Séminaire Grifes du 8.11.05

iICT
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

VoIP&Security for Enterprise

Prof. Stefano Ventura

www.ch

VoIP&Security for Enterprise

- **Introduction: VoIP 2005 le BIG Bang.**
  - La VoIP est un marché en pleine expansion ? assez des prévisions ! La parole aux utilisateurs !
  - La VoIP: rien d'autre qu'un service Internet de plus ?
- **Les étappes vers la convergence.**
  - PABX, IP enabled PBX, IP PBX.
  - Les problèmes de la convergence: La QoS.
- **Les technologies VoIP.**
  - Principes et architectures des systèmes VoIP. H.323 vs SIP.
- **Pourquoi la sécurité VoIP est si importante ?**
  - La sécurité des PABX est malgré tout déjà un vieux problème.
  - Pourquoi la sécurité VoIP est plus importante que celle des PABX.
- **La sécurité VOIP et ses enjeux.**
- **Sécurité VoIP: risques et parades.**
  - les menaces
  - les parades
- **Aspects de sécurité spécifiques à la VoIP.**
- **La problématique de Skype et conclusion.**

Introduction: VoIP 2005 le BIG Bang

Last VoIP breaking News

Ebay s'offre Skype pour 3,3 milliards d'euros

Mis à jour - Ebay a réussi là où Yahoo et News Corp ont échoué en s'emparant d'une des sociétés les plus convoitées du secteur. Il prévoit déjà de facturer les communications spéciales entre vendeurs et acheteurs sur sa plate-forme d'enchères.

Skype con… …ay, après Yahoo et News Corp

Express - …tre de toutes les convoitises: selon les …*eet Journal*, Ebay a engagé des dis… …été luxembourgeoise, numér… …La transaction pour… …de dollars.

S…

Microsoft va in…

Technologie - Tano… prudemment, Microsoft a… la start-up américaine Téléo, …

Vonage plans $…0 million IPO, report says

A public offering from the Net phone company would be an important test of investors' appetite for technology start-ups, a report says. Thu Aug 25 05:47:00 PDT 2005

▪VoIP and IP telephony ▪Funding/IPO ▪Microsoft Corp A T & T Corp ▪Yahoo! Inc

Intel dials up Skype support

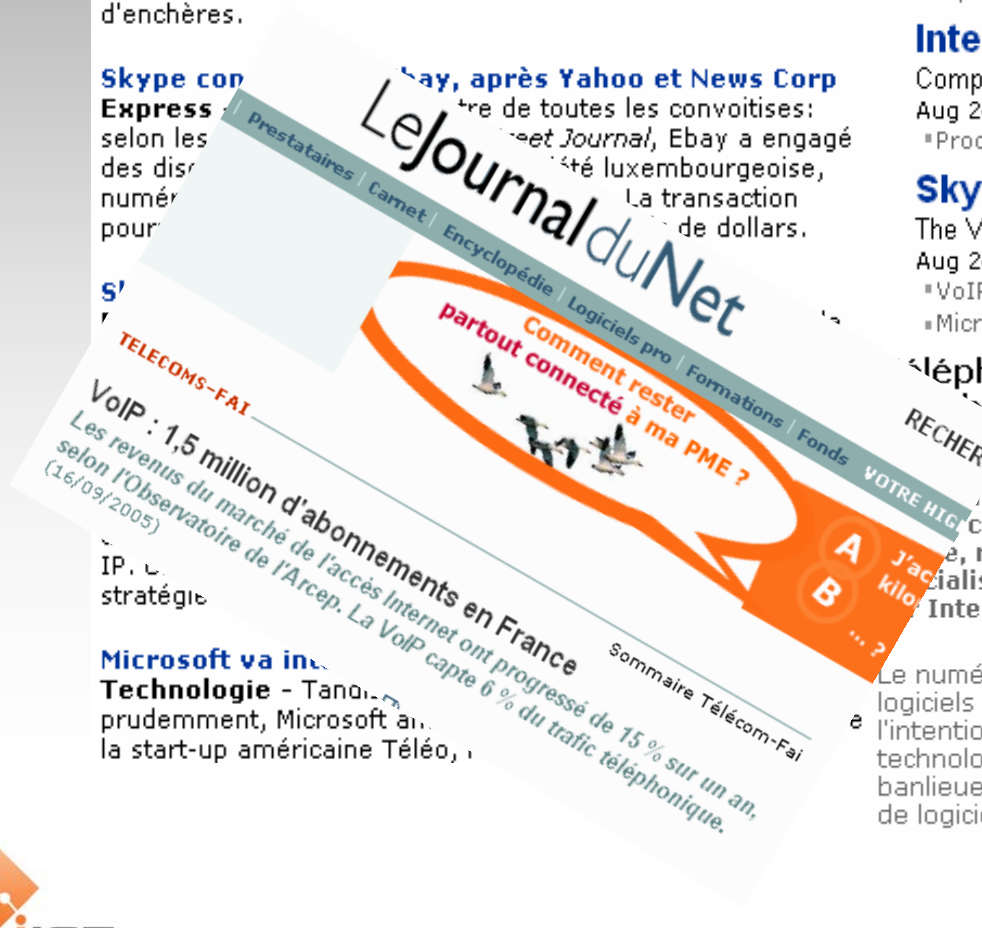
Companies pool R&D resources to ensure clear Internet phone calls or
Aug 24 15:04:00 PDT 2005

▪Processors ▪Personal computers ▪VoIP and IP telephony ▪Suppo

Skype releases IM developer tools

The VoIP giant is opening up its instant-messaging program for integra
Aug 24 00:00:00 PDT 2005

▪VoIP and IP telephony ▪Authoring ▪Software engineering/developr ▪Microsoft Corp ▪Yahoo! Inc ▪Google



…léphonie: Microsoft rachète une entreprise …oise

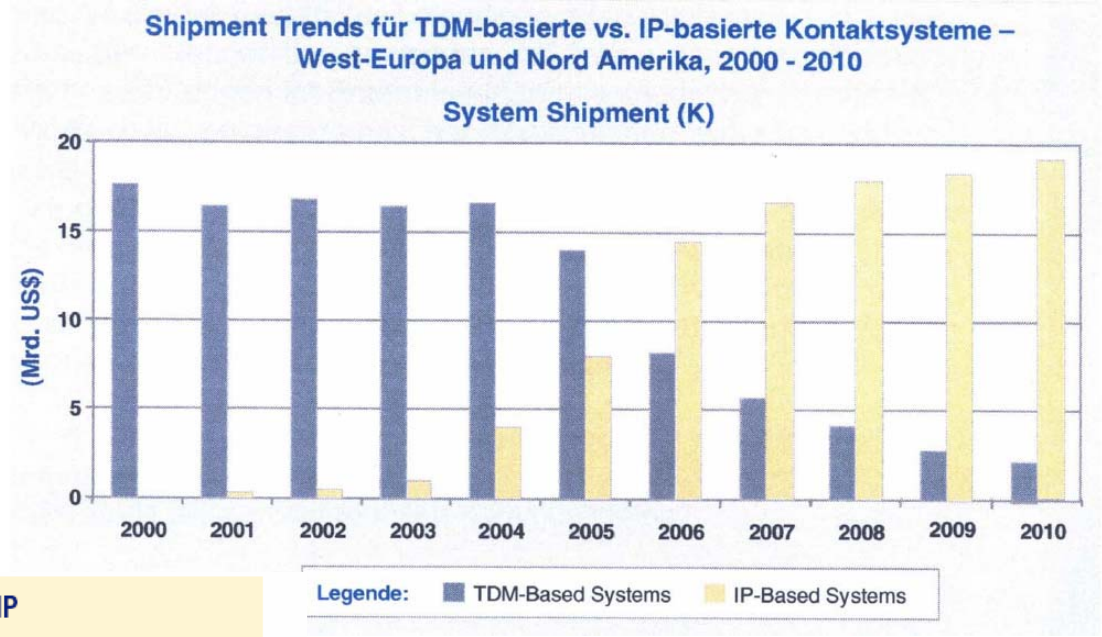
16:29 - mise à jour: 17:29

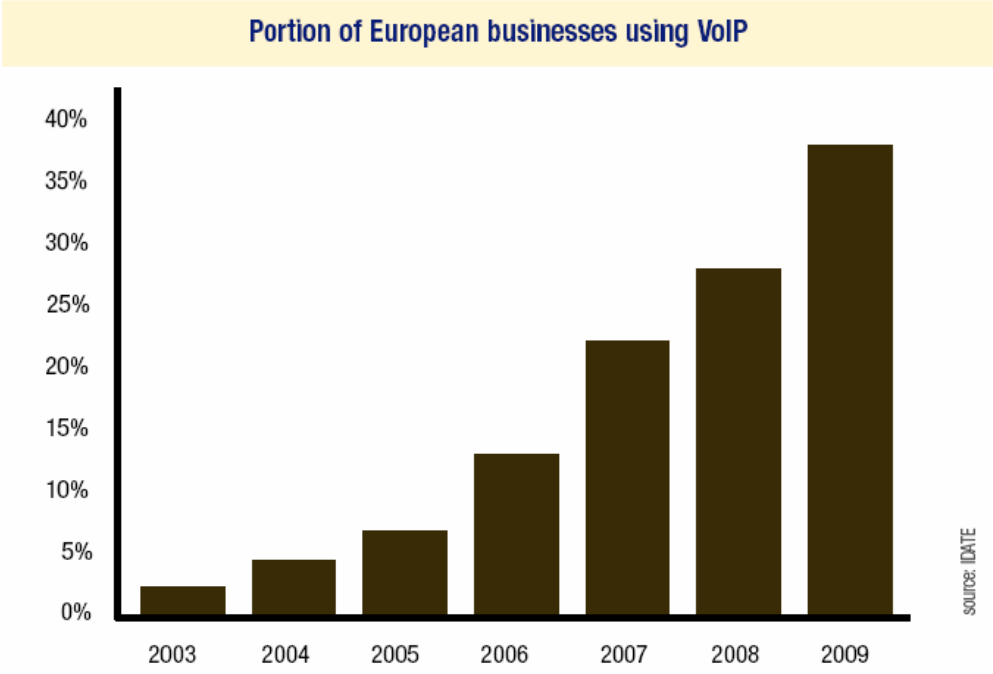
…t américain Microsoft a …contrôle d'une société …e, media-streams, …cialisée dans la téléphonie … Internet.

Le numéro un mondial des logiciels a expliqué qu'il avait l'intention d'intégrer la technologie développée dans la banlieue zurichoise dans sa suite de logiciel de bureau «Office».

Les managers de media-streams se réjouissent du contrat passé avec Microsoft. [TSR]

Introduction: La VoIP est un marché en pleine expansion





Introduction: La VoIP est un marché en pleine expansion

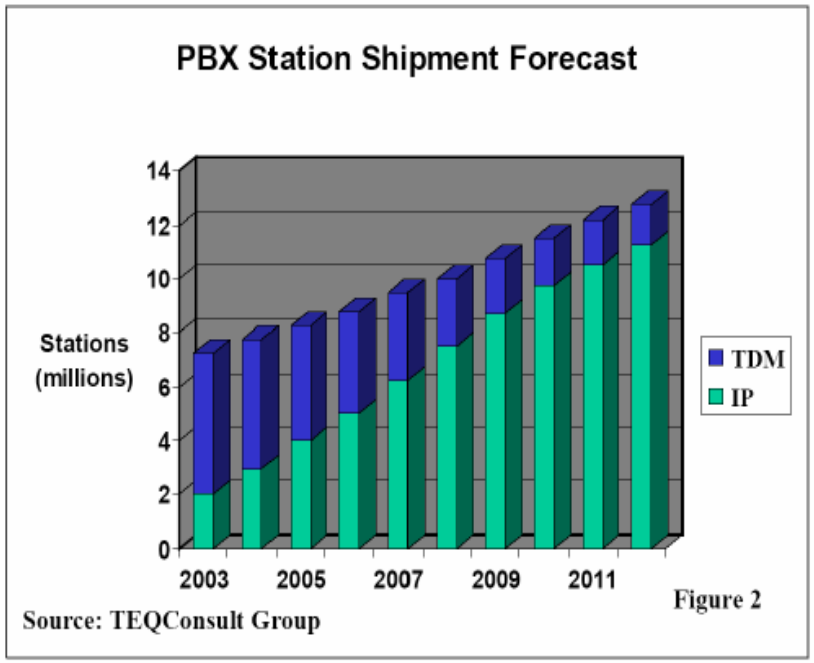
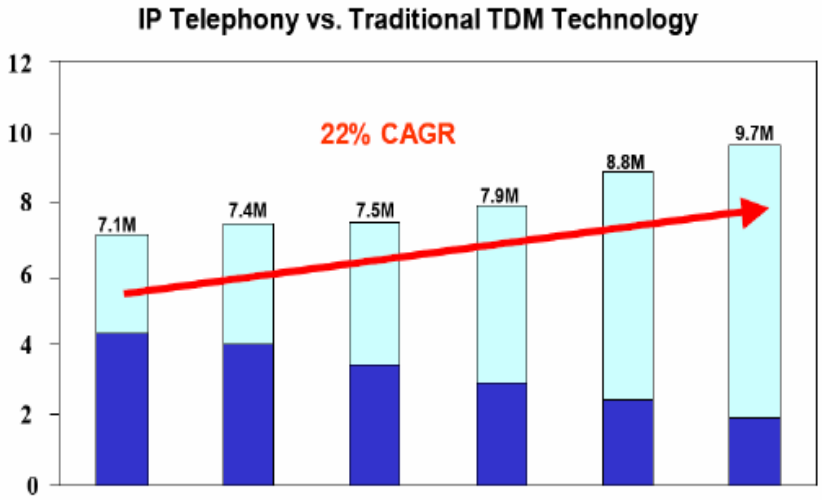


Figure 2

Source: TEQConsult Group



	2003	2004	2005	2006	2007	2008
% IP Telephony Systems	40%	46%	55%	63%	73%	80%
% Traditional TDM Systems	60%	54%	45%	37%	27%	20%

InfoTech Primary Research, *InfoTrack for Converged Communications*

Introduction: Pourquoi cet engouement pour la VoIP ?

Deux points de vue absolument différents

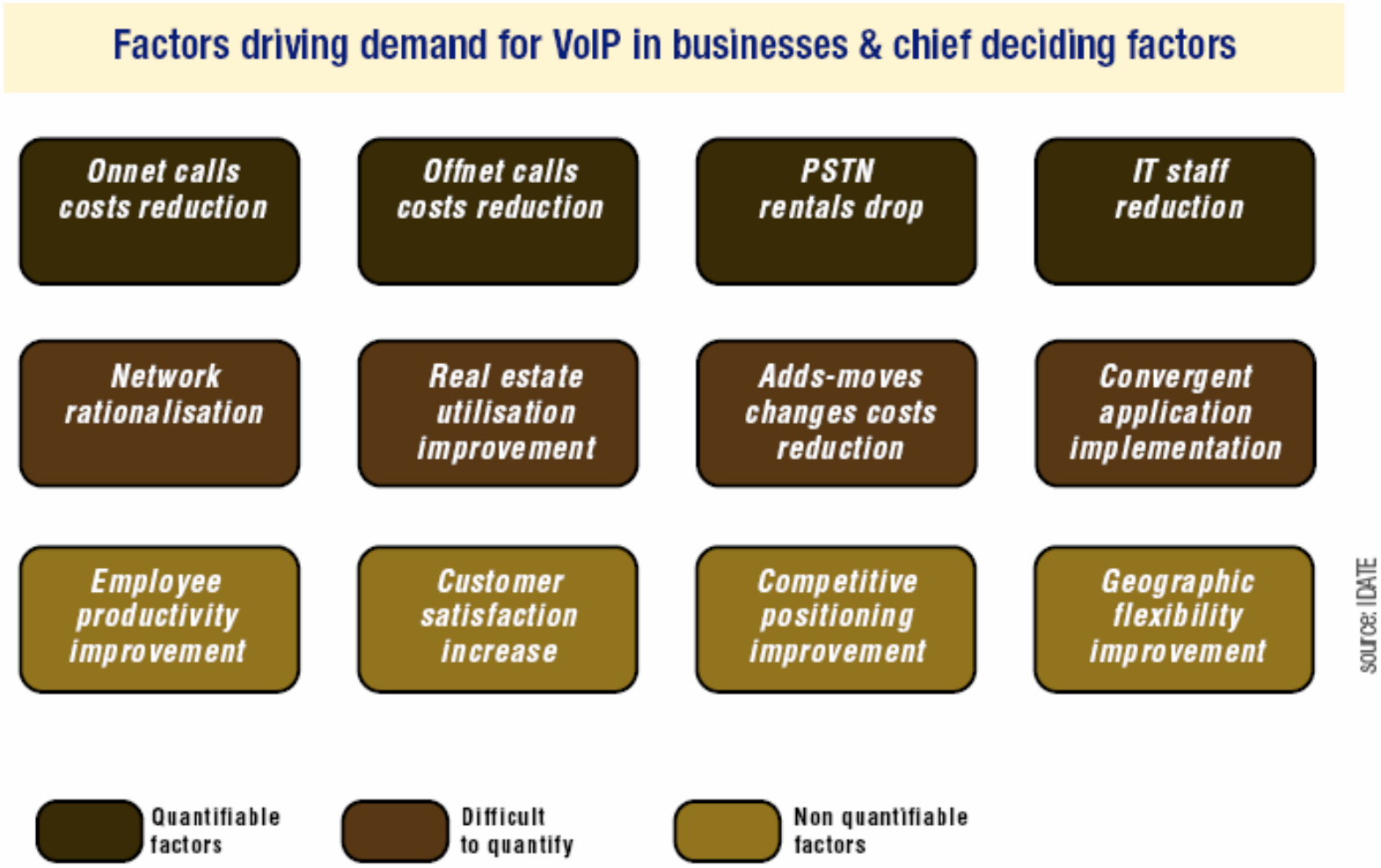
Les entreprises:

