



Etudes des failles de sécurité des protocoles de mobilité dans l'Internet Nouvelle Génération

Rapport de Soutenance de Projet de Fin d'Etudes

Projet réalisé au CNET à Issy-Les-Moulineaux
(DTL/SSR)
du 1/03/99 au 30/06/99
sous la responsabilité de Monsieur Olivier CHARLES

SOMMAIRE

Introduction	3
I. IPv6	4
a. Pourquoi une nouvelle version d'IP	4
b. Les critères techniques d'IPv6	5
c. Les principales caractéristiques d'IPv6	6
II. La mobilité	7
a. Généralités	7
b. Dans IPv6	8
III. La sécurité	13
a. Généralités	13
b. IPsec	15
c. Firewall	21
IV. La sécurité dans la mobilité	24
a. Les options de Mobile IPv6	24
b. Interactions avec les firewalls	24
c. Généralités sur la sécurité liée à la mobilité	25
d. Problèmes ouverts	25
V. Les projets	26
a. EURESCOM « Security for IP Mobility »	26
b. RNRT «MobiSecV6 »	27
VI. Objectifs du Projet de Fin d'Etudes	30
a. Projet Eurescom	30
b. Projet RNRT	31
c. Veille technologique	31
VII. Bilan du Projet de Fin d'Etudes	32
a. Etudes théoriques	32
b. Réalisations techniques	32
c. Compétences humaines	32
d. Suites envisagées	33
Conclusion	34
Bibliographie	35
Annexes	38
Planning effectif	
Schéma de la plate-forme expérimental IPv6	
Schéma simplifié de la plate-forme expérimentale IPv6	
Description de la plate-forme expérimentale IPv6	

Introduction

Le protocole IPv4 souffre de nombreuses faiblesses. Le plus gros problème est l'espace d'adressage. Les adresses IP sont d'une longueur de 32 bits, ce qui représente environ 4 milliards d'adresses. Mais aujourd'hui, avec l'extension des réseaux mondiaux et le gaspillage des adresses dû à la structure en classes, le nombre d'adresses devient insuffisant. Un autre problème, est la saturation des tables de routage sur les routeurs principaux de l'Internet, même si dès 1993, des mesures d'urgence avaient été prises. Cela a permis de retarder l'échéance de quelques années. Enfin, IPv4 n'avait pas vraiment de services de sécurité (authentification, intégrité et confidentialité). C'est ainsi que des travaux pour un nouveau protocole IP ont été lancés en 1994 sous l'égide de l'**IETF** (Internet Engineering Task Force) : ce protocole s'appellera **IPv6** ou **IPng** (IP new generation).

Contrairement à IPv4, la mobilité est devenue un objectif important dans IPv6. En effet, avec l'accroissement des utilisateurs de portable et le besoin de certains de ces utilisateurs à être connecté de manière constante à l'Internet, un nouveau marché est apparu. **Mobile IPv6** est le standard pour IPv6 qui permet de gérer cette mobilité. Actuellement de nombreuses équipes travaillent sur sa normalisation et son implantation sur divers systèmes d'exploitation.

D'un autre côté, le nombre d'utilisateurs de l'internet et l'augmentation du trafic implique un plus grande attention au niveau de la sécurité. Du coup, la sécurité est devenue l'un des principaux objectifs aussi dans IPv6. Ainsi le système de sécurité d'IPv6 (**IPsec**) est au cœur des dispositifs de sécurité. Sa fourniture devient obligatoire pour une implémentation d'IPv6 conforme.

Les utilisateurs de mobiles veulent la même garantie de sécurité que lorsqu'ils utilisent des postes fixes. Dans ce contexte, des projets scientifiques et industriels s'organisent afin de préparer des produits qui répondront à ces besoins.

L'objet de ce projet d'étude est de « plonger » dans deux de ces projets. Le premier, un projet Eurescom a pour but de comprendre les besoins en sécurité dans la Mobilité IPv6 et de poser des normes. Le deuxième, lui plus concret, est de tester des implémentations de Mobile IPv6 et d'IPsec, bases de futurs produits qui sortiront dans le futur proche.

Ce projet de fin d'étude se déroule au sein du département DTL/SSR (Sécurité des Systèmes et Réseaux) de **France Télécom - CNET** à Issy les Moulineaux sous la responsabilité d'Olivier CHARLES. Dans le cadre de ce projet, l'objectif est aussi de se former au métier d'ingénieur en sécurité des réseaux au sein de ce service.

I. IPv6

a. Pourquoi une nouvelle version d'IP ?

IPv6, appelé aussi **IPng** (*IP new generation*), est une nouvelle version d'IP qui s'inscrit comme l'évolution naturelle et normale du protocole IP en place, IPv4. Protocole IPv4 qui, tout en ayant permis l'énorme croissance de l'Internet, souffre de plusieurs faiblesses. IPv6 est conçu pour fonctionner aussi bien sur des réseaux à très hauts débits comme ATM que sur des réseaux à faible bande passante tels que les réseaux sans fils.

Les faiblesses du protocole IP actuel (IPv4)

Le problème le plus connu concerne l'espace d'adressage. Les adresses IP sont actuellement stockées sur 32 bits ce qui permet environ plus de quatre milliards d'adresses, taille suffisante à l'origine lorsque le modèle dominant était celui d'un ordinateur par campus ou centre de recherche. Aujourd'hui, l'informatique industrielle et commerciale ainsi que celle des particuliers rendent ce nombre trop faible, d'autant que de nombreuses adresses sont « gaspillées » par le mécanisme d'allocation hiérarchique. En outre, la généralisation des machines connectées en réseau risque d'aggraver ce problème.

Un autre problème est celui posé par l'explosion de la taille des tables de routage dans l'Internet. Le routage, dans un très grand réseau, doit être hiérarchique avec une profondeur d'autant plus importante que le réseau est grand. Le routage IP n'est hiérarchique qu'à trois niveaux : réseau, sous-réseau et machine. Les routeurs des grands réseaux d'interconnexion doivent posséder une entrée dans leurs tables pour tous les réseaux IP existants. Ce problème est particulièrement résolu par le « supernetting » ou CIDR (*Classless Internet Domain Routing*).

IPv4 ne permet pas d'indiquer de façon pratique le type de données transportées (TOS ou *Type of Service* dans IPv4) d'où, par conséquent, leur urgence ou le niveau de service souhaité. Ce besoin est particulièrement critique pour les applications « temps réel » comme la vidéo mais aussi celles plus classiques (par exemple, en donnant des priorités à tel ou tel trafic). Ce problème a été évoqué ou clarifié mais reste peu mis en œuvre. Il est symptomatique que les protocoles de routage les plus répandus ne tiennent pas vraiment compte du TOS dans le calcul des routes.

Enfin, IPv4 ne fournit pas de mécanismes de sécurité comme l'authentification des paquets, leur intégrité ou leur confidentialité. Il a toujours été considéré que ces techniques étaient de la responsabilité des applications elles-mêmes.

L'évolution des besoins des utilisateurs ainsi que l'apparition de nouveaux marchés ne cessent d'amplifier les « carences » du protocole IPv4 actuel.

b. Les critères techniques d'IPv6

Les spécifications d'IPv6 sont assujetties à un certain nombre de critères techniques. La liste de ces critères est la suivante :

- Etre bâties autour de standards ouverts et accessibles au public
- Définir une méthode de migration claire et réaliste
- Permettre la gestion d'au moins un milliard de réseaux, soient mille milliards de stations, avec autoconfiguration des adresses et mise en place d'un adressage global et unique de chaque équipement, même en présence d'une structure topologique
- Utiliser les méthodes de routage RIP, OSPF, etc.
- Etre indépendantes du réseau physique, le Flow Label d'IPv6 doit même pouvoir correspondre avec les circuits virtuels ATM
- Supporter les diverses topologies de réseaux interconnectés et un service de type datagramme (orienté sans connexion)
- Exploiter de façon optimisée les réseaux à hautes performances d'où le choix d'un en-tête sans contrôle de parité et cadré sur des multiples de 4 octets
- Garantir la sécurité de certaines opérations, comme l'authentification ou le chiffrement spécifique du niveau 3 (réseau)
- Supporter la diffusion de groupe (*multicast*)
- Gérer plusieurs classes de services (avec le Flow Label)
- Incorporer des protocoles de contrôle semblables à IPv4 (Ping, Traceroute)
- Permettre l'encapsulation de divers protocoles dans IPv6
- Offrir un service fiable et robuste

c. Les principales caractéristiques d'IPv6

IPv6 est la nouvelle version d'IP et représente une très forte évolution par rapport à IPv4. Les principales fonctionnalités d'IPv4 sont conservées dans IPv6 excepté certaines fonctions peu ou pas utilisées qui ont été supprimées ou rendues optionnelles. En outre, quelques priorités ont été ajoutées.

Il est possible de dégager huit grandes caractéristiques incluses dans IPv6.

- Des possibilités étendues d'adressage et de routage
La taille de l'adresse IP augmente de 32 à 128 bits afin de supporter un plus grand nombre de nœuds adressables, davantage de niveaux d'adressage hiérarchique ainsi qu'une autoconfiguration plus simple des adresses.
- Un format d'en-tête simplifié
Des champs du format de l'en-tête IPv4 ont été abandonnés ou rendus optionnels, ainsi l'en-tête IPv6 est simplifié et réduit à un traitement commun dans tous les routeurs ce qui diminue donc le coût de traitement dans ces routeurs.
- Des possibilités d'extension des en-têtes et des options
Dans IPv6, les options sont rangées dans des en-têtes supplémentaires situés entre l'en-tête IPv6 et l'en-tête du paquet transport (T-PDU, *Transport Protocol Data Unit* ou Unités de données du service de transport). La plupart des options dans les en-têtes IPv6 ne sont ni examinées, ni traitées par les routeurs intermédiaires. Contrairement à IPv4, les options IPv6 peuvent être de longueur arbitraire, il n'existe pas de taille limite.

Une des caractéristiques d'IPv6 est la possibilité de coder, dans les options, l'action qu'un routeur ou une station de travail doit réaliser si l'option est inconnue, ce qui permet l'ajout de fonctionnalités supplémentaires dans un réseau déjà opérationnel avec un minimum de perturbations.

- Des possibilités d'authentification et de confidentialité
IPv6 intègre des extensions permettant l'authentification des usagers et l'intégrité des données grâce à des outils de cryptographie.
- Des possibilités d'autoconfiguration
IPv6 dispose de plusieurs formes d'autoconfiguration comme la configuration « plug and play » d'adresses de nœuds sur un réseau isolé grâce aux caractéristiques offertes par DHCP.
- Des possibilités pour le « Source Route »
IPv6 intègre une fonction étendue de *source routing* grâce à SDRP (*Source Demand Routing Protocol*) afin d'étendre le routage à des routes interdomaines et intradomaines.
- Une transition d'IPv4 à IPv6 simple et flexible
La transition d'IPv4 à IPv6 répond à quatre objectifs essentiels :
 - ✓ Un besoin de modernisation
 - ✓ Un besoin de redéploiement
 - ✓ Un adressage facile
 - ✓ Une diminution du coût de démarrage
- Des possibilités de qualité de service
L'introduction de flux étiquetés (avec des priorités), les services de contraintes « temps réel » sont de nouveaux éléments rendant possible la qualité de service.

II. La mobilité

a. Introduction

L'idée de la mobilité dans l'Internet est assez récente. Jusqu'à maintenant, la mobilité se résumait à des ordinateurs portables qui récupéraient une adresse temporaire grâce au protocole d'autoconfiguration DHCP. Ce n'est pas vraiment une utilisation nomade des ordinateurs. En effet, il n'a pas en général un besoin d'une connexion permanente avec Internet. Mais le futur va amener des utilisateurs à être connectés à tout moment à l'Internet (finance, supervision de systèmes, ...).

