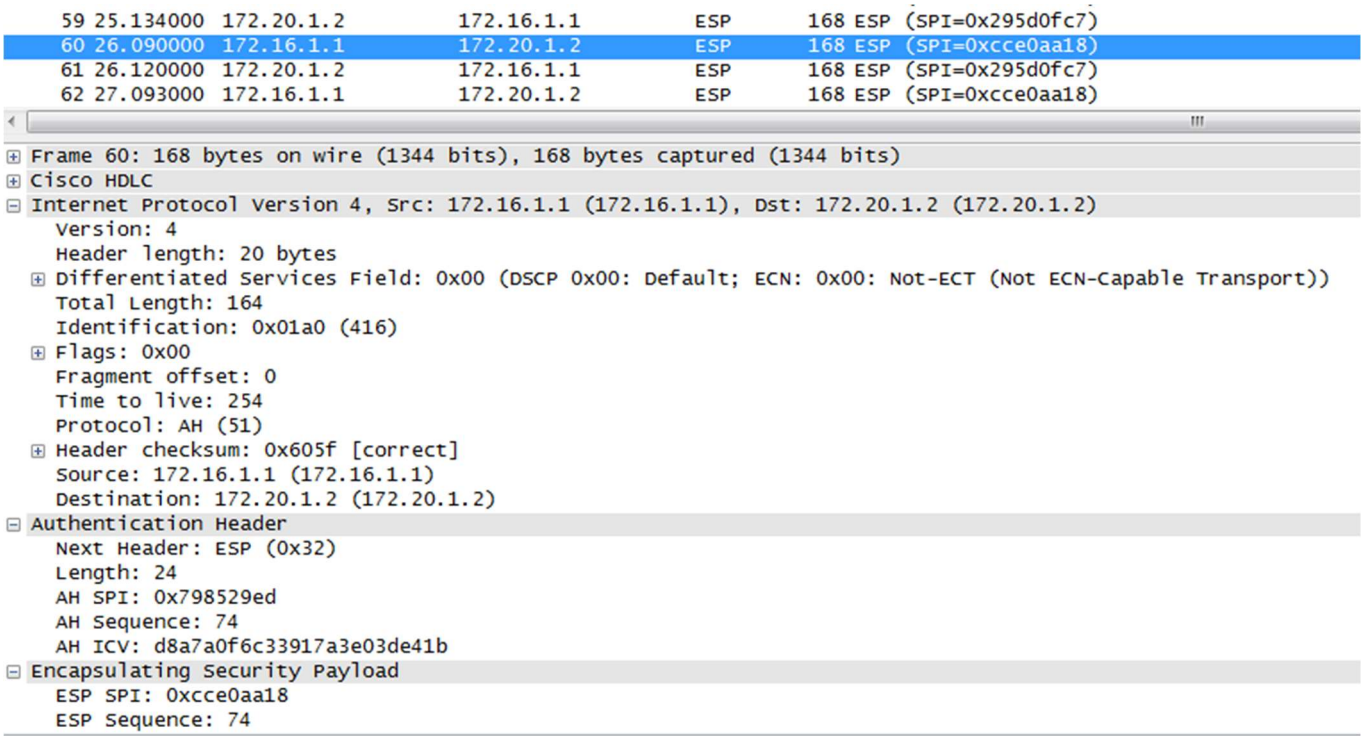

Figure 4.39 : *Capture Wireshark (suite)*

Dans ces captures, nous pouvons voir que :

- Les machines serveur ADS-B Diego et serveur ADS-B Majunga ayant pour adresse IP respective 192.168.10.10 et 192.168.30.10 envoient des paquets au groupe multicast 239.1.1.1. Bien sur le protocole de transport utilisé est UDP vu qu'en est en transmission multicast.

- Protocole IGMP (figure 4.32) : Le message est une requête d'adhésion. Le RouteurIvato ayant une interface 192.168.20.1 interroge périodiquement les machines du sous-réseau pour savoir s'il y a des machines appartenant encore à des groupes multicast. Cette interrogation se fait sur l'adresse multicast 224.0.0.1 (tous les hôtes).
- Protocole IGMP (figure 4.33) : Le message utilisant ce protocole est un rapport d'adhésion lorsque le client Ivato appartenant au sous-réseau 192.168.20.0/24 a rejoint le groupe multicast 239.1.1.1.
- Les routeurs PIM envoient régulièrement des messages de salutation afin de découvrir les routeurs PIM voisins. Les messages de salutation sont des multidiffusions utilisant l'adresse 224.0.0.13. Dans l'exemple de capture ci-dessus c'est le RouteurIvato (192.168.20.1) qui envoie des « Hello paquet » sur l'adresse 224.0.0.13
- Le protocole AH pour l'authentification et ESP qui crypte les données

4.5 **Conclusion**

A l'aide du logiciel GNS3 nous avons pu simuler notre réseau et appliquer les différents protocoles de routage multicast (PIM dense mode, IGMP) et de tunneling (GRE, IPsec). Nous avons pu observer que les données transitent bien dans les tunnels, et qu'ils arrivent en temps réel au niveau du centre Ivato.

