Téléphonie sur IP
et sécurité

Bibliographie

- Internet, Multimédia et Temps réel,
  Jean-François Susbielle, Eyrolles, 2001, 700 pages
- Réseaux - Internet, téléphonie, multimédia - Convergences et complémentarités
  D.Hardy, G.Malléus, J.Méreur - De Boeck, juillet 2002 - 798 pages
- Implementing voice over IP
  B. Khasnabish – Wiley, 2003 - 324 pages
- Portail technique sur la téléphonie sur IP :
  http://iptel.org/
- Portail des développement commerciaux des produits SIP
  http://www.sipcenter.com/
  http://www.sipforum.org

PLAN

- Pourquoi la téléphonie sur IP ?
- Risques de sécurité
- Eléments techniques
  - Architecture de ToIP : H.323 vs SIP
  - Protocoles de sécurité pour la ToIP
- Travaux pratiques

1- **Contexte et motivations**

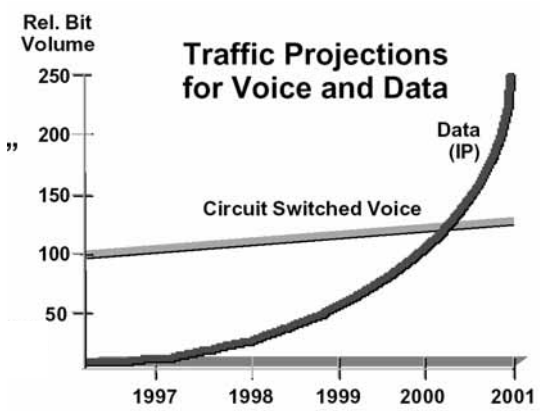
Contexte Technique

- Voix sur IP (VoIP) :
  - Transporter la voix différemment
    - dans des paquets
    - Sur des réseaux asynchrones
  - Existe déjà : Frame Relay, ATM
- Téléphonie sur IP (IPtel) :
  - Offrir un vrai service de téléphonie sur un réseau IP
  - Signalisation d'appel SS-7, Services du Réseau intelligent IN

Objectifs VoIP

1. réduction des coûts de communications (pas toujours vrai !)
2. simplifier la gestion/maintenance des infrastructures et des services téléphoniques (cela dépend et plûtot à long terme);
3. intégrer les services téléphoniques classiques (boite vocale, audioconférence, fax, …) avec les services et applications informatiques existantes (services Internet, Intranet, et Extranet)
   - Applications CTI (Couplage Téléphonie Informatique).
4. déployer rapidement des services de téléphonie aussi flexibles, programmables et configurables que les services de messagerie électronique (émail) ou du Web;

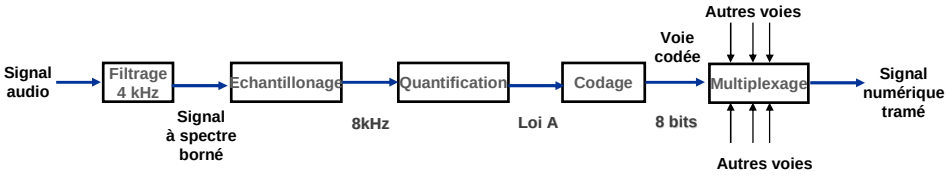
Pourquoi IP ?
Explosion du trafic IP



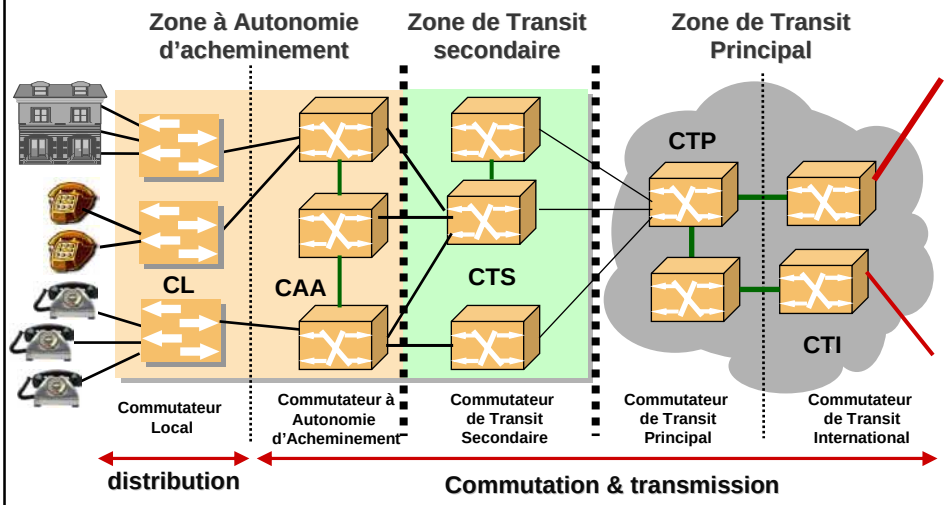
Téléphonie numérique

1. La téléphonie numérique est apparu au début des années 70, pour mieux utiliser l'infrastructure existante afin de pouvoir :
   - répondre rapidement à la très forte demande de raccordement au réseau téléphonique en utilisant l'infrastructure de câbles existante;
   - étendre l'application des techniques informatiques et micro-électroniques aux télécommunications;

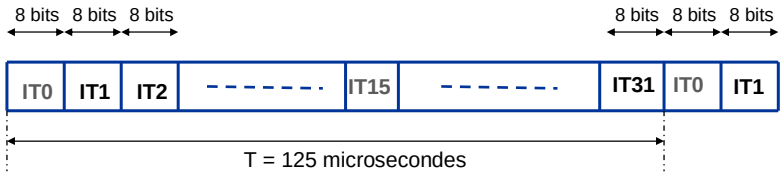
2. La téléphonie numérique repose sur 2 techniques : la Modulation par Impulsions et Codage (MIC) et le multiplexage temporel synchrone.