La véritable mobilité IP propose et définit des concepts qui permettent à leurs utilisateurs de rester connectés à Internet par divers moyens (Ethernet, Ethernet Radio, GSM). Mais aussi, que les autres utilisateurs puissent les joindre n'importe où et n'importe quand.

b. Mobilité dans IPv6

Lorsque l'on parle de mobilité, il faut mentionner 2 réseaux particuliers :

- Le réseau d'origine du mobile - **Réseau Mère**
- Le réseau accueillant le mobile - **Réseau Visité**

Et 3 entités particulières :

- La station se déplaçant - **Mobile** ou **Nœud Mobile** (*Mobile Node*)
- Le routeur gérant les mécanismes de transfert des paquets pour le mobile - **Agent Mère** (*Home Agent*)
- La station correspondant avec le mobile - **Correspondant** ou **Nœud Communicant** (*Correspondent Node*)

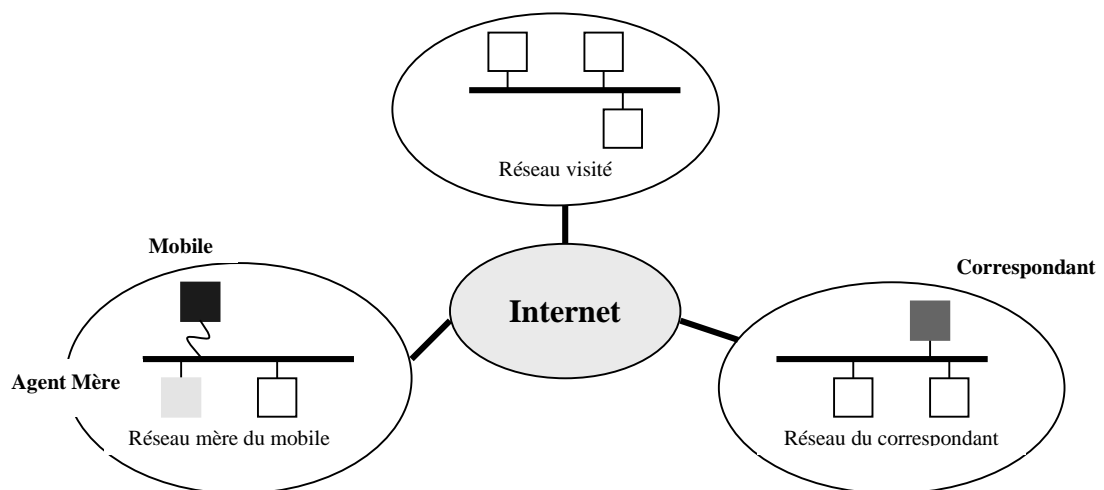


Figure II.1 : Schéma des principaux acteurs de la mobilité

- Cas où le mobile est chez lui (réseau mère)

Le mobile dispose d'une adresse principale, appelée également **Adresse Mère**, qu'il soit attaché à son réseau d'origine ou qu'il soit éloigné de celui-ci. Tant que le mobile est sur son réseau mère, le routage des paquets IPv6 est conventionnel.

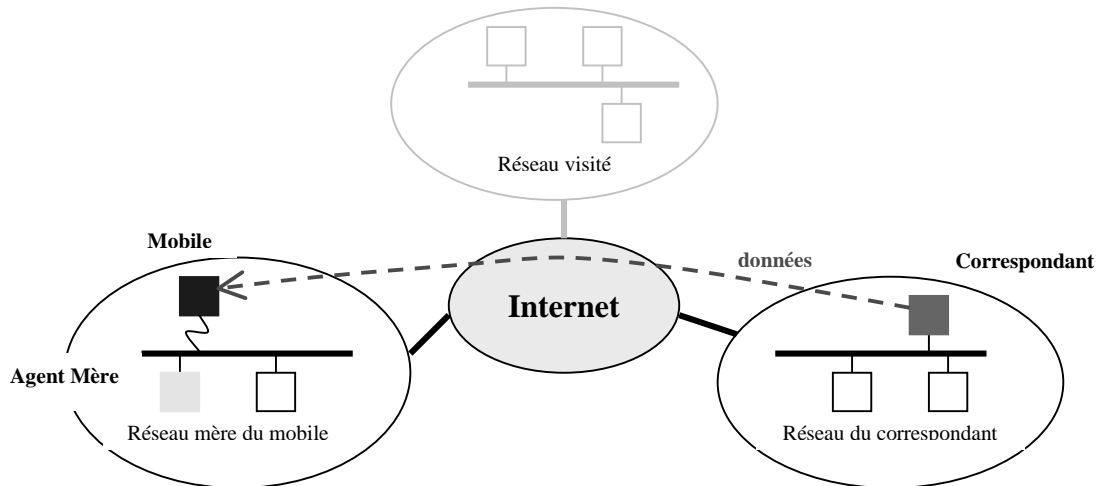


Figure II.2 : Envoi de données d'un correspondant vers un mobile situé dans son réseau mère

- Cas où le mobile est loin de chez lui (réseau visité)

Lorsque le mobile est sur un réseau étranger, il dispose d'une ou plusieurs adresses temporaires en plus de son adresse mère. En général, l'adresse temporaire est le résultat de la concaténation du préfixe du réseau et de son **Adresse Lien-Local** (*Link-Local Address*) - de la forme `fe80::XXX` (où XXX peut être l'adresse MAC de l'interface connectée) - en enlevant la partie "fe80:". Le routage des paquets adressés au mobile par une de ses adresses temporaires s'effectue de façon conventionnel.

La liaison entre l'adresse mère et une adresse temporaire est appelée **Association**. Lorsque le mobile se déplace, il enregistre une de ses associations avec un routeur situé dans le réseau mère, l'**Agent Mère**. Le terme **Adresse Temporaire Primaire** (*Care of Address*) désigne l'adresse temporaire utilisée actuellement par le mobile. Par la suite, l'agent mère agira comme proxy pour intercepter tous les paquets IPv6 destinés à l'adresse mère du mobile, et gèrera la communication entre le mobile et ses correspondants en tunnelant chaque paquet intercepté à l'adresse temporaire primaire du mobile.

La mobilité IPv6 fournit un mécanisme pour permettre aux nœuds IPv6 communiquant avec un mobile d'apprendre dynamiquement et de stocker l'association d'un mobile. Lorsqu'un nœud IPv6 veut envoyer un paquet, il vérifie les associations qu'il possède, dans un cache, pour l'adresse destination du paquet. Il y a alors 2 possibilités :

- ✓ Si une association pour cette adresse est trouvée, il utilise un **En-Tête de Routage** (*Routing Header*) pour délivrer le paquet vers le mobile situé à l'adresse temporaire liée à l'association.
- ✓ Sinon, il envoie le paquet normalement, c'est à dire, avec comme adresse destination, l'adresse mère du mobile. Alors le paquet est intercepté par l'agent mère qui tunnelera le paquet jusqu'au mobile.

Le correspondant et l'agent mère apprennent et conservent l'association d'un mobile en utilisant un ensemble d'**Options IPv6** destination. Ces options sont spécialement définies pour le support de la mobilité dans IPv6. Une option IPv6 destination de mobilité peut être envoyée de 2 manières différentes :

- ✓ Elle peut être incluse à l'intérieur de n'importe quel paquet véhiculant n'importe quelle charge utile comme TCP ou UDP.
- ✓ Elle peut être envoyée dans un paquet IPv6 séparé ne contenant aucune autre donnée.

La mobilité IPv6 définit quatre nouvelles options destinations :

- **Mise à jour de l'association** (*Binding Update*)
Cette option est utilisée par le mobile pour avertir, soit un correspondant, soit l'agent mère du mobile, de son association courante. On appelle **Enregistrement Principal** le cas où cette option est envoyée à l'agent mère.
- **Acquittement de l'association** (*Binding Acknowledge*)
Cette option est utilisée par pour acquitter la réception d'un message « Mise à jour de l'association ».
- **Demande de mise à jour de l'association** (*Binding Request*)
Cette option est utilisée pour demander à un mobile d'envoyer un message « Mise à jour de l'association » contenant son association courante. Cette option sert principalement à rafraîchir une association avec un mobile.
- **Adresse principale** (*Home Address*)
Cette option est utilisée par le mobile pour informer le correspondant de l'adresse mère du mobile. En effet, le mobile met comme adresse source, lorsqu'il est sur un réseau visité, l'adresse temporaire qu'il possède. Avec cette option, le correspondant pourra toujours joindre le mobile, en passant par son adresse mère s'il le faut.

Pour supporter la mobilité dans IPv6, il est nécessaire d'avoir certaines structures de données :

- **Cache des associations** (*Binding Cache List*)
Un cache des associations est maintenu par chaque nœud IPv6. Il existe une entrée dans le cache des associations appelée entrée **Enregistrement Principal**. Cette entrée existe lorsqu'un nœud sert d'agent mère pour un mobile. Cette entrée ne sera détruite qu'à l'expiration de la durée de vie de l'association. Les autres entrées, par contre, peuvent être modifiées suivant la politique de remplacement de la table des associations.
- **Liste des mises à jour des associations** (*Binding Update List*)
Cette liste est maintenue par les mobiles IPv6 où ils enregistrent les informations au sujet des messages « Mise à jour de l'association » émis à leurs correspondants. La liste contient une entrée avec l'adresse IPv6 du correspondant, l'adresse mère pour laquelle la mise à jour a été envoyée et la durée de vie de l'association.

Lorsque le mobile arrive sur un réseau visité, qu'il récupère une nouvelle adresse temporaire et qu'il décide de l'utiliser comme adresse temporaire principale, il enregistre cette nouvelle association avec son agent mère en envoyant un message « Mise à jour de l'association » à celui-ci en lui demandant d'acquiescer ce message. Le mobile continue d'envoyer des messages « Mise à jour de l'association » périodiquement tant qu'il n'a pas reçu d'acquiescement.

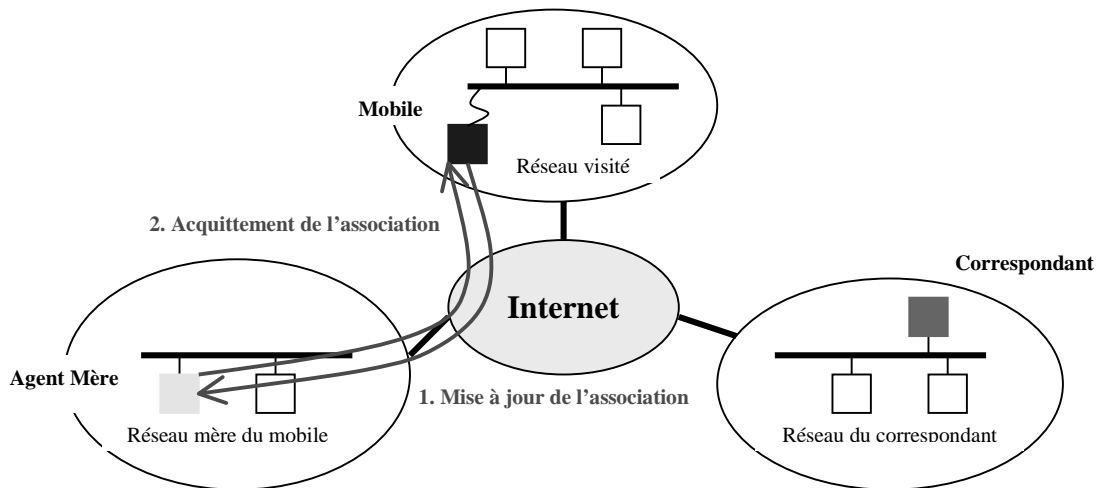


Figure II.3 : Création d'une association avec l'agent mère

Lorsqu'un mobile reçoit un paquet tunnelé par son agent mère, il suppose que l'expéditeur original ne dispose pas d'une entrée dans sa table des associations. En effet, si celui-ci disposait d'une telle entrée, il aurait envoyé ledit paquet avec un en-tête de routage. Aussi le mobile envoie-t-il un message « Mise à jour de l'association » au correspondant, lui permettant par la suite de se servir de cette information pour lui envoyer directement les futurs paquets. Le mobile peut demander, facultativement, un acquiescement pour cette mise à jour.