Disponibilité, Qualité, Services avantageux

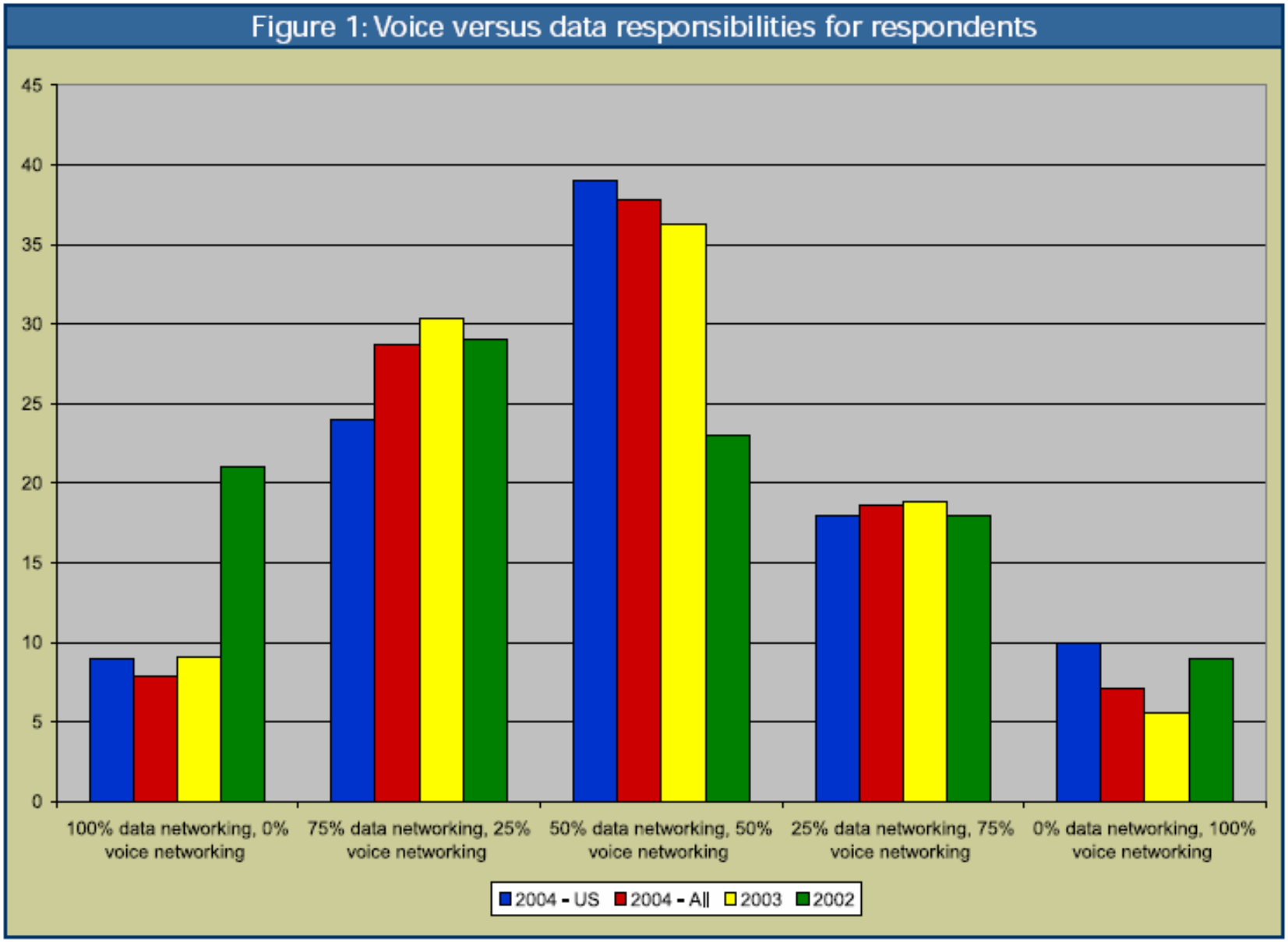
L'usager de la téléphonie sur Internet:

Le prix ! à tout prix

Les Entreprises: Pourquoi la VoIP

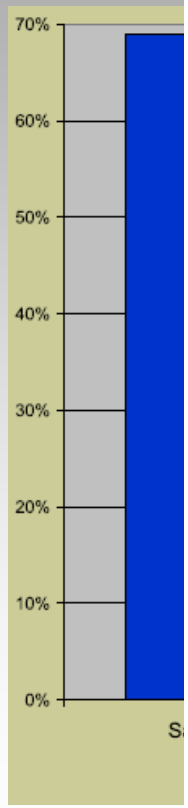


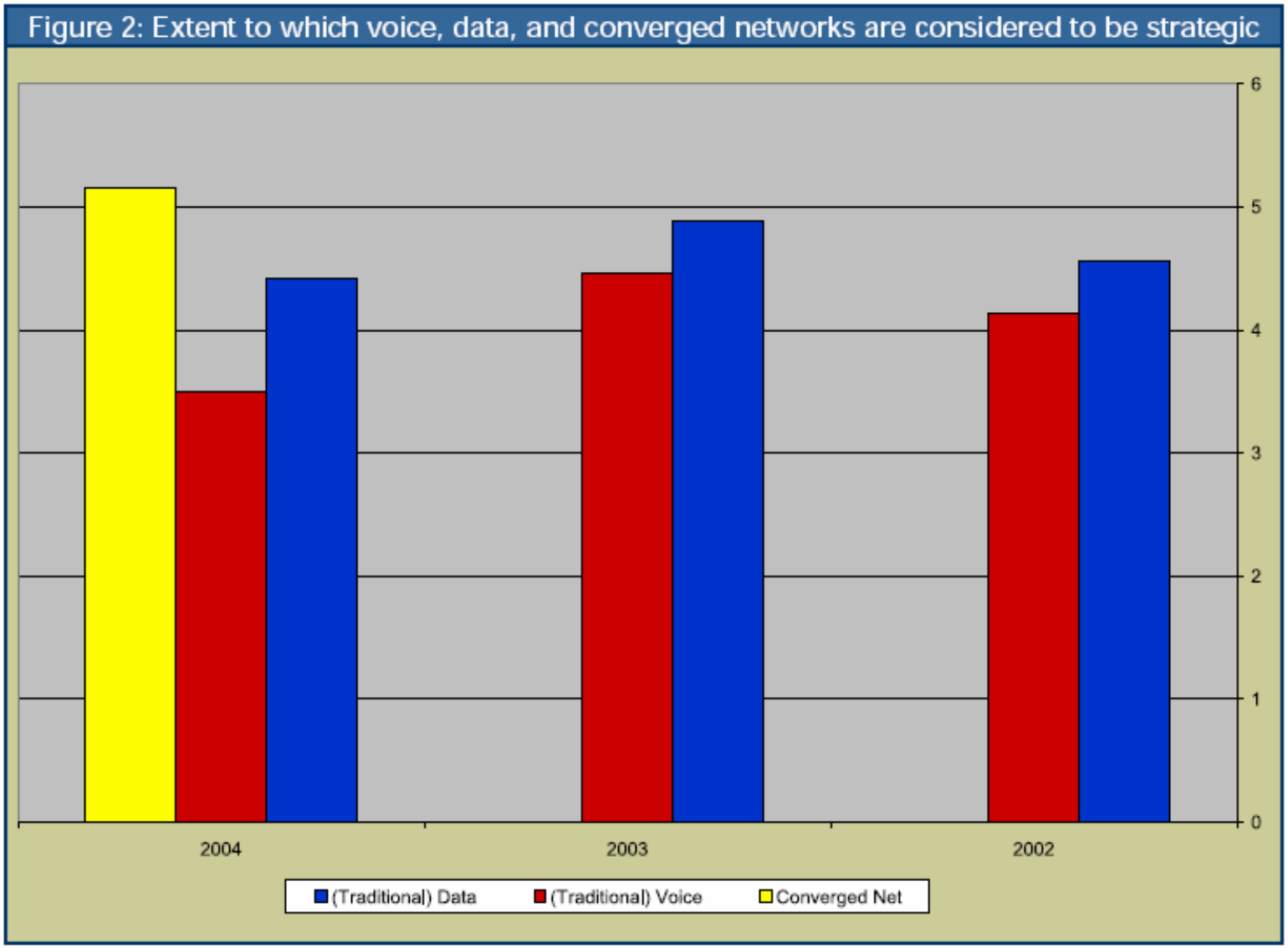
Assez des prévisions ! La parole aux utilisateurs. Les profil des professionnels interrogés: responsables uniquement des réseaux data ou voix ou des deux?



Source: Webtorials/2004 VoIP State of the Market report

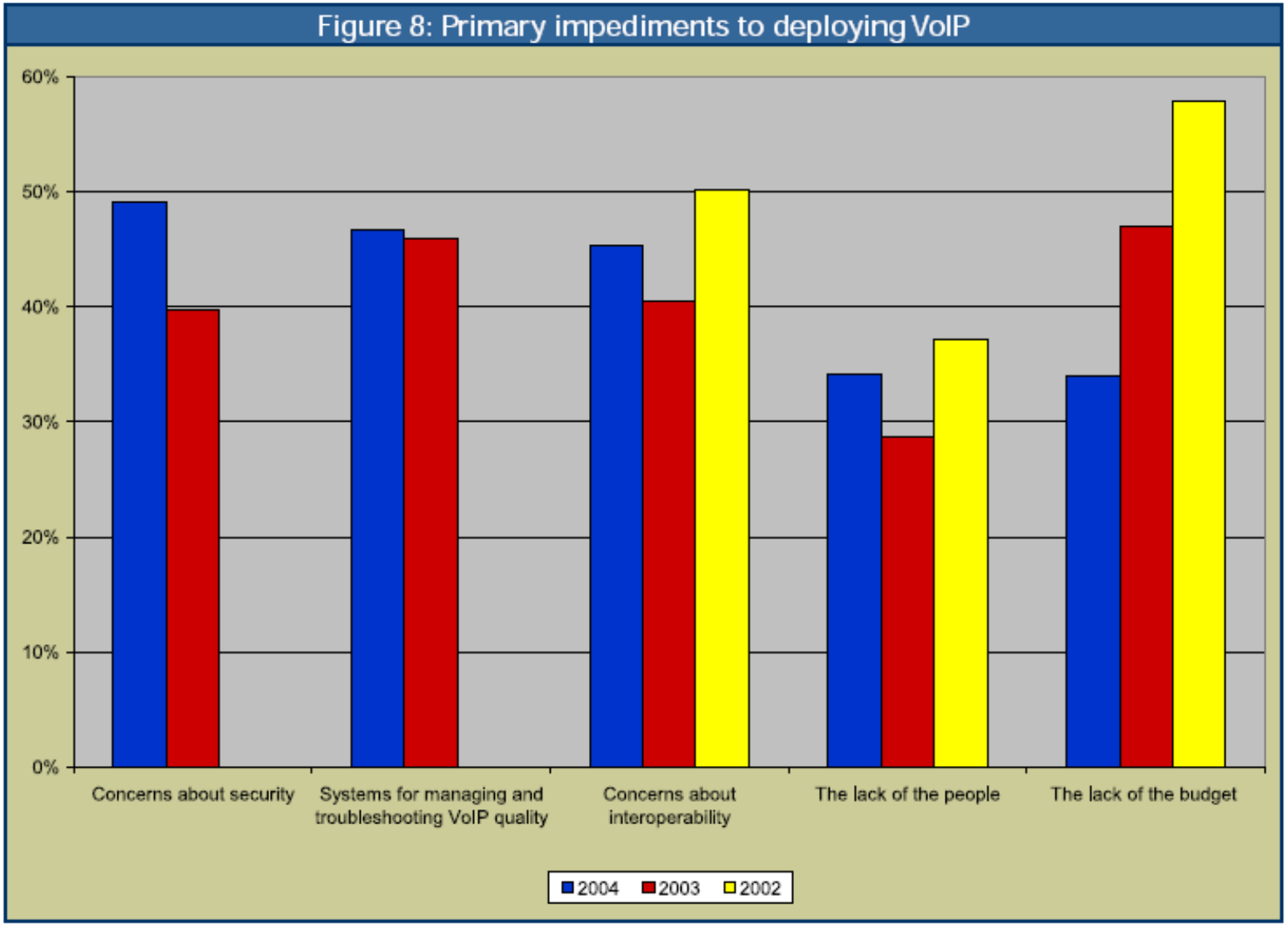
Assez des prévisions ! La parole aux utilisateurs.
La convergence est-elle perçue réellement comme stratégique





Source: Webtorials/2004 VoIP State of the Market report

Assez des prévisions ! La parole aux utilisateurs.
Les raisons principales qui freinent le déploiement de la VoIP



Source: Webtorials/2004 VoIP State of the Market report

La Voix sur IP n'est pas un service IT comme un autre!

- La téléphonie n'est pas « juste un service Internet de plus »
- Nécessité d'impliquer plusieurs groupes
  - ✓Téléphonie, réseau, applications, ….
  - ✓Habitude limitée de travailler ensemble
- Manque d'expérience interne
- Ni un projet voix, ni un projet « data », mais les deux

La téléphonie sur IP: Un environnement complexe

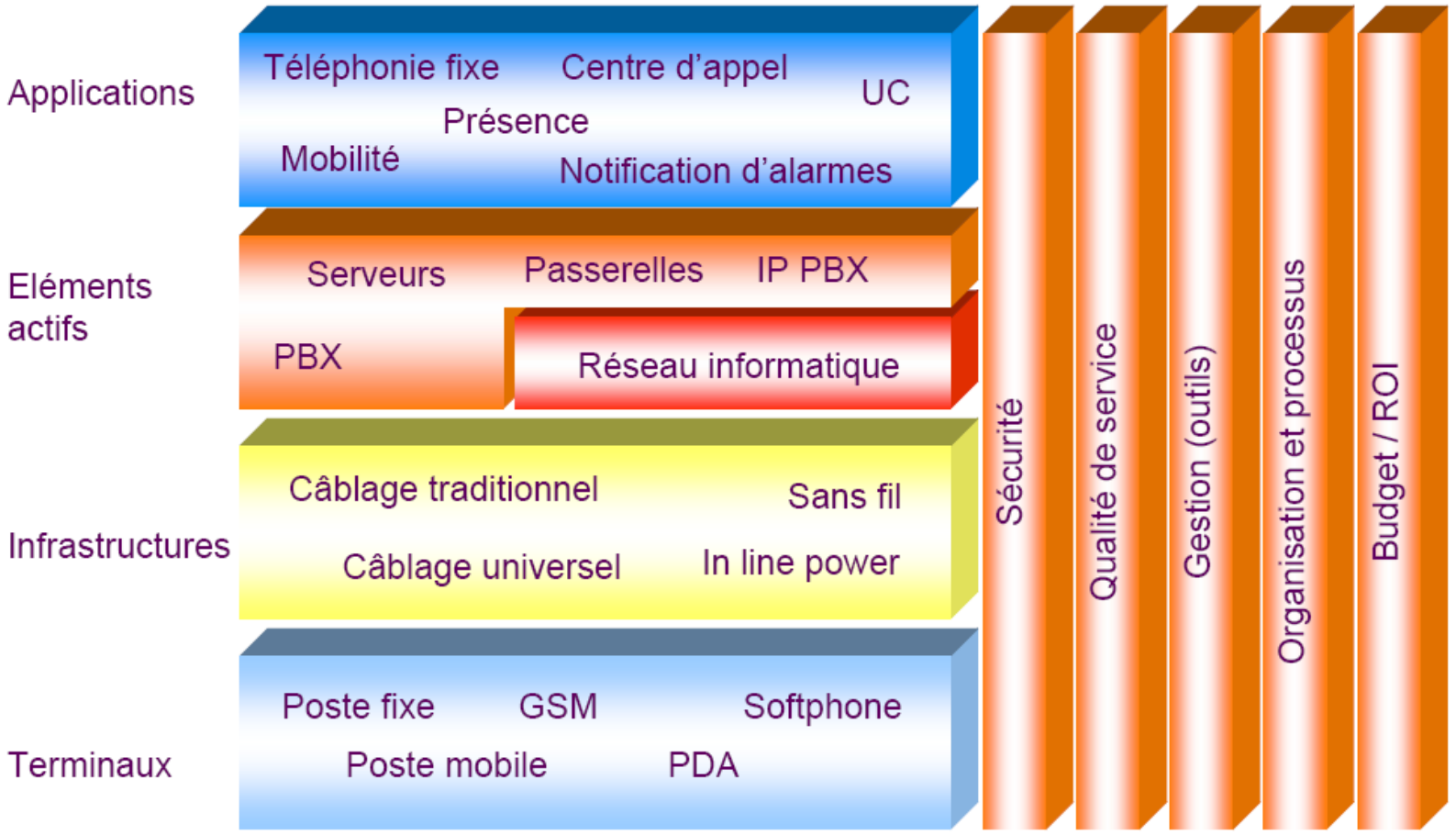


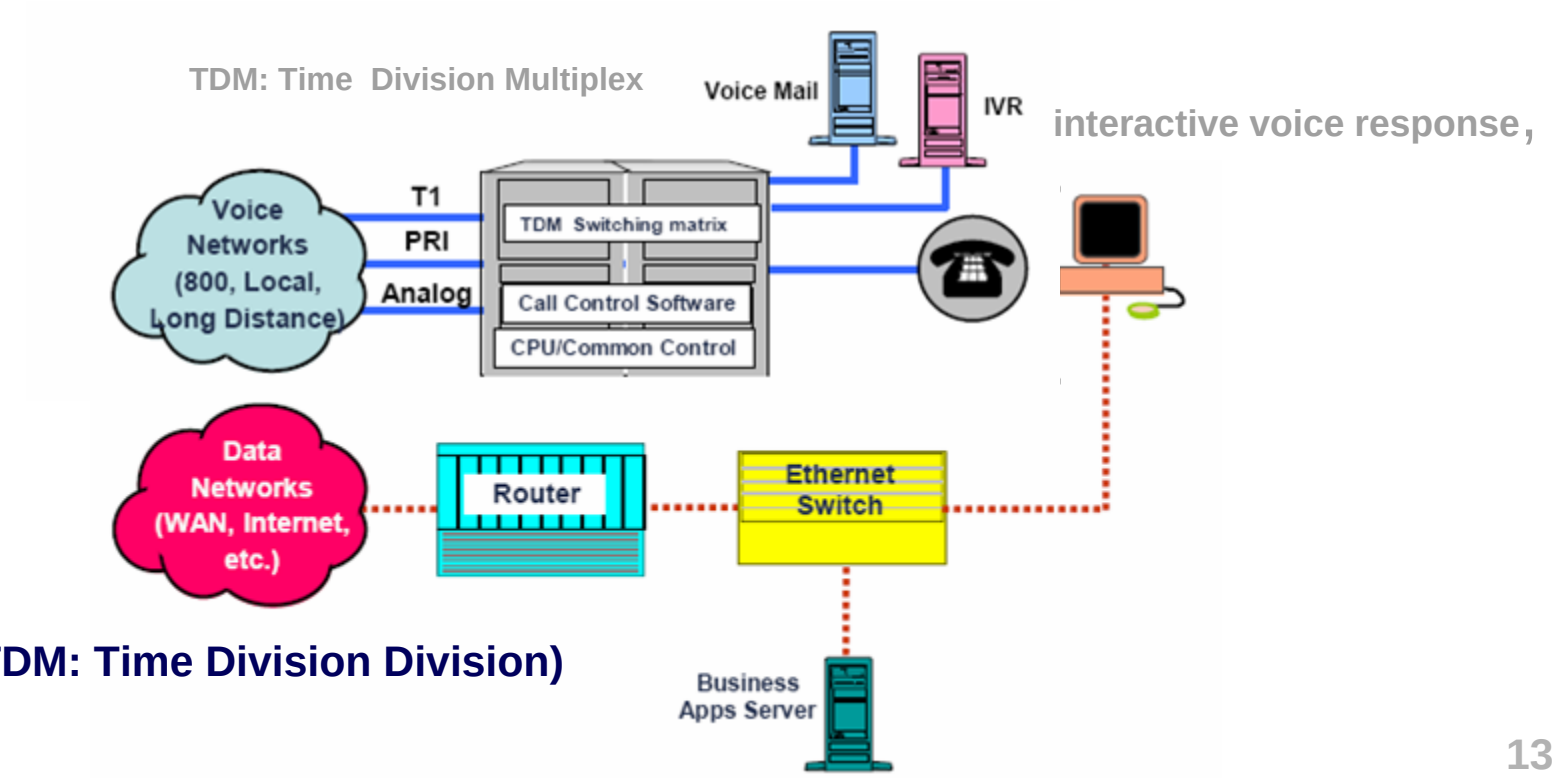
Figure de NETEXPERT CONSULTING & SERVICES