Architecture générale du réseau téléphonique



Multiplexage : Trame temporelle MIC

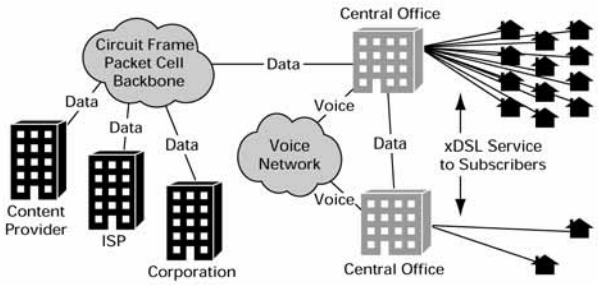


- **L'échantillon associé à une communication vocale est appelé canal. On a décidé d'insérer chaque seconde sur un circuit physique (c'est-à-dire une paire de fils) 32 canaux formant une structure, appelée trame temporelle MIC, et comportant 32 intervalles de temps successifs numérotés de 0 à 31, correspondant chacun à un canal unidirectionnel et occupant 8 bits (1 octet).**
- **Cette trame de 2.048 Kbp/s (E1) est normalisée dans G.732. Tandis qu'aux Etats-Unis une trame MIC regroupe 24 canaux de 56 Kbp/s seulement, soit un débit de 1.544 Kbp/s (DS-1).**

Boucle locale xDSL

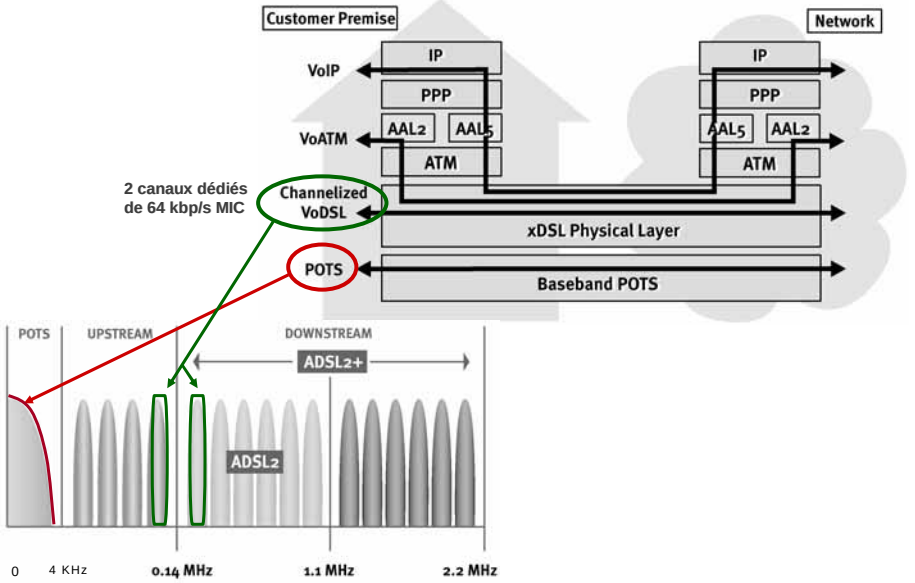
Fin 2003 : **3 Millions d'abonnées à l'ADSL (1.4 Millions - Fin 2002)**
70 % de la population dispose d'un accès ADSL (65% - Fin 2002)
34 Millions de lignes téléphonique fixe (France Telecom)
40 Millions d'abonnés à la téléphonie mobile en France (ART - Oct 2003)

Fin 2004 (Prévision) **85% de la population disposerons d'un accès ADSL (ADSL2, +15% distance)**
+ 35% de croissance par an en Europe (PriceWaterHouseCoopers)
6 millions d'abonnées Hauts débits en France
43.3 Millions d'abonnés à l'ADSL prévu en Europe Fin 2007



Distance max	Débit théorique maximum
5,5 km	1,544 Mbits/s (ADSL - 1.1 GHz)
4,9 km	2,048 Mbits/s (E1)
3,7 km	6,312 Mbits/s (DS2)
2,7 km	8,448 Mbits/s
2,7 km	10 Mbits/s (ADSL 2 - 1.1 GHz)
2,7 km	20 Mbits/s (ADSL 2+ - 2.2 GHz)
1 km	25 Mbits/s (ADSL 2+)

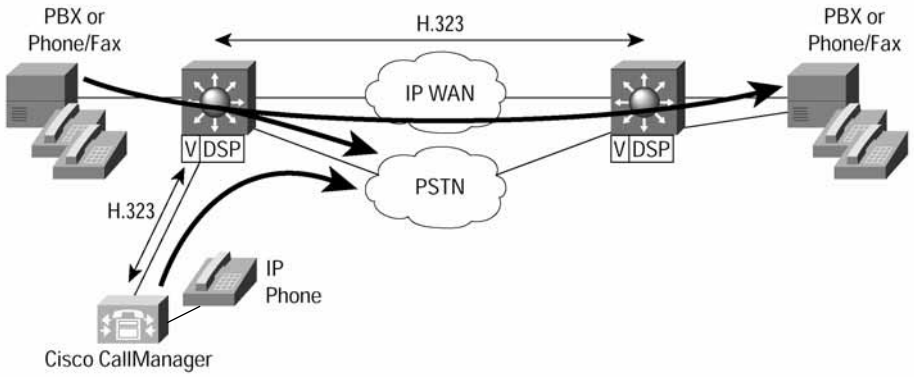
VoATM vs VoIP vs CVoDSL vs



Interconnexion de PABX

CISCO SYSTEMS

- **Module VoIP Access Gateway for Catalyst 4000 series :**



VPN IP
- Offre -

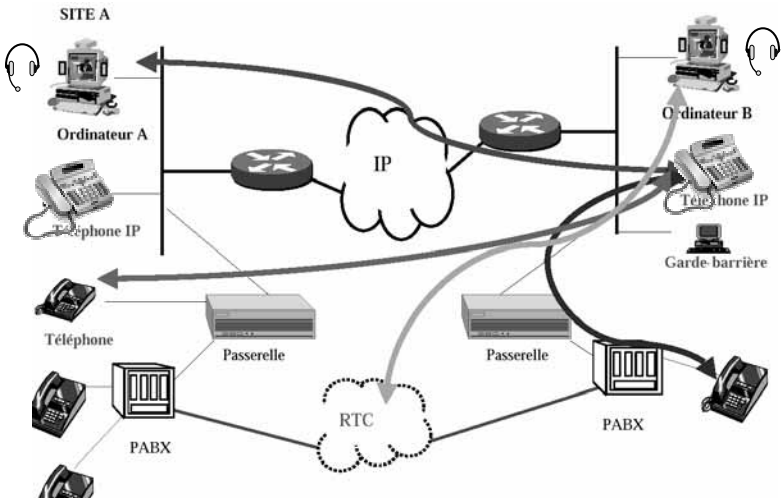
Il existent 10 offrent de réseaux privés virtuel IP en France (01réseaux/Sept. 2002)

