



# VOIP

Présenté par : Emmanuel NGASSA  
Supervisé par : Mr Florent Nolot

## Plan de la présentation

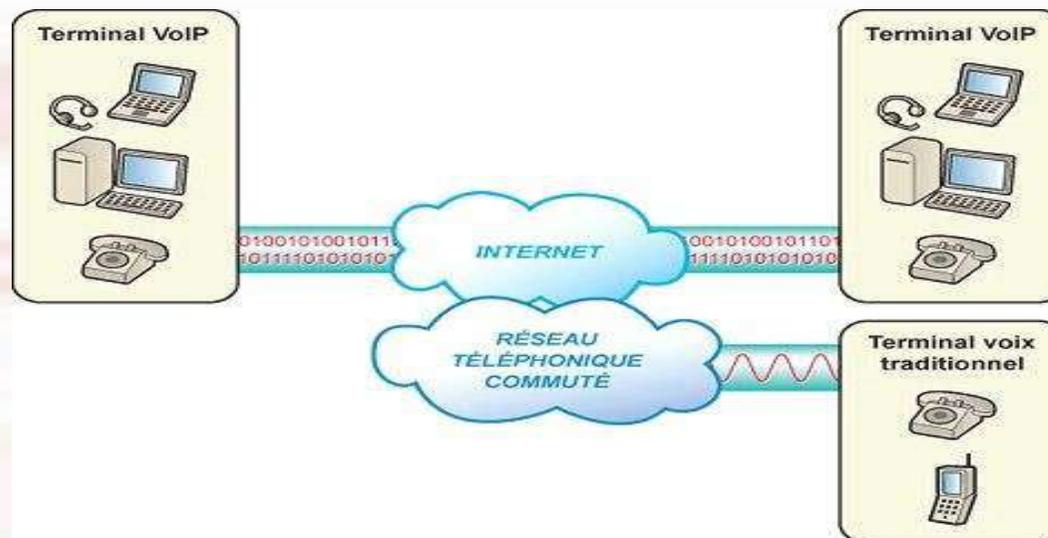
- Fonctionnement de la VoIP
- Les Failles/Attaques de La VoIP
- Sécurisation d'un Réseau VoIP
- Outils de Test de Vulnérabilité
- Conclusion

## Fonctionnement de la VoIP

- Description
- Architecture de la VoIP
- Les Protocoles de la VoIP

# Fonctionnement de la voip

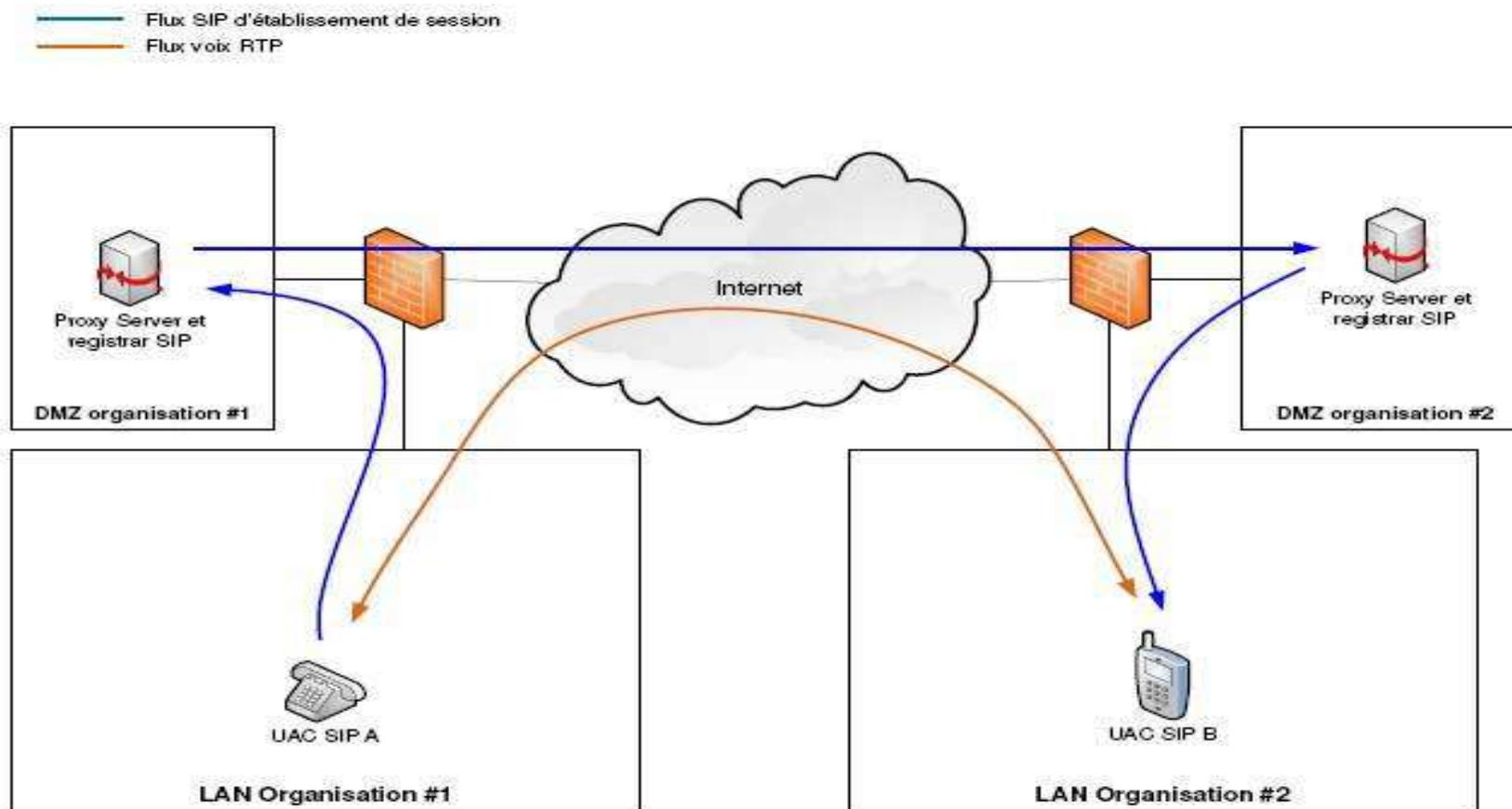
## Description



Étape	Description
1	Le son capté par un terminal VoIP est numérisé.
2	Les données sont transmises par le réseau de 2 manières, selon le type de terminal du destinataire : <ul style="list-style-type: none"><li>• si le destinataire dispose d'un terminal de VoIP, la transmission des données se fait par Internet ;</li><li>• si le destinataire possède un terminal traditionnel, une passerelle entre Internet et le réseau téléphonique commuté classique permet au destinataire de l'appel d'entendre et de répondre à son interlocuteur.</li></ul>
3	Le destinataire entend le message émis par l'émetteur sur son terminal.

# Fonctionnement de la voip

## Architecture d'un Réseau voip



# Les principaux protocoles

Les principaux protocoles permettant l'établissement de connexion

- ◆ H.323
- ◆ SIP
- ◆ IAX (Asterisk)
- ◆ MGCP (Media Gateway control Protocol)
- ◆ SCCP (propriétaire Cisco Systems)