Les étapes vers la convergence: Architecture des PABX traditionnels basée sur la commutation de circuit

IP deux réseaux différents pour les services de téléphonie et les réseaux informatiques

Réseau de donnée: Réseau à commutation de paquets

Réseau de téléphonie: Réseau à commutation de circuit
TDMCentric Architecture



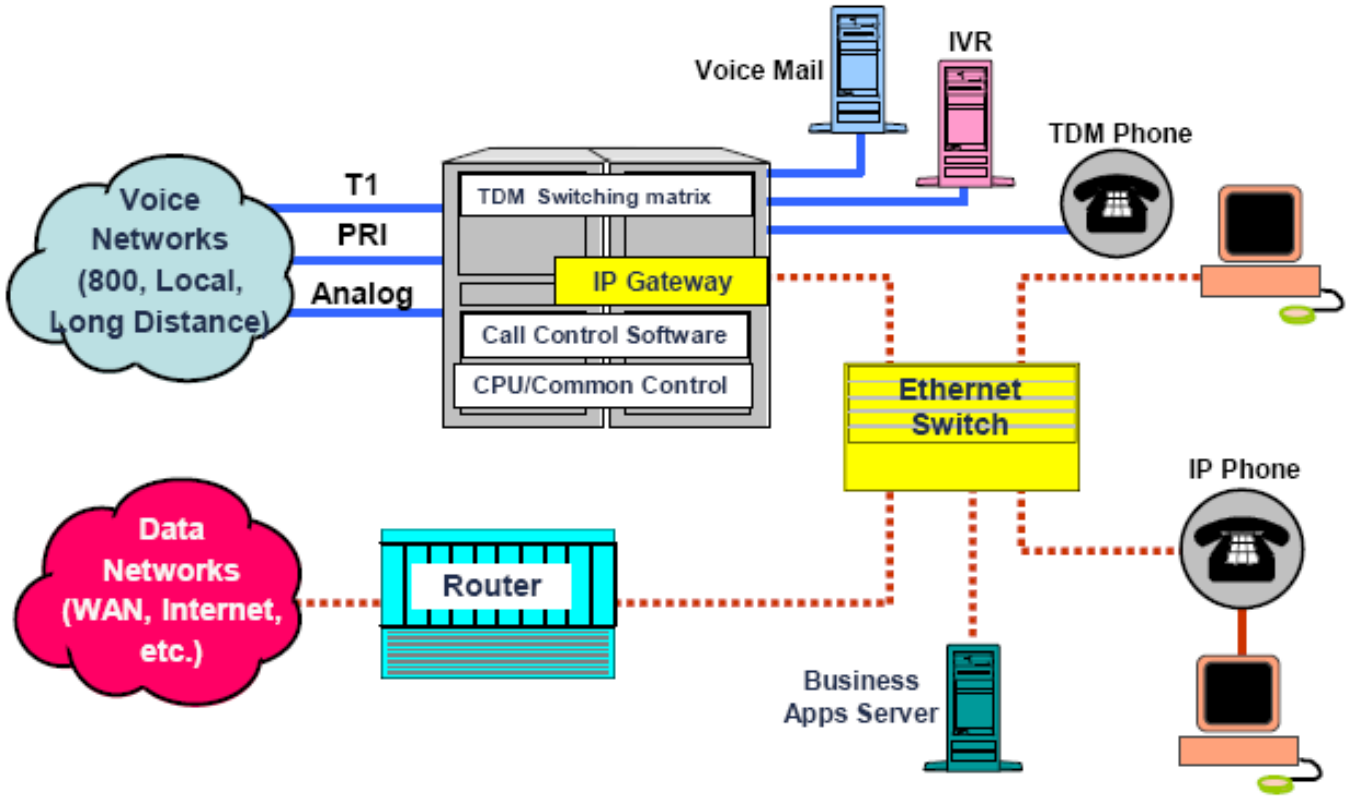
(TDM: Time Division Division)

Picture Source 2002 Vanguard Communications Corporation. www.vanguard.net

Première étape vers la convergence: IP enabled PBX

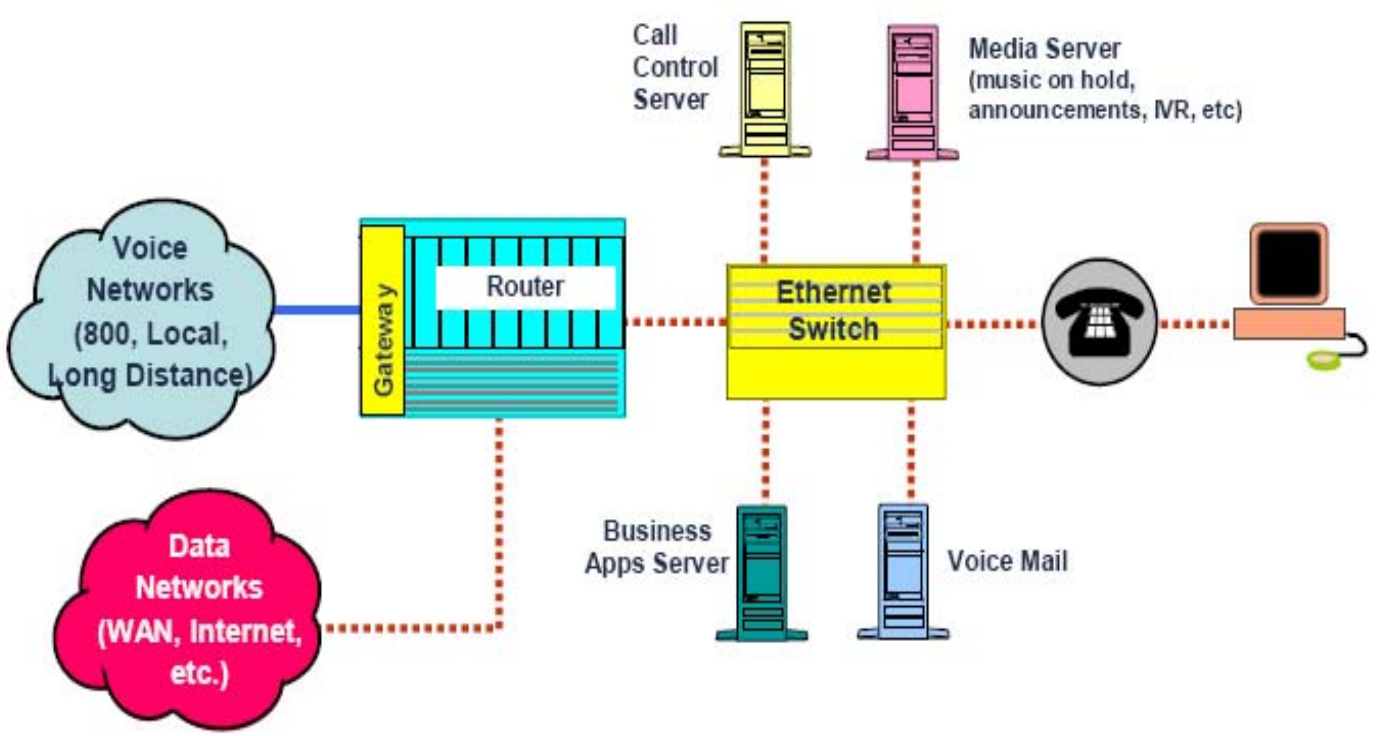
- Conserve encore les éléments les plus fiables de l'ancienne technologie (commutation de circuit)
- Permet le déploiement de services CTI (Computer Téléphonie Intégration) à des prix concurrentiels et permet aussi de services de téléphonie sur IP
- Permet l'interconnexion avec les réseaux informatiques

Première étape vers la convergence: IP enabled PBX



Picture Source 2002 Vanguard Communications Corporation. www.vanguard.net

La convergence: IP Centric Architecture ou IP PBX ou encore IP Client-Server PBX



Picture Source 2002 Vanguard Communications Corporation. www.vanguard.net

La convergence: IP Centric Architecture ou IP PBX ou IP Client-Server PBX

Les caractéristiques:

- Accomplissement de la convergence (Intégration complète du service de téléphonie au réseau d'entreprise)
- Le réseau informatique (Call Ruting) devient le réseau de commutation de la voix
- Grande flexibilité de déploiement dans le cas de petits sites éloignés
- Plus d'équipements réseau spécifique à la téléphonie
- Danger de qualité de service amoindrie.

Les problèmes de la convergence: Qualité et fiabilité
Les solutions: la qualité de service QoS et architecture

Les applications peuvent être classifiées en fonction de leur besoins en services de transports:

- Transfert de données non prioritaire: Web, FTP
- Transfert de données prioritaires: Accès base de données
- Voix sur IP: « Application Critical » VoIP: Audio- et video-Conférences

	Données non-prioritaires	Données prioritaires	VoIP / Conf. Vidéo	Streaming
Demande de débit	Moyenne à élevée	Faible à moyenne	Faible	Élevée
Sensibilité aux délais	Faible	Moyenne à élevée	Elevée	Faible
Sensibilité à la gigue	Faible	Faible	Élevée	Faible
Sensibilité aux pertes	Élevée	Elevée	Faible	Moyenne

Les problèmes de la convergence: Qualité et fiabilité
Les solutions: la qualité de service QoS et architecture

La plupart des réseaux ont un ou plusieurs liens critiques qui dégradent la performance des applications

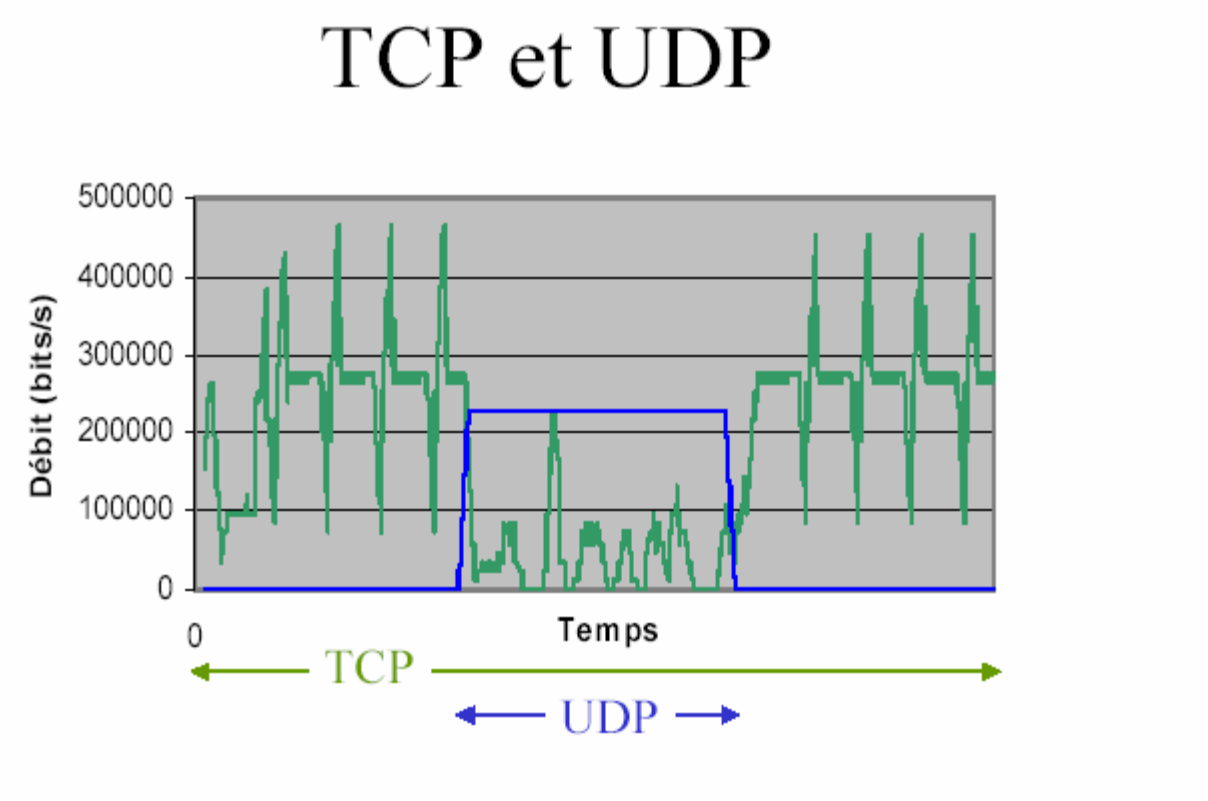
Problèmes rencontrés:
Pas de distinction entre le trafic prioritaire et non prioritaire
Exemple: le trafic Web relentit l'accès aux bases de donnés

Solution:
Séparation des deux types de trafic sur les liens critiques

Problèmes rencontrés:
Le trafic UDP peut fortement freiner le trafic TCP
Exemple: trop de connexions VoIP ne laissent plus de place pour les applications classiques.

Solution:
Limitations du nombre de connexions.

Les problèmes de la convergence. La solution: la qualité de service QoS



Les problèmes de la convergence. La solution: la qualité de service QoS: Services intégrés et différenciés

- Services Intégrés et RSVP (Resource Reservation Protocol):

  Établissement d'un circuit virtuel pour chaque flux rencontrés:

  Objectif: Séparation complète des flux individuels

- Services différenciés

  Définition de plusieurs classes de service
  Agrégation des flux de même type dans une classe

- Technologies utilisées

  MPLS

  IEEE 802.p: Utilisation des priorités sur les switches

Les technologies VoIP: Principes et architectures des systèmes VoIP: H.323 vs SIP

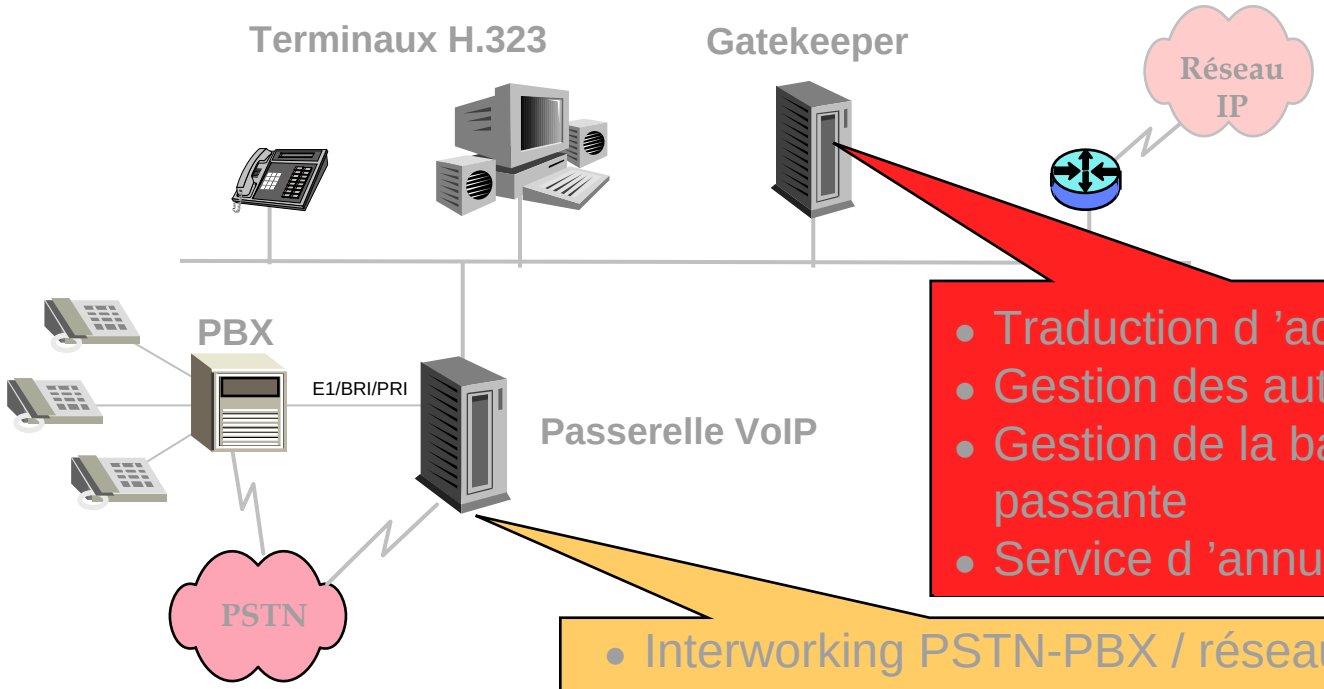
- Standard élaboré par l'UIT
- H.320 - 324 : concept global pour RNIS, ATM, réseau IP et réseau téléphonique
- Le premier à permettre l'interfonctionnement

- Standard élaboré par l'IETF
- Basé sur HTTP / SDP
- Architecture client-serveur
- Est en train de prendre le pas sur H.323

Les technologies VoIP: H.323 VS SIP

Différences techniques :	SIP	H.323
Architecture	Modulaire basé sur des services Internet	Monolitique
Codage	Text	Binaire
Call delay	Rapide	Dépend des implémentations
Extensibilité	Optimale	Problématique
Instant Messaging	Intégré d'office	non prévu
Protocole de signalisation	SIP/SDP	H.323: H.225, RAS/H.245
Différences historiques et stratégiques		
	IETF = Internet Ouverture Marché	UIT = Telco Régulation Interopérabilité

Les technologies VoIP: H.323 Principes et Architecture



- Traduction d 'adresses
- Gestion des autorisations
- Gestion de la bande passante
- Service d 'annuaire

- Interworking PSTN-PBX / réseau IP
- Numérisation
- Compression / décompression
- Modulation / démodulation
- Contrôle d 'appel
- Suppression d 'écho
- Suppression des silences