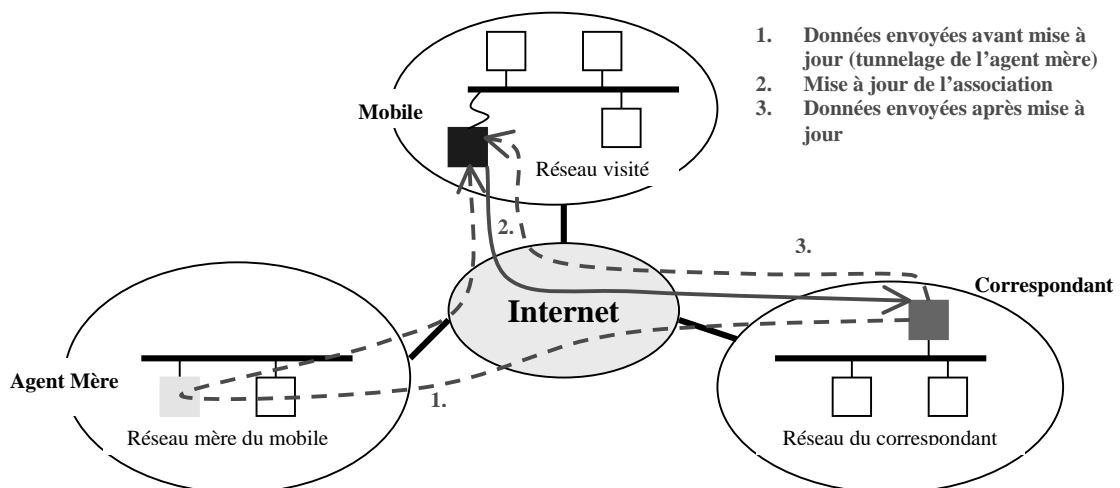


Figure II.4 : Mise à jour du cache d'un correspondant

Lorsqu'un correspondant dispose d'une entrée dans sa table des associations pour un mobile et veut rafraîchir cette association, il envoie un message « Demande de mise à jour de l'association » au mobile. Le mobile alors, répond en envoyant un message « Mise à jour de l'association ». Il peut utiliser plusieurs adresses temporaires en même temps mais une seule peut être enregistrée comme adresse temporaire primaire avec son agent mère. L'agent mère du mobile interceptera et tunnelera les paquets à l'adresse temporaire primaire du mobile, mais celui-ci acceptera tous les paquets qu'il recevra pour n'importe laquelle de ses adresses temporaires.

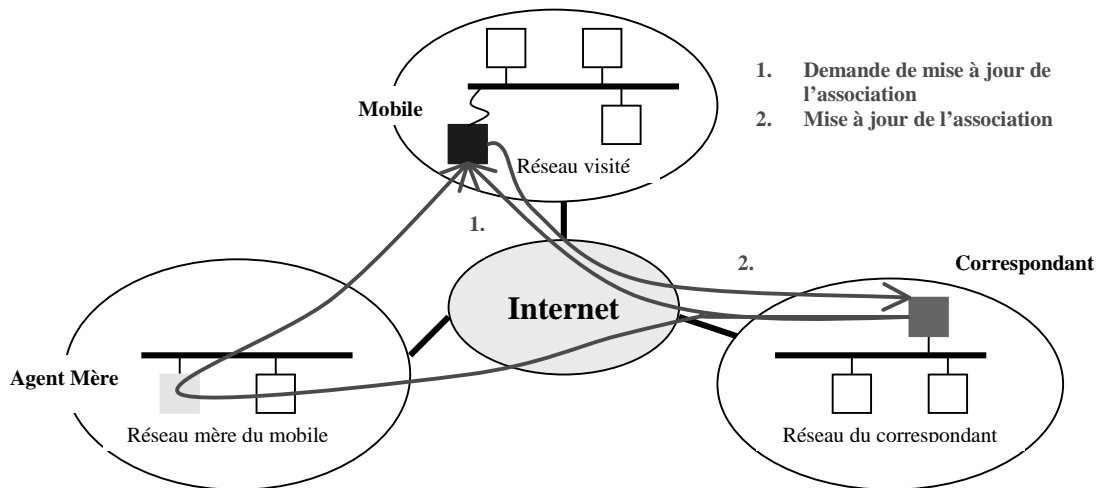


Figure II.5 : Remise à jour d'une association

Généralement, les correspondants d'un mobile disposent d'une table des associations. Aussi, il est attendu que les correspondants routeront les paquets directement à l'adresse temporaire d'un mobile. De cette manière, l'agent mère d'un mobile aura rarement à transmettre des paquets interceptés au mobile.

- Détection de mouvement

Un mobile peut utiliser n'importe quel mécanisme disponible pour détecter à quel moment son changement de point d'attache fait changer de sous-réseau IPv6. Le mécanisme illustré ci-dessous s'appuie sur les facilités du protocole de découverte de voisins, utilisant notamment la découverte des routeurs et le(s) préfixe(s) associé(s) au lien. Il peut soit envoyer des messages de « Sollicitation du routeur » (*Router Solicitation*), soit attendre l'arrivée de messages « Annonce du routeur » (*Router Advertisement*). Un mobile, comme toute autre machine IPv6, maintient une liste des routeurs par défaut ainsi qu'une liste de préfixes associés à chaque sous-réseau. Ces informations sont alimentées par les messages « Annonce du routeur » reçus.

A chacune des entrées de ces listes est associé un compte à rebours, fourni par ces mêmes messages pour invalider l'entrée, à son expiration.

D'autres moyens sont à la disposition du mobile pour détecter un mouvement. En effet, différents types d'indication peuvent être fournis par les protocoles de couches inférieures, indiquant au mobile un changement de base d'attache et le passage à une nouvelle connexion de niveau liaison de données. La détection de mouvement d'un mobile est encore en pleine discussion.

III. La sécurité

a. Généralités

Les services

Il y a 4 principaux services :

- **La confidentialité**
Protection de données émises sur le réseau compréhensibles seulement par des entités autorisées
- **L'authentification de l'origine des données**
Garantie que les données reçues proviennent bien de l'entité émettrice
- **L'intégrité**
Garantie que les données reçues n'ont subi aucune modification lors du transport dans le réseau
- **La prévention contre le jeu de données**
Garantie que les données reçues n'ont pas été précédemment jouées

L'authentification de l'origine des données et l'intégrité peuvent être regroupées dans un seul service appelé authentification.

Les mécanismes de protection

Pour se protéger des attaques classiques, il existe des mécanismes de protection généraux :

- **Confidentialité**
On utilise des algorithmes de chiffrement à clés symétriques
- **Authentification de l'origine des données**
On adjoint aux données émises une signature numérique
- **Intégrité**
On utilise ici aussi le système de signatures numériques

Les risques

Nous pouvons recenser plusieurs catégories d'attaques :

- **IP sniffing**
Un intrus écoute le trafic en transit sur un réseau
- **IP spoofing**
Un intrus réussit à usurper l'identité d'une personne
- **IP flooding**
Un intrus envoie une multitude de paquets IP vers une même destination

Les mécanismes d'attaques

Ci-dessous, les différents exemples de mécanismes d'attaques :

- **IP sniffing**
 - L'intrus est placé sur un réseau utilisant naturellement la diffusion de données
 - L'intrus réussit à utiliser un analyseur de protocoles réseau à l'insu des administrateurs du réseau
- **IP spoofing**
 - L'intrus modifie l'adresse hardware d'une station de travail
 - L'intrus crée des paquets ICMP de toute pièce afin de rediriger des paquets vers une station contrôlée par celui-ci
 - L'intrus compromet un serveur DNS pour rediriger une requête DNS vers une station contrôlée par celui-ci
 - L'intrus introduit des paquets TCP avec des numéros de séquence appropriés dans une connexion
- **IP flooding**
 - "SYN flooding" (avec la pile TCP/IP) : l'intrus émet de nombreux messages SYN d'ouverture de connexion
 - "SYN flooding + IP spoofing" : l'intrus usurpe les clients

b. IPsec

Au cours de ces dernières années, l'utilisation du protocole **IP** comme base des réseaux informatiques est devenue très importante, que ce soit par l'utilisation croissante de l'Internet ou dans le cadre de réseaux d'entreprises de type intranet. Si la flexibilité d'IP et sa simplicité ont su répondre aux besoins en matière de réseaux informatiques de ces dernières décennies, le but de ce protocole n'a jamais été d'assurer des communications sécurisées, d'où l'absence de fonctionnalités dans ce domaine. La facilité des attaques, le fait que la démocratisation de l'Internet les rende accessibles à beaucoup et la volonté croissante de pouvoir utiliser des réseaux IP pour des applications sensibles ont donc poussé au développement de diverses solutions de sécurité : gardes-barrière, routeurs filtrants, protocoles et applications sécurisées se sont multipliés.

Devant les besoins grandissants dans ce domaine, et profitant de la définition du nouveau protocole IPv6, l'**IAB** (*Internet Architecture Board*) a donc décidé d'intégrer des services de sécurité dans le protocole IP lui-même, afin de pouvoir protéger les communications utilisant ce protocole. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme **IPsec** (*IP Security Protocol*).

IPsec se présente sous la forme d'une norme, développée par un groupe de travail du même nom à l'**IETF** (*Internet Engineering Task Force*) depuis 1992. Une première version basique de cette extension d'IP a paru, sous forme de **RFC** (*Request For Comment*), en 1995. Une seconde version, comportant en plus un système de gestion dynamique des paramètres de sécurité, a été publiée en novembre 1998. La maturité grandissante de la norme conduit désormais de nombreux fournisseurs (Cisco, IBM, CheckPoint, etc.) à intégrer IPsec dans leurs produits, et l'on peut considérer que le marché commence à prendre de l'importance et sera bientôt un secteur incontournable de la sécurité réseau.

Principe de fonctionnement

La sécurisation des données échangées

La base d'IPsec est un ensemble de mécanismes de sécurisation des données circulant sur le réseau.

Où intervient IPsec ?

IPsec s'insère, dans la pile de protocoles TCP/IP, au niveau d'IP. Cela signifie qu'il agit sur chaque paquet IP reçu ou émis et peut soit le laisser passer sans traitement particulier, soit le rejeter, soit lui appliquer un mécanisme de sécurisation.

Toutes les implémentations d'une pile de protocoles TCP/IP conformes à la version six d'IP doivent intégrer IPsec. En revanche, IPsec est optionnel pour la version actuelle d'IP, IPv4, et n'est pas encore fourni en standard sur la plupart des systèmes courants. Lorsque se sera le cas ou lorsque IPv6 sera en place, il sera possible à tout utilisateur désirant des fonctions de sécurité d'avoir recours à IPsec ; en attendant, il convient, pour utiliser IPsec, d'acquérir un produit mettant en œuvre cette norme.

Le placement d'IPsec au niveau IP, c'est-à-dire au niveau réseau, présente l'avantage de le rendre exploitable par les niveaux supérieurs, et, en particulier, d'offrir un moyen de protection unique pour toutes les applications. En d'autres termes, là où d'autres systèmes sécurisent les applications au cas par cas, IPsec, lui, sécurise le réseau sous-jacent. Cette approche n'est bien sûr pas exempte de contraintes, notamment des problèmes de performances et la difficulté de pouvoir distinguer les différents flux avec précision.

Du fait de son intégration dans la pile de protocoles, IPsec peut être mis en œuvre sur tous les équipements utilisant le réseau et assurer une protection soit de bout en bout, entre les tiers communicants, soit lien par lien, sur des segments de réseau. IPsec peut donc être utilisé dans de nombreuses situations : il peut offrir une protection aux applications qui utilisent le réseau, protéger l'accès d'un réseau en agissant comme un garde-barrière évolué, servir à mettre en place des réseaux privés virtuels, sécuriser les accès distants à un intranet...

Quels services de sécurité sont fournis ?

IPsec vise à prévenir les diverses attaques rendues possibles par le protocole IP, notamment empêcher un adversaire d'espionner les données circulant sur le réseau ou de se faire passer pour autrui afin d'accéder à des ressources ou données protégées.

Dans ce but, IPsec peut fournir, suivant les options sélectionnées, tout ou partie des services de sécurité suivants :

- **Confidentialité** des données et protection partielle contre l'analyse du trafic.

Les données transportées ne peuvent être lues par un adversaire espionnant les communications.

En particulier, aucun mot de passe, aucune information confidentielle ne circule en clair sur le réseau. Il est même possible, dans certains cas, de chiffrer les en-têtes des paquets IP et ainsi masquer, par exemple, les adresses source et destination réelles. On parle alors de protection contre l'analyse du trafic.

- **Authenticité** des données et **contrôle d'accès** continu.

L'authenticité est composée de deux services, généralement fournis conjointement par un même mécanisme : l'authentification de l'origine des données et l'intégrité.

L'authentification de l'origine des données garantit que les données reçues proviennent de l'expéditeur déclaré.

L'intégrité garantit qu'elles n'ont pas été modifiées durant leur transfert.

La garantie de l'authenticité de chaque paquet reçu permet de mettre en œuvre un contrôle d'accès fort tout au long d'une communication, contrairement à un contrôle d'accès simple à l'ouverture de la connexion, qui n'empêche pas un adversaire de récupérer une communication à son compte. Ce service permet en particulier de protéger l'accès à des ressources ou données privées.