Les principaux protocoles permettant le transport de la voix

- ◆ RTP
- ◆ RTCP

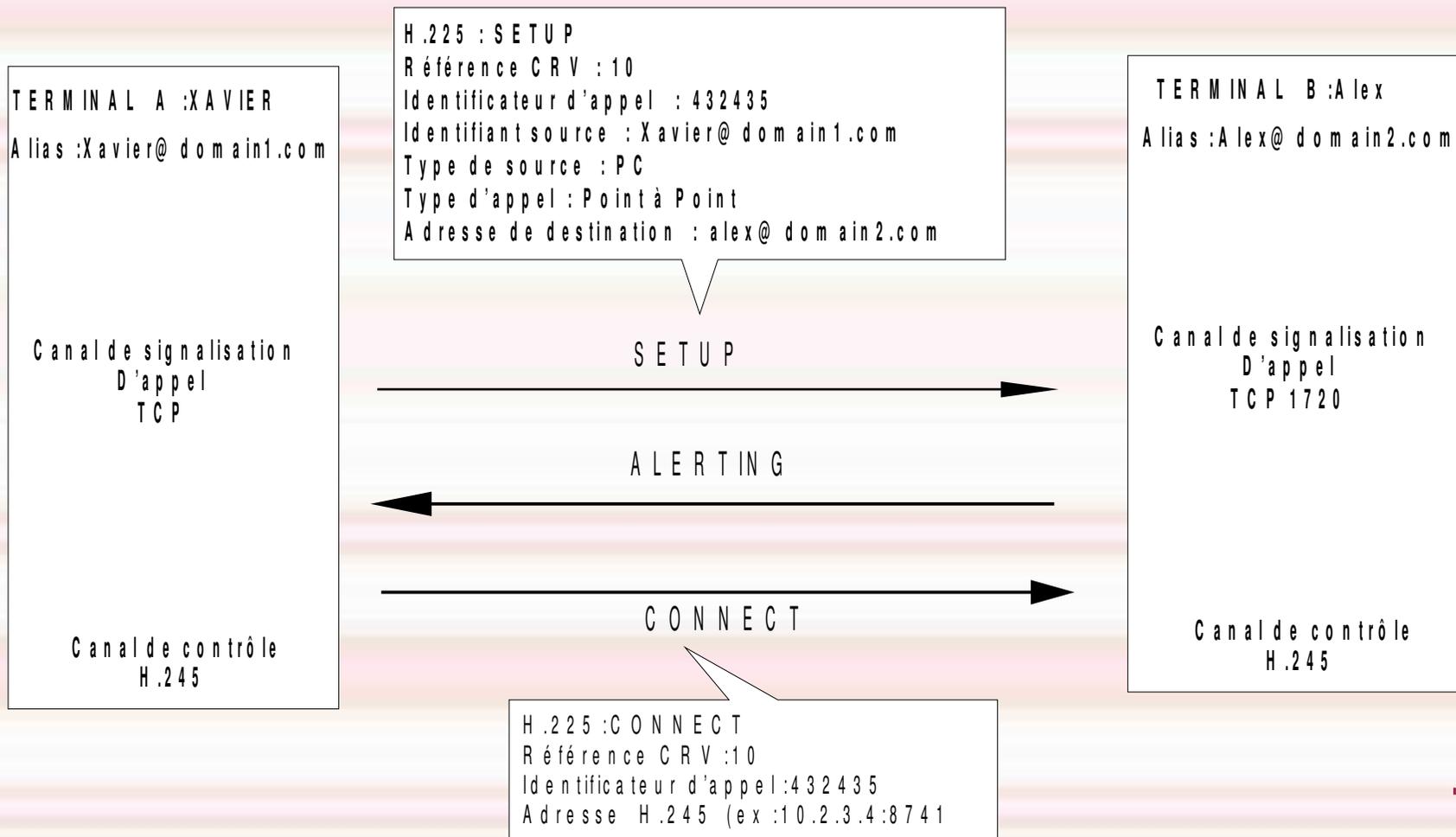
Les protocoles Secondaires

- ◆ DHCP :attribution des adresses IP,DNS
- ◆ TFTP pour la configuration et la mise à jour
- ◆ DNS pour les services d'annuaire et de localisation
- ◆ HTTP pour l'administration

### Protocole H.323

- ◆ L'établissement d'un appel point à point H.323 requiert 2 connexions TCP entre les terminaux.
  - Une première connexion pour l'établissement de l'appel
  - Une deuxième connexion pour pour les messages e contrôle des flux media et l'échange des capacités entre terminaux
- ◆ H.323 utilise un sous-ensemble de messages définis pour le RNIS dans la norme Q.931
  - SETUP
  - ALERTING
  - CONNECT

## INITIALISATION D'APPEL H.323



### Protocole SCCP (Skinny Client Control Protocol)

- ◆ Le H.323 étant très rigoureux pour certaines utilités de la téléphonie IP (comme le renvoi d'appel, le transfert, la mise en attente).
- ◆ Cisco a mis en place le protocole SCCP qui est plus léger. Il utilise le port 2000.
- ◆ L'avantage est qu'il utilise des messages prenant très peu de bande passante c'est pourquoi il est utilisé pour les communications entre les téléphones IP et les CallManager ainsi que pour contrôler les conférences.

# Protocole SIP (session Initial Protocol)

### ◆ Plusieurs éléments constituent le protocole sip

#### → User Agent

Les User Agents désignent les agents que l'on retrouve dans les téléphones SIP, les softphones (logiciels de téléphonie sur IP) des ordinateurs et PDA ou les passerelles SIP.

#### → Registrar

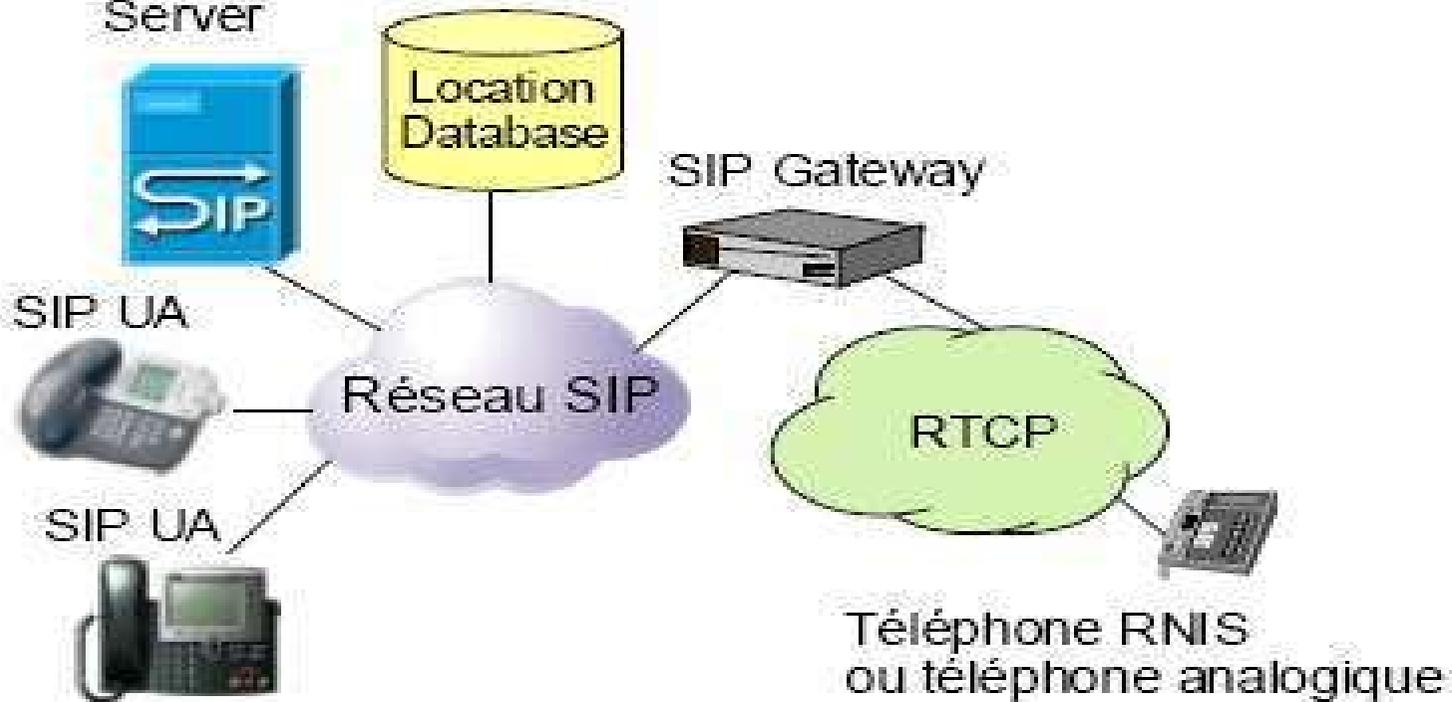
Le Registrar est un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données.

#### → Proxy Sip

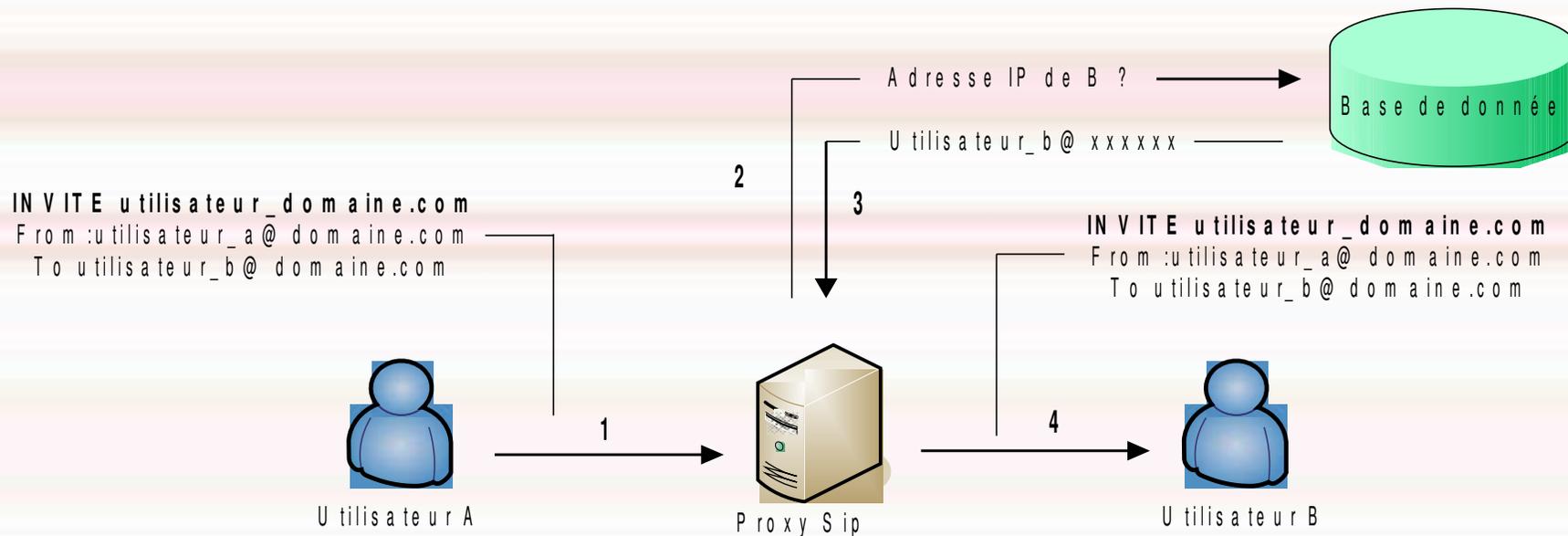
Un Proxy SIP sert d'intermédiaire entre deux User Agents qui ne connaissent pas leurs emplacements respectifs (adresse IP).