- Cable & Wireless (IPsec, aucune classe, 50 PoP nat, 49 PoP int.)
- Equant (FT) (MPLS, 5 classes, 140 pays)
- Cegetel / Infonet (MPLS, 3 classes: Std, Data, Tps réel, 160, 55 pays)
- Colt (UK) (IPsec, 4, 13, oui via offre IP Corporate)
- FT/Global One (MPLS, 3, 60, 140)
- KPNQwest (IPSec, 5 classes, 30, 300)
- Maiaah (MPLS, 5, 7, via réseaux tiers)
- QoS Networks (IPSec, 5 classes, 1, 9)
- LDcom/Siris (MPLS, 4 classes, 77, 0)
- MCI (MPLS)

Types de VPN des entreprises françaises (Cabinet d'analyse Cesmo et Colt)

- en 2001 : VPN IP (8%) et FrameRelay (92%)
- en 2003 : VPN IP (27%), 2 appels d'offres sur 3.

2- scénario de déploiement
Opérateurs / Entreprises
CTI



IP Phone Productivity Service

Cisco IP Phone 7960

- **Application Cisco permettant de consulter et gérer Via l'écran LCD de n'importe quel IP Phone de l'entreprise (gamme 7960 et 7940) :**
  - **ses appels,**
  - **sa messagerie vocale,**
  - **ses e-mails,**
  - **pon agenda**
  - **Et son annuaire personnelle**
- **Gain de productivité**

Le 7960 supporte des fonctionnalités :

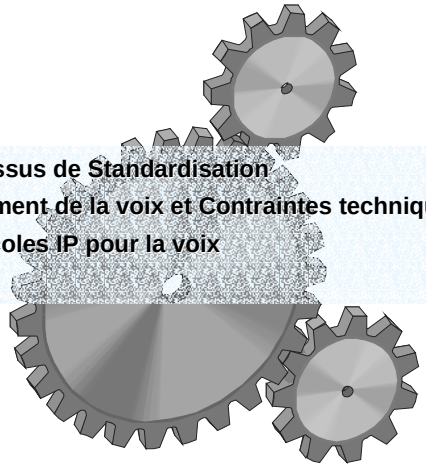
- **Renvoi d'appel**
- **Recomposition**
- **Annuaires d'entreprises**
- **Services d'Information**
- **Effectuer une audioconférence**
- **Accéder à la messagerie vocale**

Avantages de la VoIP

- Synthèse -

1. réduction des coûts
   - d'acquisition des équipements (-15% pour une solution de 100 postes)
   - des communications (pas toujours vrai !)
2. simplifier la gestion/maintenance des infrastructures et des services téléphoniques/réseaux (cela dépend et plûtot à long terme);
   - Administration à distance via le réseau et plus besoin d'intervention sur PABX
   - Souplesse d'attribution des n° d'appel; plus liés à un poste physique
   - Possibilité d'envoi simple d'un appel d'urgence sur tout un réseau (Alertes)
3. intégrer les services téléphoniques classiques (boite vocale, audioconférence, fax, …) avec les services et applications Intranet/Extranet existantes :
   - Applications CTI (Couplage Téléphonie Informatique).
4. déployer rapidement des services de téléphonie aussi flexibles, programmables et configurables que les services de messagerie électronique (émail) ou du Web (e-commerce);

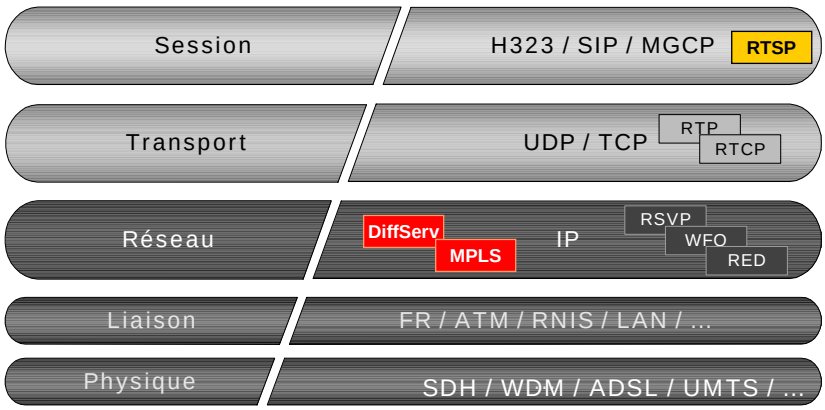
2-Éléments techniques



- Processus de Standardisation
- Traitement de la voix et Contraintes techniques
- Protocoles IP pour la voix

2- Éléments techniques

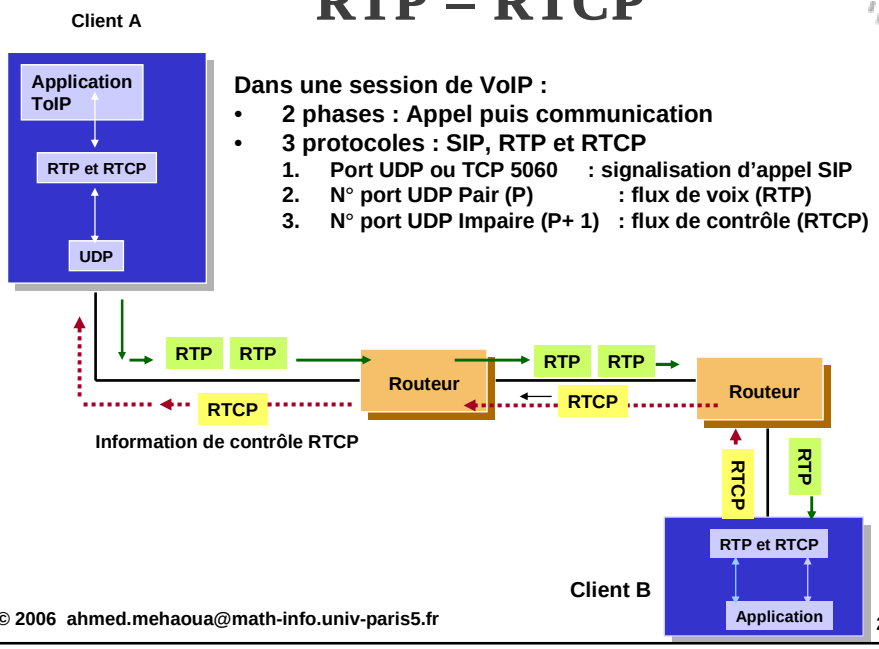
Architecture Voix sur IP



La standardisation

- IETF (www.ietf.org)
- UIT (www.itu.org)
- ETSI – TIPHON (www.etsi.org)
- MS FORUM / SoftSwitch (www.msforum.org)
- SIP Forum (www.sipforum.org)
- 3GPP (UMTS) (www.3gpp.org)