Les technologies VoIP: architecture H.323

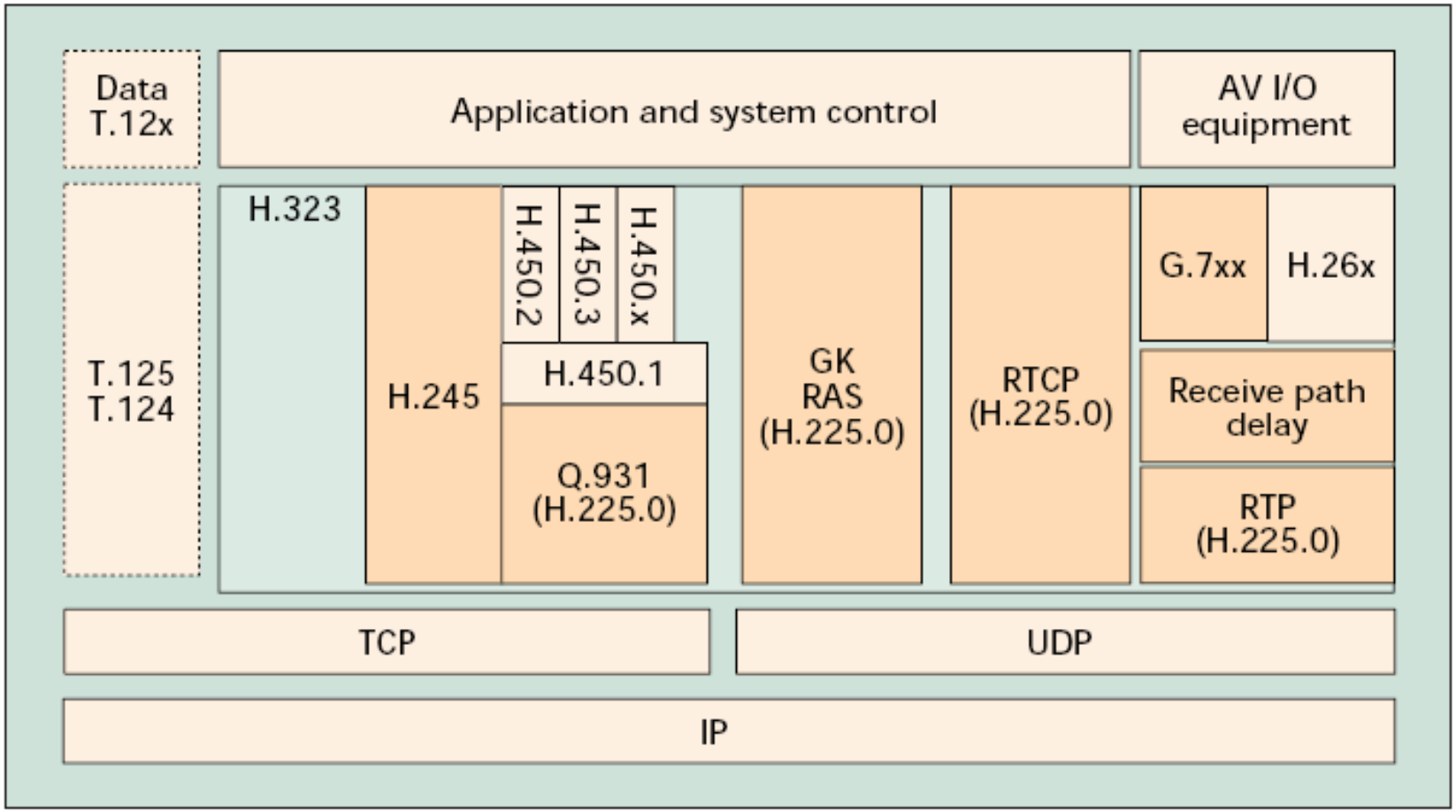
Portier (GateKeeper)

- Conversion d'adresses (adressess IP <-> E.164)
- Contrôle de largeur de bande
- Contrôle d'admission
- Gestion de zone (enregistrement, …)
- Gestion des appels
- Autorisation d'appel
- Signalisation de commande d'appel
- Gestion de la largeur de bande

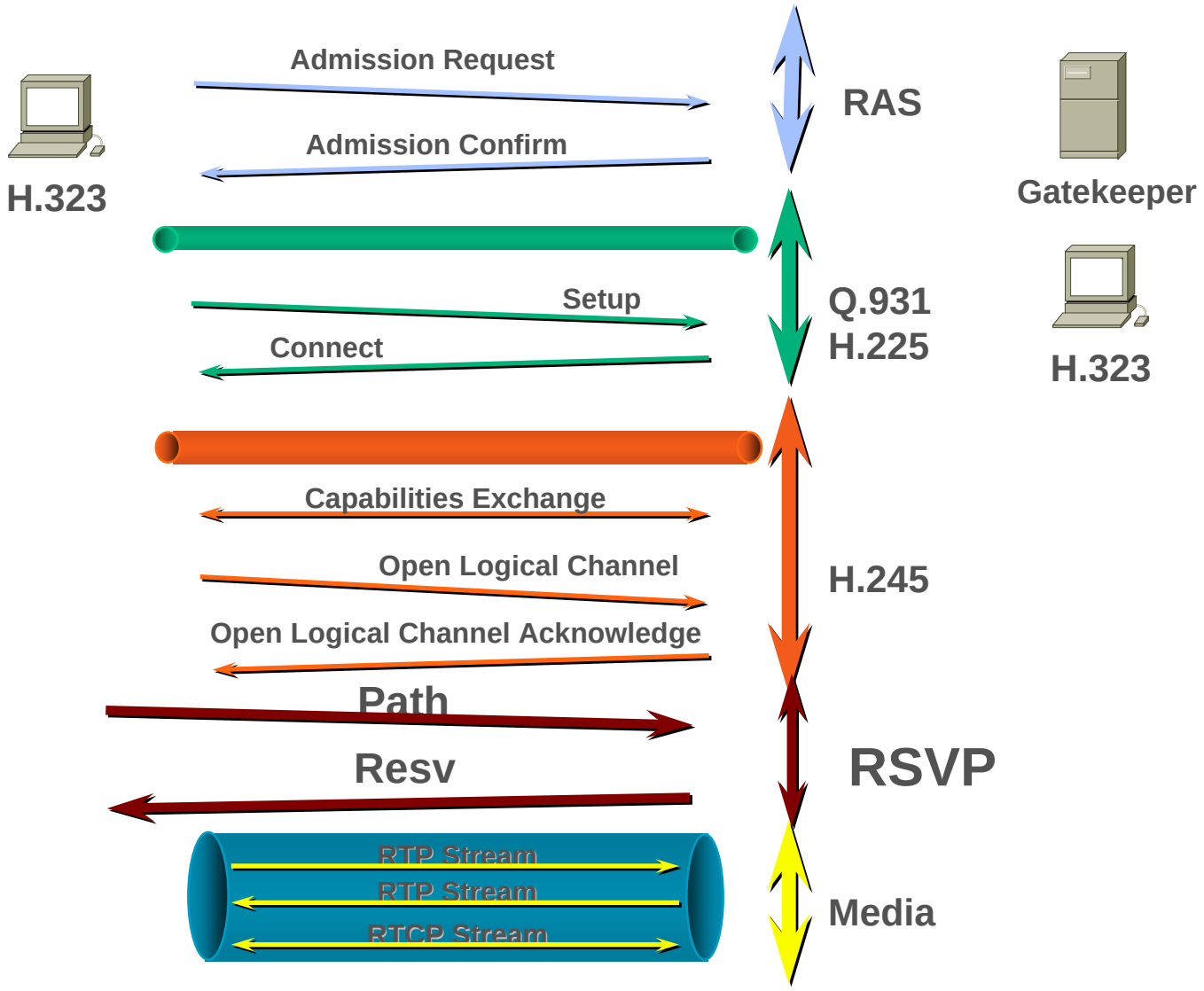
Passerelle (GateWay)

- Conversion du protocole de signalisation et des protocoles Media vers d'autres réseaux
- (ex. IP to PSTN, IP to ATM, IP_{SIP} to $IP_{H.323}$)

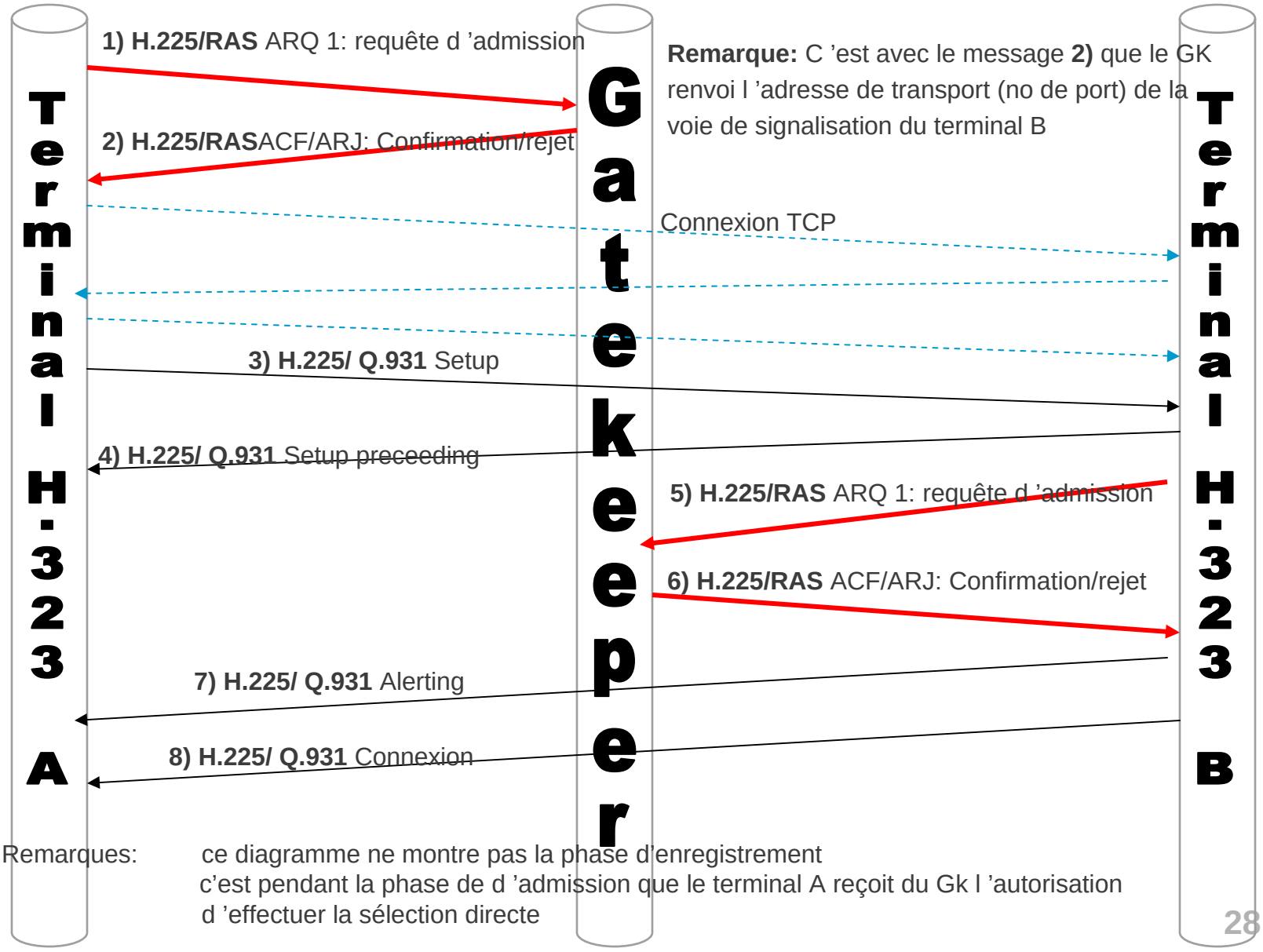
Les technologies VoIP: H. 323 « Protocol suite »



Les technologies VoIP: H.323 Signaling



Les technologies VoIP: H.323 Enregistrement des deux points d 'extrémités auprès du même GK, signalisation directe: DRC

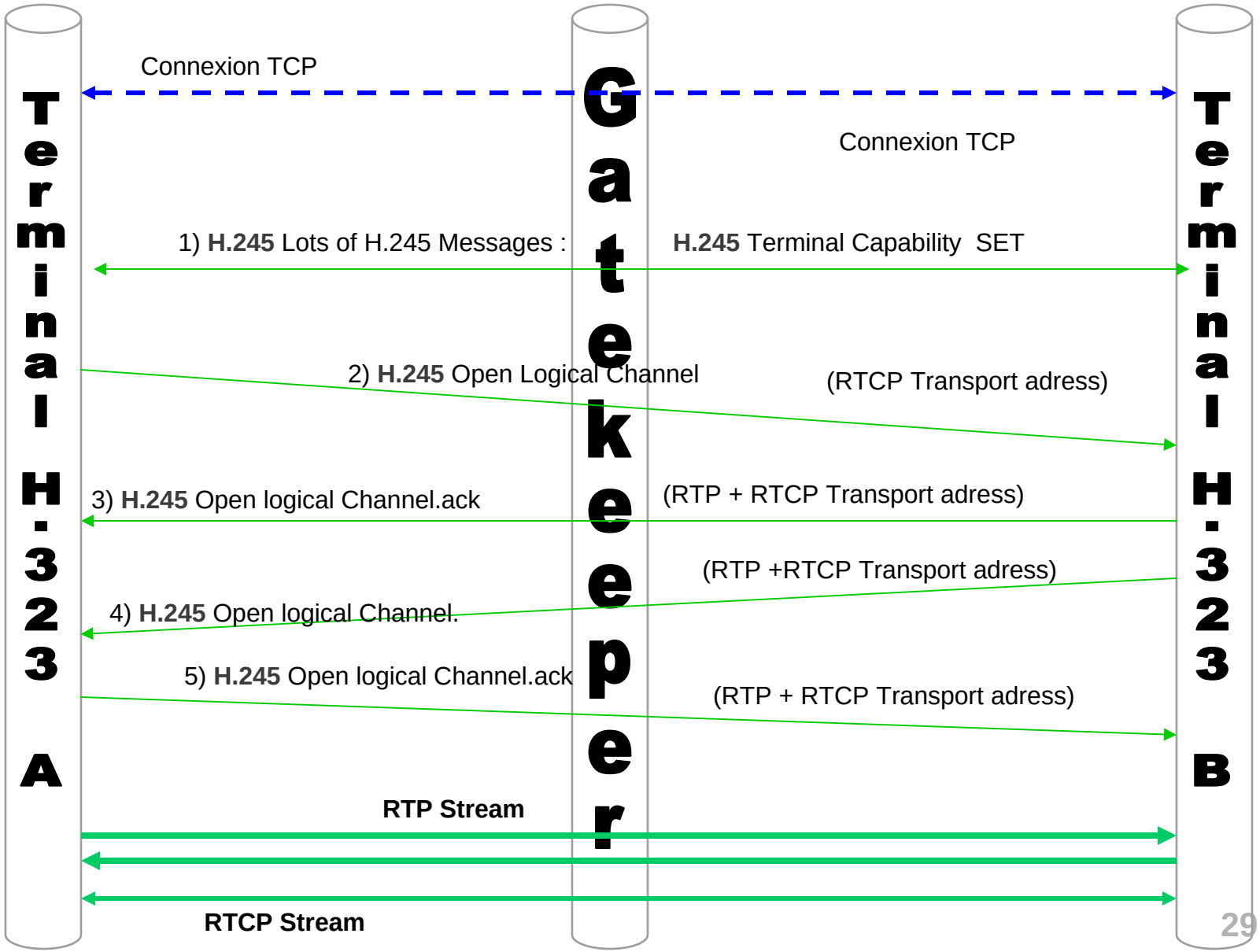


Remarque: C 'est avec le message **2)** que le GK renvoi l 'adresse de transport (no de port) de la voie de signalisation du terminal B

DRC: Directed Routed Call

Remarques: ce diagramme ne montre pas la phase d'enregistrement
c'est pendant la phase de d 'admission que le terminal A reçoit du Gk l 'autorisation d 'effectuer la sélection directe

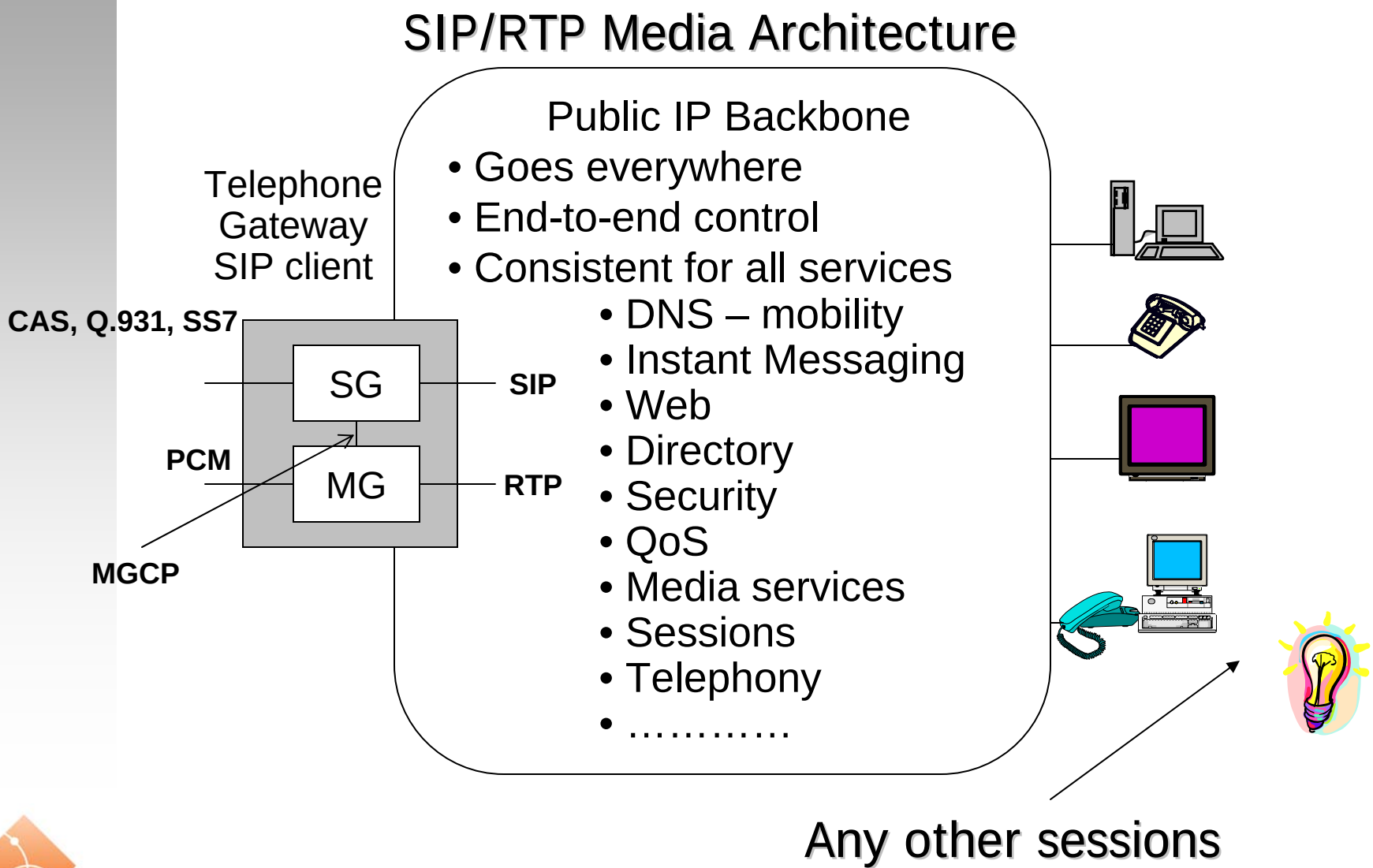
Les technologies VoIP: H.323 Connexion de deux points d'extrémités au travers d 'un GK, voie de signalisation et de commande H.245 directe.