## Entité d'un Réseau SIP

Proxy/Redirect/Registrar  
Server

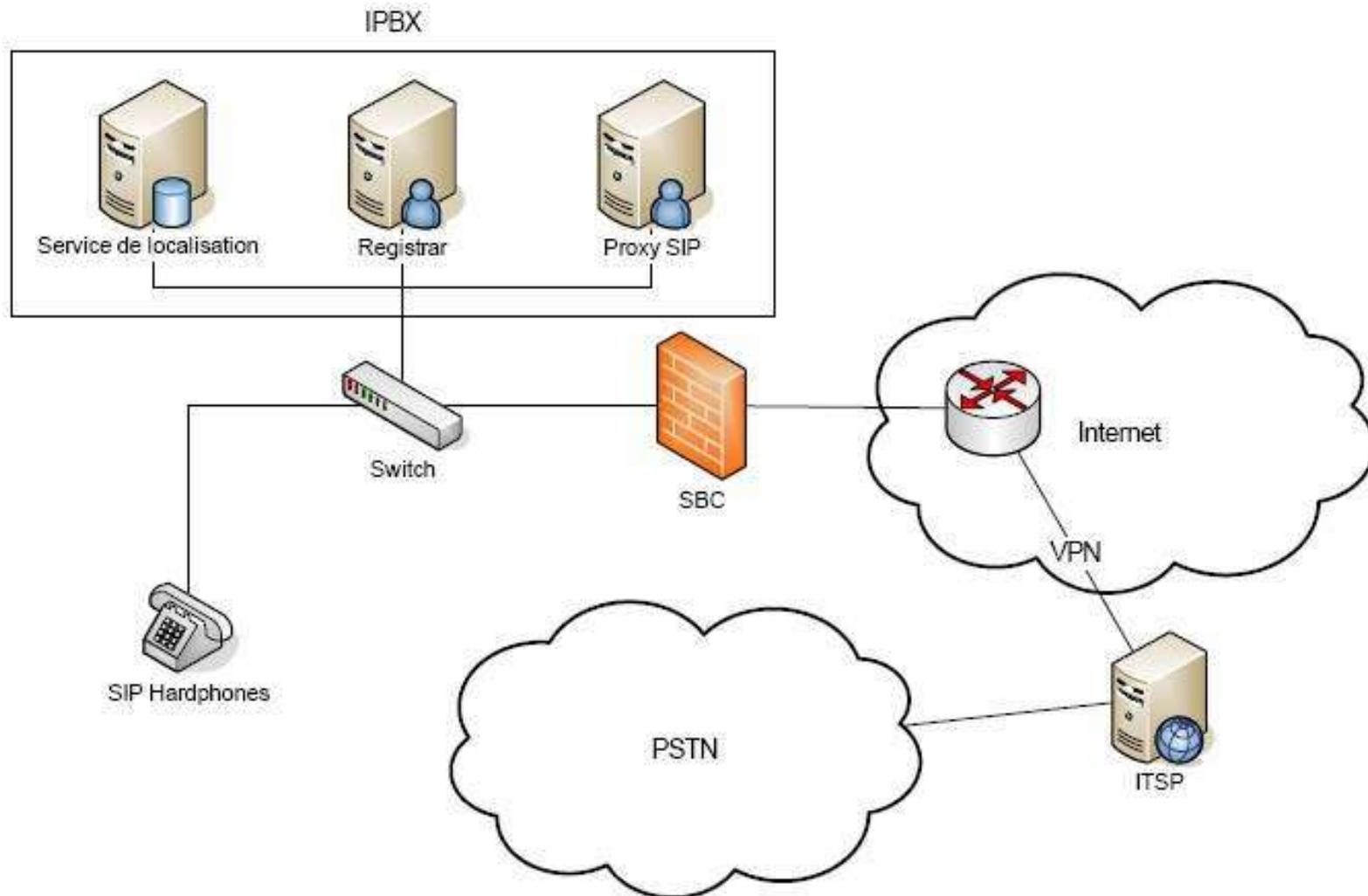


### Principes d'un Proxy SIP(1)



- 1) Envoi d'une requête INVITE au Proxy
- 2) Le Proxy interroge la base de données
- 3) La base de données renvoie l'adresse IP du destinataire
- 4) Le Proxy relaie le message au destinataire

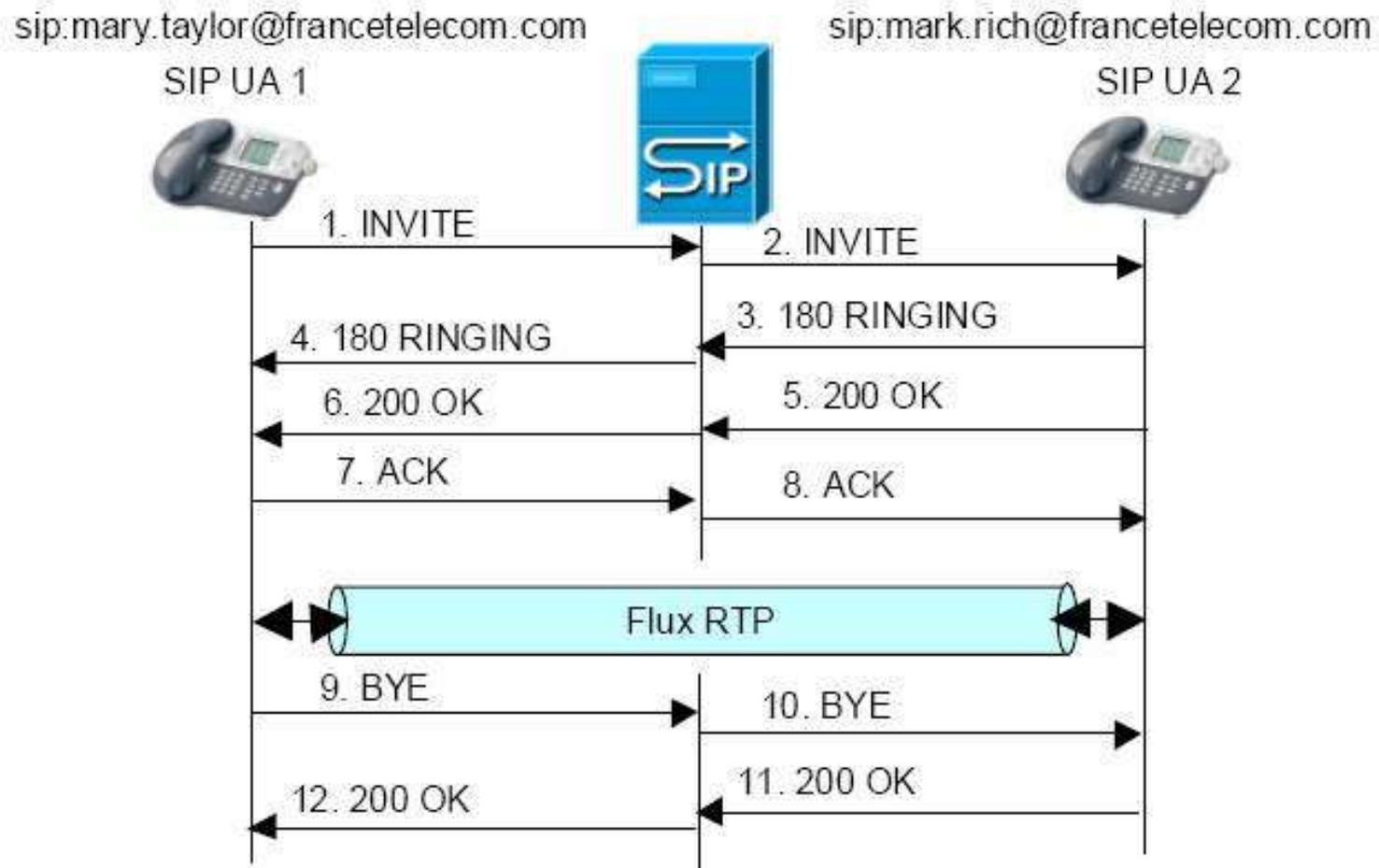
## Exemple d'architecture



# Protocoles SIP

- ◆ Sip partage de nombreux similitude avec le protocole HTTP :Le client envoie des requêtes au serveur qui lui envoie une réponse.Les méthodes de base sont les suivantes
  - INVITE permet à un client de demander une nouvelle session
  - ACK Confirme l'établissement de la connexion
  - CANCEL annule un INVITE en supens
- ◆ ~~Les codes de réponses sont similaires à HTTP~~
  - 100 Trying
  - 200 OK
  - 404 Not Found
  - BYE termine une session en cours
- ◆ Les codes supérieur ou égaux à x80 sont spécifiques à SIP
  - 180 Ringing
  - 486 Busy
  - etc..