CONCLUSION GENERALE

L'ADS-B est un moyen de surveillance où les aéronefs diffusent leurs positions, calculées à partir du GPS de bord ou des moyens inertiels, vers des stations implantées au sol ou les aéronefs au voisinage qui y sont équipés, en utilisant le 1090 MHz Extended Squitter comme support de transmission dans l'aviation internationale. Les plages de couverture des stations sol peuvent aller jusqu'à 250 NM.

Parmi les trois moyens de surveillance existant dans la FIR d'Antananarivo l'ADS-B est celui qui présente beaucoup plus d'avantages tant en termes de cout qu'en terme de précision. Ainsi il s'avère intéressent d'augmenter le nombre de station ADS-B dans cette FIR, ce afin d'effectuer le couplage de plots (Radar et ADS-C) pour améliorer la couverture et la précision pour une meilleur sécurité de la circulation aérienne.

L'ASECNA ayant placé plusieurs stations VHF déportées dans des zones stratégiques où le trafic est le plus dense, nous avons trouvé intéressant de choisir ces emplacements pour co-implanter des stations ADS-B sol. Ces zones sont les régions d'Antalaha, Antsiranana, Maintirano, Mananjary, Mahajanga, Toamasina, Tolagnaro, Toliary, et Moroni. L'acheminement des données vers le centre Ivato, qui est le Hub du réseau, se fera en multicast à l'aide du protocole PIM Dense mode, via VSAT ou internet. Et afin de sécuriser les données qui transitent dans le réseau nous avons créé des tunnels GRE et appliqué le protocole IPsec.

La simulation sous le logiciel GNS3 nous a permis de mettre en évidence tous ces protocoles.

En somme, vu l'accroissement du trafic aérien régional, la densification de la couverture ADS-B dans la FIR d'Antananarivo serait un grand atout pour l'ASECNA dans la zone de l'océan Indien afin de relever d'avantage le niveau de sécurité aux usagers.

ANNEXE : PRESENTATION DE L'ASECNA

A.1 Présentation

A.1.1 Identification

L'ASECNA ou Agence pour la SECurité de la Navigation Aérienne en Afrique et à Madagascar est un établissement public multinational doté de la personnalité morale et jouissant de l'autonomie financière. Créée par une convention signée à St. Louis du Sénégal le 12 Décembre 1959, c'est un ANSP (Air Navigation Service Provider) ou fournisseur de services de navigation aérienne.

A.1.2 Siège

Direction Générale de l'ASECNA	Représentation de l'ASECNA à Madagascar
32-38, Avenue Jean Jaurès, au Sénégal Boîte Postale : 3144 Dakar Sénégal Téléphones : 23 10 40/ 23 93 30/ 23 95 70 Fax: 23 46 54, site web: www.asecna.org **Directeur général :** Mr **Amadou Ousmane GUITTEYE**	Ivato Aéroport, Antananarivo 105 Boîte Postale : 46 Téléphones : 22 581 13 / 22 581 14 Fax : 22 581 15 **Représentant :** Mr **RAMANANANDRO Désiré**

Tableau A.01 : Siège de l'ASECNA

Figure A.01 : *Représentation de l'ASECNA à Madagascar (Ivato aéroport)*

(A gauche : Bloc technique (BT) avec la tour de contrôle ; à droite : Station Terrienne (ST))

A.1.3 Etats membres

L'ASECNA est actuellement composée de 18 Etats membres, dont : Bénin, Burkina Faso, Cameroun, Centrafrique, Comores, Congo, Côte d'Ivoire, France, Gabon, Guinée Bissau, Guinée équatoriale, Madagascar, Mali, Mauritanie, Niger, Sénégal, Tchad et Togo.

A.1.4 Ressources financières

Les principales ressources de l'agence proviennent des redevances d'atterrissages, de balisages, d'aides en route, des passagers, et d'autres prestations diverses, comme la calibration en vol ou les revenus de location d'immeuble et de parking.

A.2 Historique

L'ASECNA fut créée le 12 Décembre 1959 à Saint-Louis (Sénégal) par des Chefs d'Etat et de Gouvernement des Etats autonomes issus des ex-Fédérations de l'AEF, l'AOF et de Madagascar.

Elle constitue l'un des meilleurs exemples de coopération Nord-Sud ainsi que l'organe de l'unité africaine par excellence en matière d'aviation civile. Même si au début, la base était une coopération franco-africaine et malgache, elle est maintenant devenue une coopération interafricaine et malgache. Cette transformation a aidé à africaniser le poste de Directeur Général et des postes de Directeurs depuis 1974.