- **Protection contre le rejeu**

La protection contre le rejeu permet de détecter une tentative d'attaque consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau.

Ces services sont basés sur des mécanismes cryptographiques modernes qui leur confèrent un niveau de sécurité élevé lorsqu'ils sont utilisés avec des algorithmes forts.

Comment sont fournis ces services ?

Les services de sécurité mentionnés ci-dessus sont fournis au moyen de deux extensions du protocole IP appelées **AH** (*Authentication Header*) et **ESP** (*Encapsulating Security Payload*) :

- AH est conçu pour assurer l'authenticité des datagrammes IP sans chiffrement des données (i.e. sans confidentialité).

Le principe d'AH est d'ajouter au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Un numéro de séquence permet de détecter les tentatives de rejeu.

- ESP a pour rôle premier d'assurer la confidentialité mais peut aussi assurer l'authenticité des données.

Le principe d'ESP est de générer, à partir d'un datagramme IP classique, un nouveau datagramme dans lequel les données et éventuellement l'en-tête original, sont chiffrés. ESP peut également assurer l'authenticité des données par ajout d'un bloc d'authentification et la protection contre le rejeu par le biais d'un numéro de séquence.

Ces deux extensions peuvent être utilisées séparément ou combinées pour obtenir les services de sécurité requis.

AH et ESP sont basés sur l'utilisation d'algorithmes cryptographiques et ne sont pas restreints à un algorithme particulier : ils sont utilisables avec de nombreux algorithmes. Chaque produit comportant IPsec sera donc livré avec un ensemble d'algorithmes, parmi lesquels l'utilisateur ou l'administrateur du réseau pourront choisir. Cette façon de procéder permet notamment, pour se conformer à des contraintes législatives par exemple, de limiter les algorithmes de chiffrement fournis à une longueur de clef donnée voire de fournir uniquement des algorithmes d'authentification, sans possibilité de chiffrement. IPsec comporte une liste d'algorithmes proposés pour être utilisés avec IPsec et dont l'utilisation est négociable en ligne par le biais d'un protocole appelé **IKE**. À l'heure où ce document est rédigé, cette liste contient notamment les algorithmes de chiffrement NULL (pas de chiffrement), CAST-128 (clef de 40 à 128 bits), Blowfish (40-448 bits), RC5 (40-2040 bits), DES (56 bits) et DES triple (clef de 168 bits mais de force équivalente à 112 bits). Pour garantir l'interopérabilité entre les équipements, la norme IPsec rend certains de ces algorithmes obligatoires. Actuellement, **DES-CBC** et **3DES-CBC** sont obligatoires pour le chiffrement ; pour l'authentification, **HMAC-MD5** et **HMAC-SHA-1** doivent être présents dans toute implémentation conforme d'IPsec.

D'autre part, deux modes de protection existent :

- Le **mode transport** protège uniquement le contenu du paquet IP sans toucher à l'en-tête ; ce mode n'est utilisable que sur les équipements terminaux (postes clients, serveurs).
- Le **mode tunnel** permet la création de tunnels par "encapsulation" de chaque paquet IP dans un nouveau paquet. Ainsi, la protection porte sur tous les champs des paquets IP arrivant à l'entrée d'un tunnel, y compris sur les champs des en-têtes (adresses source et destination par exemple). Ce mode est celui utilisé par les équipements réseau (routeurs, gardes-barrière...).

La gestion des paramètres de sécurisation

Les mécanismes mentionnés ci-dessus font appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes utilisés, clefs, mécanismes sélectionnés...). Afin d'échanger des données de façon sécurisée, il est donc nécessaire, dans un premier temps, de se mettre d'accord sur les paramètres à utiliser, et notamment d'échanger des clefs de façon sûre.

L'approche la plus simple pour cet échange préalable est la gestion manuelle, qui consiste à laisser l'administrateur configurer manuellement chaque équipement utilisant IPsec avec les paramètres appropriés. Si cette approche s'avère relativement pratique dans un environnement statique et de petite taille, elle ne convient plus pour un réseau de taille importante. De plus, elle implique une définition totalement statique des paramètres et un non-renouvellement des clefs. La première version d'IPsec, parue en 1995, se basait sur cette méthode manuelle pour la configuration des équipements.

La seconde approche est la gestion automatique au moyen d'un protocole approprié. Les développements dans ce domaine ont abouti à un protocole de gestion des paramètres relatifs à IPsec connu sous le nom de **IKE** (*Internet Key Exchange*). Bien que ce nom insiste sur le rôle d'échange de clefs, IKE se charge en réalité de la gestion (négociation, mise à jour, suppression) de tous les paramètres relatifs à la sécurisation des échanges. Contrairement aux mécanismes AH et ESP qui agissent directement sur les données à sécuriser, IKE est un protocole de plus haut niveau, dont le rôle est l'ouverture et la gestion d'une pseudo-connexion au-dessus d'IP. En particulier, IKE inclut, au début de la négociation, une authentification mutuelle des tiers communicants qui peut se baser soit sur un secret partagé préalable soit sur des clefs publiques. L'échange des clefs publiques utilisées par IKE peut se faire soit manuellement, soit directement dans le cadre d'IKE par un échange de certificats en ligne, soit par le biais d'une infrastructure à clefs publiques (*Public Key Infrastructure*, **PKI**) extérieure.

Afin de stocker et de manipuler facilement l'ensemble des paramètres gérés par IKE et utilisés par les mécanismes de sécurisation, IPsec a recours à la notion d'association de sécurité (*Security Association*, **SA**). Une association de sécurité est une structure de données qui regroupe l'ensemble des paramètres de sécurité associés à une communication donnée. Pour stocker l'ensemble des associations de sécurité actives, on utilise une "base de données des associations de sécurité" (*Security Association Database*, **SAD**). Les éléments stockés dans cette base de données sont créés et modifiés par IKE puis consultés par la couche IPsec pour savoir comment traiter chaque paquet reçu ou à émettre.

La configuration

Les protections offertes par IPsec sont basées sur des choix définis par l'administrateur du réseau par le biais de politiques de sécurité. Ces politiques sont généralement stockées dans une "base de données de politique de sécurité" (*Security Policy Database*, **SPD**) et se présentent sous forme d'une liste ordonnée de règles, chaque règle comportant un certain nombre de critères qui permettent de déterminer quelle partie du trafic est concernée. La consultation de la base de données des politiques de sécurité permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, sera autorisé à passer outre ou sera rejeté. C'est également cette base qui indique à IKE quelles associations de sécurité il doit négocier, et, en particulier, quels tunnels sécurisés il doit établir. Pour le moment, la configuration des équipements IPsec passe par la configuration manuelle des politiques de sécurité sur chaque équipement. Des systèmes de gestion centralisée et dynamique de ces politiques sont en cours d'élaboration.

Synthèse

Le schéma ci-dessous représente les différents composants d'IPsec et leurs interactions. On y retrouve notamment :

- AH et ESP, les mécanismes de sécurisation au niveau IP qui protègent les données transférées. Les paramètres relatifs à l'utilisation de ces mécanismes sont stockés dans des associations de sécurité.
- IKE, le protocole orienté connexion utilisé par les équipements IPsec pour gérer les associations de sécurité. Une configuration manuelle des associations de sécurité est également possible.
- Un ensemble de politiques de sécurité, qui sont les règles à appliquer au trafic traversant un équipement donné. C'est par elles que l'administrateur du réseau configure IPsec et notamment indique à IKE quels sont les tunnels sécurisés à créer.

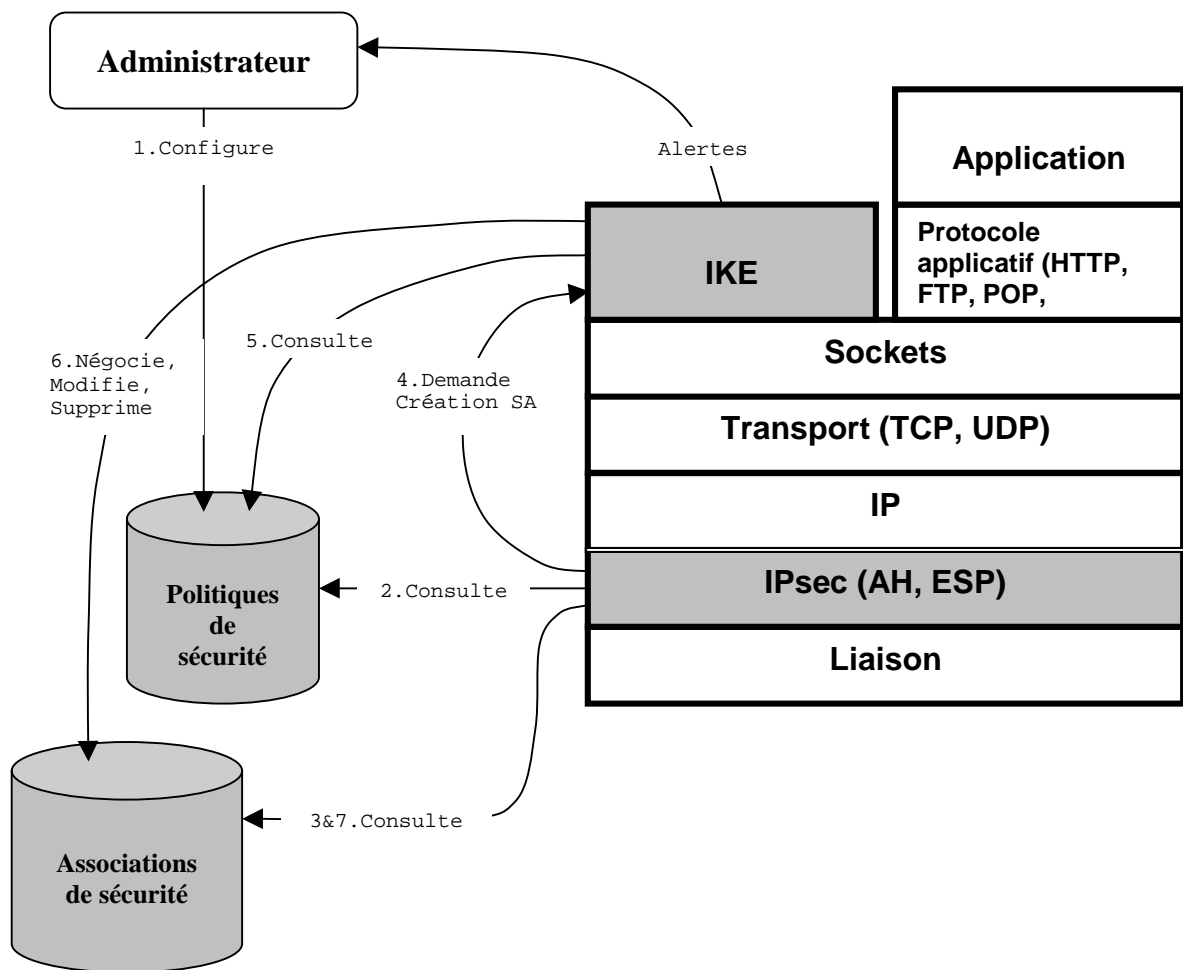


Figure III.1 : Composants d'IPsec et actions à l'émission de données

c. « Firewalls »

Qu'est-ce qu'un « firewall » ?

Un « firewall », appelé en français « pare-feu » ou « garde-barrière », prévient des dangers de l'Internet pouvant s'insinuer sur un réseau intranet.

Il a plusieurs facultés :

- ✓ Il restreint les gens à entrer par un point particulièrement contrôlé
- ✓ Il prévient des attaquants en les poussant vers les autres défenses
- ✓ Il restreint les gens à partir par un point particulièrement contrôlé

Un « firewall » est souvent installé à l'interconnexion d'un réseau intranet et de l'Internet. Ainsi tout le trafic venant ou partant vers l'Internet passe par le « firewall ». Cela permet de rendre sûr tout ce trafic.

Un « firewall » est un séparateur, un « restricteur », un analyseur. L'implantation physique d'un « firewall » varie d'un site à l'autre. Le plus souvent, un « firewall » est une combinaison de composants hardware – un routeur, un ordinateur « host », ou une combinaison de routeurs, stations, et réseaux avec un software approprié.