## Etablissement et libération de session

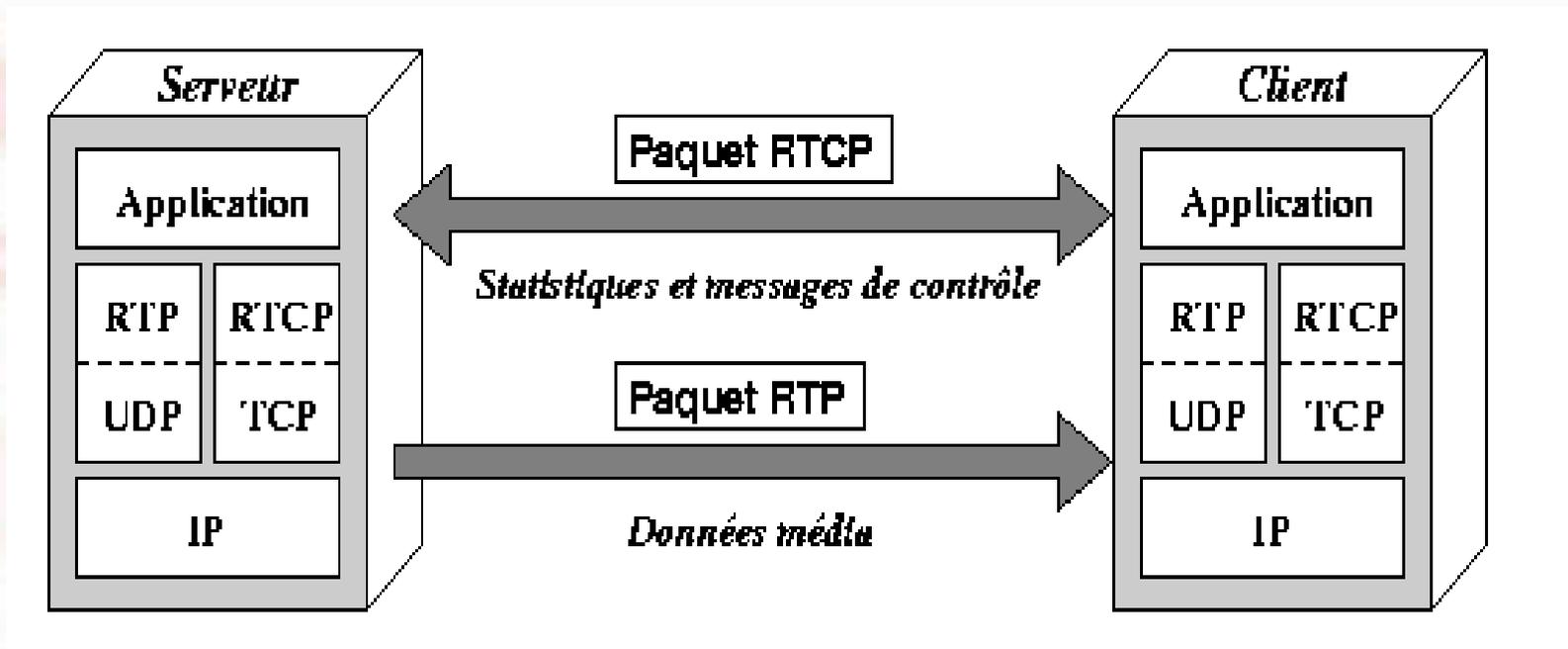


## Réquête INVITE/BYE

```
INVITE sip:mark.rich@francetelecom.com SIP/
2.0 Via : SIP/2.0/UDP
station1.francetelecom.com:5060
Max-Forwards : 20
To : Mark Rich
<sip:mark.rich@francetelecom.com>
From : Mary Taylor
From : Mary Taylor
<sip:mary.taylor@francetelecom.com>
Call-Id:
23456789@station1.francetelecom.com
23456789@station1.francetelecom.com
CSeq: 1 INVITE
Contact: mary.taylor@192.190.132.20
Content-Type: application/sdp
Content-Length:162
v = 0
c = IN IP4 192.190.132.20
m = audio 45450 RTP/AVP 0 15
```

```
BYE sip:mark.rich@francetelecom.com SIP/2.0
Via : SIP/2.0/UDP station1.francetelecom.com:5060
Max-Forwards : 20
To : Mark Rich
<sip:mark.rich@francetelecom.com>
From : Mary Taylor
<sip:mary.taylor@francetelecom.com>
Call-Id: 23456789@station1.francetelecom.com
CSeq: 2 BYE
SIP/2.0 200 OK
Via : SIP/2.0/UDP ps1.francetelecom.com:5060
Via : SIP/2.0/UDP station1.francetelecom.com:5060
Max-Forwards : 20
To : Mark Rich
<sip:mark.rich@francetelecom.com>
From : Mary Taylor
<sip:mary.taylor@francetelecom.com>
Call-Id: 23456789@station1.francetelecom.com
CSeq: 2 BYE
```

### Protocole RTP et RTCP



- Les protocoles temps réel RTP et RTCP sont construits au dessus des protocoles TCP et UDP
- Le protocole RTP s'occupe principalement du transfert de données du serveur au(x) client(s)
- le protocole RTCP se charge de transférer des paquets portant les statistiques **16** sur le transfert et les messages de contrôle entre le serveur et le client

## Failles/Attaques

- Failles/Attaques du protocole sip
- Failles/Attaques du protocole RTP/RTCP
- Failles/Attaques sur Les vlans

## Attaque Sip

### DoS en Utilisant les Réquêtes BYE

- ◆ Cette attaque consiste à couper la communication entre deux terminaux
  - Le pirate écoute le Réseau
  - Récupère le message de Réquête Bye entre l'appelant et l'appelé
  - Analyse le message afin de récupérer suffisamment d'informations sur la communication en cours.
  - Le pirate peut façonner un faux message BYE et l'envoyer soit à l'appelant soit l'appelé, ou les deux afin de terminer la communication

## Attaque Sip

### Contrefaçon des Réquêtes

- ◆ Cette attaque a pour but de modifier l'identité de l'expéditeur d'un message afin de faire croire au destinataire d'un appel qu'il parle à un utilisateur légitime alors qu'en fait il parle au pirate.
- ➔ Le Pirate va tout d'abord écouter le réseau afin de récupérer un message de requête soit du type REGISTER, soit du type INVITE et modifie certains champs contenus dans l'en-tête avant d'envoyer ce faux message de requête.
- ➔ L'appelé pense qu'il parle à un utilisateur spécifique alors qu'en fait il parle au pirate
- ➔ Ainsi, la victime ne pourra plus enregistrer son téléphone comme étant une adresse de contact convenable et tous les appels pour la victime seront redirigés vers le pirate.

## Attaque Sip

### Appel Spam

- Cette attaque a pour but de jouer un message préenregistré à la personne décrochant le combiné.
- Ce type de spam est défini comme étant une série d'essais d'initiation de session (par ex. des requêtes INVITE), essayant d'établir une session de communication vocale.
- Quand l'appelant décroche le combiné, l'attaquant (spammeur) relaie son message à travers le media temps réel.

## Attaque Sip

### Vol d'identité et détournement d'inscription

- ◆ En règle générale l'inscription sur un serveur sip nécessite un login et un mot de passe
  - ➔ L'ensemble des messages sip ne sont pas cryptés
  - ➔ Si une personne malveillante aspire les processus d'authentification, elle peut utiliser une combinaison nom utilisateur/mot de passe pour être authentifié par le serveur
  - ➔ Une telle attaque n'est plus possible avec les derniers implementations de la voip

## Les Attaques

### Inondation du serveur Proxy

- ◆ Cette attaque a pour but d'inonder les serveurs proxy avec des messages INVITE afin d'empêcher les utilisateurs légitimes de communiquer.
  - Le pirate envoie un gros volume de messages INVITE au proxy, qui doit normalement les transférer vers le destinataire
  - le nombre de sessions concurrentes supportées par un serveur proxy est limité
  - les ressources sont donc rapidement épuisées, ce qui a pour conséquence que les appels placés par des utilisateurs légitimes en utilisant le proxy victime ne peuvent prendre place.

## Les Attaques

### Détournement d'appel à l'aide du serveur registrar

- ◆ Cette attaque a pour but de détourner un appel en altérant les liaisons du serveur registrar.
  - ➔ Le Pirate profite du rôle du serveur registrar dans le système tout d'abord en récupérant les liaisons d'une URI particulière afin de récupérer la liste des adresses lui correspondant.
  - ➔ Ensuite, il va associer son URI avec tous les enregistrements corrects dans un message de requête REGISTER et en stipulant à ces enregistrements une priorité plus élevée en utilisant le paramètre « q »
  - ➔ Ce paramètre indique une préférence relative pour ce champ Contact particulier par rapport aux autres liaisons pour cette adresse d'enregistrement. Ceci a pour conséquence que le dessein de l'attaquant a abouti car son URI sera utilisé à la place de celle de l'utilisateur légitime.

## Les Attaques

### Débordement de la table des enregistrements

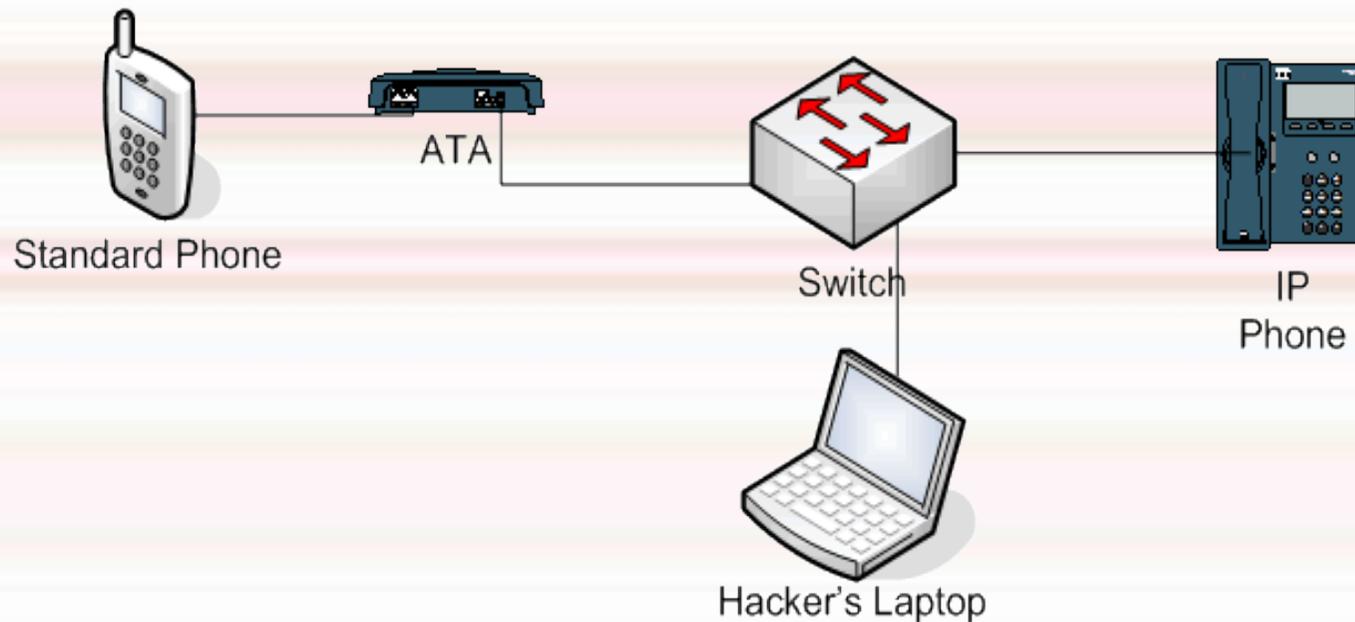
- Cette attaque a pour but de provoquer un débordement de la table des enregistrements afin d'empêcher les utilisateurs légitimes de s'enregistrer sur le serveur registrar.
- L'attaquant envoie un grand nombre de messages de requête REGISTER (avec des URIs différentes) au serveur des enregistrements afin de remplir la table des enregistrements et ainsi empêcher les utilisateurs légitimes de s'enregistrer et d'utiliser le service.