Voici quelque Evolution de l'ASECNA :

- Au début de 1960 : entrée en vigueur des activités.
- 25 Octobre 1974 : Signature d'une nouvelle convention concernant son statut et son organisation. Le siège a été transféré de Paris à Dakar. L'Africanisation du poste de Directeur Général et des postes des Directeurs de divers départements.
- 22 Avril 1987 : Adhésion de la République de Guinée Equatoriale à l'ASECNA.
- 1990 : Affectation d'un Délégué permanant de l'ASECNA au siège de l'Organisation de l'Aviation Civile Internationale (OACI) Canada (Montréal).
- 2005 : Mise en service des avions à réaction, puis des avions gros porteurs B.747
- 2005 : Mise en place de la Délégation de l'ASECNA Paris. Les raisons de cette ouverture sont les suivantes :
    - Pour assurer la liaison avec : les administrations aéronautiques et

météorologiques, les organisations internationales, les compagnies aériennes.

- Pour le recouvrement des redevances de route
- Pour l'édition des informations aéronautiques
- Pour l'achat et l'acheminement des matériels pour les Représentations et le Siège à Dakar.

- 12 Décembre 2009 : Célébration des 50 ans de service de l'agence
- 28 avril 2010 : La Convention de Dakar devient la « Convention de Dakar révisé adopter à Ouagadougou, au Burkina Faso, signé à Libreville en République Gabonaise ».

A.3 Activités de l'ASECNA

A.3.1 Missions de l'ASECNA

La principale mission de l'Agence est la gestion des espaces aériens de ses Etats membres et ceux pour lesquels ces Etats ont été chargés de fournir les services de circulation aérienne et de météorologie aéronautique. Soit une superficie totale de 16,12 millions de km², c'est-à-dire 1.5 fois la superficie de l'Europe.

Mais plus concrètement, il a été confié à l'ASECNA la conception, la réalisation et la gestion, aussi bien pour la circulation en route que pour l'approche et l'atterrissage, des installations et services ayant pour objet :

- La transmission des messages techniques et de trafic
- Le guidage des aéronefs
- Le contrôle de la circulation aérienne
- L'information des aéronefs en vol
- La prévision et la transmission des informations dans le domaine météorologique
- L'informatisation de ses systèmes d'information et de gestion
- Les aides terminales sur les 27 aéroports principaux des 17 Etats africains et malgache membres, à travers :
    - le contrôle d'aérodrome,
    - le contrôle d'approche,
    - le guidage du roulement des aéronefs au sol,

- l'aide radio et visuelle à l'approche et à l'atterrissage,
- les transmissions radio, les prévisions météorologiques,
- le bureau de piste et d'information aéronautique,
- les services de sécurité incendie (pompier),
- la maintenance de l'ensemble des installations nécessaires à la mise en œuvre de ces différentes prestations.

A.3.2 Aérodromes assurés par l'Agence dans les états membres

Voici les 27 aérodromes où l'agence assure ses missions :

Douala, Port-Gentil, Mahajanga, Garoua, Malabo, Bamako, Bangui, Ouagadougou, Gao, Brazzaville, Bobo-Dioulasso, Niamey, Point Noire, Nouakchott, Dakar, Abidjan, Nouadhibou, N'Djamena, Cotonou, Toamasina, Sarh, Libreville, Ivato Antananarivo, Lomé, Moroni, Yaoundé, Mopti.

A.3.3 FIR (Flight Information Region) gérées par l'ASECNA

L'espace aérien ASECNA est regroupé en six (06) Régions d'Information de Vol ou FIR : Antananarivo, Brazzaville, Dakar Océanique, Dakar Terrestre, Ndjamena et Niamey.

La carte de la Figure A1.02 illustre en couleur orange l'emplacement de celles-ci.