RTP – RTCP



Dans une session de VoIP :

- **2 phases : Appel puis communication**
- **3 protocoles : SIP, RTP et RTCP**
  1. **Port UDP ou TCP 5060 : signalisation d'appel SIP**
  2. **N° port UDP Pair (P) : flux de voix (RTP)**
  3. **N° port UDP Impaire (P+ 1) : flux de contrôle (RTCP)**

RTP/RTCP : principes

- **Qu'est ce que c'est ?**

  RTP (Real-time Transport Protocol) est un protocole de transport de flux temps-réel en mode multicast ou unicast :
  - **Conférence audio, vidéo interactive, diffusion vidéo, audio**

  Indépendant des couches réseaux mais habituellement implémenté au dessus de UDP/IP.

  Fortement couplé aux applications qu'il transporte : notion de PROFIL

  Combiné a un protocole de signalisation de la qualité des transmissions RTCP (Real-time Transport Control Protocol) pour la mesure des performances et le contrôle de la session en cours,

- **Qui l'a développé ?**

  IETF (RFC 1889 puis RFC 3550 depuis juillet 2003)

RTP/RTCP : principes

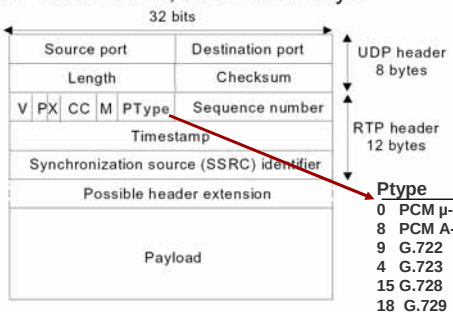
- **A quoi sert RTP ?**
  - **Segmentation / Réassemblage des données**
  - **Synchronisation des flux**
  - **Indication du type de données**
  - **Identification de l'emetteur (communication multipoint)**
  - **Détection des pertes**
  - **Sécurisation des échanges (cryptage)**

- **A quoi sert RTCP ?**
  - **Fournir périodiquement des rapports sur la qualité des échanges entre récepteurs et émetteur**
    - **Downlink : données envoyé, estampilles de temps**
    - **Uplink : pertes, délais, gigue**
  - **Garder une trace de tous les participants à une session**
    - **CNAME (Canonical Name) : identifiant unique et permanent pour un participant**
    - **SSRC (Synchronisation Source Identifier)**

Identification des paquets RTP

- How to identify RTP packets ?
  - Layer 4 classification ?
    - No, RTP can use any even port number
    - RTCP uses an odd port number
    - UDP ports 5004−5005 are often used, but not always
  - Heuristic
    - look at RTP constants

```
If (UDP) AND
   (Dest_port is even) AND
   (RTP_Version==2) AND
   (PType == assigned value)
    { /* looks like RTP packet */ }
else
    { /* should be something else */
```



Ptype

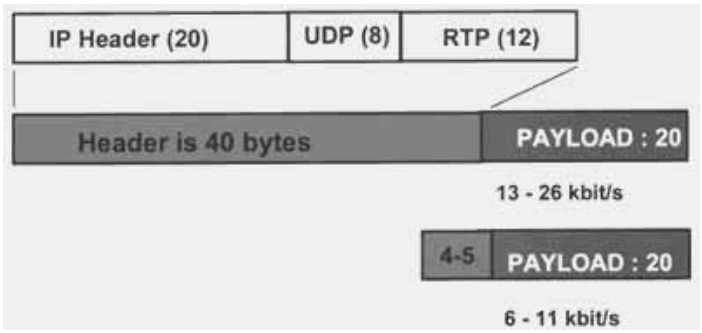
0	PCM µ-Law
8	PCM A-law
9	G.722
4	G.723
15	G.728
18	G.729
31	H.261
34	H.263
94	MP4V
96	MP4A

V : version RTP
P : padding
X : en tête suivi d'une extension
CC : Nbre de source inclus dans le paquet RTP
M: marqueur (fin d'image par exemple)

RTP – Encapsulation

• 20ms de parole à 8 Kbits/s (G.729) : soit 160 échantillons ou 20 octets de payload, sont transportés avec 40 octets d'entête.

• Compression des en-têtes (option non interopérable entre systèmes).



IETF
Session Initiation Protocol

- **Qu'est ce que c'est ?**

  SIP est un protocole de signalisation **extensible** en mode client/serveur pour la gestion de sessions multimédia (audio, vidéo) indépendant du protocole de Transport (UDP ,TCP, IPX) car il intégrant ses propres mécanismes de fiabilité de fonctionnement;

  Il utilise typiquement **UDP** et le n° port **5060**

  RFC **3261** : 170 pages (6 messages au format ASCII)

- **Qui l'a développé ?**

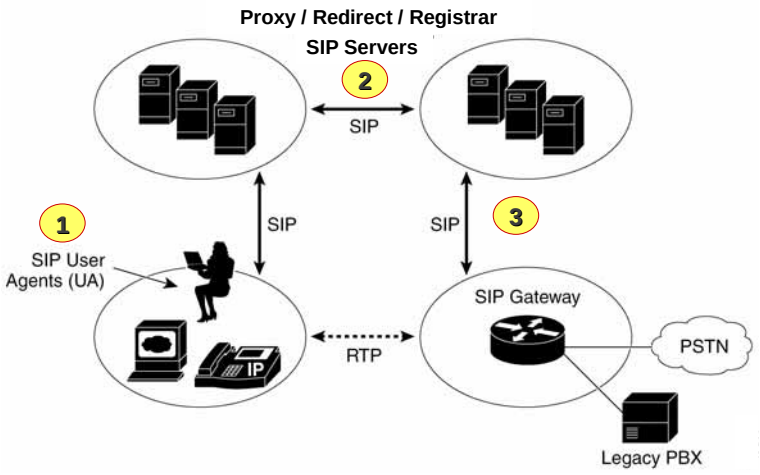
  Standard proposé par le groupe de travail de l'IETF MMUSIC (Multiparty Multimedia Session Control) de Fév. 1996 à mars 1999 [RFC 2543], puis repris et amélioré par un nouveau groupe de travail appelé SIP [RFCs 3261-3265],