## Attaque RTP/RTCP

### Tromper la taxation

- ◆ Cette attaque a pour but de passer des appels gratuits.
  - Le Pirate et son complice vont mettre en place un schéma où les messages SIP seront dissimulés à l'intérieur de messages RTP/RTCP.
  - Le proxy SIP sera incapable de détecter le trafic de signalisation (SIP), alors que le flux de média (RTP/RTCP) continuera de transiter. Le CDR (*Call Detail Recording*) ne sera pas exécuté.
  - ainsi, les deux partis peuvent effectuer des appels téléphoniques gratuits

### MITM : Man-In-The-Middle



- ◆ L'attaque « man in the middle » est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.

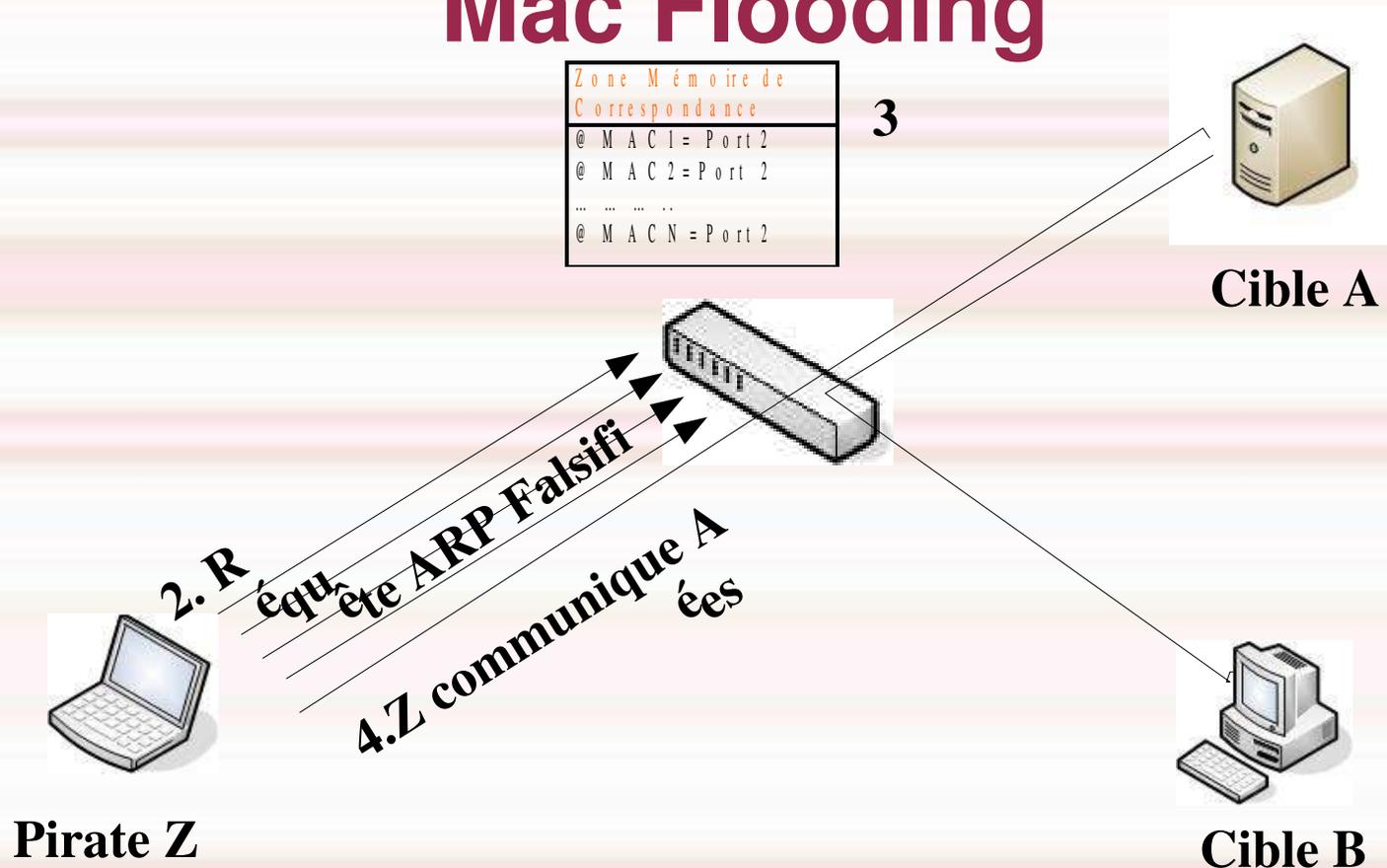
## Attaques sur Les Vlan

- attaque par MAC Flooding
- attaque par 802.1Q (standard) ISL (CISCO) tagging
- attaque par double encapsulation de 802.1 Q ou nested VLAN
- attaques ARP classiques
- attaques sur les privates VLAN
- attaques par force brute multicast
- attaques sur le spanning tree
- attaques de type random frame stress

## Attaque Mac Flooding

- ◆ Cette attaque est basée sur le fait que la table des switchs/ponts permettant le « routage » des paquets est limitée.
  - le pirate va flooder le switch avec des arp query/ arp response avec pour chaque demande une adresse MAC différente.
  - pour chaque adresse MAC différente, le switch va l'associer dans sa table au port concerné.
  - Le mécanisme est répété jusqu'à saturation de la mémoire à ce moment le switch ne peut plus enregistrer dans sa table.
  - il se transforme en HUB et broadcaste alors toutes les requêtes sur le réseau.

# Mac Flooding

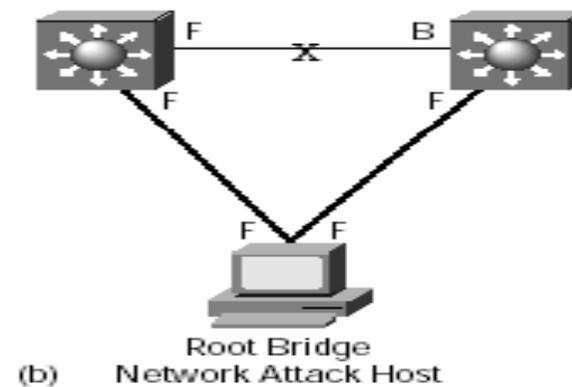
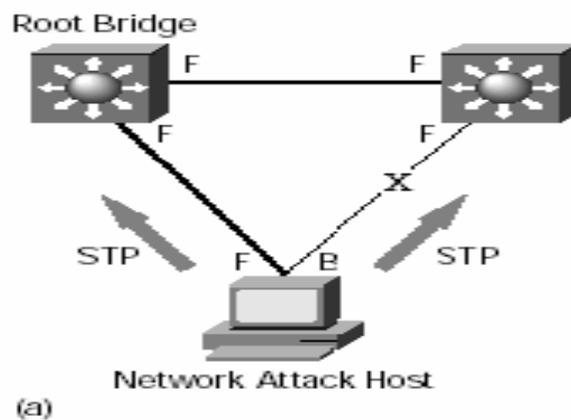


- 1 -Les cibles A et B s'echangent des informations normalement
- 2-Le pirate Z envoi plein de requêtes ARP avec des adresses MAC différentes,
- 3-Le Switch met à jour sa table de correspondance jusqu'à saturation de la mémoire
- 4-Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi du fait que le Switch fonctionne désormais en HUB.