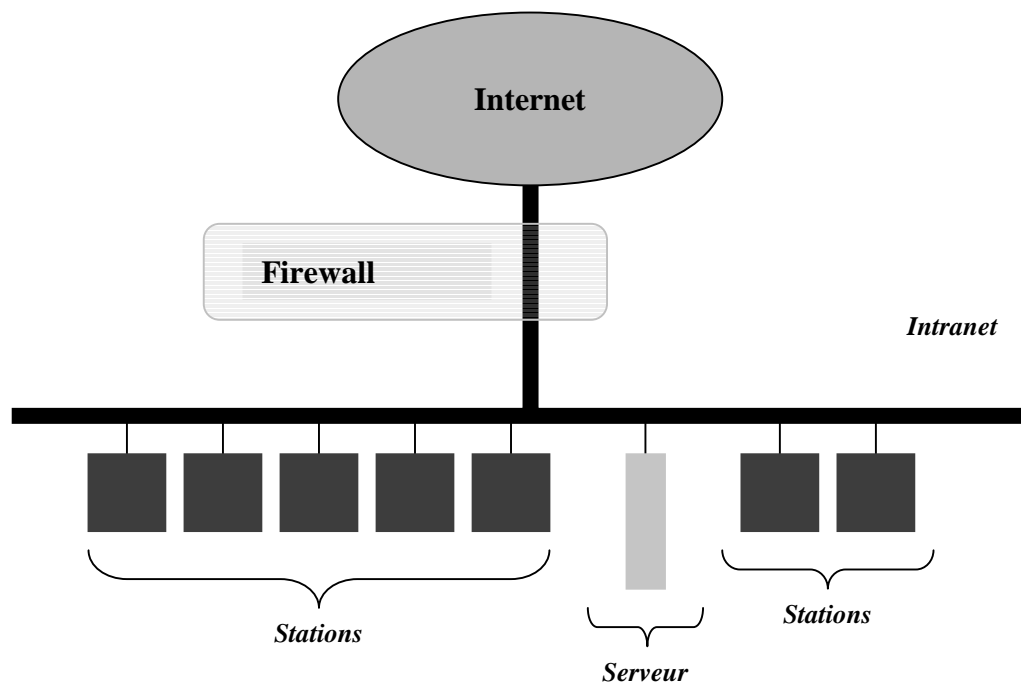


Figure III.2 : Le firewall, point d'interconnexion

Architecture de « firewall »

Voici deux approches utilisées pour construire un « firewall » :

- Filtrage de paquets
Les systèmes de filtrage de paquets routent les paquets entre les stations internes et externes, mais d'une manière sélective.
Le type de routeur utilisé dans un « firewall » filtreur de paquets est appelé « screening router »

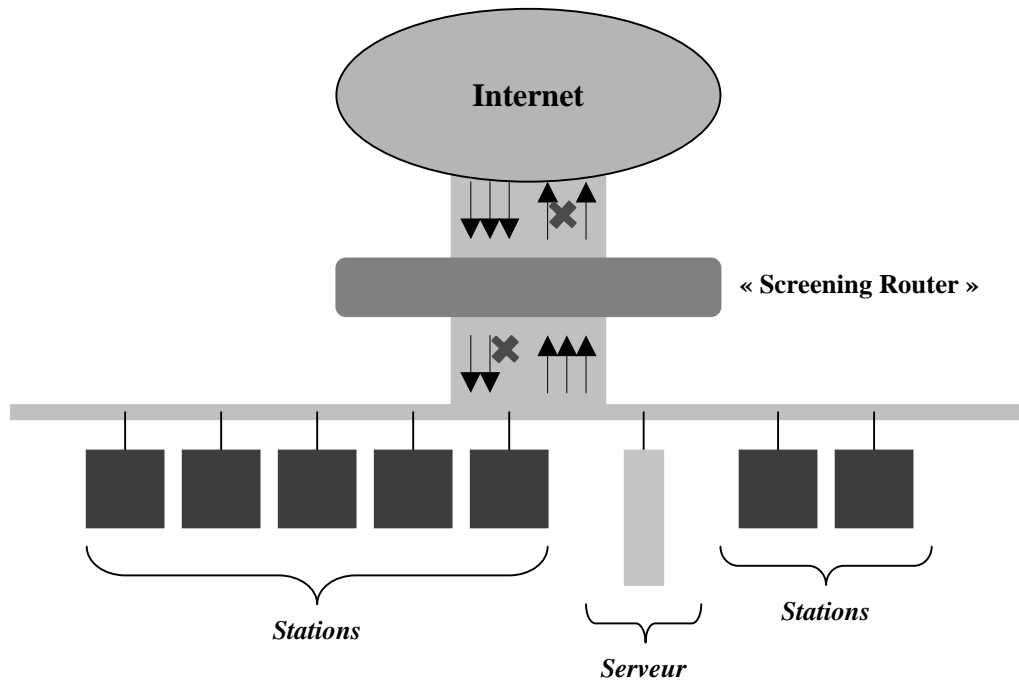


Figure III.3 : Le « Screening Router » route ou bloque les paquets, suivant la politique de sécurité

- Services de proxy
Les services proxy sont des applications ou des programmes de serveurs spécialisés qui tournent sur un « firewall ». Ces programmes prennent les requêtes des utilisateurs pour des services Internet (FTP, Telnet) et les transmettent, en accord avec la politique de sécurité, aux services appropriés. Les proxys fournissent des connexions de remplacement et agissent comme des passerelles pour les services. La transparence est le bénéfice majeur des services d'un proxy.

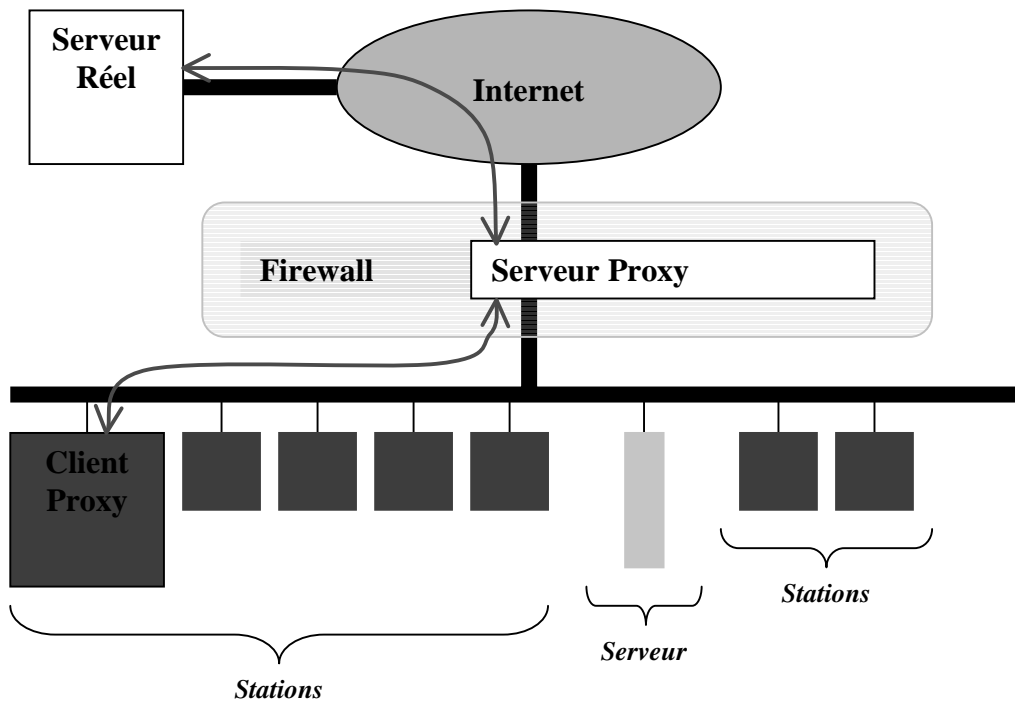


Figure III.4 : Utilisation des services d'un proxy

IV. La sécurité dans la mobilité

Après avoir présenté le nouveau protocole IPv6 ainsi que la mobilité dans ce protocole, après avoir présenté la sécurité dans les réseaux, nous allons voir quel doit être la sécurité appliquée à la mobilité dans IPv6.

a. Les options de Mobile IPv6

L'option « Mise à jour de l'association » décrite auparavant permet aux paquets destinés à un mobile d'être routés vers l'adresse temporaire du mobile. Toutefois, cette capacité de changer le routage des paquets peut être un point de vulnérabilité. Aussi, tout paquet contenant cette option doit être authentifié.

L'option « Acquiescement de l'association » nécessite aussi d'être authentifié. En effet, un attaquant peut, par exemple, tromper le mobile envoyant un acquiescement de l'agent mère falsifié.

Aucune authentification n'est nécessaire pour l'option « Demande de mise à jour de l'association » vu que cette option ne modifie, ni ne crée un nouvel état chez l'expéditeur ou le receveur. Par contre, l'aspect privé de cette option peut être sauvegardé grâce aux mécanismes de chiffrement d'IPsec ou à l'utilisation de « firewalls ».

Aucune authentification pour l'option « Adresse principale » n'est nécessaire, excepté le cas où l'en-tête IPv6 d'un paquet est authentifié, dans ce cas alors l'authentification doit aussi porter sur l'option « Adresse principale ».

L'utilisation de l'option « Adresse principale » autorise les paquets envoyés par un mobile à passer au travers de routeurs implantant le filtrage.

c. Interactions avec les « firewalls »

Le fait qu'un mobile se situe sur un réseau étranger visité ne doit pas faire contrarier la politique de sécurité mise en place par les « firewalls » sur ce réseau. En effet, un mobile peut être une faille dans le système de sécurité car il récupère une adresse temporaire de ce réseau et donc fait partie intégrante de ce réseau. Inversement, s'il n'est pas un attaquant potentiel, il doit pouvoir effectuer ses communications sans entraves. Tel est le cas pour les "Mises à jour de l'association" et les échanges de clés pour IPsec.

De plus, si son réseau mère a un ou plusieurs « firewalls », ceux-ci peuvent bloquer les paquets adressés à son agent mère ou des correspondants sur ce réseau. Du coup, la politique de sécurité de(s) « firewall(s) » du réseau doit être adaptée afin de permettre la communication entre le mobile et son agent mère (le problème le plus important) ou ses correspondants.

Enfin, un des principaux avantages des « firewalls » dans IPv4 est de bloquer les paquets contenant des en-têtes de routage. Hors, lors d'une communication entre un correspondant et un mobile, le correspondant, lorsqu'il possède une entrée pour le mobile dans son cache des associations, envoie un paquet avec un en-tête de routage de type routage contenant l'adresse du mobile dans son réseau mère. Du coup, la politique de sécurité des « firewalls » doit être modifiée afin de permettre ce type de communication. Cette modification entraînera alors une vulnérabilité sur les attaques par routage.

d. Généralités sur la sécurité liée à la mobilité

L'environnement informatique d'un mobile est très différent de celui des environnements informatiques habituels. Dans beaucoup de cas, les mobiles sont connectés à un réseau via des liens sans fil qui sont particulièrement vulnérables aux oreilles indiscretes et aux différentes attaques possibles.

S'il est nécessaire de cacher la position du mobile, celui-ci peut créer un tunnel avec son agent mère. Ainsi les paquets destinés aux correspondants du mobile paraîtront venir du sous-réseau mère du mobile, il sera donc plus difficile de connaître la position exacte du mobile.

Enfin lors de visites sur des réseaux étrangers, les communications du mobile sont plus à risque qu'une station fixe. En effet, elles doivent être protégées d'une attaque du réseau visité. De même, le réseau étranger visité doit pouvoir se protéger des attaques du mobile en visite.

e. Problèmes ouverts

La politique de sécurité standard, c'est à dire pour des réseaux de stations fixes, est mal adapté à la Mobilité IPv6. Pourtant faut-il relâcher la sécurité afin d'avoir plus de liberté d'action et vice-versa ? Que faut-il privilégier ou plutôt que faut-il modifier ?

De plus, la sécurité au niveau de la mobilité est liée à des échanges de clés si la gestion des clés s'effectue de manière dynamique. Or ces échanges sont vitaux lors de la mise en place d'IPsec ou plus simplement du chiffrement. Quelle politique faut-il adopter au niveau de la circulation de ces échanges ?

Enfin, les **Réseaux Virtuels Privés** (*Virtual Private Networks*), aujourd'hui de plus en plus utilisés, ne doivent pas interagir de manière néfaste avec les tunnels entre l'agent mère et le mobile. En effet, lorsqu'il y a besoin d'un tunnel entre l'agent mère et son mobile, et qu'il existe déjà un tunnel entre le routeur du réseau visité par le mobile et le réseau mère, que se passe-t-il ? L'agent mère doit-il créer un nouveau tunnel qui sera alors en concurrence avec le premier tunnel ou alors les paquets de correspondants tunnelés par l'agent mère passeront-ils par ce tunnel, possible soit-il ?