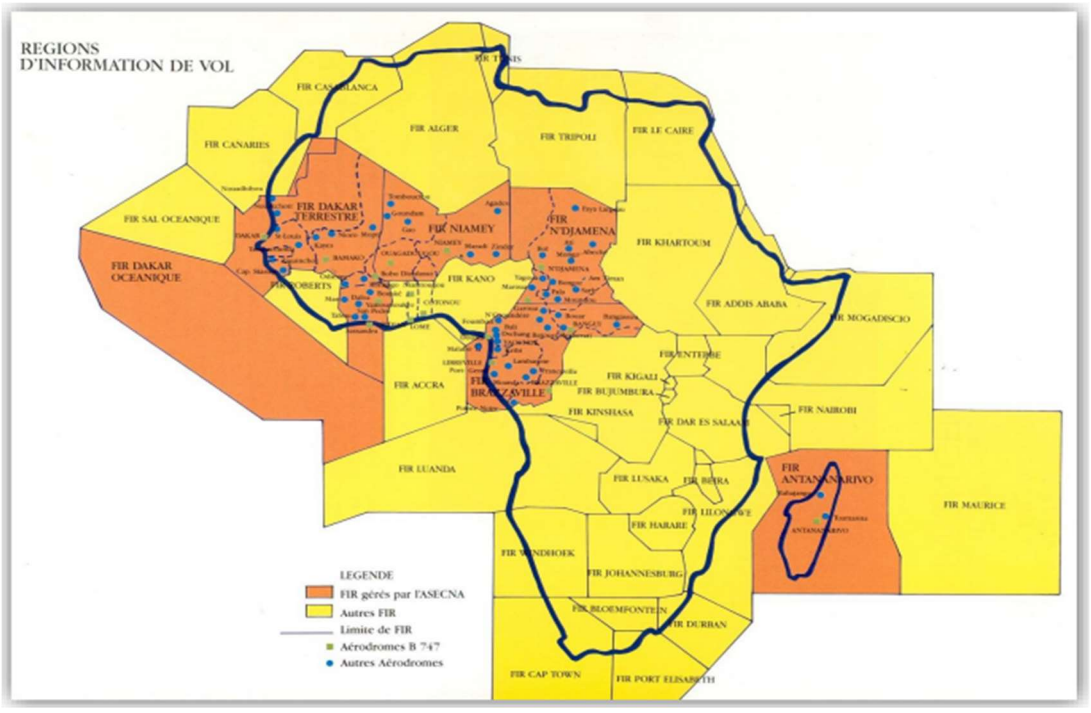

Figure A.02 : *Ensemble des 6 « Flight Information Region » géré par l'ASECNA*

A.4 Organisation de l'ASECNA

A.4.1 Structures statuaires

Chaque entreprise de taille doit avoir un statut pour que leurs missions soient menées à bien. Voici donc la hiérarchie statutaire des dirigeants de l'ASECNA et le rôle de chaque membre :

- **Le Comité des Ministres de tutelle** : Définit la politique générale de l'Agence. Se réunit au moins une fois par an en session ordinaire ; la présidence est tournante à rythme annuel.
- **La Commission de Vérification des Comptes** : Elle établit un rapport sur la régularité de la gestion comptable de l'Agence pour le Conseil d'Administration et pour chaque Ministre de tutelle et formule des propositions sur le quitus à donner à l'Agent comptable.
- **Le Conseil d'Administration** : Prend les mesures nécessaires au fonctionnement de l'ASECNA au moyen de délibérations relatives notamment aux budgets annuels de fonctionnement et d'équipement. Se réunit au moins deux fois par an.
- **La commission de vérification de la sécurité** : Assiste le Conseil d'Administration dans ses attributions relatives à la sécurité et suit la mise en place et le bon fonctionnement d'un système de gestion de la sécurité (SGS) conforme aux normes et pratiques recommandées par l'OACI.
- **Agent comptable** : C'est celui qui tient la comptabilité générale et la comptabilité analytique d'exploitation et surtout celui qui prépare le compte financier, qui est présenté au Conseil d'Administration après avoir été soumis au contrôle de la commission de vérification des comptes. Il est nommé par le Conseil d'administration.
- **Le Directeur Général** : Assure la gestion de l'Agence. Il recrute tout le personnel de l'Agence à l'exception de l'Agent Comptable et du Contrôleur Financier et est responsables de la gestion administrative de l'Agence. C'est aussi lui qui prépare le compte financier, présenté au Conseil d'administration après avoir été soumis au contrôle de la Commission de vérification des Comptes. Il est assisté par six Directeurs.
- **Contrôleur Financier** : Contrôle la gestion de l'établissement et surveille toutes les opérations susceptibles d'avoir une répercussion économique et financière.

La Figure A.03 illustre cette hiérarchie.