## Les Attaques

### Attaques sur le Spanning tree

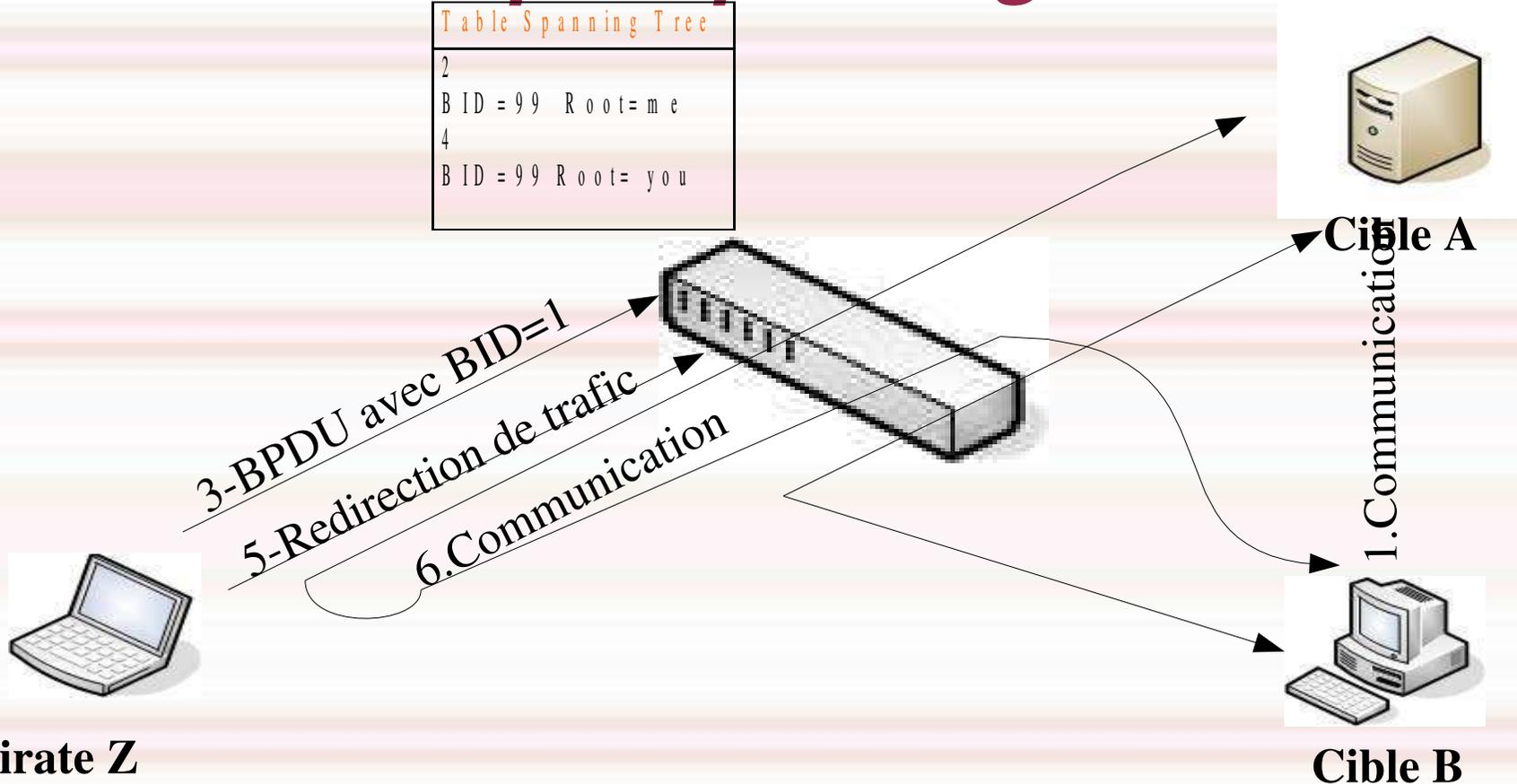
- ◆ Cette attaque consiste à injecter des BPDU (bridge protocol data unit) falsifiés afin de forcer les équipements à recalculer l'arbre en permanence ce qui rend le réseau inopérant. Il est également possible que sous l'inondation, les switch se transforment en HUB.
- ◆ Par défaut, le protocole STP est activé sur tous les ports. L'attaquant se comporte comme un switch et envoie un BPDU demandant de devenir root (a). L'arbre est recalculé et inopérant.



topologie

# Attaque Spanning Tree

Table Spanning Tree	
2	
B ID = 99	Root = me
4	
B ID = 99	Root = you

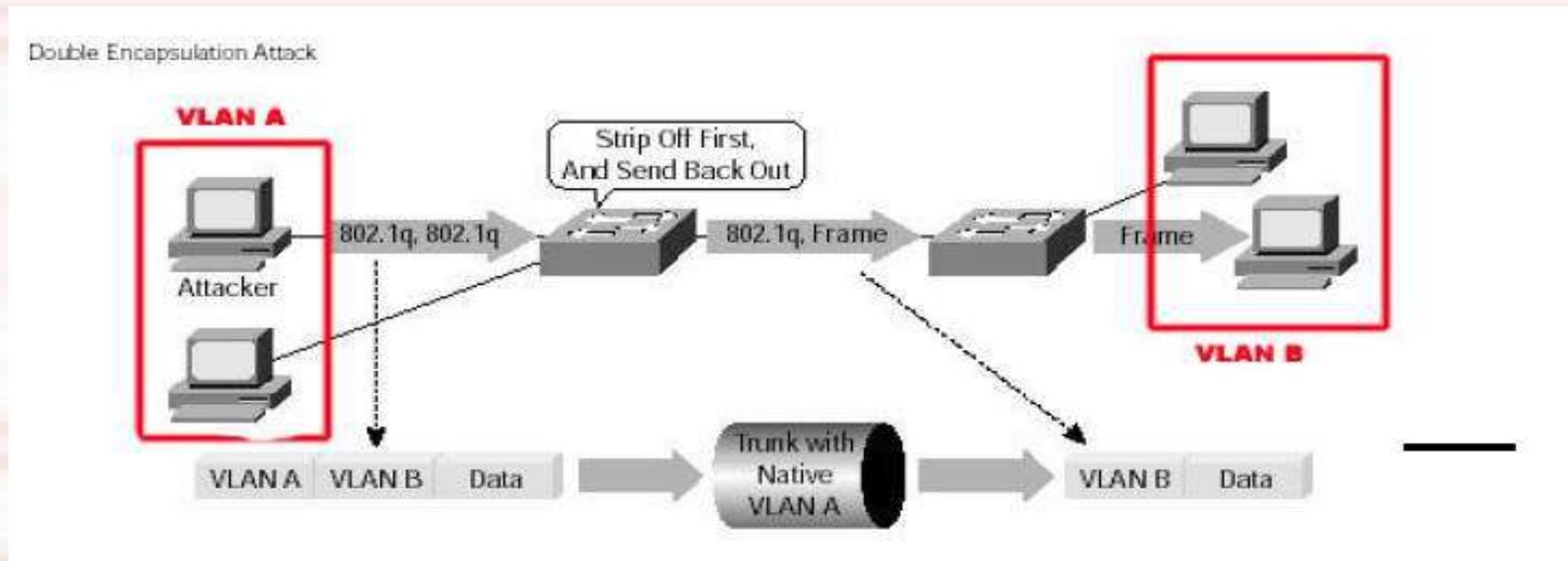


## Pirate Z

- 1-Les cibles A et B s'echangent des informations normalement
- 2-Le switch est le maître du contexte de Spanning Tree
- 3-Le pirate Z envoi une trame BPDU avec un BID très faible
- 4-Le commutateur admet que le pirate Z est devenu le maître du contexte STP
- 5-Le hacher redefinis la Topologie afin de rediriger les flux vers lui
- 6-Les cibles A et B s'echangent des informations ,mais le pirate les reçoit aussi

## Attaques par double encapsulation de 802.1Q (1)

- ◆ L'attaque consiste à injecter des paquets encapsulés dans 2 trames 802.1q. La trame injectée comporte 2 entêtes 802.1q.



- L'attaquant est sur le VLAN natif (non taggués 802,1Q)
- L'attaquant envoie une trame taggués deux fois
- Le switch vlan natif reçoit 1 trame qui ne devrait pas être tagguée et enlève le 1er TAG

### Attaques par double encapsulation de 802.1Q (2)

- ◆ Le switch reçoit une trame venant d'un VLAN natif avec une entête VLAN A
- ◆ Il n'est pas normal de recevoir des trames taggées de la part du VLAN A qui est natif.
- ◆ Le switch enlève le premier tag. En théorie, il devrait se retrouver avec une trame Ethernet sans en tête et dans ce cas la forwarder sur le port physique correspondant au VLAN A.
- ◆ Lors du traitement de la trame il considère le tag interne VLAN B et à la place dirige la trame vers le VLAN B : le saut de VLAN a été réalisé.

## Attaques par force Brute Multicast

- Cette attaque consiste à floodier le switch avec des trames de niveau 2 (trame ARP)
- certains switchs changent l'algorithme de broadcast et se comportent comme un hub lorsque leur processeur atteint une charge de 70-80% d'utilisation.

## Attaques random frame stress

- ◆ Cette attaque consiste à trouver des failles dans l'implémentation des différents protocoles. Pour cela on fait une attaque exhaustive:
- ◆ Au niveau de la trame Ethernet :
  - On fixe @ mac source et @ mac destination (sur autre VLAN)  
On essaie toutes les combinaisons possibles sur les autres champs de la trame Ethernet : de la trame : type, bourrage, crc, la taille du paquet
  - On observe pour voir si un paquet à fait un saut de VLAN ou si le paquet a provoqué une erreur dans le switch par exemple une taille de paquet annoncée différente de la réalité, Cette erreur peut être à l'origine d'un buffer overflow.

## Les Attaques

### Attaques par 802.1Q (standard), ISL (CISCO) tagging

- ◆ L'idée de cette attaque est de forger des trames permettant d'avoir accès à un autre Vlan en modifiant les tags de la norme 802.1Q
  - ➔ Une telle attaque repose sur la capacité de forger un tag dans une trame afin de tromper le switch et de sauter de VLAN.
  - ➔ L'attaquant envoie des trames forgées avec des tags 802.1Q sur un port quelconque. En principe le switch va rejeter ces trames ou les détagguer étant donné qu'elles ne devraient pas l'être (seul le port du trunk est taggué)
  - ➔ Sur les switch cisco si le DTP (dynamic trunk protocol) est activé, le port quelconque va se mettre à considérer le port comme un trunk. A partir de la, l'attaquant peut très facilement atteindre tous les VLAN en forgeant une en tête 802.1Q adaptée.