V. Projets

a. EURESCOM / P912 - PF / « Security for IP Mobility »



Informations Générales

Date de labellisation : Décembre 1998
Coordinateur du projet : Thierry Baritaud (France Télécom)
Superviseur du projet : Anastasius Gavras (Eurescom)
Partenaires : British Telecom
Deutsche Telekom
Norway Telecom
Telefonica España
France Télécom
Date de début de projet : Janvier 1999
Date de fin de projet : Décembre 1999

Objectifs

Les **principaux objectifs** de ce projet sont les suivants :

- Revue (orienté sécurité) des protocoles de gestion de la mobilité dans IP
- Analyse des protocoles de sécurité IPsec requis pour la mobilité
- Analyse des menaces liées à l'addition de services de mobilité sur IP et identification et évaluation des risques.
- Définition et proposition de services de sécurité devant être implémentés dans un environnement mobile comme contre-mesures aux menaces identifiées.

Résultats

Les **principaux résultats attendus** de ce projet sont les suivants:

- Soumettre des propositions de normalisation en collaboration avec les opérateurs de télécommunications.
- Examiner les normes existantes dans le domaine des protocoles de sécurité et de mobilité IP.
- Pousser les vendeurs à développer des systèmes plus flexibles et ouverts.
- Définir et fournir des guides sur la sécurité aux Opérateurs de Réseaux Publics pour introduire les services de mobilité sur Internet et accroître la politique de sécurité.

Délivrables

- **D1**
"Les conditions de sécurité pour l'introduction de la mobilité dans IP"
Juin 1999
- **D2**
"Directives de sécurité pour l'introduction de la mobilité dans l'Internet"
Novembre 1999

b. RNRT / « MobiSecV6 »



Informations Générales

Date de labellisation : Août 1998
Coordinateur du projet : Aimé Le Rouzic (Bull S.A.)
Superviseur du projet : Pierre Bouchara (Ministère de l'Industrie)
Partenaires : INRIA
Francis Dupont - Rocquencourt
Claude Castelluccia - Montbonnot
Ludovic Bellier - Montbonnot
Bull S.A.
Aimé Le Rouzic - Grenoble
Patrice Romand - Grenoble
Frédéric Soinne - Grenoble
Daniel Monges - Grenoble
Daniele Silvestre - Grenoble
Jean-Louis Clavaud - Grenoble
Jean-Paul Lauranson - Grenoble
France Télécom - CNET
Olivier Charles
Thierry Baritaud
Jean-Michel Combes
Date de début de projet : Septembre 1998
Date de fin de projet : Novembre 2000

Objectifs

Le **but de ce projet** est de permettre à des utilisateurs mobiles :

- de se déplacer dans l'Internet tout en conservant leurs connexions actives
- de disposer d'une adresse principale universelle permettant au mobile d'être accessible dans tout l'Internet
- de pouvoir accéder à des services et des données via les protocoles de mobilité avec la même sécurité qu'ils soient dans leur réseau d'origine ou à l'extérieur de ce dernier.

Les **principaux objectifs** de ce projet sont :

- d'étudier et d'implanter
 - les nouveaux protocoles de la gestion de la mobilité dans IPv6,
 - une gestion hiérarchique de la mobilité en fonction du type d'environnement: global ou local.
- d'étudier les protocoles de sécurité (IPSec) nécessaire à la mobilité.
- de faire évoluer la technique pare-feu dans un tel environnement mobile.
- d'expérimenter et évaluer les briques logicielles réalisées.

Rôle des partenaires

Les rôles des partenaires sont les suivants :

- Le rôle de l'Inria dans ce projet est de contribuer à la spécification du protocole de gestion de la mobilité au sein de l'IETF (*Internet Engineering Task Force*) en proposant notamment une gestion hiérarchique de la mobilité pour mieux répondre aux besoins de performances et de sécurité.
L'INRIA participe à ce projet pour réaliser une implantation sur le logiciel libre FreeBSD afin de valider le protocole MobileIPv6 de l'IETF et de proposer une gestion hiérarchique de la mobilité à l'IETF pour standardisation.
- Le rôle de Bull est de proposer les services offerts par ces protocoles afin d'avoir une offre différenciée sur ses serveurs ESCALA^r et de valoriser le pare-feu SecurWare^r/Netwall^r que Bull commercialise en gérant IPv6 et de la mobilité.
Bull travaillera sur les implantations de MobileIPv6 dans AIX^r et complètera son pare-feu SecurWare/NetWall pour le contrôle des paquets IPv6 et ceux liés aux protocoles de la mobilité.
- Le rôle de France Télécom (CNET - Branche Développement) est de capitaliser un savoir-faire autour de ces nouvelles technologies (protocoles et produits) afin de permettre à l'opérateur d'être en mesure de proposer rapidement des services innovants dans son offre commerciale (Entreprises et Grand Public) et une évolution des infrastructures IP sous-jacentes.
France Télécom de son côté est intéressé par l'intégration de toutes briques développées dans le projet et réalisera un démonstrateur sur une plate-forme mettant en oeuvre les différentes réalisations en utilisant des réseaux fixes et mobiles (GSM, WaveLAN).

Résultats

Les résultats du projet seront valorisés par des publications scientifiques dans les revues et les conférences internationales et par la réalisation d'un démonstrateur qui permettra de mettre en évidence les avantages et le bon fonctionnement des résultats du projet.

Ce démonstrateur se composera de briques logicielles (SecurWare/NetWall) et de serveurs Bull (ESCALA) d'ordinateurs personnels portables avec un système d'exploitation FreeBSD fourni par l'INRIA ainsi que de réseaux filaires et sans fil mis en place par le CNET.

Selon les résultats de cette expérimentation :

- L'INRIA contribuera à l'amélioration du protocole MobileIPv6 et proposera au groupe de travail de l'IETF un document sur la gestion hiérarchique permettant à l'INRIA de participer encore plus au développement des protocoles Nouvelle Génération. Cela avait déjà été le cas avec IPv6 quand l'INRIA avait fourni une des premières souches implantant le protocole IPv6.
- Bull pourra constituer une offre différenciée sur ses serveurs en gérant la mobilité MobileIPv6 après avoir été un des premiers constructeurs à commercialiser IPv6.
Bull pourra être aussi en mesure de valoriser son pare-feu SecurWare/Netwall en intégrant IPv6 et en gérant la mobilité après avoir été un des premiers constructeurs à disposer d'une offre sécurité complète.
L'entité de Bull SecurWare offre déjà à ses clients un catalogue de solutions logicielles relatives à la sécurité des réseaux, SecurWare/NetWall étant la solution pare-feu. Ce pare-feu "avancé" conjugue le filtrage dynamique IP avec des relais applicatifs (proxies). Cette solution pare-feu est déjà opérationnelle chez beaucoup d'utilisateurs.
- France-Télécom-CNET pourra offrir aux entreprises des services et une infrastructure supportant la mobilité IP tout en leur garantissant la sécurité des connexions sur leurs réseaux d'entreprise.

Délivrables

- **SP1**
Le sous-projet 1 confié entièrement à l'INRIA a pour but d'étudier et d'implanter les protocoles IETF MobileIPv6 et IPSec dans le système d'exploitation FreeBSD.
- **SP2**
Le sous-projet 2 confié entièrement à Bull a pour but de gérer l'ensemble du projet MobiSecV6, d'étudier et d'implanter les protocoles IETF MobileIPv6 dans AIX en se référant à l'étude du sous-projet 1, d'implanter les protocoles de gestion hiérarchique définis dans le sous-projet 3, d'étendre IPSec dans le système d'exploitation AIX.
- **SP3**
Le sous-projet 3 confié entièrement à l'INRIA a pour but de spécifier et d'implanter un protocole de gestion hiérarchique de la mobilité dans FreeBSD compatibles avec Mobile IPv6 développé dans le sous projet 1.
- **SP4**
Le sous-projet 4 confié entièrement à Bull a pour but d'intégrer les protocoles IPv6 et les protocoles de gestion de la mobilité dans le pare-feu à partir du produit Bull SecurWare/NetWall.
- **SP5**
Le sous-projet 5 confié entièrement au CNET a pour but d'expérimenter et d'évaluer les briques réalisées par les autres sous-projets 1,2,3,4 par la réalisation d'un démonstrateur en utilisant des réseaux fixes et mobiles. Les portables utilisés auront FreeBSD comme système d'exploitation. Les stations fixes auront AIX et FreeBSD comme système d'exploitation.

VI. Objectifs & Résultats du Projet de Fin d'Etudes

a. Projet Eurescom

Le but de ma participation à ce projet était double :

- Sur le plan technique, étudier les aspects de la sécurité dans la mobilité IPv6 d'une manière théorique.
- Sur le plan organisation, voir la complexité de la mise en place et gestion d'un projet de taille européenne.

Les objectifs initiaux étaient :

- Etude d'IPv6.
- Etude de la mobilité IPv6.
- Etude de la sécurité (Attaques, IPsec).
- Synthèse des parades aux risques en sécurité mis en évidence dans l'analyse des scénarios liés à la mobilité fournis par les partenaires du projet (**D1**).
- Rapport décrivant cette étude (**D1**).

Les objectifs ont été modifiés de la façon suivante :

- Etude d'IPv6.
- Etude de la mobilité IPv6.
- Etude de la sécurité.
- Etude interne des parades aux risques en sécurité liés à la mobilité IPv6.

Les raisons des modifications des objectifs :

- Retard dans la remise des livrables des partenaires européens.
- Prise de temps beaucoup plus importante que prévue sur le projet RNRT (voir ci-dessous).

Les résultats :

- Les études sur IPv6, la mobilité IPv6 et la sécurité ont été réalisées tout au long de ce projet.
- La synthèse des parades aux risques en sécurité n'a pas atteint son terme. Nous avons fourni une liste de scénarios décrivant les principales situations rencontrées lors de l'utilisation de Mobile IPv6. Or sur la base de ces scénarios, chaque partenaire devait fournir une étude des risques qu'il jugeait critique de son point de vue. Un décalage dans le planning s'étant produit, la synthèse n'a pu être réalisée.

b. Projet RNRT

Le but de ce projet était double aussi :

- Sur le plan technique, voir de près les problèmes liés à l'implantation du nouveau protocole IPv6 et manipuler concrètement la mobilité IPv6 ainsi que la sécurité.
- Sur le plan organisation, organiser son temps entre l'étude et l'expérimentation.

Les objectifs initiaux étaient :

- Etude d'IPv6.
- Etude de la mobilité IPv6.
- Etude de la sécurité (IPsec, Firewalls).
- Réalisation du démonstrateur Mobile IPv6 (**SP5**).
- Test des sources Mobile IPv6 FreeBSD livrée par SP1 (**SP5**).
- Rédaction d'un document de description du démonstrateur Mobile IPv6+IPSec (**SP5**).

Les objectifs ont été modifiés de la façon suivante :

- Etude d'IPv6.
- Etude de la mobilité IPv6.
- Etude de la sécurité (IPsec, Firewalls).
- Réalisation du démonstrateur Mobile IPv6 (**SP5**).
- Test des sources Mobile IPv6 FreeBSD livrée par le sous-projet 1 (**SP5**).

Les raisons des modifications des objectifs :

- Retard dans la remise des sources de SP1
- Présence de bugs dans les sources remises
- Absence de documentations des implémentations fournies
- Non implémentation de certaines fonctionnalités (en débat que cela soit au niveau de la normalisation, que des implémenteurs)

Les résultats atteints :

- Les études sur IPv6, la mobilité IPv6 et la sécurité ont été réalisées tout au long de ce projet.
- Le démonstrateur a été réalisé pour la première campagne de tests liée à la mobilité IPv6 (**SP5**).
- La campagne de tests liée à la mobilité IPv6 a été réalisée ainsi que le Rapport de Validation (**SP5**).

c. Veille technologique

Les buts de cette partie du projet de fin d'études sont :

- Se familiariser avec le monde de la sécurité informatique

Les objectifs initiaux étaient :

- Connaissance des besoins en matière de sécurité
- Connaissance des produits sur le marché de la sécurité
- Connaissance des mécanismes d'attaques en sécurité
- Connaissance des mécanismes de parades en sécurité

Les résultats atteints sont les suivants :

- Meilleure connaissance des besoins et des produits en matière de sécurité
- Compétences théoriques des mécanismes d'attaques et de parades en sécurité

VII. Bilan du Projet de Fin d'Etudes

a. Etudes théoriques

Les études qui ont porté sur IPv6, la mobilité IPv6 ainsi que sur la sécurité se sont déroulés tout au long de la période du projet de fin d'études. La synthèse est décrite au début de ce rapport.