IETF
Session Initiation Protocol

- **A quoi sert il ?**

1. Il permet aux utilisateurs de mettre en place, modifier, clore des conférences multimédia (pas seulempent audio) entre deux ou « plusieurs » participants, en véhiculant l'information de contrôle nécessaire,
2. Permet d'enregister, de localiser et de gérer la mobilité des utilisateurs;
3. d'integrer les applications Web avec les applications vocales et vidéo
4. de créer et contrôler des services multimédia/téléphonique de bout en bout (Instant messaging, vidéoconférence, PABX, partage d'applications …)

SIP: Architecture



SIP: Composants

User Agent	Système qui initie et reçoit des appels	Envoi (UAC) et reçoit (UAS) des requêtes SIP	Terminal H.323
Redirect Server	Serveur qui oriente les clients vers les destinataires	- translation d'adresses (DNS)	Gatekeeper
Registrar Server	BD/Annuaire qui enregistre les clients	Basé sur n'importe technologies (LDAP, SQL,…)	Gatekeeper HLR GSM
Proxy Server	Serveur qui traite les requêtes des clients et détermine quel est le prochain serveur a contacter pour atteindre le destinataire. Une sorte de Routeur SIP	- Routage d'appel (TRIP) - Load Balancing d'appel - Authentification, Autorisation, Facturation (RADIUS, DIAMETER, PGP …) - Firewall / NAT	Gatekeeper

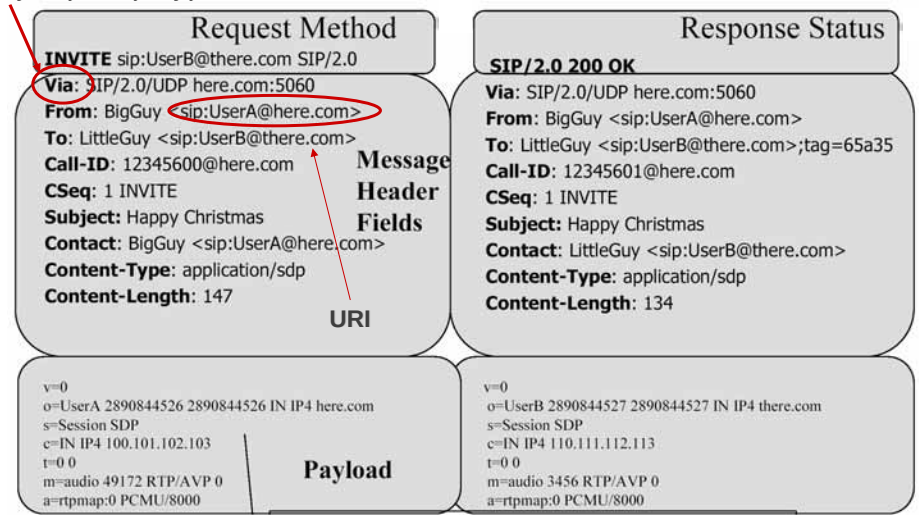
6 Requêtes SIP
et Codes Réponses

Requête	*Description*
REGISTER	Enregistrement des clients dans un serveur Registrar/location
INVITE	Initie un appel
ACK	Confirme l'établissement d'un appel
BYE	Termine ou transfert un appel
CANCEL	Met fin à une procéedure/sonnerie d'appel
OPTIONS	Négociation des capacités d'un client ou d'un serveur

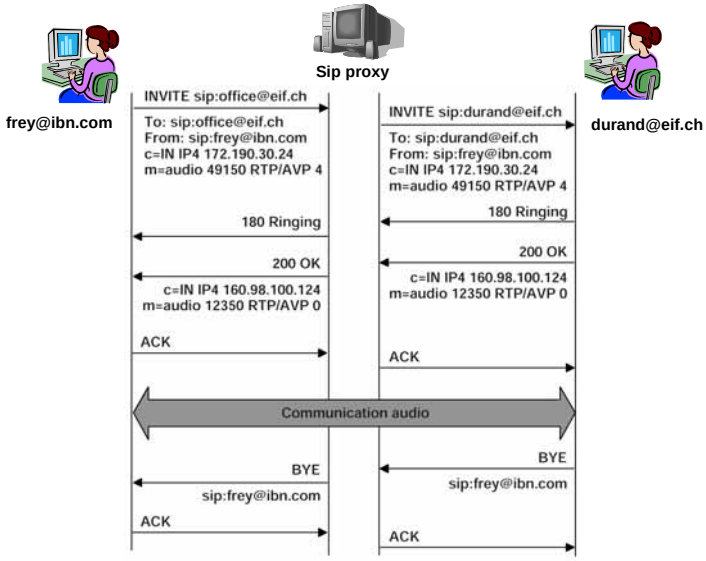
Code	*Types de réponses*
1xx	Information d'appel
2xx	Confirmation de succès
3xx	Redirection d'appel
4xx	Echec d'appel
5xx	Erreurs de serveurs
6xx	Echec général

Structure des messages

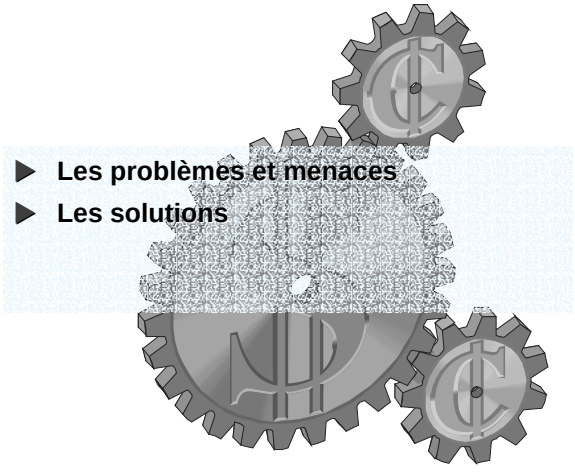
Ajouté par les proxy pour identifier le chemin au retour et éviter les boucles