### Les attaques ARP Spoofing

- ◆ Cette type d'attaque consiste à s'attribuer l'adresse ip de la machine cible. c'est-à-dire à faire correspondre son adresse IP à l'adresse MAC de la machine pirate dans les tables ARP des machines du réseau.
- ◆ Soit la machine de la victime
  - IP 10.0.0.171
- ◆ Soit la machine du pirate
  - Passerelle par défaut 10.0.0.1
  - IP 10.0.0.227
- ◆ Avant l'attaque un traceroute donne le résultat

```
[root@cible]$ traceroute 10.0.0.1
```

```
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 40 byte packets  
1 10.0.0.1 (10.0.0.1) 1.218 m s 1.061 m s 0.849 m s
```

### Les attaques ARP Spoofing

- ◆ Le cache ARP de la machine cible est

```
[root@cible -> ~]$ arp
```

Address	HW type	HW Address	Flags	Mask	Interface
10.0.0.1	ether	00:b0:c2:88:de:65	C		eth0
10.0.0.227	ether	00:00:86:35:c9:3f	C		eth0

- ◆ Le Pirate lance alors ARPspooft ( générateur de paquet ARP)

```
[root@pirate]$ arpspoof -t 10.0.0.171 10.0.0.1
```

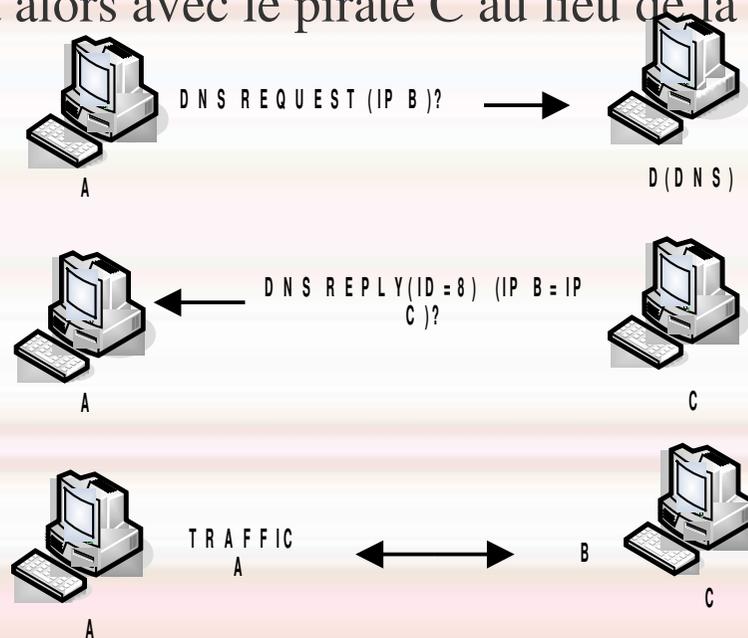
```
0:0:86:35:c9:3f:0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
```

### DNS ID SPOOFING

- Imaginons qu'un client A veuille établir une connexion avec une machine B. La machine A connaît le nom de la machine B mais pas son adresse IP.
- La machine A va donc envoyer une requête au serveur DNS du réseau de B pour connaître l'adresse IP de B. Cette requête sera identifiée par un numéro d'identification (ID).
- Le serveur répond à cette requête en fournissant l'adresse IP de B et en utilisant le même numéro d'ID.
- Le DNS ID spoofing a pour but de d'envoyer une fausse réponse à une requête DNS avant le serveur DNS. De cette façon, le pirate peut rediriger vers lui le trafic à destination d'une machine qu'il l'intéresse.

### DNS SPOOFING :Illustration

- ◆ Dans notre exemple, un pirate C doit répondre à A avant le serveur DNS (D) du réseau de B. Ainsi, il envoie à A son adresse IP associée au nom de la machine B. A communiquera alors avec le pirate C au lieu de la machine B



## Sécurité de la VoIP

- ◆ Mise à jour des logiciels
- ◆ Verrouillages de la configuration
- ◆ Séparation grâce aux Vlan
- ◆ Filtrage Inter-Vlan
- ◆ Utilisations des cartes réseau supportant 802.1Q
- ◆ Echange DNS avec DNSSEC
- ◆ Authentification et chiffrement
- ◆ Protections contre les attaques ARP

### Mise à jour du software (IPBX, hardphone et softphone)

- ◆ L'IPBX, les hardphones et les softphones contiennent tous un logiciel. Le code de ces logiciels peut contenir des failles (buffer overflow) et donc être vulnérable à diverses attaques.
- ◆ Il est donc très important de maintenir à jour la version de ces logiciels, notamment lorsqu'une faille de sécurité les concernant a été découverte.
- ◆ Consulter régulièrement les sites des fabricants hardware/logiciel des équipements introduit dans l'infrastructure VoIP, ou mieux, être inscrit à leurs *newsletters* de manière à être automatiquement informés si une nouvelle version/*patch* est disponible.
- ◆ Tester le patch sur des équipements de test
- ◆ Mettre à jour les équipements de production si le test précédent est Concluant

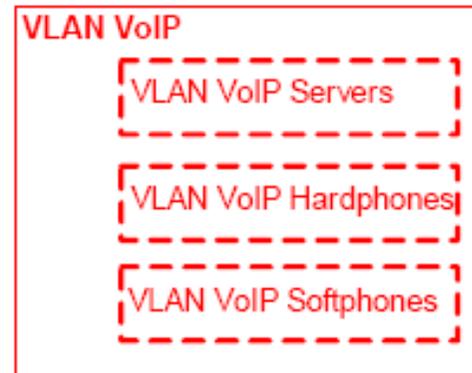
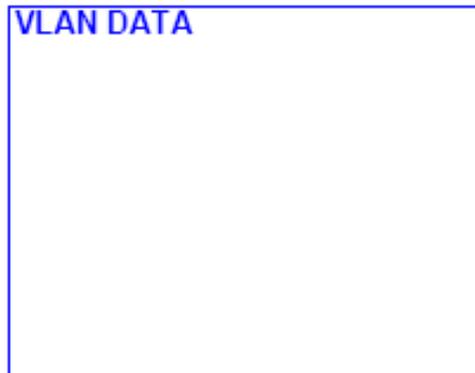
### Verrouillage de la configuration (hardphone/softphone)

- ◆ Une fois le hardphone/softphone configuré, il est important de verrouiller par mot de passe sa configuration afin d'empêcher qu'un utilisateur ne puisse modifier les paramètres (désactiver l'authentification).
- ◆ De plus, des mesures organisationnelles devraient être prises de manière à interdire aux employés toute modification de la configuration des équipements de l'infrastructure VoIP.

### Séparation grâce aux VLAN (layer 2)

- ◆ Cette solution consiste à définir un VLAN DATA dédié aux équipements réseaux présents dans le réseau DATA et un VLAN VoIP dédié aux équipements VoIP. Afin d'obtenir une meilleure séparation, il est conseillé de créer à la place du VLAN VoIP, un VLAN pour chaque catégorie d'équipement VoIP comme suit:

- Les hardphones : VLAN VoIP hardphone
- Les softphones : VLAN VoIP softphone
- 

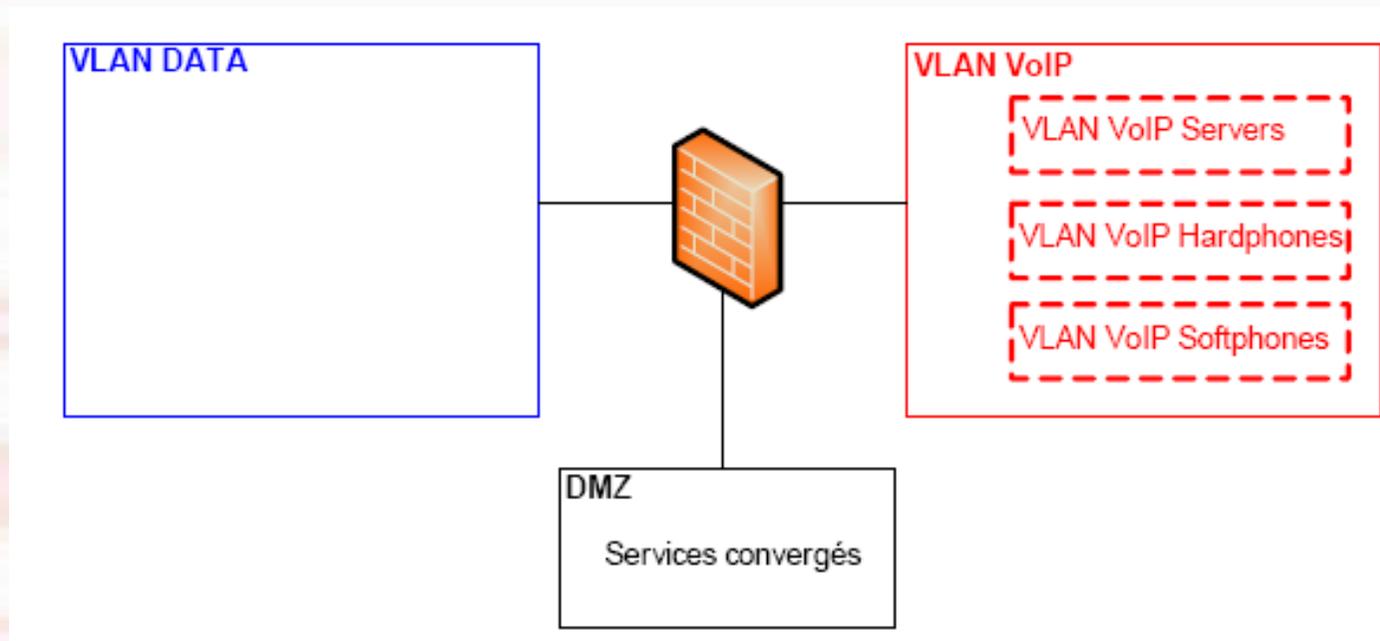


### Filtrage Inter-VLAN

- ◆ Les communications entre les VLAN doivent être rigoureusement filtrées de manière à n'autoriser que les flux nécessaires. seuls les flux définis sont autorisés.
  - ➔ Le filtrage peut s'effectuer comme suit:
    - ➔ en définissant des ACL sur les *switches* et/ou les *routers* interconnectant les VLAN , en plaçant Les firewall entre les VLANs
- ◆ Les règles de filtrage devraient être basées sur les adresses IP, les numéros de ports/protocoles et les *flags* TCP/IP de manière à être le plus strict possible et à n'autoriser que les communications nécessaires.
- ◆ Par exemple, les IP Phones n'ont pas besoin d'envoyer un flux média (ex : RTP) aux serveurs VoIP. Donc, au lieu d'autoriser toutes communications entre les VLAN VOIP Hardphones/Softphones et le VLAN VoIP Servers, seul le trafic concernant le protocole de signalisation (ex : SIP) devraient être autorisé.