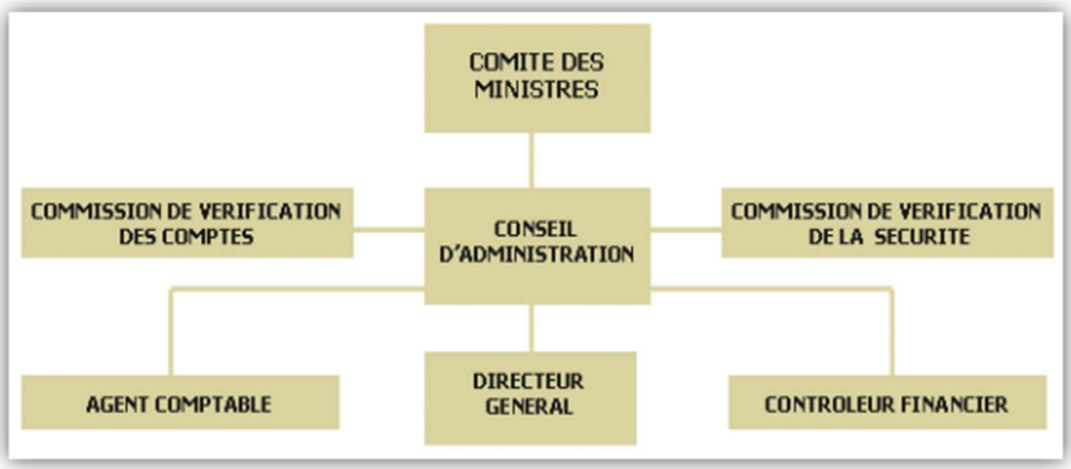

Figure A.03 : *Structure statutaire de l'ASECNA*

A.4.2. Organigramme central

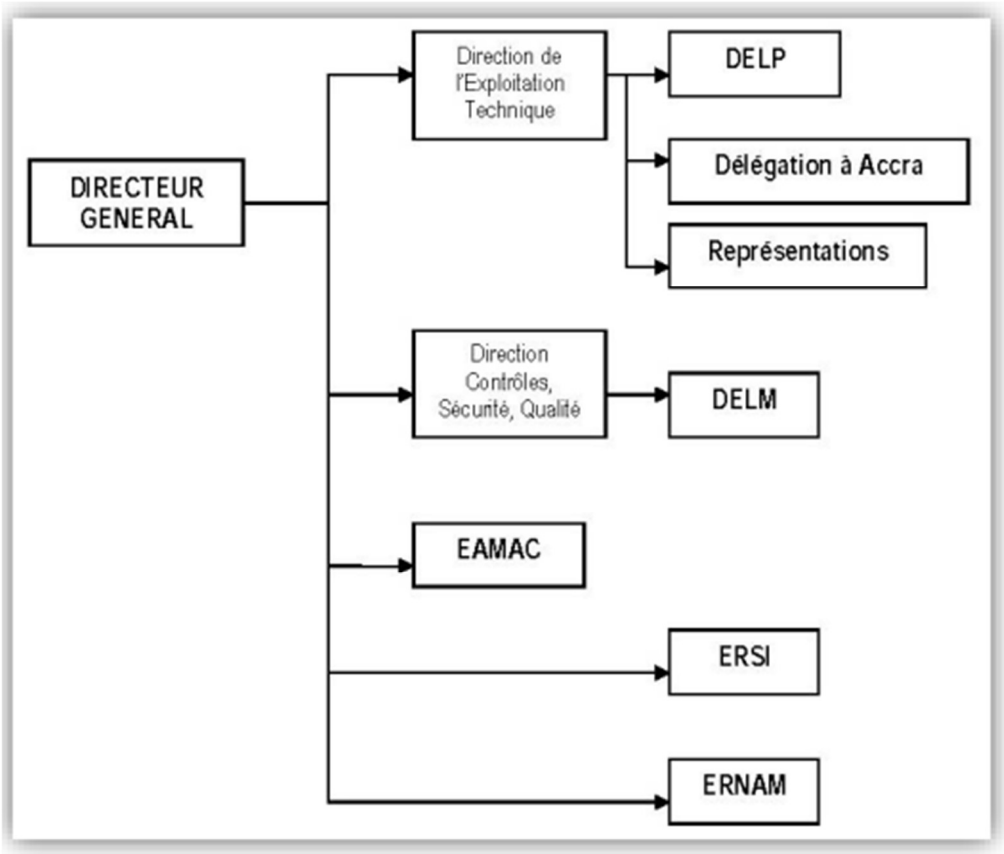

Figure A.04 : *Organigramme de la direction général de l'ASECNA*

L'Organigramme de la Figure A.04 représente principalement les locaux de travail de l'Agence, qui sont :

- La direction générale dont le siège est à Dakar
- La DELP, la délégation à Accra et le DELM qui sont des délégations de l'Agence se

situant respectivement à Paris, à Accra (République de Ghana) et à Montréal.

- Les représentations qui illustrent les 17 Etats membres de l'ASECNA

On note particulièrement aussi dans cet organigramme, l'existence des trois établissements de formation initiale et continue pour pouvoir assurer la compétence des agents et dont l'ASECNA consacre plus de 7% de son budget de fonctionnement :

- l'EAMAC ou Ecole Africaine de la Météorologie et de l'Aviation Civile, situé à Niamey au Niger,
- l'ERSI ou Ecole Régionale de Sécurité Incendie, situé à Douala au Cameroun,
- l'ERNAM ou Ecole Régionale de la Navigation Aérienne et du Management, situé à Dakar au Sénégal.

A.5 Politique de qualité du service

A.5.1 Formation des agents

Pour réussir sa mission, l'ASECNA mise tout d'abord sur la compétence de ses agents grâce à la formation professionnelle à laquelle elle accorde une place privilégiée. A ce titre, elle dispose des trois établissements (EAMAC, ERSI et ENAM) pour la formation initiale et continue de ces agents. En plus de ces Ecoles, l'ASECNA a aussi implanté des CELICA ou Cellules d'Instruction dans les Centres de l'ASECNA dans les domaines de circulation aérienne, de la maintenance et de la météorologie, installées dans chaque Représentation de l'Agence visant à favoriser le recyclage sur place des agents.

A.5.2 Equipements performants et à la pointe des technologies modernes

En effet, le parc de l'ensemble des équipements de l'Agence a connu une croissance notable ces dernières années, intimement liée à la mise en œuvre des nouveaux concepts CNS/ATM de l'OACI. Ainsi dans tous les domaines : Communication, Navigation, Surveillance, Gestion du Trafic Aérien et Météorologie, les équipements ont évolué tout en faisant appel aux technologies de pointe numériques, utilisant les satellites et les nouveaux modes de télécommunications.