L'étude liée au projet Eurescom n'a pu atteindre son terme par manque de temps.

Les connaissances sur le monde de la sécurité ne font pas lieu de parties dans ce rapport mais servent plutôt de formation pour la suite des projets rencontrés.

b. Réalisations techniques

Sur le plan technique, la principale tâche a été de monter une plate-forme expérimentale IPv6. Cela a consisté à l'installation, la configuration, la mise en réseau, l'administration, et l'exploitation de cette plate-forme. Celle-ci est constituée actuellement de 10 machines et ne fonctionne que sous IPv6. L'architecture et la composition de la plate-forme sont en Annexes. Voici l'historique de cette plate-forme :

Dans un premier temps, la plate-forme ne contenait que 3 machines FreeBSD : 2 PC "host" et un PC configuré en routeur, le tout étant sous IPv6.

Puis, ont été intégrées dans la plate-forme 3 machines AIX et 4 machines FreeBSD. Les Power PC AIX ont été configuré en routeur et les machines FreeBSD en "host".

Ensuite, la mobilité IPv6 a été implantée dans ces machines. Il a fallu attendre début juin pour avoir une souche "sans bugs majeurs" de Mobile IPv6. De plus, la version actuelle ne contient pas toutes les fonctionnalités (détection de mouvement et découverte automatique des correspondants : points encore en cours de débat dans les communautés scientifiques). En fait, la majeure partie du temps alloué à ce projet a été gaspillée à "tester" les versions successives de Mobile IPv6, ce qui était contraire au fait que nous devions recevoir une seule version sans bugs.

Entre deux installations d'une nouvelle source Mobile IPv6, des services ont été configurés dans la plate-forme: un serveur FTP, un serveur WWW Apache, un client WWW Lynx, un serveur PPP et un serveur DNS. Malheureusement, un problème technique lié à la connectique au sein du CNET à Issy, empêche momentanément d'avoir une connexion avec le 6Bone, ce qui entraîne un problème de mise en service du serveur DNS. De plus, le serveur PPP ne fonctionne pas actuellement en raison de problèmes liés à la version IPv6.

Dans un deuxième temps, la véritable campagne de tests portant sur la Mobilité IPv6, prévue début Mai, n'a commencé que début juin. De plus, le rapport de Validation de cette campagne de tests est à délivrer au Ministère de l'Industrie pour le 15 Juin.

Enfin dans un dernier temps, une présentation ainsi qu'une démonstration de la mobilité IPv6 doit être réalisé devant des représentants du Ministère de l'Industrie le 17 Juin.

Le planning effectué se situe en Annexes.

c. Compétences humaines

Ce projet m'a apporter les techniques de conduite de réunion, de gestion de projet, de rédaction de rapport aux travers des deux projets rencontrés.

De plus, il m'a initié au métier d'un opérateur, à savoir ses besoins et les services qu'il désirait mettre sur le marché.

De plus, ce projet m'a permis d'apprendre à gérer les relations entre différents partenaires. En effet, que cela soit avec le projet Eurescom, qui comporte 4 autres partenaires, ou le projet RNRT, qui lui comporte 2 autres partenaires, la dépendance entre ces partenaires sur l'évolution du projet est importante.

Enfin, le fait de travailler en équipe dans le service m'a permis d'apprendre à écouter et à discuter avec mon entourage.

d. Suites envisagées

Dans un futur proche :

Pour le projet RNRT, la plate-forme expérimentale, après mon départ, doit intégrer un firewall selon l'analyse faite dans la partie "La sécurité dans la mobilité", ainsi que de nouvelles stations mais aussi une implémentation d'IPsec. De plus, normalement, une nouvelle version de Mobile IPv6 comportant toutes les fonctionnalités, doit être implantée. Le but final de cette plate-forme étant de tester Mobile IPv6 disposant de services de sécurité conséquents.

Pour le projet Eurescom, une nouvelle réunion sera organisée entre les divers partenaires afin de mettre leurs travaux en commun, de consolider les résultats dans un document et d'attribuer les nouvelles tâches.

Dans futur un plus lointain:

La mobilité est un nouveau secteur économique à exploiter. En effet, un opérateur comme France Télécom pourrait offrir un nouveau type de service : il pourrait héberger les agents mères, distribuer des adresses permanentes en faisant payer le service de mobilité. En effet, la gestion des mobiles (surtout au niveau sécurité) est quelque chose de complexe et demandant beaucoup de moyens pour un nombre important de mobiles.

Conclusion

Au bout de quatre mois de projet et avec un peu de recul, j'ai pu voir que le temps dans ce genre de projets est compté. D'un côté, par le fait d'une interdépendance entre les partenaires. D'un autre côté, par les limites de temps imposé par les engagements contractuels que peut avoir un industriel.

Ce projet de fin d'études m'a permis de découvrir une vision différente du monde des télécommunications. En effet, je me suis trouvé au cœur de projets assez impressionnants. L'un porte sur la normalisation d'une technologie qui touchera des millions de personnes dans le futur. Et l'autre porte sur une mise en œuvre d'une technologie que nous trouverons bientôt sur le marché des télécommunications. De plus, ces deux projets sont d'une dimension impressionnante pour un jeune étudiant (Budget, « manpower », matériel, etc.).

A côté de cela, j'ai pu découvrir la véritable face de la sécurité au niveau des réseaux de télécommunications. En effet, étant entouré d'ingénieurs travaillant sur d'autres projets, ils m'ont enseigné d'autres besoins que ceux étudiés dans ce rapport. J'ai pu voir le rôle et la responsabilité que peut avoir un ingénieur sécurité réseaux (audit de réseaux ou exploitation engageant la sécurité du réseau commercial ou technique de France Télécom).

Je tiens à remercier tout le département de m'avoir accueilli chaleureusement et de m'avoir intégrer rapidement dans le groupe. Je remercie tout particulièrement Olivier CHARLES de m'avoir fait confiance (même s'il ne m'égalera jamais au flipper...) tout au long de ce projet de fin d'études.

Bibliographie

IPv6

- IPv6, Théorie et Pratique
Gizèle Cizault
Ed. O'Reilly
- <http://phoebe.urec.fr/G6/>
Site Web du G6
Souches IPv6 & Applications
- <http://phoebe.urec.fr/G6/G6Rech.html>
Compte rendus des réunions du G6
- <http://playground.sun.com/ipng/>
Site Web de Sun sur IPv6
Liens vers site de l'IETF et du 6Bone
- <http://playground.sun.com/ipng/specs/standards.html>
Spécifications d'IPv6
- <http://www.ipv6.org/>
Site Web Officiel d'IPv6
- <http://www.join.uni-muenster.de/JOIN/ipv6/texte-englisch/>
Site Web du G6 « hollandais » - tests, implantation,...
- <http://www.v6.wide.ad.jp/>
Page Web du G6 « japonais » – Explication du passage de SwIPe à IPSec
- <http://www.kame.net/>
Site Web d'un projet portant sur IPSec/IPv6 sur BSD
- http://www.rennes.enst-bretagne.fr/Rapports/IPngMM/IPng_ToC.html
Rapport de Mastère sur IPng
- <http://www.research.microsoft.com/msripv6/>
Site Web de Microsoft Research sur IPv6
- <http://www.terra.net/ipv6/>
IPv6 sur Linux

MobileIP

- draft-ietf-mobileip-ipv6-07
David B. Johnson & Charles Perkins
1998
Statut : Draft
- Mobile IP, the Internet Unplugged
James D. Solomon
Ed. Prantice Hall
- Mobile IP, Design Principles and Practices
Charles E. Perkins
Ed. Addison Wesley
- <http://hplbwww.hpl.hp.com/people/jt/MobileIP/known.html>
Problèmes rencontrés avec Mobile IP
- http://www.cis.ohio-state.edu/~jain/refs/wir_refs.htm
Site avec des références sur Mobilite IP
- <http://www.computer.org/internet/v2n1/nomad.htm>
Article - Comment la mobilité affectera la couche de protocoles
- <http://www.it.kth.se/~d91-fta/exjobb/exjobb.html>
Sujet de Thèse sur MobileIP
- http://www.net-tech.bbn.com/moips/moips_project_sum.html
Projet de sécurisation de MobileIP

Sécurité

- Security Architecture for the Internet Protocol
RFC 2401
S. Kent & R. Atkinson
Novembre 1998
Statut : Proposed Standard
- IP Authentication Header
RFC 2402
S. Kent & R. Atkinson
Novembre 1998
Statut : Proposed Standard
- IP Encapsulating Security Payload
RFC 2406
S. Kent & R. Atkinson
Novembre 1998
Statut : Proposed Standard
- La sécurité des communications sur les réseaux IP
M. Laurent-Maknavičius
Paris 1999
Conférence du G6
- Internet and Intranet Security
Rolf Oppliger
Ed. Artech House Publishers
- Building Internet FIREWALLS
D. Brent Chapman
Elizabeth D. Zwicky
Ed. O'Reilly
- Internet & TCP/IP Network Security - Securing Protocols and Applications
Uday O. Pabrai
Vijay K. Gurbani
Ed. McGraw-Hill
- Practical Unix & Internet Security
Simson Garfinkel
Gene Spafford
Ed. O'Reilly
- <http://idm.internet.com/foundation/tunneling.shtml>
Étude du tunneling – Comparaison entre PPTP (Microsoft) et IPsec
- <http://ipsec-wit.antd.nist.gov/>
Plate-Forme de tests d'IPsec et de IKE
- <http://ipsec-wit.antd.nist.gov/newipsecdoc/pluto.html>
Description d'IKE
- <http://snad.ncsl.nist.gov/cerberus/>
Description d'IPsec sur Linux
- <http://www.clusif.asso.fr/>
Page Web du CLUSIF
- <http://www.entrust.com/>
Page d'Entrust
Description d'une PKI
- <http://www.hsc.fr/veille/ipsec/index.html.fr>
Description d'IPsec et de la gestion des clés
- <http://www.merit.edu/~nanog/mtg-9806/ppt/fergeson/index.htm>
Description d'un VPN
- <http://www.ossir.org/>
Page Web de l'OSSIR
- <http://www.vpnc.org/ietf-ipsec/>
IPsec mailing list

Etudes des failles de sécurité des protocoles de mobilité dans l'Internet Nouvelle Génération

Projet de Fin d'Etudes

Rapport de Soutenance

- <http://www2.s390.ibm.com/products/mvs/firewall/>
Page Web d'IBM
IPSec & Firewall

Projets

- <http://www.eurescom.de/public/projects/P900-series/P912/p912.htm>
Site officiel du projet EURESCOM « Security for IP Mobility »
- <http://www.telecom.gouv.fr/rnrt/>
Site officiel du projet RNRT « MobiSec V6 »

FreeBSD

- The Complete FreeBSD
Greg Lehey
Ed. Walnut Creek CDROM Books

AIX

- AIX Version 4 – System and Administration Guide
James DeRoest
Ed. McGraw-Hill

Annexes

Planning

		Mars																						
Tâches		1	2	3	4	5	8	9	10	11	12	15	16	17	18	19	22	23	24	25	26	29	30	31
Etude IPv6		◆	◆				◆	◆	◆	◆	◆						◆	◆						
Etude Mobilité							◆	◆	◆	◆	◆									◆	◆	◆	◆	
Etude Sécurité							◆	◆	◆	◆	◆									◆	◆	◆	◆	
Réseau FreeBSD	Installation FreeBSD	◆	◆	◆	◆	◆	◆	◆	◆															
	Installation IPv6			◆	◆	◆	◆	◆	◆	◆														
	Upgrade IPv6																							
Réseau AIX	Installation AIX 4.3.1											◆	◆											
	Upgrade AIX 4.3.2																◆	◆		◆	◆			
	Upgrade AIX																				◆	◆	◆	
Plate-Forme IPv6	Conception																							
	Installation																							
Campagne de Tests																								
Rapports de Validation																								
Veille Technologique		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			◆	◆	◆		◆	◆	◆	◆	◆
Rapport de Pré Soutenance							◆	◆	◆	◆	◆	◆	◆			◆	◆	◆						
Rapport de Soutenance																								