Les technologies VoIP: SIP: La téléphonie service d'internet: Les composants

- Real Time Protocol (RTP) – media packets
- Real Time Control Protocol (RTCP) – monitor & report
- Session Announcement Protocol (SAP)
- Session Description Protocol (SDP)
- Session Initiation Protocol (SIP)
- Real Time Stream Protocol (RTSP) – play out control
- Synchronized Multimedia Integration Language (SMIL) mixes audio/video with text and graphics

La téléphonie sur Internet “Telephony on the Internet “may not be a stand-alone business, but part of IP services”



Les technologies VoIP: L'architecture SIP

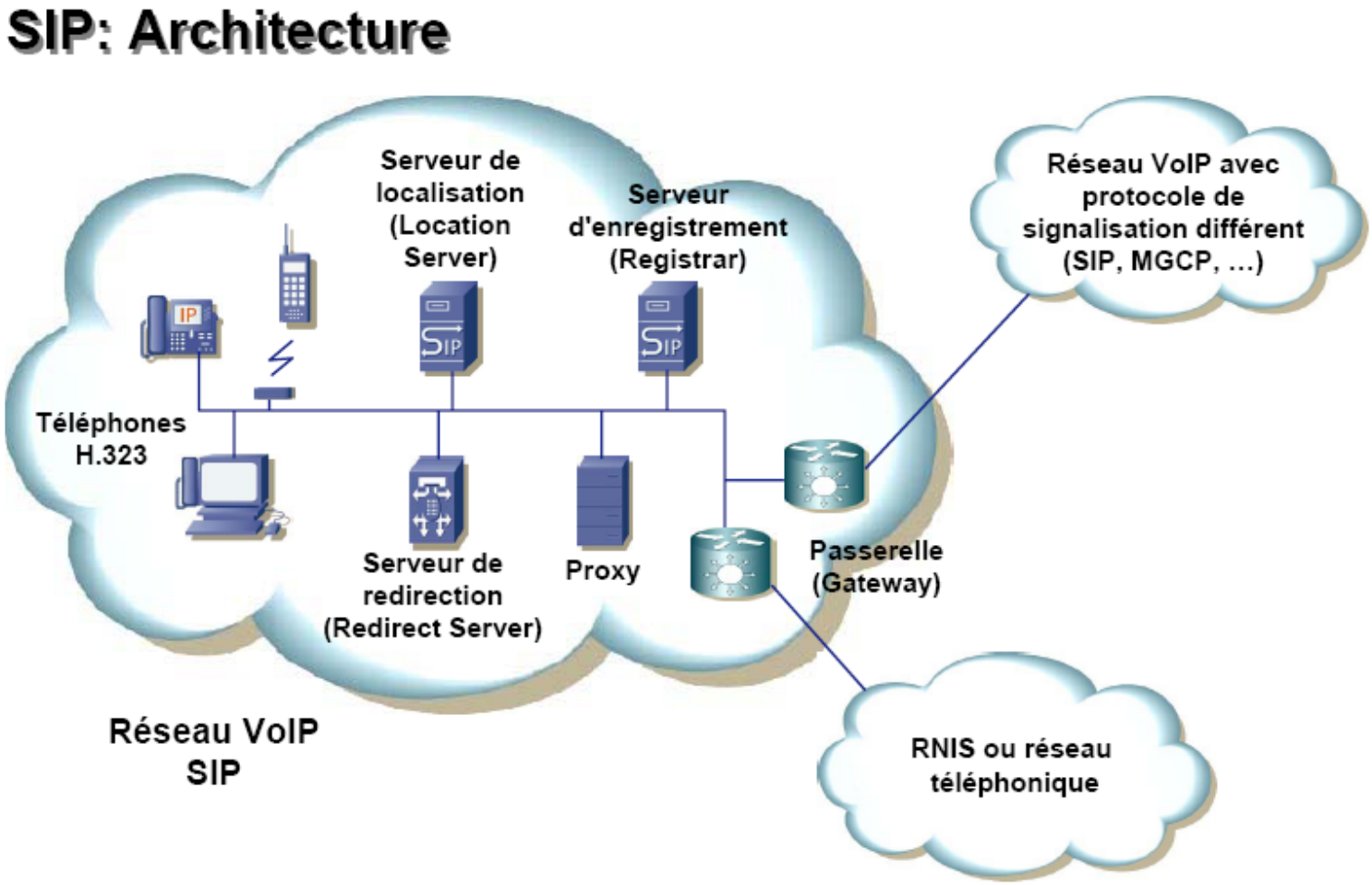


figure: Cours VoIP du Prof. A. Delley de l'EIF

Les technologies VoIP: L'architecture SIP

USER Agent Client (UAC):	Initie les requêtes SIP User Agent
User Agent Server (UAS):	Renvoie les réponses SIP
Serveur d'enregistrement:	gère les informations relatives aux usagers, pour le réseau ou pour un segment du réseau
Serveur de redirection :	livre, sur demande, l'adresse SIP de l'usager requis, ou bien celle du serveur susceptible de connaître l'adresse de cet usager
Serveur de localisation :	permet au proxy et au serveur de redirection d'obtenir les informations relatives à "l'emplacement" d'un usager
Serveur proxy :	reçoit, traîte et, au besoin, ré-achemine les messages de signalisation SIP

Les technologies VoIP: L'architecture SIP: L'adressage SIP

Utilise les URL d'internet

- Uniform Resource Locators
- Utilise les adresses IP(SIP) et les addresses PSTN
- Le format général de l'adresse SIP est: name@domain
- Tout appel comprends une phase de résolution de nom de type User@Host
- Examples:

  sip:alan@wcom.com

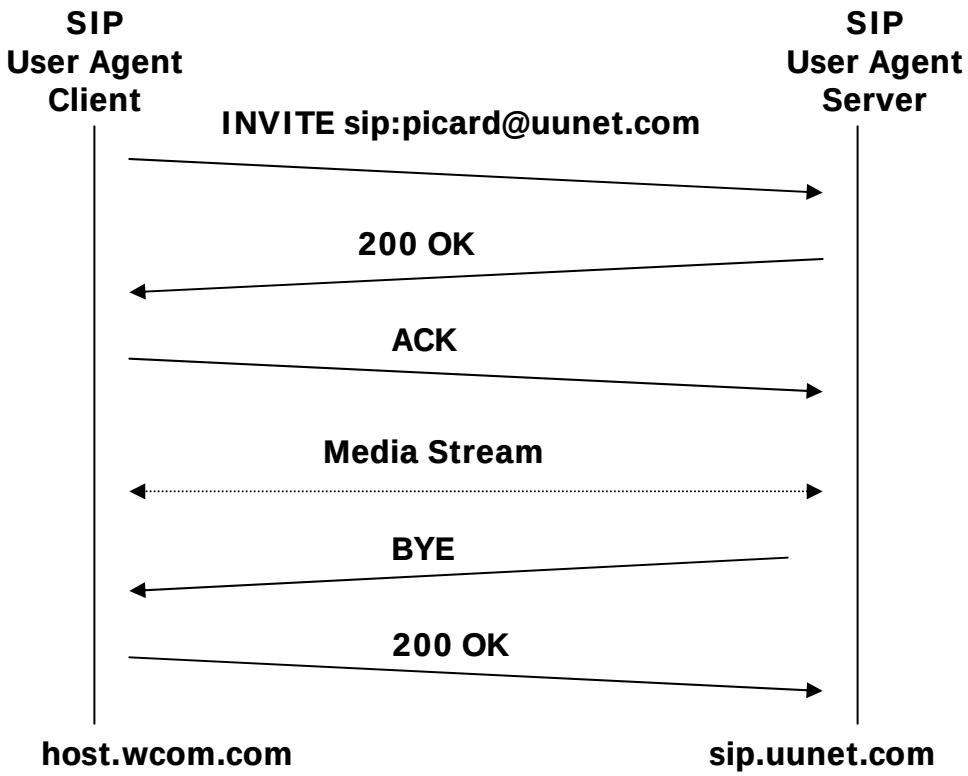
  sip:J.T. Kirk <kirk@starfleet.gov>

  sip:+1-613-555-1212@wcom.com

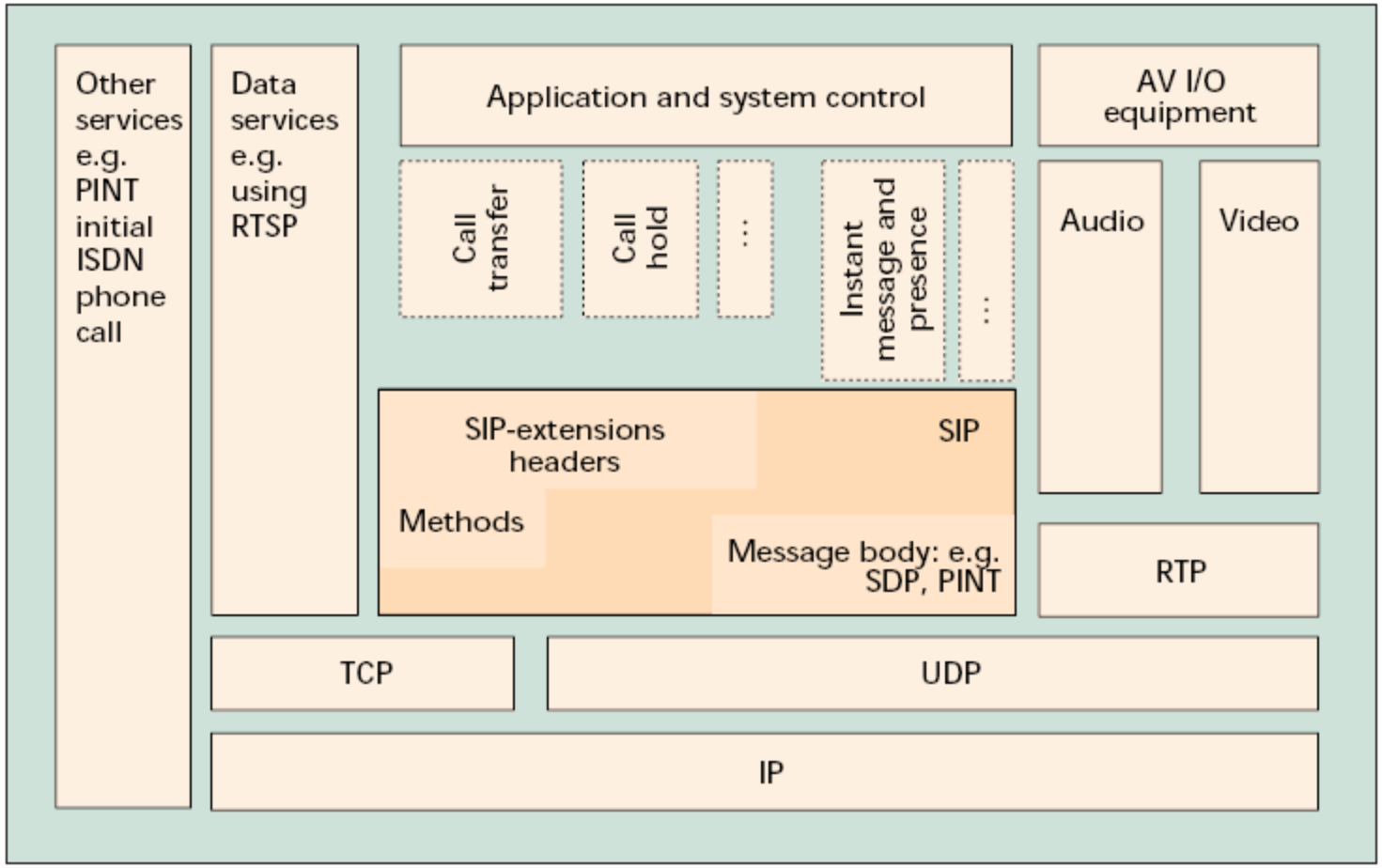
  sip:guest@10.64.1.1

  sip:790-7360@wcom.com;phone-context=VNET

Les technologies VoIP: Example: SIP Session Setup



Les technologies VoIP: IETF SIP Protocol suite



Les technologies VoIP: Exemple de messages SIP lors de l'établissement d'une connexion

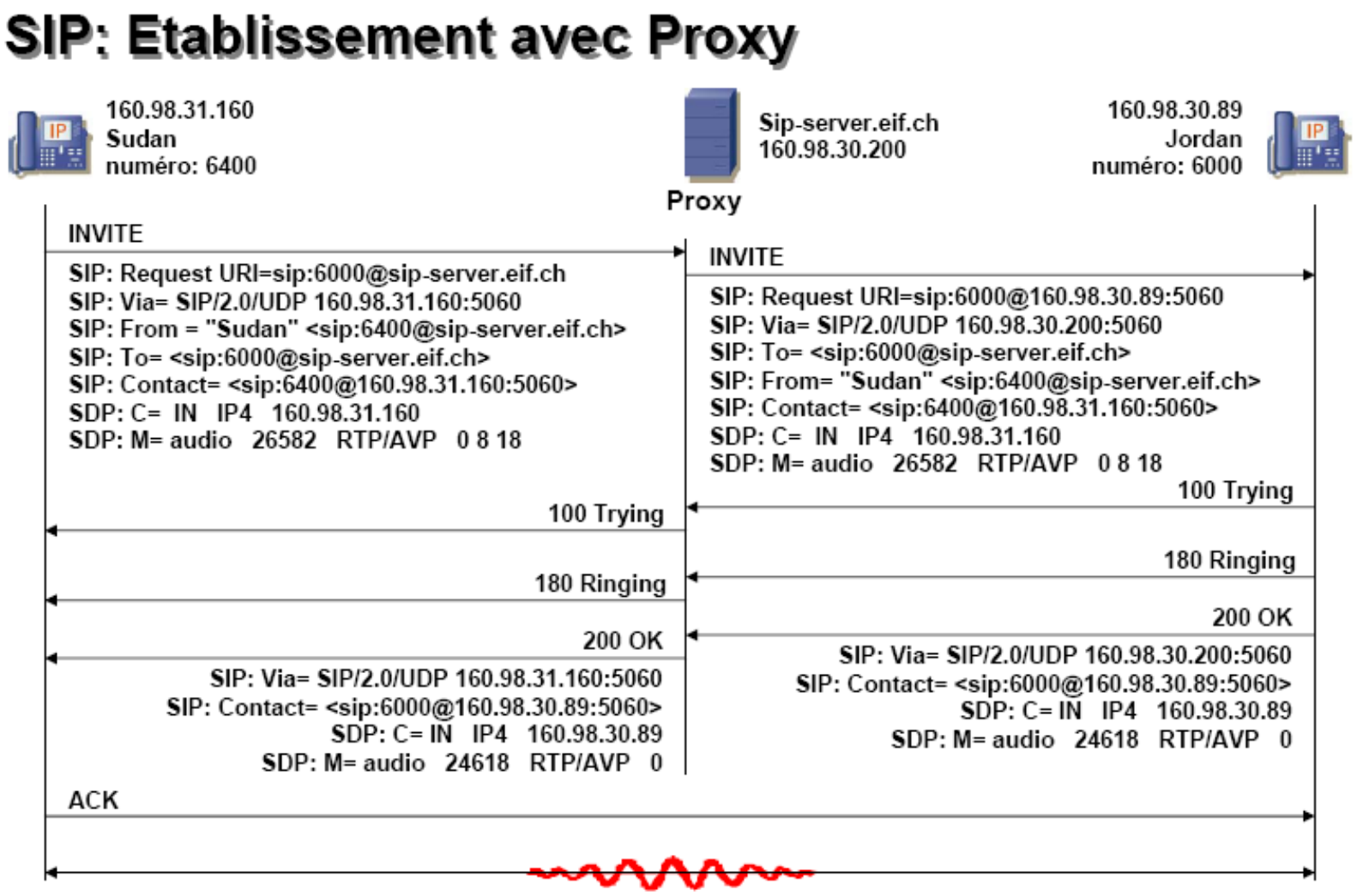
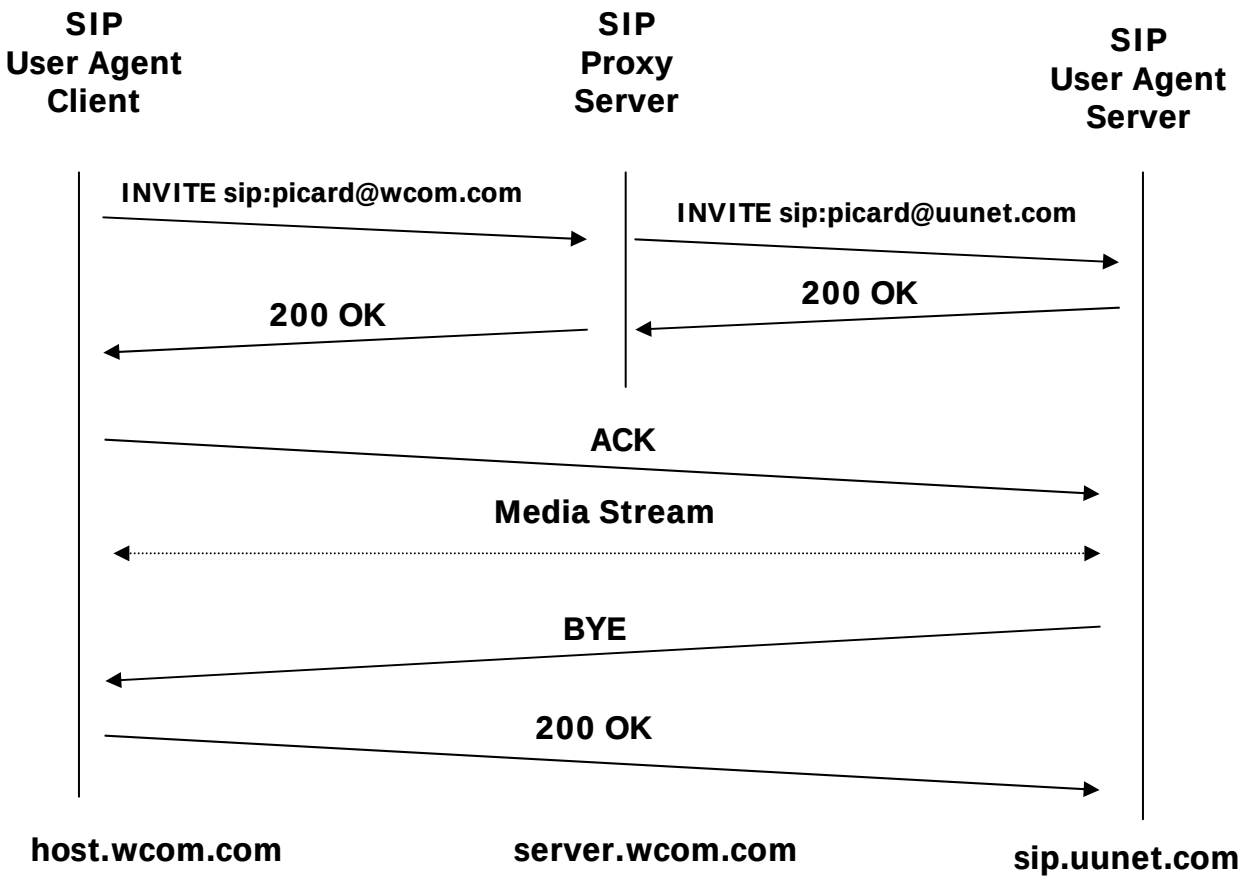
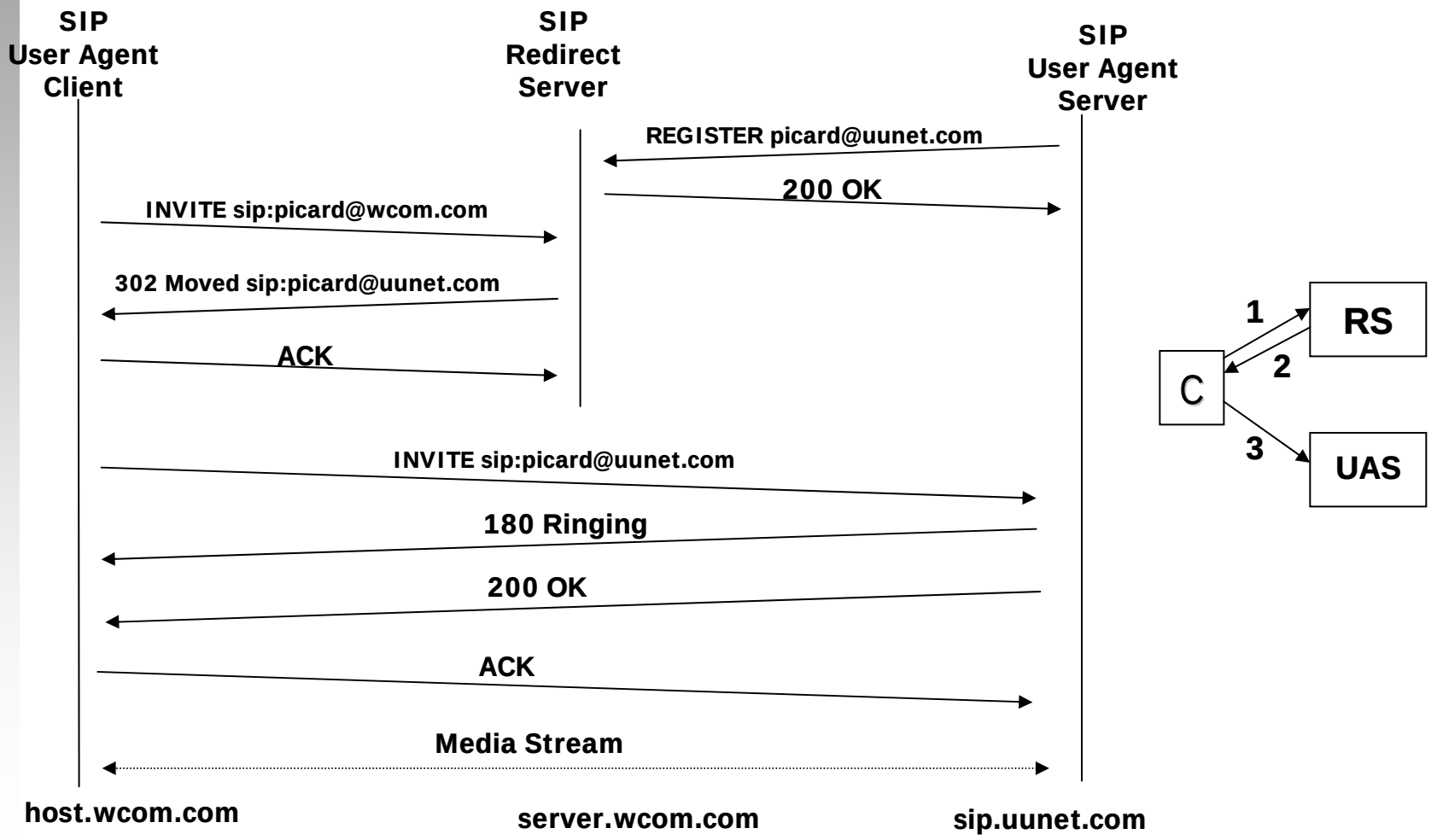