Procédure d'appel SIP
UA/UA indirect via proxy



3-ToIP et sécurité



- Les problèmes et menaces
- Les solutions

Les problèmes & menaces

- Firewalls and NATs
- Security
  - Privacy
  - Encryption
  - Authentication
  - Denial of Service (DoS) attacks
  - Intrusion attacks
  - SPAM over Internet Telephony (SPIT)

Nat et ToIP

- Different issues with
  - SIP signaling
  - Media
- SIP signaling and media transport is done peer-to-peer
- Media ports are negotiated per call

NAT : Fonctionnement

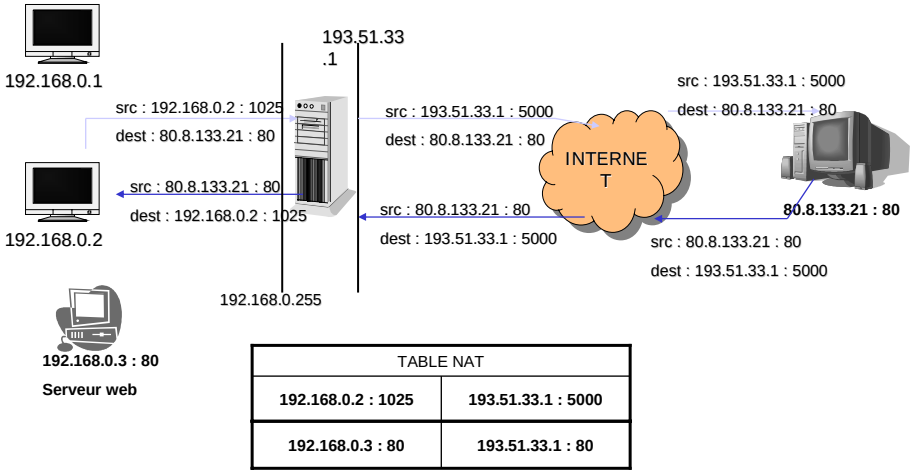
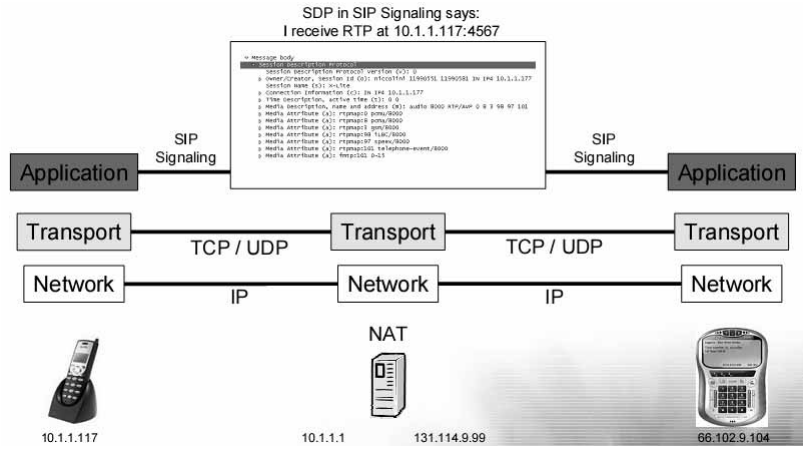


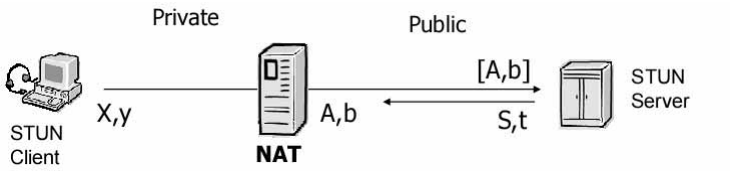
TABLE NAT	
192.168.0.2 : 1025	**193.51.33.1 : 5000**
192.168.0.3 : 80	**193.51.33.1 : 80**

2 – ToIP et sécurité

Nat et ToIP



ToIP & NAT: STUN



- IETF RFC 3489 "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)"
  - discover public IP address (and port mapping rules) of NAT between client and Internet
  - requires a STUN client in the SIP UA
    - best SIP UA have STUN support (Xten software, Zyxel WiFi phone)
  - requires additional deployment of a STUN server placed in the public space (normally co-located with the SIP Proxy server)

ToIP & DoS

SIP Denial of Service (DoS) attacks

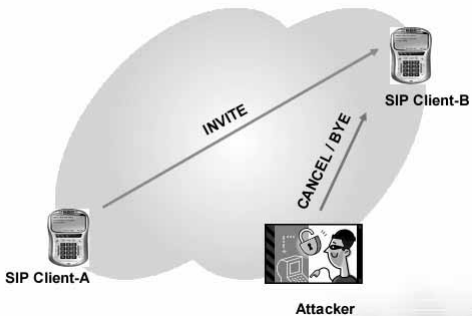
- Using SIP CANCEL message
  - preventing UAs from making and receiving calls
  - making UAs drop the call
- Using SIP BYE message
  - making UAs drop the call

RTP Denial of Service (DoS)

- The way RTP handles SSRC Collisions
  - Sending command using SSRC of another participant of a session
    - Result: The ability to drop users from a certain session
  - Claiming SSRC of a user
    - Result: Transmission will stop, new selection of SSRC needs to take place and the transmission should resume
- RTCP "BYE", not in sync with the Signaling protocol
  - Result: The Signaling protocol is not aware that there is no exchange of voice samples any more
- Forging Reception Reports
  - Reporting more Packet Loss
    - Result: usage of a poor quality codec with an adaptive system

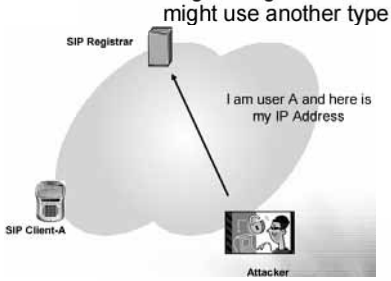
SIP DoS

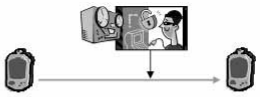
Preventing SIP Client-A from making call