# Placer Les services convergés dans DMZ

- ◆ Afin de ne pas compromettre la séparation des VLAN DATA et VoIP, les services convergés (services nécessitant un accès au VLAN DATA et au VLAN VoIP) doivent être placés dans une DMZ. Les règles du *firewall* doivent être le plus strict possible afin de n'autoriser que les flux nécessaires.



### Utilisation d'une carte réseau supportant 802.1Q

- ◆ Le principal danger lorsque l'on installe un *softphone* sur un ordinateur provient du fait que cet ordinateur, déjà connecté au réseau DATA, devient un terminal VoIP.
- ◆ Il existe cependant une solution pour maintenir la séparation des VLANS.
- ◆ Cette solution consiste à équiper les ordinateurs d'une carte Ethernet supportant le protocole 802.1q et de les configurer pour utiliser ce protocole.
- ◆ De telle carte Ethernet permettent de séparer le trafic DATA du trafic VoIP (issue du *softphone*) en mettant chaque type de trafic dans leur VLAN respectif.
- ◆ L'OS, la carte Ethernet et le *softphone* doivent supporter 802.1q.

## Echange DNS avec DNSSec

- ◆ DNSSEC permet de sécuriser les données envoyées par le DNS. Contrairement à d'autres protocoles comme SSL, il ne sécurise pas juste un canal de communication mais il protège les données, les enregistrements DNS, de bout en bout. Ainsi, il est efficace même lorsqu'un serveur intermédiaire trahit.
- ◆ DNSSEC signe cryptographiquement les enregistrements DNS et met cette signature dans le DNS. Ainsi, un client DNS méfiant peut donc récupérer la signature et, s'il possède la clé du serveur, vérifier que les données sont correctes. La clé peut être récupérée via le DNS lui-même .
- ◆ Utilisation de tunnel IPsec.

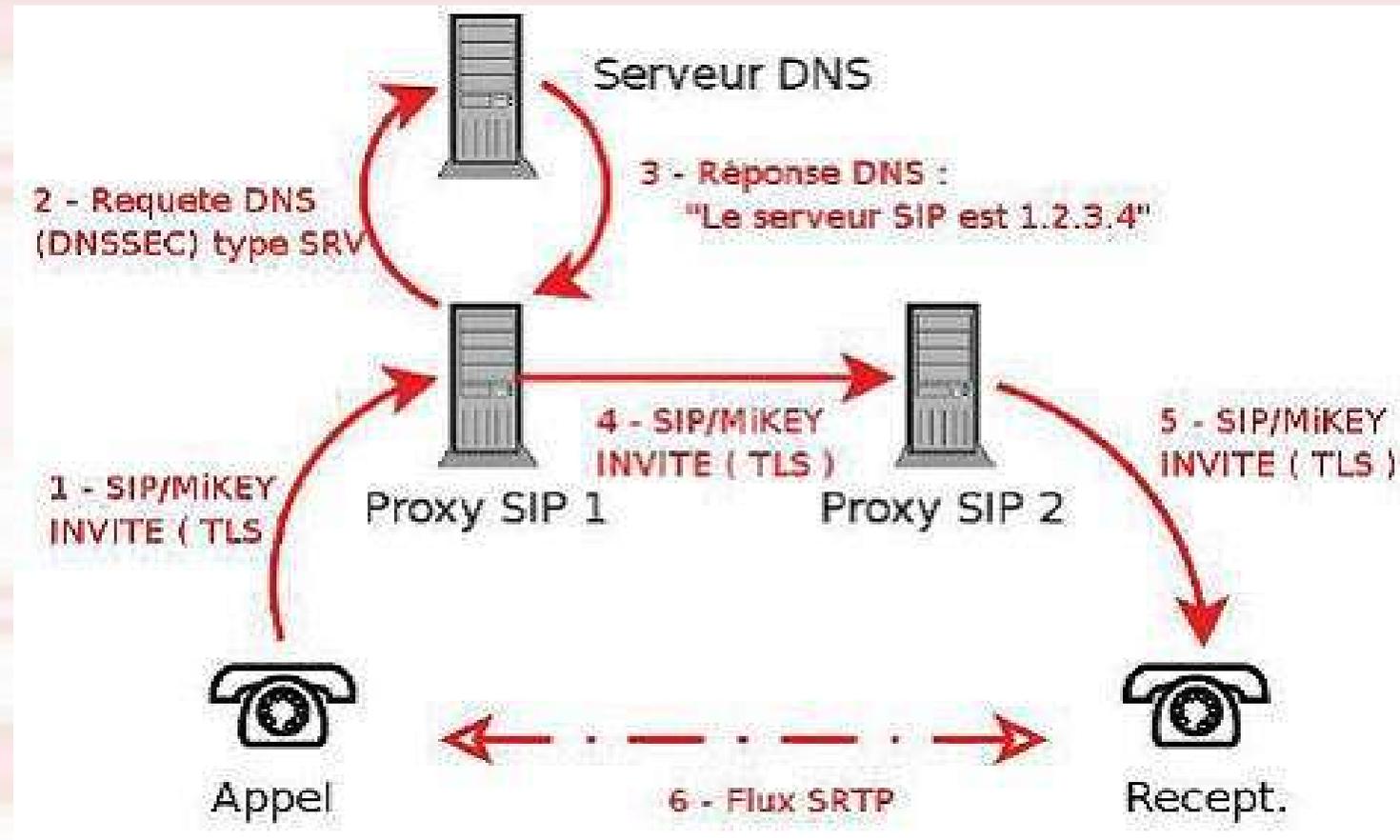
## Authentification et chiffrement SSL / TLS

- ◆ Transport Layer Security (TLS) un protocole qui sécurise les échanges sur internet. Il fonctionne en mode client-serveur .il fournit quatre objectifs de sécurité:
  - l'authentification du serveur ;
  - la confidentialité des données échangées (ou session chiffrée) ;
  - l'intégrité des données échangées ;
  
- ◆ Utilisation de Secure RTP / Secure RTCP (SRTP/ SRTCP)  
il ajout les fonctions suivantes
  - Confidentialité (cryptage AES 128 bits)
  - Authentification des messages (HMAC-SHA1)
  - Ajout de protection

## Protection contre les attaques ARP

- ◆ Cette methode consiste à empêcher la connexion du pirate sur le réseau
  - Securiser l'accès physique du réseau pour un réseau filaire
  - En Wi-Fi, avec le Wep, tous les paquets sont rejetés si le pirate ne connaît pas la clé secrète
  - Installer un pare feu
  - Implementer les tables ARP statiques
  - Analyser les historiques

## Solution sécurisée



## Outils de Test d'analyse et Vulnérabilité de la VoIP

- ◆ **SiVuS** est l'un des scanners de vulnérabilité les plus connus et les plus fiables supportant le protocole SIP. Ce scanner propose un grand nombre de fonctionnalités qui permettent de mesurer la sécurité d'un composant SIP
- ◆ **VOMIT** Voice Over Misconfigured Internet Telephone  
le logiciel permet de convertir une conversation d'un téléphone IP Cisco en un fichier son de format wav. Pour cela, L'utilitaire demande un fichier de capture de type tcpdump.
- ◆ **Wireshark** (anciennement Ethereal) est un logiciel de surveillance des réseaux IP

## Conclusion

- ◆ Nous avons couvert le sujet de la voix sur IP d'un point de vue technique et nous pensons qu'aujourd'hui une solution de voix sur IP peut-être sécurisée à un niveau acceptable.
- ◆ Un projet de voix sur IP est complexe, car il n'existe pas de solution générique, et une étude au cas par cas s'impose avant la mise en oeuvre de cette technologie. Le facteur sécurité doit être pris en compte avant même la phase de conception en posant les bonnes questions aux vendeurs que vous êtes en train de sélectionner.

## Références

- ◆ [http://www.iict.ch/Tcom/Projets/VoIP/VoIP\\_and\\_Mobility/Tutoriaux/Tutorial\\_SII](http://www.iict.ch/Tcom/Projets/VoIP/VoIP_and_Mobility/Tutoriaux/Tutorial_SII)
- ◆ Hacking VoIP Exposed de David Endler et Mark Collier
- ◆ <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/voip/I332-009R-2006.pdf>
- ◆ <http://www.terena.nl/activities/iptel/contents1.html>
- ◆ <http://iase.disa.mil/stigs/stig/network-stig-v6r4.pdf>
- ◆ <http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V2R2.pdf>
- ◆ <http://www.vopsecurity.org>, <http://vomit.xtdnet.nl/>, [http:// www.wireshark.org](http://www.wireshark.org)