figure: Cours VoIP du Prof. A. Delley de l'EIF

Les technologies VoIP: Example: Proxy Server



Les technologies VoIP: Example: Redirect Server



- **Constat:**
  Après l'euphorie de la découverte de la téléphonie sur Internet qui amène de plus en plus d'entreprises à remplacer leur « vieux » PABX par un IP-PABX (VoIP), celles-ci découvrent les nouveaux problèmes de disponibilité et sécurité liés à cette nouvelle technologie.

- Objectifs de la dernière partie de l'exposé: **vous permettre de:**
  - Découvrir les risques liés à l'introduction de la VoIP dans l'entreprise.
  - Cerner le type de mesure à prendre pour y pallier.

Pourquoi la sécurité de la téléphonie en entreprise est si importante.

- **La téléphonie en entreprise: un service qui ne tolère aucune défaillance**.
  - Combien parmi vous se rappellent d'avoir vécu une défaillance du central de téléphonie (PBX) ?
  - Disponibilité des cinq 9.
  - Barrière psychologique.
- **La téléphonie en entreprise, un service qui ne tolère aucune indiscrétion.**
  - Aucune violation de la confidentialité n'est tolérée.
- **La téléphonie en entreprise est un service qui ne tolère aucune intrusion.**
  - Un service de téléphonie doit être invulnérable et disposer d'un système d'accès spécifique.

Pourquoi la sécurité de la téléphonie VOIP est plus importante que celle des PABX *Old Fashion*.

La sécurité des PABX est malgré tout déjà un vieux problème..

- Mais malgré tout, la sécurité des PABX a été jusqu'à l'avènement de IP-PBX sous-estimée.
- Les entreprises préfèrent être discrètes quant aux dommages subis.
- La convergence des réseaux et services Télécom avec les réseaux informatiques des IP-PBX découple les risques.

Pourquoi la sécurité de la téléphonie VOIP est plus importante que celle des PABX *Old Fashion*.

- La convergence des réseaux informatiques implique comme corollaire **une accumulation** des risques au niveau sécurité.

- Les attaques au réseau et services Informatiques peuvent affecter aussi le service de téléphonie.

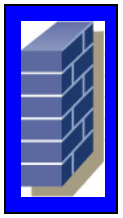
- L'introduction du service VoIP peut aussi affaiblir les défenses informatiques.

Les enjeux pour l'entreprise.

- Les vulnérabilités mal maîtrisées peuvent avoir pour l'entreprise des conséquences graves pour l'entreprise:

  - **Conséquences financières.**
  - **Conséquences sur l'image de marque.**
  - **Conséquences sur le core business.**
  - **Conséquences pénales.**

La problématique de la sécurité voip: beaucoup de nouveaux équipements à protéger

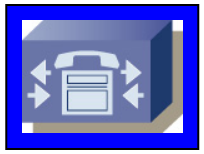


VoIP-enabled Firewall

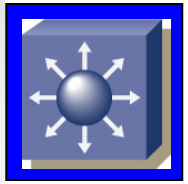
IP Telephone

Application Server

QoS Enabled Switch



IP PBX (call manager
SIP Proxy)



Layer 2/3 Switch

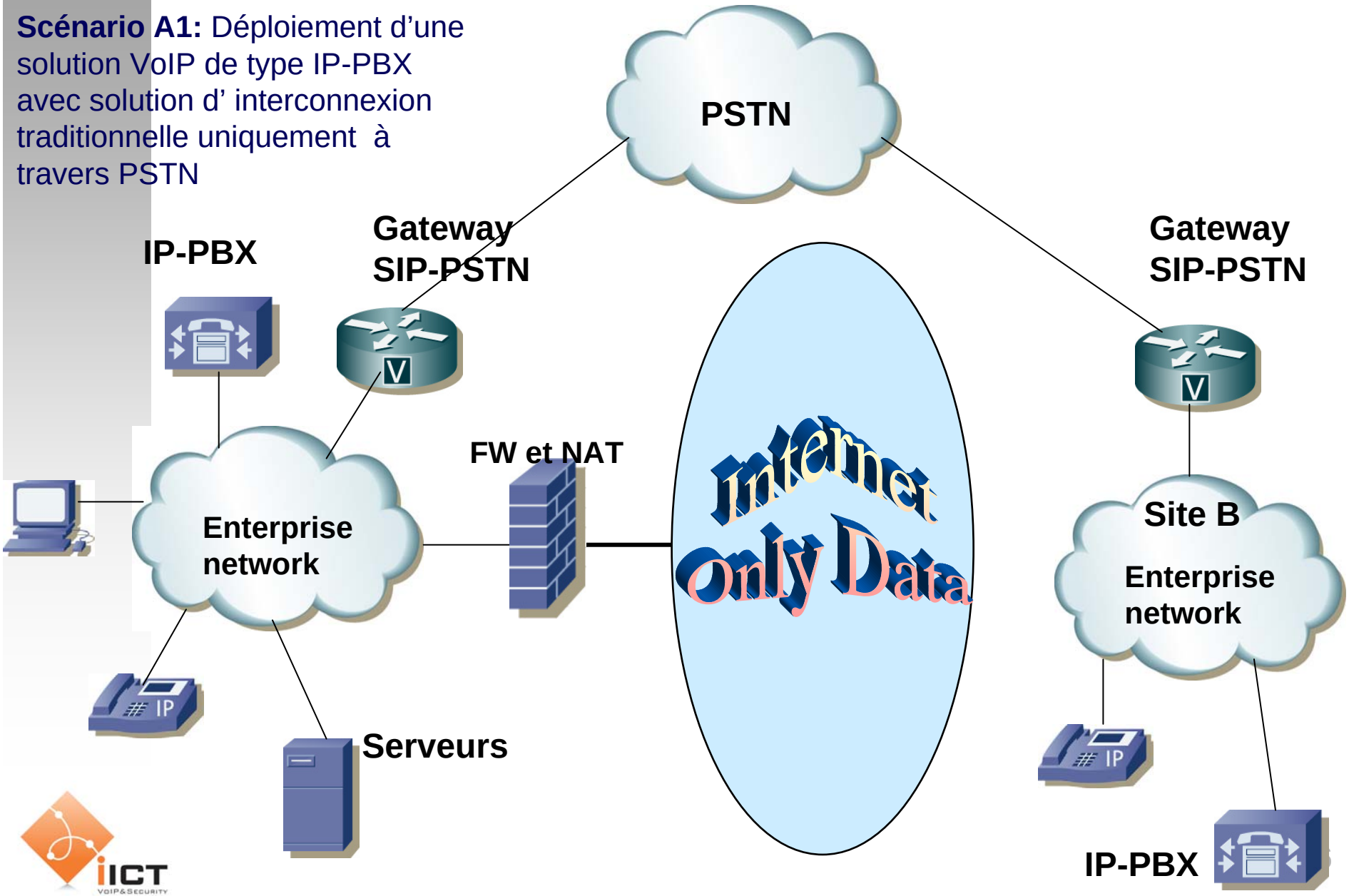
Unified Messaging/UM

Voice Gateway/Router

Workstation / Softphones

La politique de sécurité de l'entreprise est déterminante dans la selection du type de solution VoIP

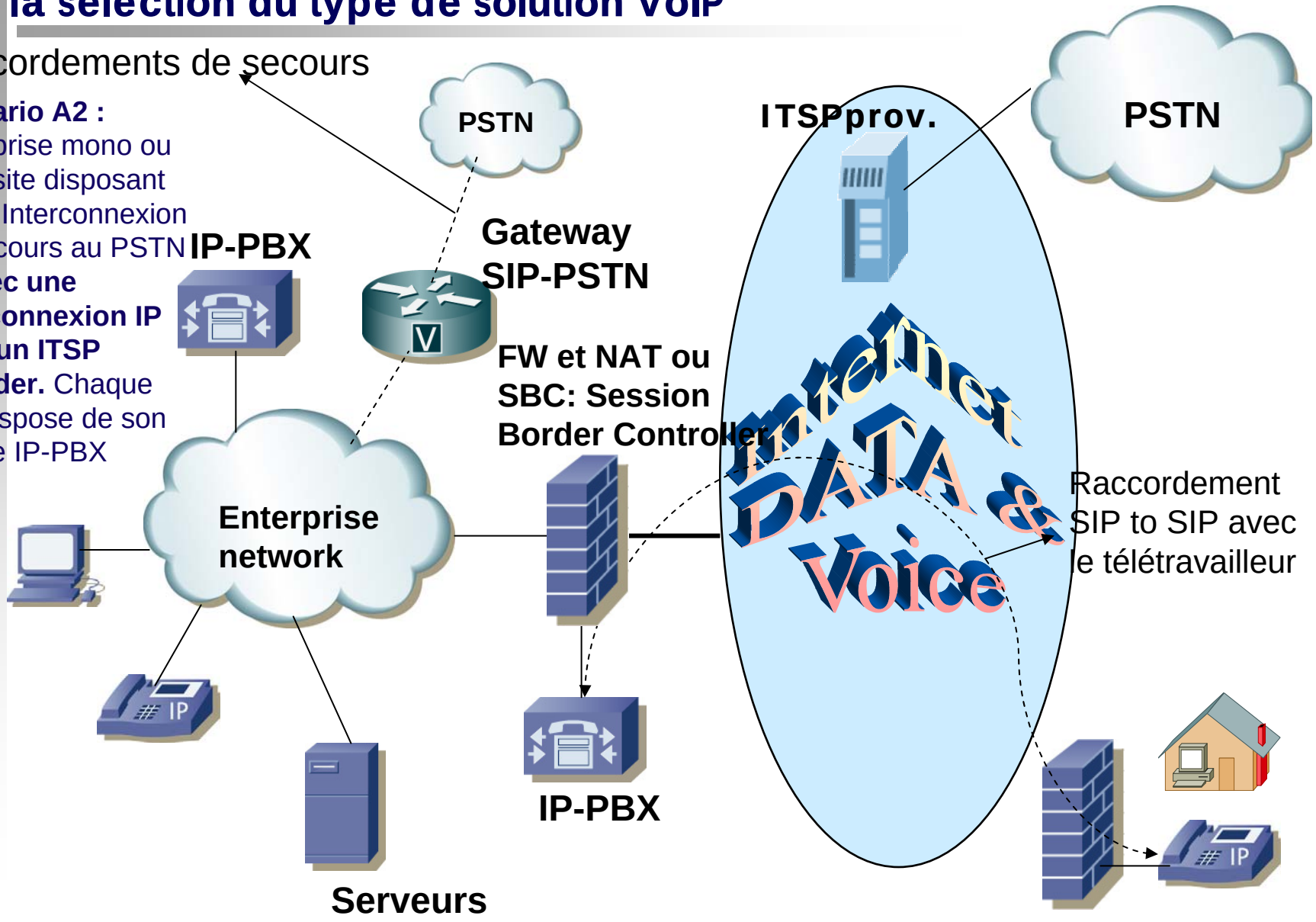
Scénario A1: Déploiement d'une solution VoIP de type IP-PBX avec solution d' interconnexion traditionnelle uniquement à travers PSTN



La politique de sécurité de l'entreprise est déterminante dans la selection du type de solution VoIP

Raccordements de secours

Scénario A2 : Entreprise mono ou multi site disposant d'une Interconnexion de secours au PSTN et **avec une interconnexion IP avec un ITSP provider.** Chaque site dispose de son propre IP-PBX



Les vulnérabilités de la VoIP: Cumul des vulnérabilités IP et celles spécifiques au services VoIP

- Denis de service (DoS) : Privation d'accès à un service réseau en bombardant les serveurs (proxy, gateway, …) avec des paquets malveillants.
- Intégrité de message **(message integrity)** : Vérification que le message reçu n'a pas été altéré durant la transmission**.**
- Capture de paquets **(paquets sniffing)** : Obtention d'informations (adresse IP/MAC, protocoles utilisés).
- Mot de passe **(password attack) :** Casser des mots de passe afin d'obtenir des privilèges.
- Personne au milieu (man-in-the-middle) : Paquets modifiés de manière à usurper une identité ou permettant la récupération d'information de transmission sur des utilisateurs.
  - ARP Spoofing
  - IP Spoofing
  - Hijacking
  - DoS
  - etc.
- Malware : virus, vers (worms), trojans : MALicious softWARE : Applications malicieuse faisant référence à des programmes crapuleux.

Les vulnérabilités de la VoIP: Cumul des vulnérabilités IP et celles spécifiques au services VoIP

- Exploits de vulnérabilité : Programme ou technique profitant d'une vulnérabilité dans un logiciel et qui peut être utilisé pour casser la sécurité ou pour attaquer une station à travers le réseau.
- Détournement (hijacking) : Attaque dans laquelle l'attaquant prend procession d'une connexion en cours entre deux entités en se faisant passer pour l'une des deux entités.
- Mauvaise utilisation (misuse) : Modifier le but inhérent d'une fonction ou autre afin de pouvoir abuser du système.
- Coupure de courant

Vulnérabilités propres à l'utilisation de la VoIP/SIP :

La particularité de la VoIP face aux données IP standard est principalement associée à la notion de qualité de service. En effet, comme dans tout système de téléphonie, la VoIP apporte une très importance à la QoS. Ceci augmente notablement l'exposition aux attaques de types DoS. Cela affecte principalement:

- Délai/latence
- Perte de paquet
- Variation du délai de transfert de l'information (jiter)
- Bande passante
- Techniques de codage de la parole

Les menaces

- Disponibilité ou Dénis de Service (DoS).
- Confidentialité.
- Vol de ressources.
- SPIM.
- Intégrité.
- Imputabilité (Authentification).
- Erreurs de configuration

Sécurité VoIP: les menaces: disponibilités/DoS.