A.5.3 Taux de disponibilité élevé des équipements

L'Agence mise aussi sur un taux de disponibilité élevé de ces équipements pour mener à bien ses missions et pour une plus grande qualité de service. Cette haute disponibilité des matériels se base sur :

- la redondance physique des matériels critiques (serveurs, source d'alimentations,…),
- la maintenance préventive et curative basé sur la télémaintenance et la télésurveillance.

Ainsi, il y a toujours un suivi quotidien de l'ensemble des installations et infrastructures.

A.5.4 Règlementations en vigueurs

En aéronautique, il y a des règlementations en vigueur que l'ASECNA doit aussi appliquer pour assurer son fonctionnement, voici ces règlements :

- Internationales : Annexes et Documents OACI, Documents OMM, Documents UIT
- Nationales : CMAC, RCA, RMA

A.6 Organisation de l'Aviation Civile Internationale (OACI)

En anglais **International Civil Aviation Organisation (ICAO)**

La réglementation de la circulation aérienne procède de la volonté des Etats de construire un cadre juridique et réglementaire harmonisé pour la sécurité de la Navigation Aérienne Internationale. Cette volonté s'exerce depuis 1947 au travers des mécanismes définis par la Convention de Chicago : Au cours d'une conférence tenue à Chicago sous l'égide des Etats-Unis, une convention sur l'Aviation Civile a été signée par cinquante-deux (52) Etats. Cette convention connue sous le nom de Convention de Chicago, signée le 07 Décembre 1944, est à l'origine de la création de l'Organisation de l'Aviation Civile Internationale (OACI). Elle est rentrée en vigueur en 1947 après sa ratification par le vingt sixième (26ème) Etat.

A.6.1 Buts et objectifs

L'OACI a pour buts et objectifs d'élaborer les principes et les techniques de la navigation aérienne internationale et de promouvoir la planification et le développement du transport aérien international de manière à :

- Assurer le développement ordonné et sûr de l'aviation civile internationale dans le monde entier ;
- Encourager les techniques de conception et d'exploitation des aéronefs à des fins pacifiques ;
- Encourager le développement des voies aériennes, des aéroports et des installations et services de navigation aérienne pour l'aviation civile internationale ;
- Répondre aux besoins des peuples du monde en matière de transport aérien sûr, régulier,

efficace et économique ;

- Prévenir le gaspillage économique résultant d'une concurrence déraisonnable ;
- Assurer le respect intégral des droits des Etats contractants et une possibilité équitable pour chaque Etat contractant d'exploiter des entreprises de transport aérien international.

A.6.2 Structure de l'OACI

L'OACI est composé :

- D'une Assemblée, qui est organe législatif
- Du Conseil, qui est l'organe exécutif dont le siège à Montréal
- Des Commissions (dont la Commission de la Navigation Aérienne)
- Du Secrétariat général
- Des Comités spécialisés

A.6.3 Les annexes à la convention de Chicago

Le Conseil de l'OACI adopte, conformément aux dispositions du chapitre VI art.37 de sa convention, des Normes et des Pratiques Recommandées internationales ; pour des raisons de commodité, il les désigne comme Annexes à la présente convention et les notifie aux Etats contractants.

Il existe actuellement dix-neuf (19) Annexes à la convention de Chicago qui sont :

Annexe 1 : Licences du personnel

Annexe 2 : Règles de l'air

Annexe 3 : Assistance météorologique à la Navigation aérienne

Annexe 4 : Cartes aéronautiques

Annexe 5 : Unités de mesure à utiliser dans l'exploitation en vol et au sol

Annexe 6 : Exploitation technique des aéronefs

Annexe 7 : Marques de nationalité et d'immatriculation des aéronefs

Annexe 8 : Certificats de navigabilité des aéronefs

Annexe 9 : Facilitation du transport aérien

Annexe 10 : Télécommunications aéronautiques

Annexe 11 : Services de la circulation aérienne

Annexe 12 : Recherche et sauvetage

Annexe 13 : Enquêtes

Annexe 14 : Aérodromes

Annexe 15 : Service d'information aéronautique

Annexe 16 : Protection de l'environnement

Annexe 17 : Sûreté et protection contre les interventions illicites

Annexe 18 : Sécurité du transport aérien des marchandises dangereuses

Annexe 19 : Système de gestion de la sécurité

A.7 Représentation de l'ASECNA à Madagascar

A.7.1 Présentation

Madagascar est un Etat membre et fondateur de l'ASECNA, actuellement représenté par Monsieur RAMANANANDRO Désiré. Elle est l'un des sites pilotes de l'agence dont l'aérodrome primaire se trouve à Ivato (Antananarivo), et deux autres à Toamasina et Mahajanga.