◆ planning effectif

Etudes des failles de sécurité des protocoles de mobilité dans l'Internet Nouvelle Génération

Projet de Fin d'Etudes

Rapport de Soutenance

		Avril																						
Tâches		1	2	5	6	7	8	9	12	13	14	15	16	19	20	21	22	23	26	27	28	29	30	
Etude IPv6																								
Etude Mobilité																								
Etude Sécurité																								
Réseau FreeBSD	Installation FreeBSD																							
	Installation IPv6																							
Réseau AIX	Upgrade IPv6																			◆	◆	◆	◆	◆
	Installation AIX 4.3.1																							
Plate-Forme IPv6	Upgrade AIX 4.3.2																							
	Upgrade AIX	◆	◆		◆	◆	◆																	
Plate-Forme IPv6									◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	
Campagne de Tests																								
Rappports de Validation																								
Veille Technologique		◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	
Rapport de Pré Soutenance																								
Rapport de Soutenance																								

◆ planning effectif

Etudes des failles de sécurité des protocoles de mobilité dans l'Internet Nouvelle Génération

Projet de Fin d'Etudes

Rapport de Soutenance

		Mai																				
Tâches		3	4	5	6	7	10	11	12	13	14	17	18	19	20	21	24	25	26	27	28	31
Etude IPv6																						
Etude Mobilité																						
Etude Sécurité																						
Réseau FreeBSD	Installation FreeBSD																					
	Installation IPv6																					
	Upgrade IPv6	◆	◆	◆	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆
Réseau AIX	Installation AIX 4.3.1																					
	Upgrade AIX 4.3.2																					
	Upgrade AIX																					◆
Plate-Forme IPv6	Conception																					
	Installation	◆	◆	◆	◆	◆	◆	◆	◆		◆	◆	◆									
Campagne de Tests																						
Rapports de Validation																						
Veille Technologique		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
Rapport de Pré Soutenance																						
Rapport de Soutenance																						

◆ planning effectif

Etudes des failles de sécurité des protocoles de mobilité dans l'Internet Nouvelle Génération

Projet de Fin d'Etudes

Rapport de Soutenance

		Juin																					
Tâches		1	2	3	4	7	8	9	10	11	14	15	16	17	18	21	22	23	24	25	28	29	30
Etude IPv6																							
Etude Mobilité																							
Etude Sécurité																							
Réseau FreeBSD	Installation FreeBSD																						
	Installation IPv6																						
Réseau AIX	Upgrade IPv6	◆																					
	Installation AIX 4.3.1																						
	Upgrade AIX 4.3.2																						
Plate-Forme IPv6	Upgrade AIX	◆						◆															
	Conception																						
	Installation																						
Campagne de Tests					◆	◆	◆	◆	◆	◆	◆	◆	◆										
Rapports de Validation					◆	◆	◆	◆	◆	◆	◆	◆											
Veille Technologique		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Rapport de Pré Soutenance																							
Rapport de Soutenance		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆												

DEMO RNRJT

SOUTENANCE

◆ planning effectif

Schéma de la plate-forme IPv6 expérimentale du CNET-DTL/SSR/SII

09/06/1999

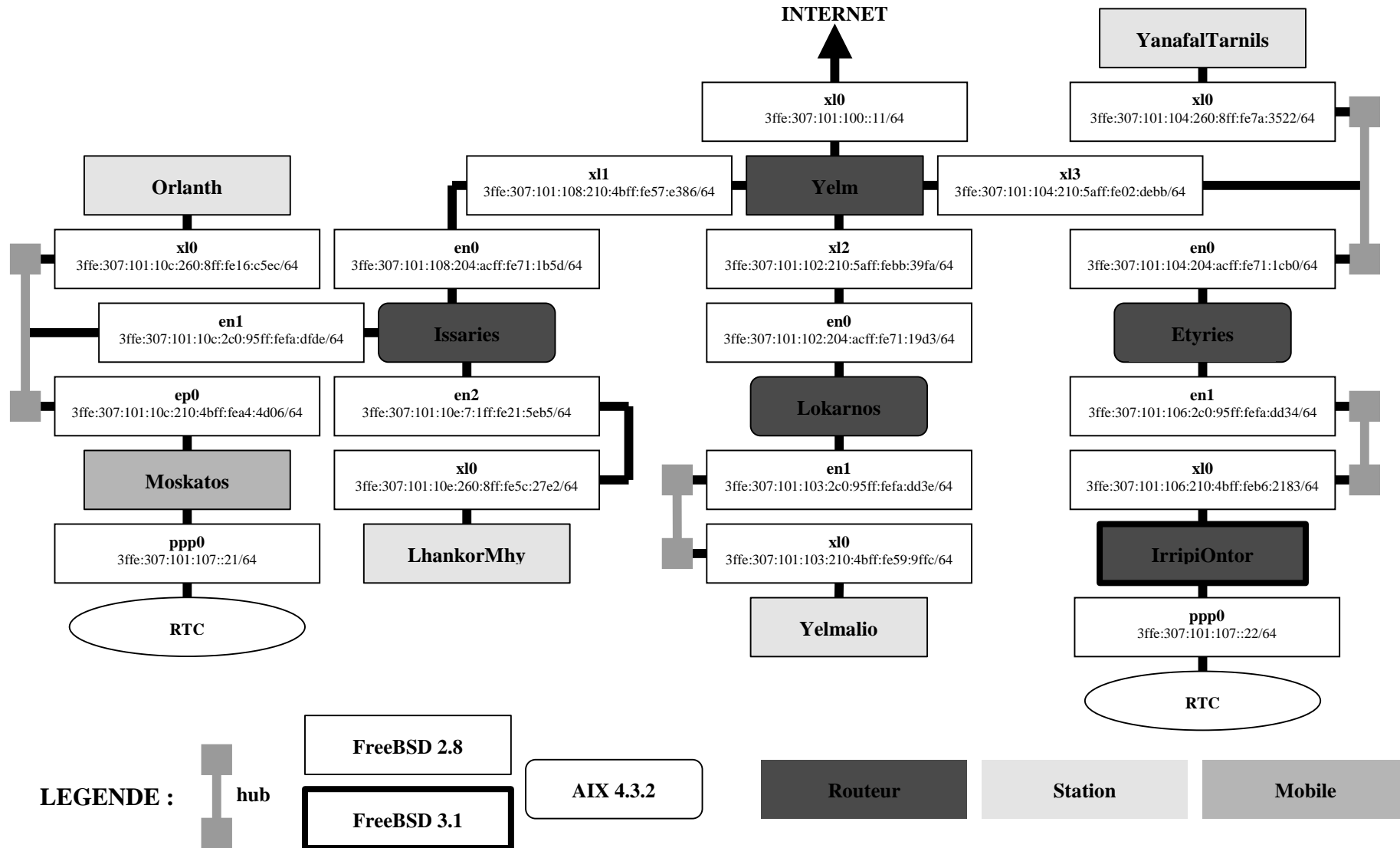
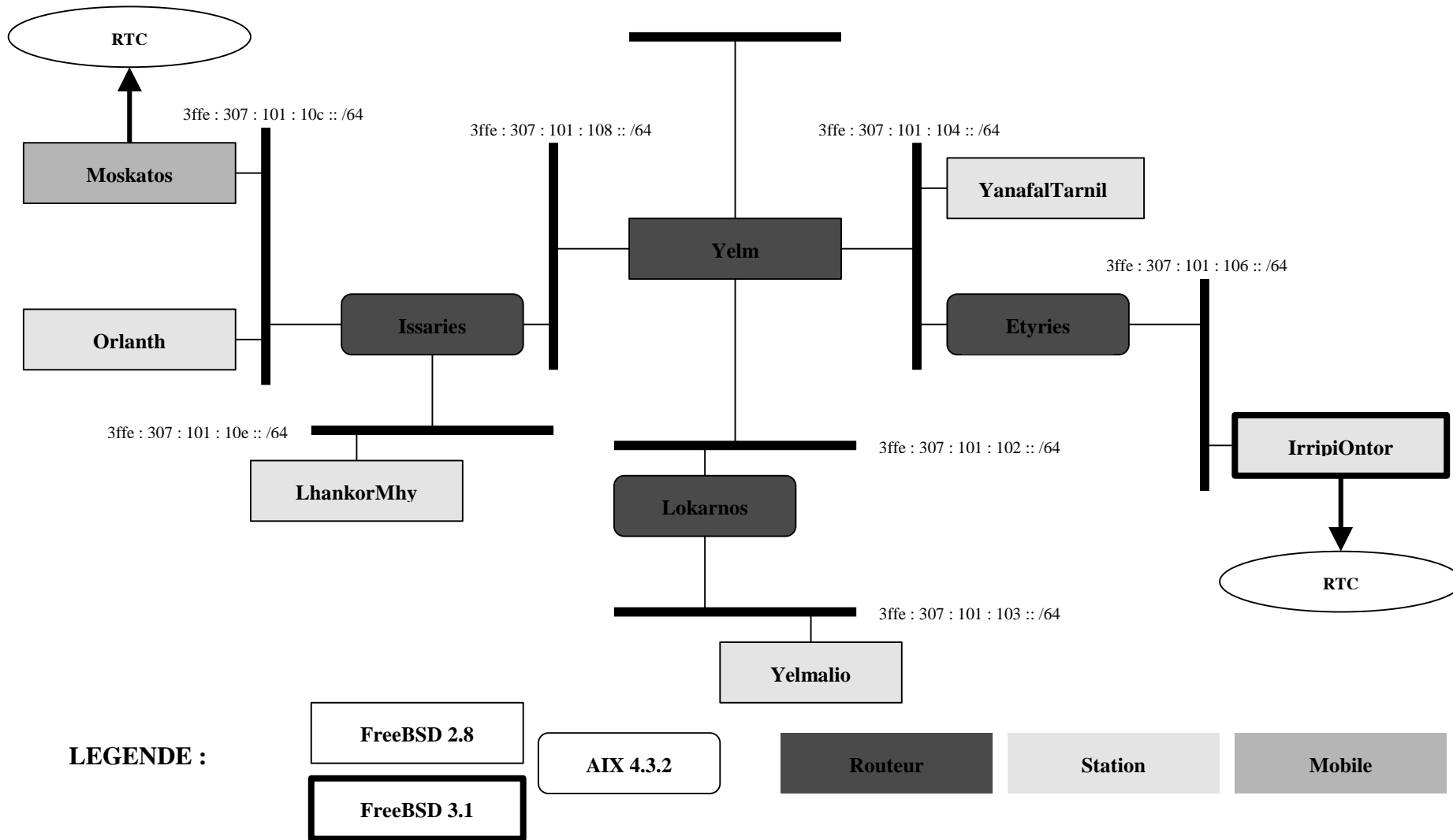


Schéma simplifié de la plate-forme IPv6 expérimentale du CNET-DTL/SSR/SII

03/06/1999



Description de la plate-forme expérimentale IPv6 du CNET/DTL/SSR/SII

MH	<i>Mobile Home</i>	Réseau Mère
CN	<i>Correspondent Node</i>	Nœud Correspondant
HA	<i>Home Agent</i>	Agent Mère
RTC	Réseau Téléphonique Communauté	

La plate-forme expérimentale IPv6 est constituée de 10 stations :

- 3 machines AIX 4.3.2

Nom	Type	Rôle réseau	Rôle mobilité	Nb Interfaces	Applicatifs
Etyries	Escala S100	Routeur	HA/CN	2	
Issaries	Escala S100	Routeur	HA/CN	3	
Lokarnos	Escala S100	Routeur	HA/CN	2	Serveur Web

- 6 machines FreeBSD 2.2.8 (+ PAO pour le mobile)

Nom	Type	Rôle réseau	Rôle mobilité	Nb Interfaces	Applicatifs
Yelm	Gateway G6 400	Routeur	HA/CN	4	
LhankorMhy	Gateway G6 300	Host	CN	1	Serveur DNS
Orlanth	Gateway G6 300	Host	CN	1	
Yelmalio	Gateway G6 300	Host	CN	1	
YanafalTarnils	Gateway G6 333	Host	CN	1	
Moskatos	Compaq A. 3500	Host mobile	MH	1 + Modem	

- 1 machine FreeBSD 3.1

Nom	Type	Rôle réseau	Rôle mobilité	Nb Interfaces	Applicatifs
IrripiOntor	Gateway G6 400	Passerelle Ethernet -RTC	HA/CN	1 + Modem	Serveur PPP Serveur FTP