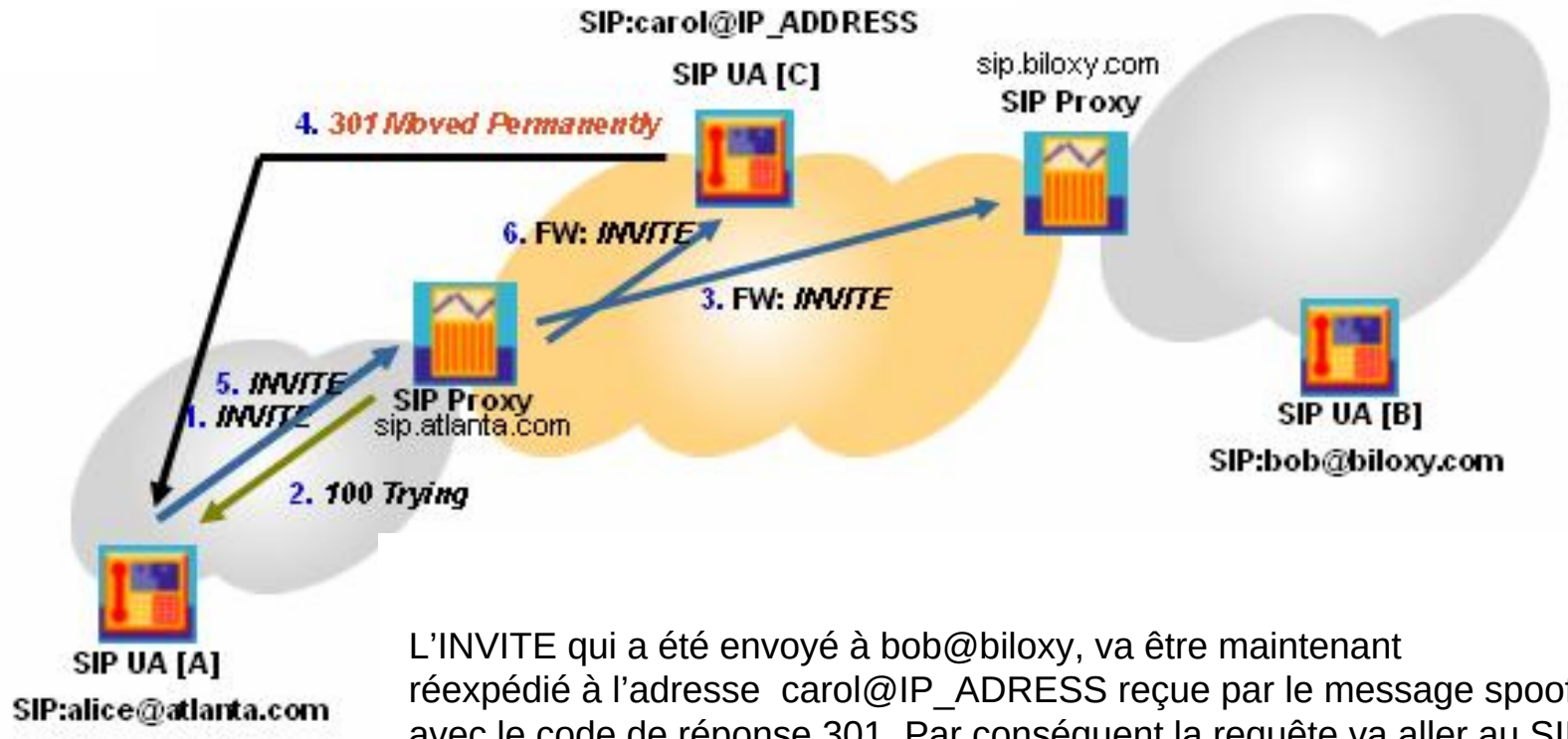
Les menaces les plus redoutées du service de téléphonie sont celles qui touchent à la disponibilité du service. La VoIP, vu sa complexité est très vulnérable par rapport à cette menace. Les vulnérabilités suivantes permettent une panoplie d'attaques ayant comme but du DoS (Déni de Service).

- Vulnérabilités des protocoles.
- Vulnérabilité de la QoS.
- Vulnérabilités des composants.
- Vulnérabilités des infrastructures réseau.

Sécurité VoIP les menaces: DoS: vulnérabilités des protocoles.

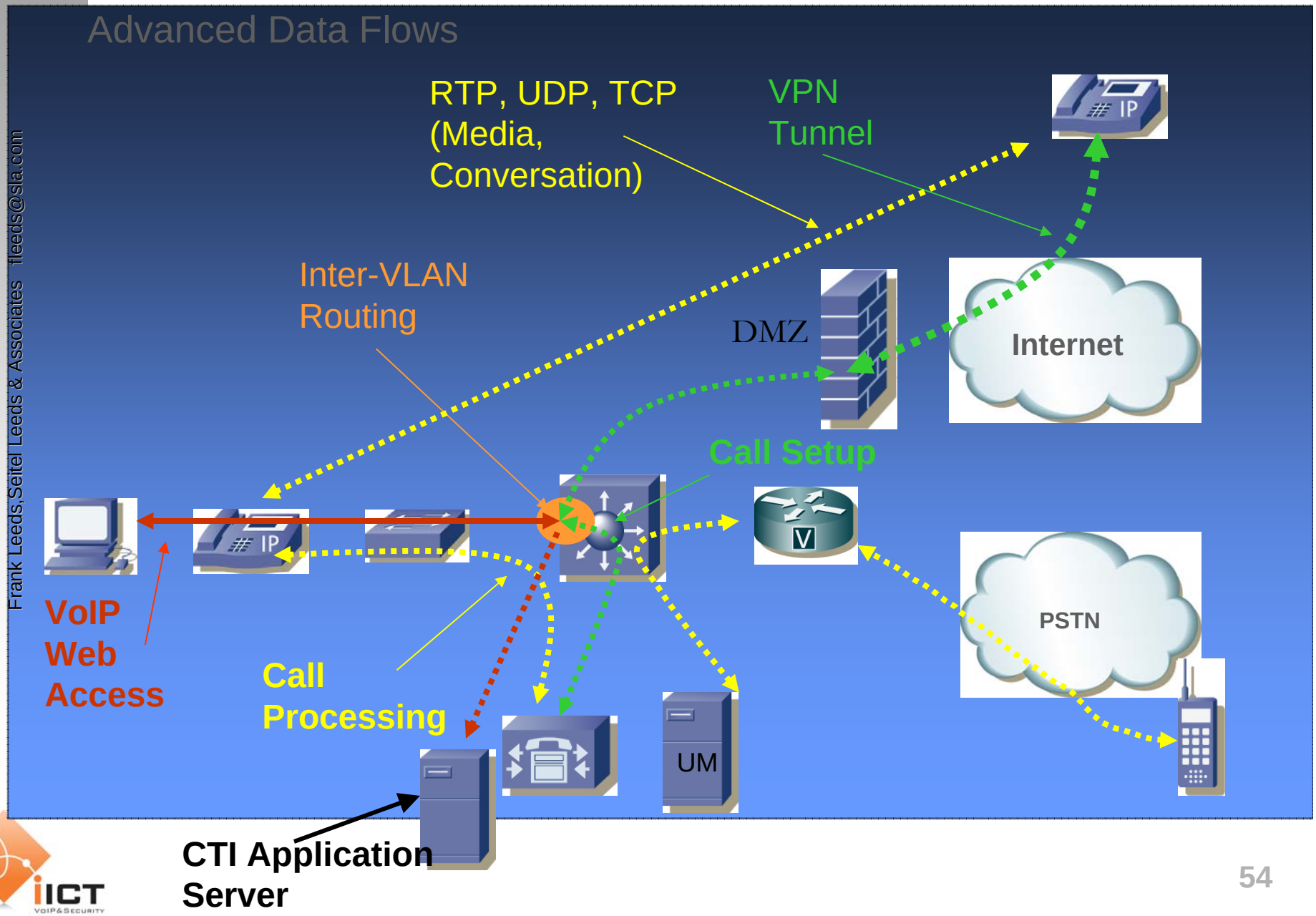
- **L'établissement d'une connexion implique la collaboration et l'échange de message entre différents composants de la plate-forme VOIP. Il suffit de modifier, détourner ces messages pour perturber ou saboter la communication.**

Détournement d'appel et utilisant un message 301 « Moved Permanently »



L'INVITE qui a été envoyé à bob@biloxy, va être maintenant réexpédié à l'adresse carol@IP_ADRESS reçue par le message spoofé avec le code de réponse 301. Par conséquent la requête va aller au SIP phone de Carol plutôt qu'à BOB

Sécurité VoiP: les menaces: DoS: vulnérabilités des protocoles.



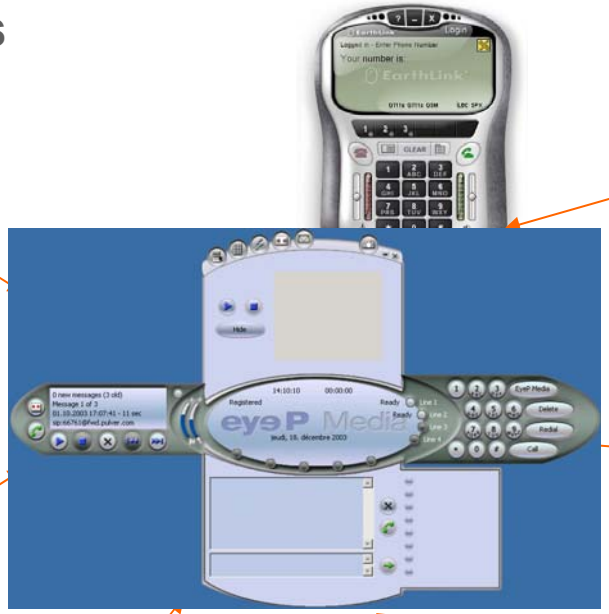
Sécurité VoIP: les menaces: DoS: QoS.

- La QoS définit les contraintes réseaux pour que la communication téléphonique soit de bonne qualité.
- Les attaques à la QoS correspondent à des attaques DoS.
- Les attaques à la QoS sont faciles et les défenses difficiles (l'introduction de FW ou du cryptage aggrave le problème).
    - Par l'introduction d'un retard.
    - Par l'augmentation de la gigue (Jitter)
    - Par la perte de paquets.

Sécurité VoIP: les menaces: DoS: vulnérabilités des composants.

Example - Softphones

Viruses and Worms (Code-Red, Nimda Buffer Overflow)



OS Vulnerabilities (security holes)

Application Vulnerabilities (macro viruses)

Network Vulnerabilities (ARP sniffing)

Denial of Service (UDP flood)

Power Outages

Sécurité VoIP: les menaces: DoS: vulnérabilités des composants réseaux .

- **Imperméabilité des VLAN Voix et DATA**
- **Mise à jour des Firewall Tunnels**
- **Réseaux WiFI**
- **Attques de type “Man-in-the-Middle” grâce au spoofing.**
- **Mise à jour des Logs en ce qui concerne les message les transactions VoIP**
- **Mise à jour des IDS pour l’analyse des messages VoIP**

Sécurité VoIP: les menaces: confidentialité, Intégrité Imputabilité.

- Ecoute téléphonique à l'intérieur et extérieur de l'entreprise.
  - ARP Spuffing.
  - Mid Session Tricks / "Re-INVITE" ou "Session Replay".
  - Écoute des messages vocaux déposés.
- Détournement d'appel (call hijacking):
- Détournement d'enregistrement (registration hijacking).
- Modification d'identité (request spoofing).
- Trafic de taxation (fooling billing).
- Attaques involontaires: Erreurs de configuration.

Sécurité VoIP: les menaces: SPIT, SPIM.

- Les failles dans les différents protocoles utilisés permettent les attaques de type SPIT (Spam over internet telephony). Il existe déjà des systèmes SPIT capables d'inonder des milliers d'abonnés simultanément de messages publicitaires.

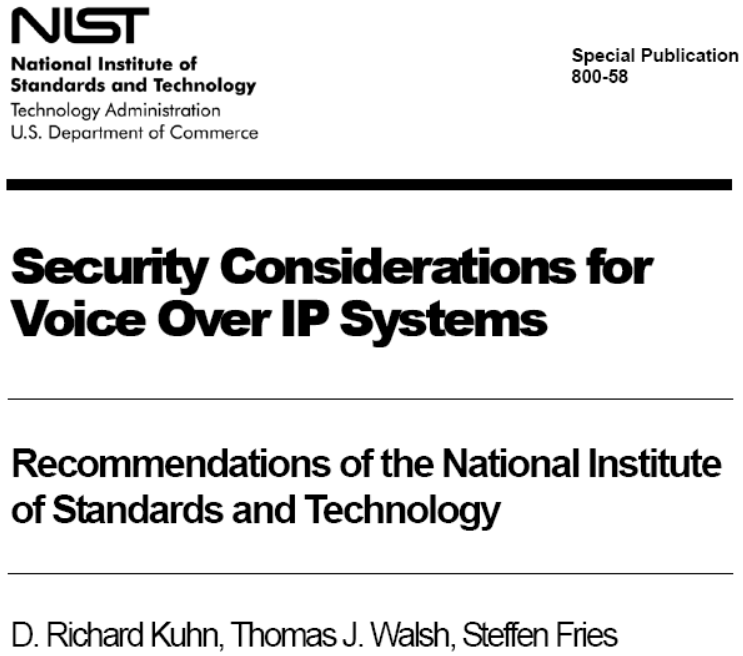
- le SPIM (Spam de la messagerie instantanée, apparue l'année dernière) totalise déjà 10 % du trafic de la messagerie instantanée, selon les experts.

VoIP Security Axioms

- Les réseaux voix sont des cibles potentielles
- Le partitionnement des réseaux voix et donnée est un élément de sécurité essentiel
- Les équipements de téléphonie ne sont pas criptés
- Attention sans partitionnement des réseaux voix et données, les équipements DATA permettent d'accèder aux données voix !!
- Même en cas de partitionnement les softphones ne sont pas à l'abri d'une écoute
- Le contrôle du partitionnement des réseaux voix des réseaux données est indispensable
- Vérification de l'identité du correspondant
- Les réseaux WIFI sont à bannir du réseau voix
- Securiser et monitorer tous les serveurs et segments voix

Sécurité VoIP: les parades: pourquoi sécuriser la VoIP est un challenge.

Le NIST et le DOD, conscients des nouveaux périls de sécurité encourus par les entreprises, ont lancés début 2005 un avertissement (security warning) à toutes les entreprises voulant se lancer dans l'exploitation de ces services.

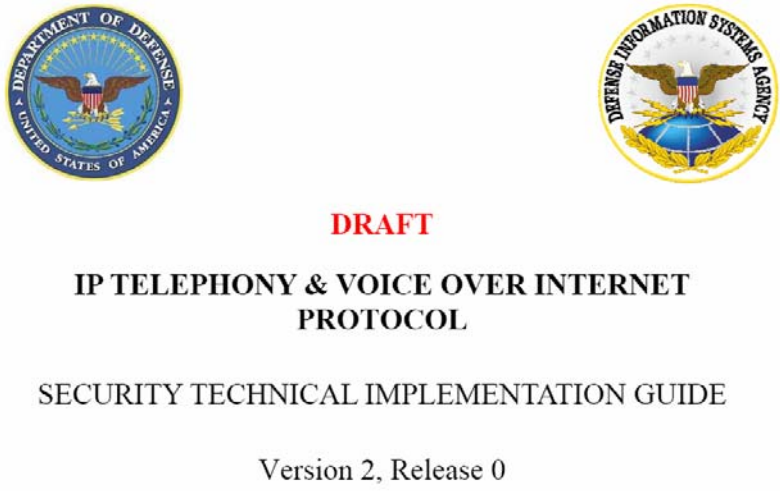

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-58

Security Considerations for Voice Over IP Systems

Recommendations of the National Institute of Standards and Technology

D. Richard Kuhn, Thomas J. Walsh, Steffen Fries


DRAFT

IP TELEPHONY & VOICE OVER INTERNET PROTOCOL

SECURITY TECHNICAL IMPLEMENTATION GUIDE

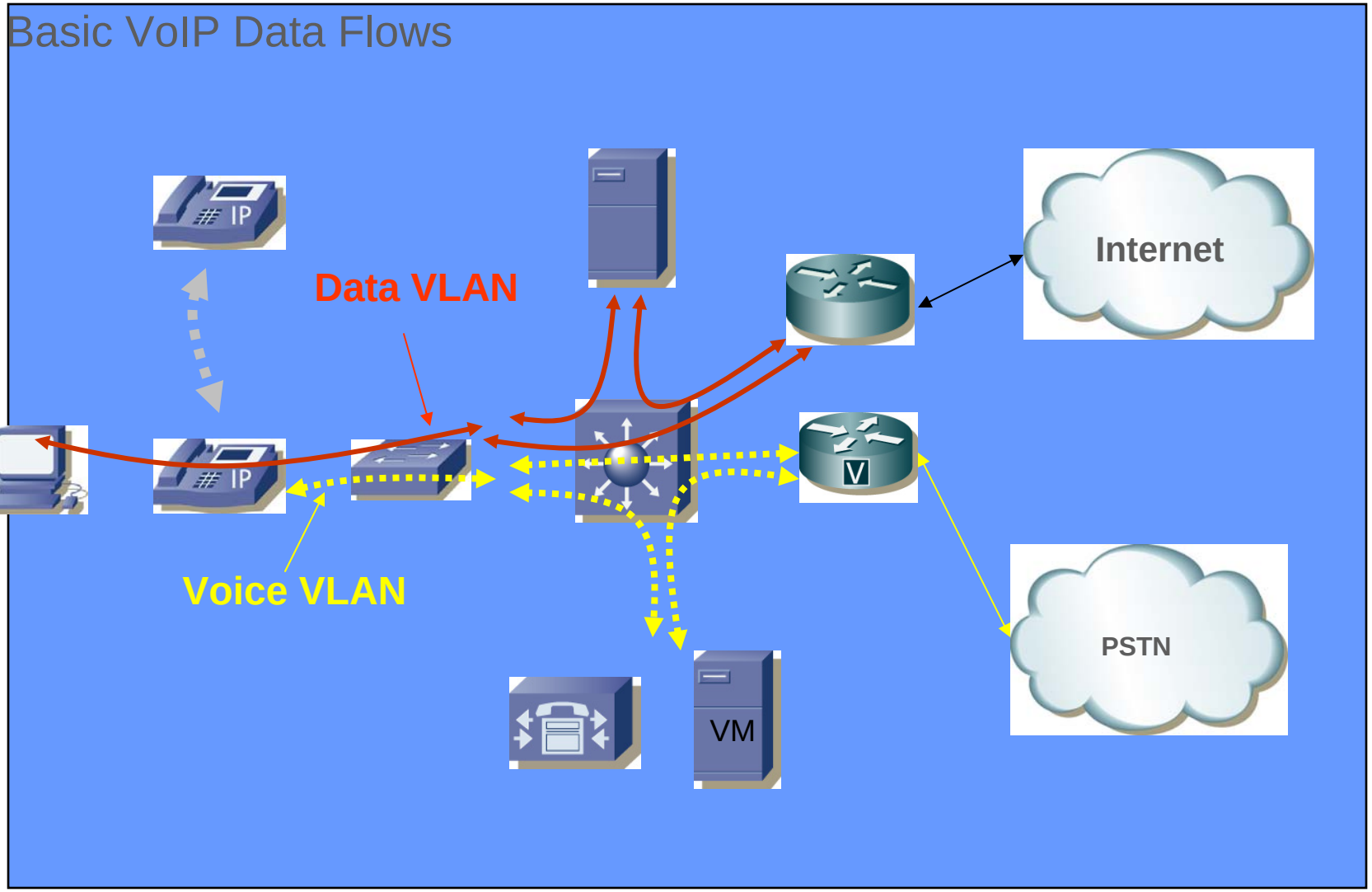
Version 2, Release 0

Sécurité VoIP: les parades: sécurisation de l'environnement de VoIP/SIP.