A.7.2 Locaux de travail

Voici les différents locaux de travail des agents :

Localisation	**Locaux**
Ivato	Bâtiment administratif, Bloc Technique, Centrale électrique, Station terrienne, Caserne du SSLI, Bâtiment de l'IGC et garage, Station radiosondage, Centre médical, Centre de réception à distance, Centre d'émission à distance (à Antanetibe)
Mahajanga	Bloc technique, SSLI, Centrale électrique
Toamasina	Bloc technique, SSLI, Centrale électrique
Taolagnaro	Station météo
Radiobalises	Moramanga, Soavinandrina, Ankazobe, Maromamy
Stations VSAT déportées	Antsiranana, Antalaha, Maintirano, Mananjary, Toliara, Tolagnaro, Moroni, St Denis, Maurice, Dzaoudzi.

Tableau A.02: Différents locaux de travail de l'agence

Spécialement pour la représentation à Ivato :

- Le bâtiment administratif : regroupe tous ce qui concerne les services administratifs.
- Le Bloc Technique : loge la majorité des postes opérationnels et techniques, il est surplombé par la tour de contrôle.
- La Centrale électrique : rassemble toutes les infrastructures d'alimentation en électricité.
- La caserne du SSLI : est utilisé par le service de secours
- La Station Terrienne : abrite non seulement les équipements techniques dans presque tout le premier niveau, mais aussi le CRNA à l'étage.
- Le bâtiment de l'IGC : sert à la fois de locaux pour les agents de l'IGC mais aussi de garage pour les véhicules de transport en commun de l'agence.
- La Station Radiosondage : regroupe les matériels utilisés pour la radiosondage
- Centre médical : abrite les matériels et personnels assignées pour les soins médicaux.

A.7.3 Moyens CNS

Les moyens de Communication, de Navigation et de Surveillance du trafic aérien sont primordiaux pour un ANSP. C'est à partir de ces moyens que la sécurité de la navigation aérienne est assurée. Il existe 3 catégories :

- Les moyens de Communication : ils sont utilisés pour la communication vocale ou via chat entre le contrôleur aérien et le pilote.
- Les moyens de Navigation : constituent les équipements aux sols qui servent d'aide à la navigation des aéronefs.
- Les moyens de Surveillance : ce sont les matériels électroniques et informatiques utilisés par l'Agence afin de suivre l'évolution des aéronefs dans la FIR.

Le Tableau A.03 montre les moyens opérationnels de l'ASECNA.

COMMUNICATION	NAVIGATION	SURVEILLANCE
HF	3 VOR : Ivato, Toamasina, Mahajanga	FDP
VHF via VSAT	2 DME de route: à Ivato et à Mahajanga	Radar
CPDLC	2 ILS/DME atterrissage : Ivato, Toamasina	ADS-B et ADS-C
SATCOM (secours)	GNSS*	TopSky

Tableau A.03 : Moyens de Communication, de Navigation et de Surveillance

A.7.4 Moyens d'intervention d'urgence

La disposition des moyens d'intervention d'urgence constitue un critère indispensable pour un fournisseur de service de navigation aérienne comme l'ASECNA. Ils doivent toujours être prêts à intervenir et toujours disponibles en cas d'accident. Pour cela l'Agence dispose de pompiers bien formés dans le domaine, et des véhicules SLI et Flycos qui répondent aux normes de l'OACI.

A.7.5 Organigramme de la représentation de l'Agence à Madagascar

La Figure A.05 montre l'organigramme de la représentation de l'ASECNA à Madagascar