ToIP & Confidentiality

- Identity Theft
  - Registering address instead of other (if requires authentication might use another type of attack)

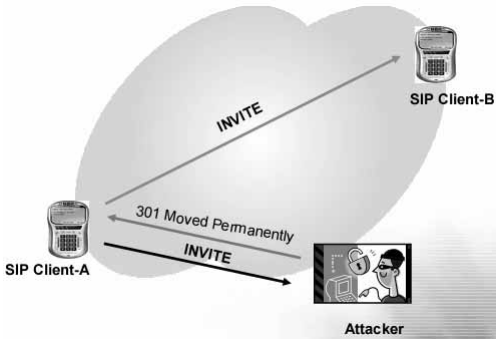




- Call Eavesdropping
  - Capturing RTP flows
    - Since RTP identifies the codec being used (statically) or either using a "dynamic" identified codec it is easy to reconstruct the voice sampling (even in real time)
    - Result: listen/record conversations
    - Result: listen DTMF tones to steal passwords and PINs

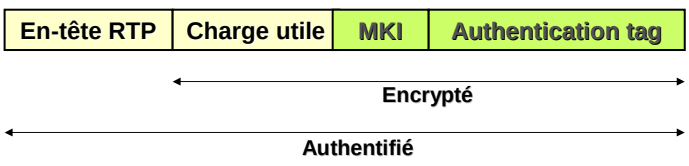
ToIP & Confidentiality

- Call Hijacking
  - After INVITE message, a 301 “Moved Permanently” message would hijack the call towards whoever the attacker decides (himself of another client)



Secure RTP

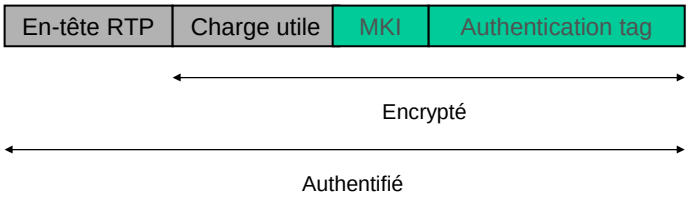
- **RFC Défini un canevas pour l'encryption et l'authentification des messages des flux RTP et RTCP.**
- **Transformations basées sur :**
  - **L'ajout d'un flux de cryptage (confidentialité),**
  - **Une empreinte de hash pour l'authentification et intégrité,**
  - **Un index implicite (SRTP) contre le rejeux.**



Fonctionnement de SRTP

- **Du côté émetteur : Intercepte les paquets RTP et retransmet leur équivalent SRTP.**
- **Du côté récepteur : Intercepte les paquets SRTP et retransmet l'équivalent RTP.**

- **Format d'un paquet :**



Fonctionnement SRTP

- **L'index est déterminé.**
- **Pour encrypté les paquets RTP : Utilisation d'une « Master Key » et de « Sessions keys ».**
  - **La Master Key est une séquence obtenue aléatoirement, identifié par le MKI**
  - **Une fonction de dérivation permet de calculer les Sessions Keys**
  - **Le message est crypté grâce aux Sessions Keys**
- **Si nécessaire, le message est authentifié et l'authentification tag est renseigné.**

Composants d'IPsec

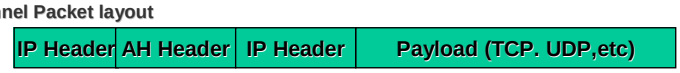
- **Services de sécurité :**
  - **Confidentialité**
  - **authentification**
  - **Non rejeux**
- **Protocoles de sécurité :**
  - **Authentication Header (AH)**
  - **Encapsulation Security Payload (ESP)**
- **Protocole d'échange de clefs :**
  - **Internet Key Exchange (IKE)**
- **Bases de données internes :**
  - **Security Policy Database (SPD)**
  - **Security Association Database (SAD)**

IPSec protocols – AH protocol

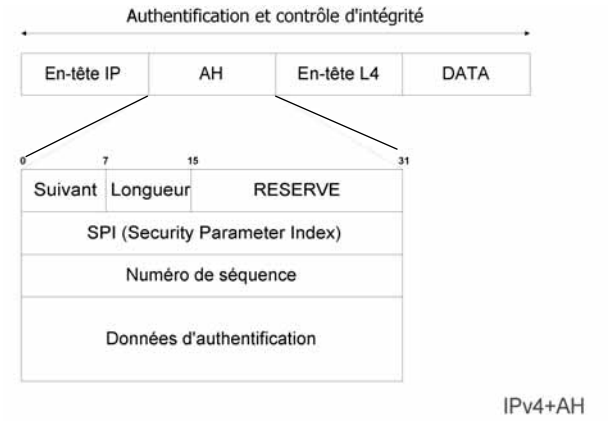
- AH - Authentication Header
  - Defined in RFC 1826
  - Integrity: Yes, including IP header
  - Authentication: Yes
  - Non-repudiation: Depends on cryptography algorithm.
  - Encryption: No
  - Replay Protection: Yes

Transport Packet layout

Tunnel Packet layout

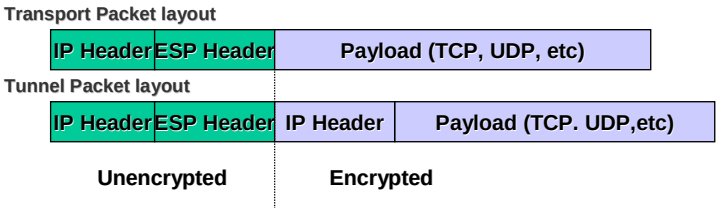


III. Protocole de sécurité AH

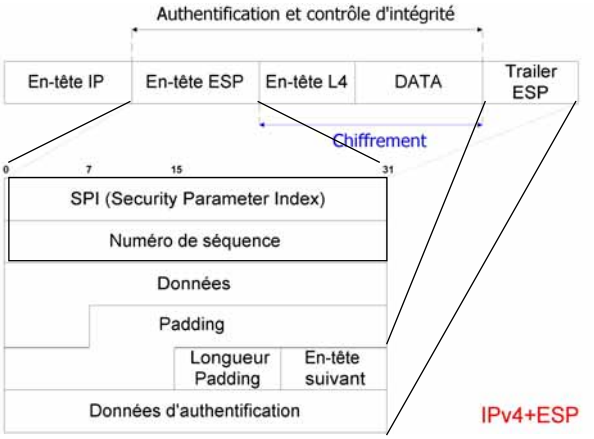


IPSec protocols – ESP protocol

- ESP – Encapsulating Security Payload
  - Defined in RFC 1827
  - Integrity: Yes
  - Authentication: Depends on cryptography algorithm.
  - Non-repudiation: No
  - Encryption: Yes
  - Replay Protection: Yes