1. Sécurité physique
2. Protection des serveurs physiques
3. Protection des configurations du système
4. Séparation des réseaux Data et Voix
    1. Séparation des adresses
    2. Séparation physique VLAN
5. Proscrire les IP Phones et Soft-Phones
6. Confidentialité et authentification
7. Protection du réseau

    Firewall et Nat
8. Analyse du trafic
9. Gestion VoIP

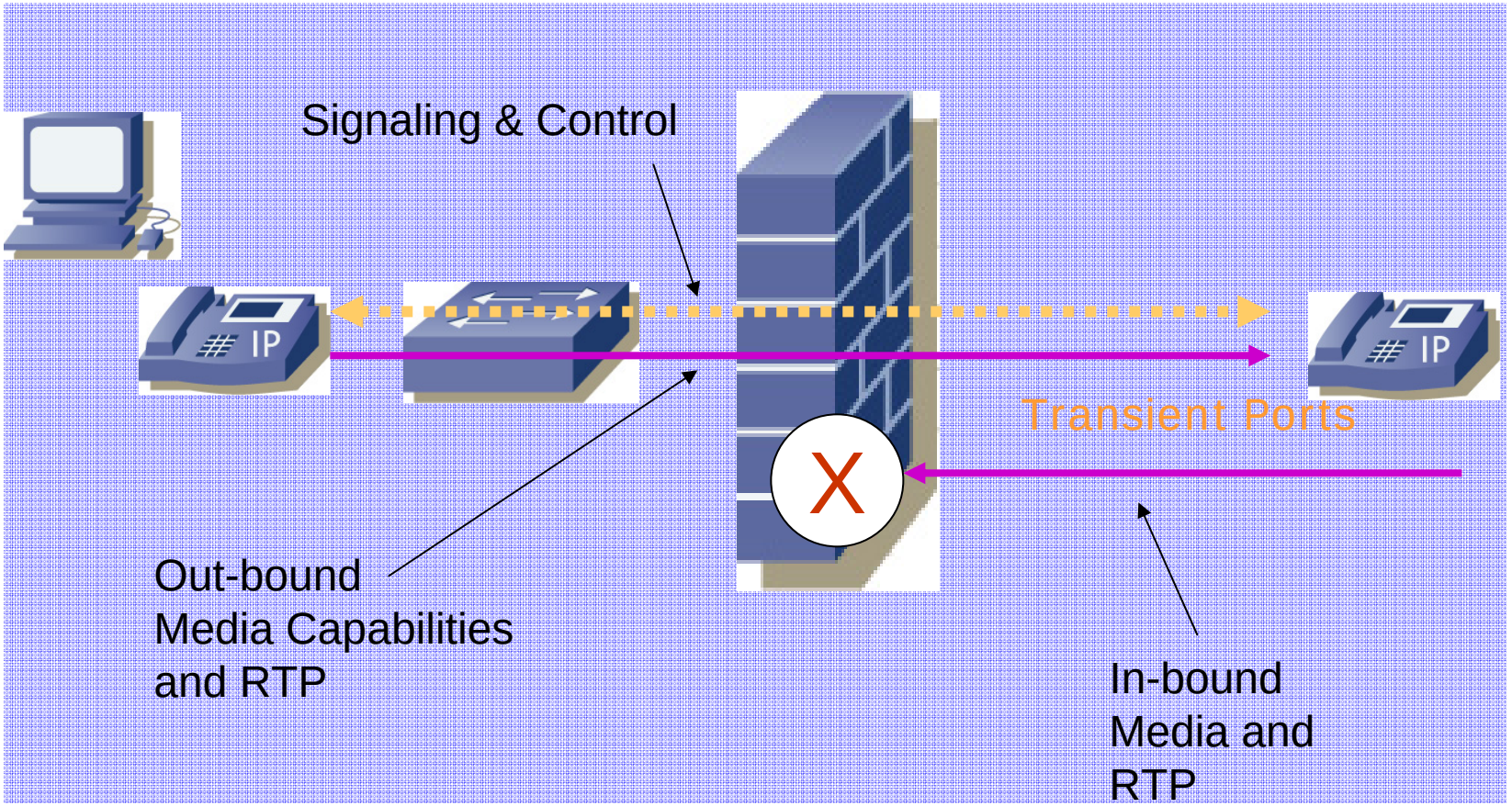
Sécurité VoIP: les parades: séparation des réseaux Data et Voix.



Frank Leeds,Seitel Leeds & Associates fleeds@sla.com

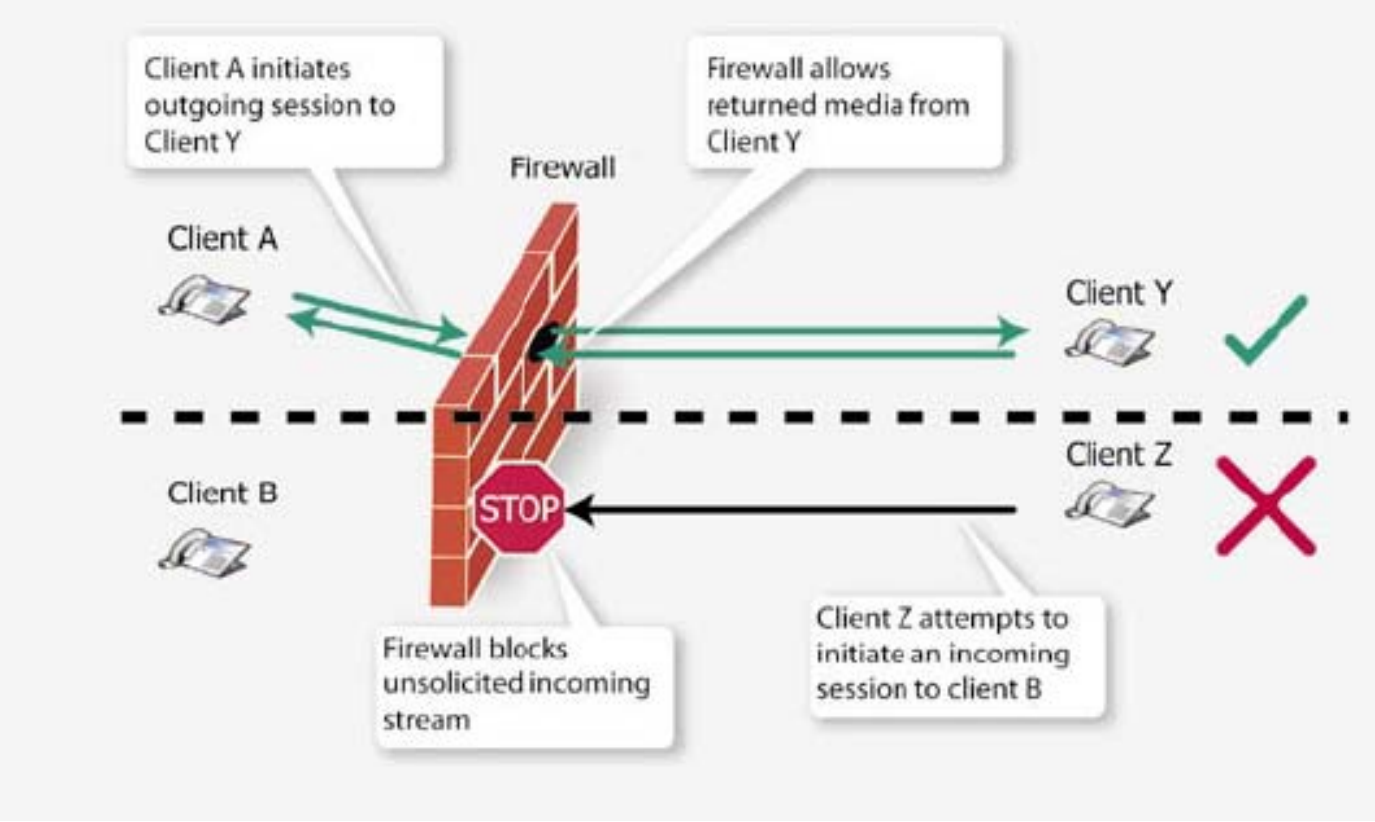
Aspects de sécurité spécifiques à la VoIP: Le problème du FW:

Frank Leeds,Seitel Leeds & Associates fleeds@sla.com



Aspects de sécurité spécifiques à la VoIP

- Le problème du FW:



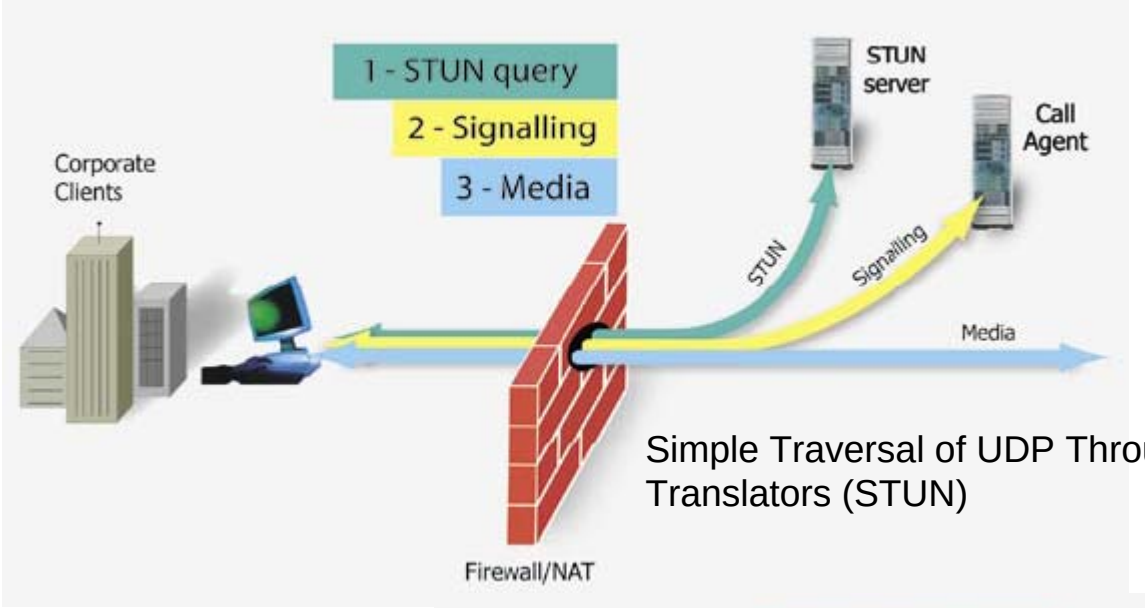
www.newport-networks.com

Aspects de sécurité spécifiques à la VoIP

- **Le problème du NAT**
  - Le NAT reste un outil de protection indispensable puisqu'il contribue à dissimuler la structure du réseau de l'entreprise vis-à-vis du réseau public. Cependant le NAT ainsi que le FW bloque le trafic ainsi que les appels entrants.

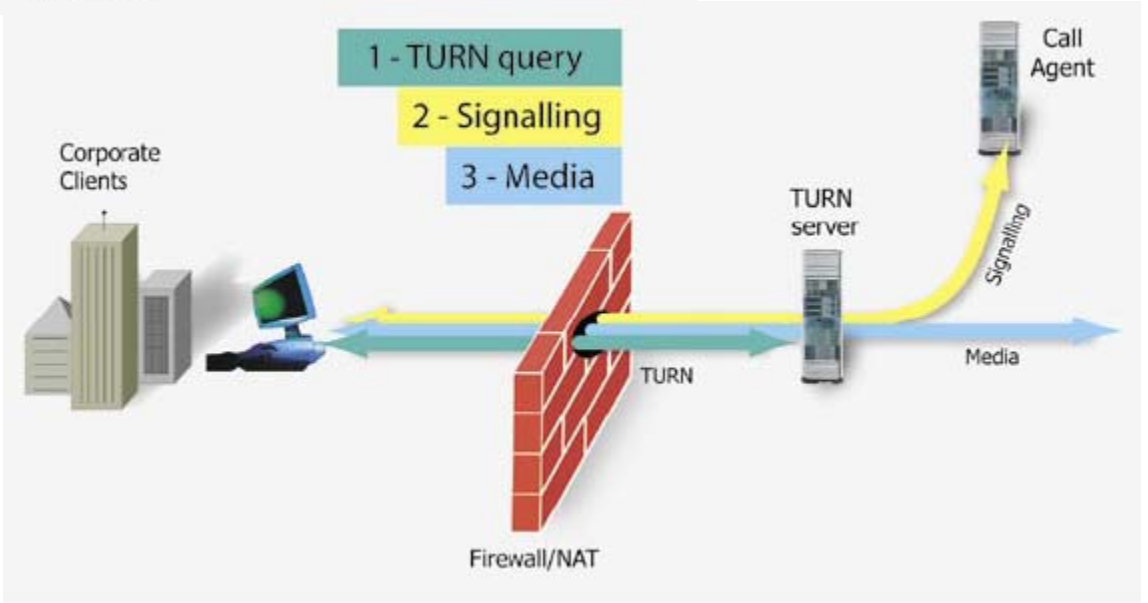
- **Les solutions**
  - Utilisation de fonctions supplémentaires appelées TURN (Traversal Using Relay NAT) et STUN (Simple Traversal of UDP Trough NAT) ou de FW avec des ALG (Application Layer Gateway particulièrement performants appelés aussi SBC (Session Border Controller).

Aspects de sécurité spécifiques à la VoIP: Fonctions TURN et STUN.



Solution pas compatible avec le NAT symétrique

Simple Traversal of UDP Through Network Address Translators (STUN)



www.newport-networks.com

Aspects de sécurité spécifiques à la VoIP: problème du cryptage et d'authentification.

Problème du cryptage:

Dans le cadre de la VoIP le problème du cryptage et de l'authentification est double:

- Authentification et cryptage de la session de signalisation.
- Authentification et cryptage du flux voix.

Solutions:

Authentification de la session et cryptage de la session dépendent du type de protocole VoIP:

- H.323: définit une norme H335 V2.
- SIP: S/MIME ou SIPS (TLS=>SSLv3) .

Authentification et cryptage du flux Voix : SRTP et MIKEY (Multimedia Internet KEYing RFC3830):

- H.323: définit une norme H.335 V2

Problématique Skype

Du points de vue sécurité Skype pose un double problème:

- Protocole n'est pas publié
  Bien que depuis cet été le code à été officiellement inspecté par Tom Berson d'Anagram Laboratories voir: http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf
- Basé sur les protocoles P2P

Conséquences:

- En cas de détection de vulnérabilités seul Skype peut les corriger.
  Actuellement déjà 5 exploits ont été publiés et corrigés avec la (http://www.skype.com/security/bulletins.html) version 1.4 :
- L'utilisation de Skype exige l'octroi d'accès à votre ordinateur et à votre réseau à de tiers.

  En effet en chargeant le softphone gratuitement vous octroyez à Skype la permission d'utiliser Votre ordinateur en acceptant: « Pour recevoir les bénéfices fournis par le Logiciel Skype, vous accordez par la présente la permission pour le Logiciel Skype d'utiliser le processeur et la largeur de bande de votre ordinateur pour le but limité de faciliter la communication entre Vous et d'autres utilisateurs de Logiciel Skype." Bien que Skype refuse d'expliquer les détails de leur protocole, il est probable que les ordinateurs clients SKype derrière des coupe-feux (firewalls) parcourent l'Internet cherchant des super-noeuds, avec les quels ils établissent des connexions.

Conclusion.

Face à la montée du risque lors du déploiement de la VOIP dans une entreprise il faut:

- Définir une politique de sécurité VoIP (Soft phones et applications CTI souhaitées?).
- Faire un audit QoS du réseau.
- Séparer le réseau DATA du réseau VoIP et vérifier constamment leur isolation.
- Surveiller le trafic voix (tarifs) pour détecter des attaques et intrusions et expliquer toutes les anomalies.
- Faire auditer le réseau régulièrement par des professionnels différents.

Conclusion

Actuellement les avis continuent à diverger

Certains spécialistes de la sécurité d'entrerprises comme M Hervé Schauer, de la sécurité continuent à douter de la maturité de la VoIP: Ce dernier déclarait sur ZDnet

« Je pense que la VoIP n'est pas une technologie mature et qu'elle pose incontestablement une problématique de sécurité »

« une entreprise souhaitant intégrer un service de VoIP à son système d'information doit prendre en compte la problématique de sécurité dès l'idée initiale du projet. Elle doit être intégrée lors de sa définition et dans le premier cahier des charges. Ainsi les risques de panne des logiciels sont explicitement prévus dès le départ. Les solutions pour y faire face sont donc déployées en même temps que le projet »

Références

- **Bill Douskalis** : *IP Telephony – The Integration of Robust VoIP Services*. Edition Hewlett-Packard Professional Book
- **Ofir Arkin :** *VoIP - The Next Generation of Phreaking*
- http://www.sys-security.com/html/projects/VoIP.html
- **DISA :** *VoIP - Security Technical Implementation Guide*
- http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V1R1R-4PDF.pdf
- **Bureau de la protection des infrastructures essentielles** : Protection VoIP
- http://www.ocipep.gc.ca/opsprods/info_notes/IN03-001_f.pdf
- **Pingtel** : *Secure IP Telephony For The Enterprise*
- http://www.checkpoint.com/products/downloads/voip_whitepaper.pdf
- **Inkra Networks Corp**. : *Securing enterprise voice over IP networks*
- http://downloads.lightreading.com/wplib/inkra/Inkra_VoIP_Security.pdf
- **By James P. Cavanagh** : *Secure Business Telephony With VoIP*
- http://itresearch.forbes.com/detail/RES/1039129120_961.html
- **TippingPoint Technologies** : *Intrusion Prevention - The Future of VoIP Security*
- http://www.preferredcomputers.com/whitepapers/download/VoIPSecurity.pdf
- **Ofir Arkin et Josh Anderson** : *Multiple Vulnerabilities with Pingtel xpressaSIP Phones*
- http://lists.virus.org/vulnwatch-0207/msg00023.html
- **Draft Rosenberg** : The Session Initiation Protocol (SIP) and Spam
- http://www.jdrosen.net/papers/draft-rosenberg-sipping-spam-01.txt
- **CISCO :** *Adding MSN Messenger Services to Cisco Packet Voice Networks*
  http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a0080092946.shtml
- **Andreas Steffen, Daniel Kaufmann, Andreas Stricker :** *SIP Security*
- http://security.zhwin.ch/DFN_SIP.pdf
- *Sécurisation des communications avec SSLv3*
- http://securit.free.fr/ressources/ssl_v3.pdf
- **Johan Bilien** : *Key Agreement for Secure Voice over IP*
- ftp://ftp.it.kth.se/Reports/DEGREE-PROJECT-REPORTS/031215-Johan-Bilien-report-final-with-cover.pdf
- **Johan Bilien, Erik Eliasson and Jon-Olov Vatn** : *Call establishment delay for secure VoIP*
- http://www.minisip.org/publications/secvoip.pdf
- **Israel M. Abad Caballero, Gerald Q. Maguire Jr., Pedro G. Vilda - Royal Institute of Technology (KTH)** : *Secure Mobile Voice over IP*
- ftp://ftp.it.kth.se/Reports/DEGREE-PROJECT-REPORTS/030626-Israel_Abad_Caballero-final-report.pdf
- **C. Jennings** : Example call flows using SIP security mechanims
- http://www.softarmor.com/wgdb/docs/draft-jennings-sip-sec-flows-01.html
- **Draft Sterman** : RADIUS Extension for Digest Authentication
- http://www.softarmor.com/wgdb/docs/draft-sterman-aaa-sip-00.txt

Références

- **Webtorials** : 2004 VoIP state of the Market Report
- **Best practices for SIP NAT traversal** By Adrian Georgescu
- **SERVICE ARCHITECTURES IN H.323 AND SIP: A COMPARISON:** JOSEF GLASMANN, MUNICH UNIVERSITY OF TECHNOLOGY (TUM)