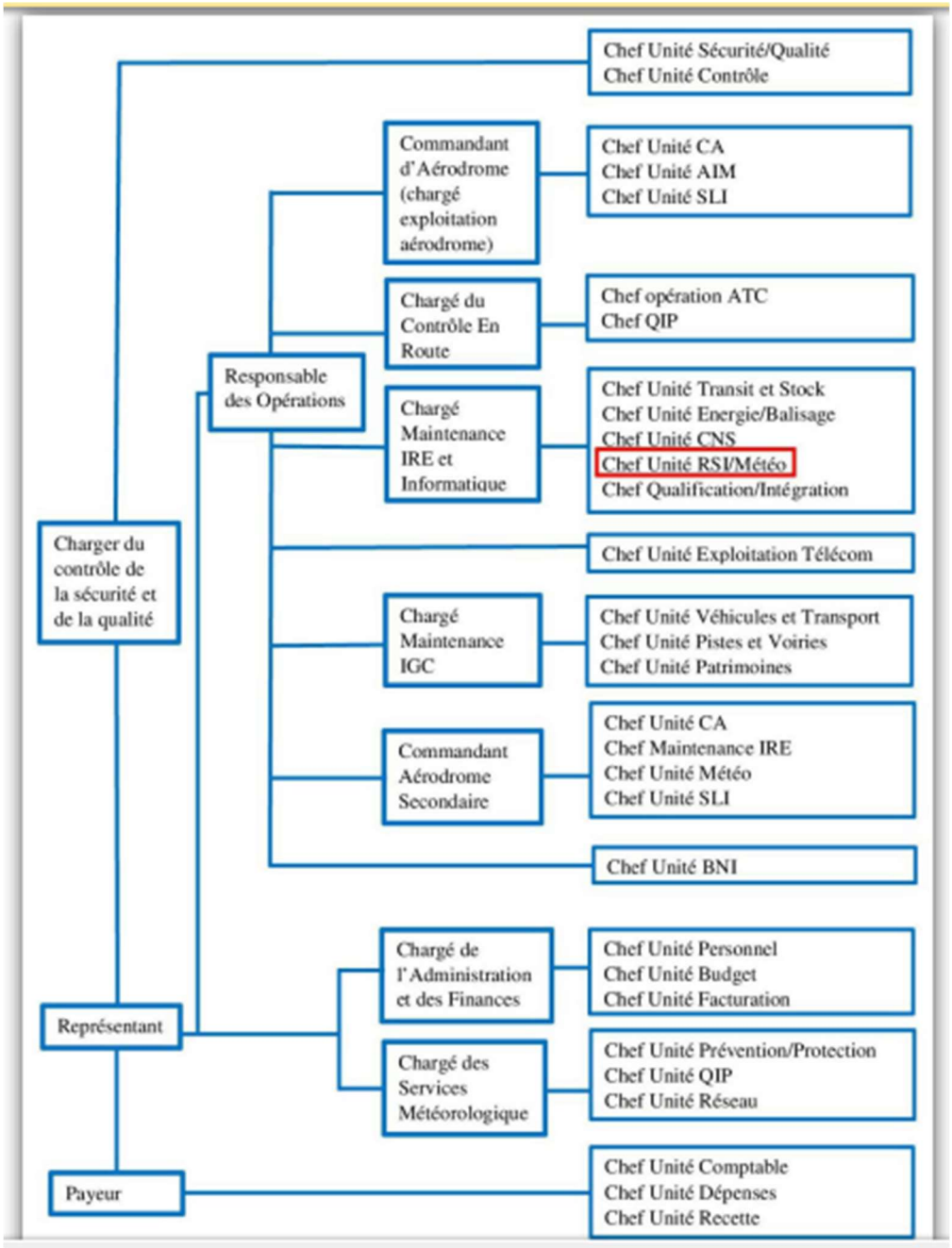

Figure A.05: *Organigramme de la représentation de l'ASECNA à Madagascar*

BIBLIOGRAPHIE

[1] M. Kizito, *« Techniques Radar – ADS »,* Formation CCA, EAMAC, version janvier 2008

[2] O.B. OUATTARA/N'd. M. SYLLA, *« Automatic Dependant Surveillance (ADS)»* , Formation CCA, Ecole Africaine de la Météorologie et de l'Aviation Civile (EAMAC), A.U : 2015-2016

[3] O. J. BELINGA, « ADS », Formation CNA, EAMAC, 2009

[4] http://www.asecna.aero, 2016

[5] *https://fr.wikipedia.org/wiki/**Satellite**_artificiel*

[6] http://www.intelsat.com, 2016

[7] L. RABEHARIMANANA, « Technique avancée de transmission », cours TCO M2, ESPA, 2016

[8] J. Parrend, *« Présentation de l'ADSL »,* IUT de Mulhouse, Juin 2004

[9] Marc PERRUDIN, *« Le multicast IP: Protocoles et mise en œuvre de la famille PIM »*, 2004

[10] http://www.iana.org/assignments/multicast-addresses, 2016

[11] X. Lasserre, T. Klein, _SebF, *« Réseaux Privés Virtuels – VPN »*, 2016

[12] P. Roudel, A. M. ENIC, *«Les VPNs et les protocoles SLIP, PPP, PPTP, L2F, L2TP, LCP, IPSec, MPLS, NAT »***,** TTV02, Janvier 2002

[13] http://www.cisco.com/cisco/web/support/CA/fr/109/1093/1093876_IPSECpart8.html, généré le 18 Octobre 2014

[14] https://www.thalesgroup.com, 2016

[15] http://www.cisco.com, 2016

[16] M. Fuszner, « Graphical Network Simulator », version 1.0, 2016

[17] www.gns3.net, 2016

[18] https://framasoft.org/article4996.html, 2016

[19] B. Darties, *« Tutoriel d'utilisation de Wireshark »,* 2016

FICHE DE RENSEIGNEMENT

Nom : ABDOURAMANE ATTOU BOUNOU

Prénom : Nafissa

Adresse : logt 01 Cité Crémont ASECNA Ivato Aéroport

e-mail : nafi_attb@yahoo.fr

Tél : +261346327554/+22789358636

Titre du mémoire : *« DENSIFICATION DE L'ADS-B DANS LA FIR D'ANTANANARIVO »*

Nombre de pages : 109

Nombre de tableaux : 03

Nombre de figures : 79

Encadreur pédagogique :

Nom : RAKOTONDRAINA

Prénom : Tahina Ezéchiel

e-mail : tahina.ezechiel@gmail.com

Encadreur professionnel : :

Nom : RAFANAMBINANTSOA

Prénom : Valohery

e-mail : rvaloheryc@yahoo.fr