IV. Protocole de sécurité ESP

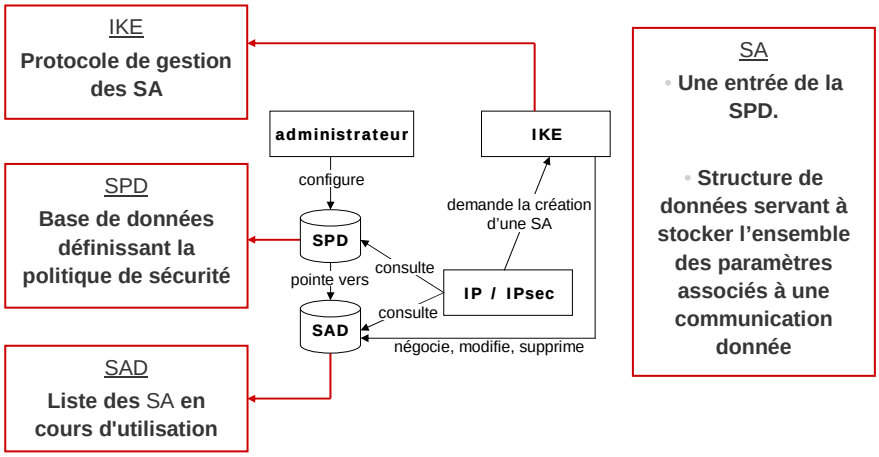


Quel protocole pour quel service de sécurité ?

Table 16.1 IPSec Services

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

IP SEC – Principe de fonctionnement



2 – ToIP et sécurité

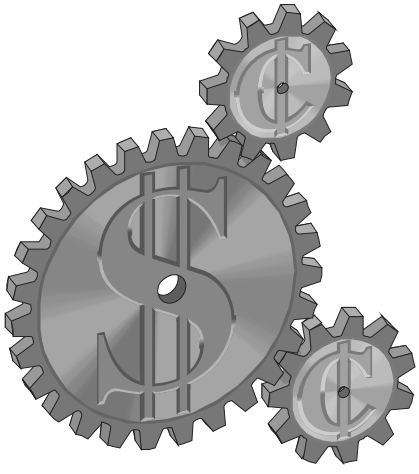
ToIP & Security solutions

- Signaling
  - End-to-end
    - S/MIME (Secure/Multipurpose Internet Mail Extensions), IETF RFC 2633
      - provides a way to send and receive secure MIME data. Based on the MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption)
  - Hop-by-hop
    - Lower-Layer solutions (e.g. IPsec)
      - IPSec is actually a suite of protocols being developed by the IETF in the IPsec charter for authentication and encryption
    - SIPS (requires Transport Layer Security, TLS, on whole signaling path)
      - TLS version 1.0, detailed in IETF RFC 2246 but going to be updated to version 1.1, is a client/server protocol that allows peers to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery
- Media
  - Lower-Layer security (e.g. IPsec)
  - SRTP (Secure Real Time Protocol), IETF RFC 3711
    - provides confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP
    - key exchange done using MIKEY (Multimedia Internet KEYing), IETF RFC 3830
      - a key management scheme that can be used for real-time applications (both for peer-to-peer communication and group communication) supporting SRTP

VoIP & Security solutions

Communication layers	Security protocols
Application layer	S/MIME, Secure RTP
Transport layer	SSL, TLS
Network layer	IPsec
Data Link layer	WPA
Physical layer	Scrambling

4- Travaux pratiques



5-Approche commerciale

- Les Produits et Solutions
  - Offre pour Entreprises (PME/PMI)
  - Offre pour Opérateurs

3- Produits et solutions d'entreprises

SIEMENS

OptiPoint 300 (H.323) & 400 (SIP)

HiPath 3700

HiPath 4000
Migration à partir du HiCom 300

OptiPoint 600

HiPath 3300

HiPath 3500

HiPath 5500

3- Produits et solutions d'entreprises

Module Access Gateway
Catalyst 4000 series

Téléphones IP Cisco

Cisco ICS-7500

Cisco VG200 VoIP Gateway

3- Produits et solutions pour Opérateurs

Cisco MGX8000 series

- **Voice over IP (VoIP) et Voice over ATM (VoATM)**
- **Interfaces : Fast-Gigabit Ethernet / Packet over SONET (POS), ATM, TDM, ISDN**
- **Session Initiation Protocol (SIP) et H.323**
- **Routage et Commutation IP (MPLS)**
- **Administration : SNMP, MGCP, CORBA, Interfaces SoftSwitch**

3- Produits et solutions d'entreprises

SIEMENS

OptiPoint 300 (H.323) & 400 (SIP)

HiPath 3700

HiPath 4000
Migration à partir du HiCom 300

OptiPoint 600

HiPath 3300

HiPath 3500

HiPath 5500

3- Produits et solutions d'entreprises

ALCATEL

Alcatel Premium IP Reflexes
170 Euros HT

- 2 ports switch Ethernet (10/100BT)
- Compression de la voix G711 et G723.1
- Détection de l'activité voix (VAD) et confort de génération de bruit
- QoS de niveau 3 : TOS et Diffserv
- 12 services téléphoniques
- Affichage 1 x 20
- Poids : 880 g

Alcatel OmniPCX Office

- Utilisateurs 200 max
- Firewall NAT
- Proxy/cache 1.5 GB
- Services LAN DNS, DHCP, mail POP3/SMTP
- Stockage email 3.7 GB
- Serveur CTI (Gatekeeper) H323 H323 V2
- Switch 2 à 8 ports
- Stockage émail vocal jusqu'a 200 h
- acces Internet ISDN (128kbps) External ADSL modem(2 Mbps)
- Authentication PAP/CHAP
- VPN PPTP/IPSec