Ministère de l'enseignement supérieure et de la recherche scientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU

Faculté de Génie électrique et Informatique

Département électronique

Mémoire de fin d'études

En vue d'obtention du diplôme de MASTER en électronique

Option : Télécommunication et Réseaux

Thème :

PROJET D'UNE PLATEFORME VISIOCONFERENCE

Présenté par :

OUILES Saïd Adlane

Encadreur :

Mr HAFERSAS Fouad

Promoteur :

Mr AIT BACHIR Youcef

2012 /2013

Remercîments

Mes remerciements

A Monsieur AZAZENE Hamza, le chef de division Djaweb /Algérie Télécoms, pour m'avoir permis de mener à bien ce projet au sein de l'entreprise, je remercie également Madame KACI, sous directrice des projets au sein de Djaweb, Monsieur HAFERSAS Fouad, AKLI Mohand mes encadreurs au sein d'Algérie Télécoms pour leurs suivi et leurs remarques qui m'ont aidés à mener à bien ce travail et pour m'avoir guidé tout en me laissant un maximum de liberté et d'initiative.

Je tiens aussi à remercier mon promoteur Monsieur AIT BACHIR , pour m'avoir guidé et corrigé tout le long de ce projet.

Ma gratitude va également à tous mes enseignants de l'université Mouloud MAMMERI.

Je remercie aussi tout mes amis, qui mon soutenus tout le long de ce projet.

Je tiens à remercier surtout toute ma famille qui m'a soutenue et encouragée tout le long de ma scolarité .

Dédicace

Je dédie ce modeste travail à celle qui m'a donnée la vie, symbole de tendresse, et qui s'est sacrifiée pour mon bonheur et ma réussite, à ma mère .

A mon père, école de mon enfance, qui a été mon ombre durant toutes mes années d'études, et qui a veillé tout au long de ma vie à m'encourager, à me donner toute l'aide dont j'avais besoin . Que dieu les garde et les protège.

Je dédie ce travail à mes grands parents, qui ne sont plus de ce monde.

A ma sœur, à mon frère qui mon bien aidés et encouragés tout au long de ma vie.

A tous mes amis , Nasser, Mohand, Juba, Karim et Atmane et à tous ce qui mon encouragés tout au long de mon projet.

A tous ceux qui me sont chèrs.

Sommaire

Résumer

Dans cette optique, notre travail consiste à implémenter une conférence sous un logicielle spécifique de Cisco (Jabber Vidéo). Ce travail à été proposé par Algérie Télécoms, où nous avons effectué un stage de 2 mois.

Nous avons réparti ce mémoire en 4 chapitres, le 1er concerne l'étude du système existant : nous parlerons des différent services et équipements proposés pour une plateforme visioconférence au sein des Directions de l'éducation nationale et ensuite nous aborderons le sujet des interconnexions et la sécurité utilisée pour ces derniers.

Le second chapitre présente le fonctionnement de la visioconférence : nous aborderons les différents modes de diffusion, les différents protocoles utilisés, et nous ferons une comparaison entre ces protocoles. Nous parlerons aussi des différentes normes de compression pour les signaux audio et vidéo et aussi des cryptages, puis nous parlerons de la Qualité de services et de la résolution optique, ainsi que de proxy et firewalls utilisés pour la partie sécurité.

Le chapitre 3 présente l'optimisation du QoS et de la bande passante, nous parlerons des caractéristiques et ordonnancements du QoS et des mises en forme du trafic et surtout des problèmes de la qualité de services et des solutions proposés. Nous aborderons aussi les problèmes de l'optimisation de la bande passante pour une meilleure transmission de données.

Le chapitre 4; qui concerne la réalisation de ce projet, présente la mise en place de la plateforme visioconférence, à travers les différentes étapes mises en œuvre pour avoir une conférence simple et multiple.

Introduction

Introduction

Ces dernières années, en a connu une véritable révolution technologique avec l'explosion des systèmes multimédias et des réseaux hauts débits. A la base, ceci a été rendu possible par les nouvelles techniques de digitalisation qui ont permis de coder de façon numérique tous les médias ; on parle d'un monde de l'information « tout numérique ». A partir de là, tous les médias, en particulier l'audio et la vidéo, ont pu être intégrés et traités par des ordinateurs, et delà on parvient donc à un nouveau monde dans lequel l'informatique et les télécommunications se rejoignent pour donner naissance aux systèmes distribués hauts débits multimédias, ce qui a permis un jour d'envisager des appels vidéos aussi appelé visioconférence.

La visioconférence, aussi appelé vidéoconférence est un outil permettant de voir et d'entendre en directe son interlocuteur à distance. L'idée de la vidéoconférence ne date pas d'hier . en effet, la mise en œuvre de cette idée a débuté dans les années 60 purement à but de démonstration dans des expositions mais n'a jamais réellement vu le jour dans ces années –là . A cette époque, l'installation d'une telle technologie était très couteuse et donnait des résultat médiocres. A cause de la lenteur des lignes téléphoniques utilisées pour le transport du signal, il aura fallu attendre jusque dans les années 80 pour que les premiers appels visiophoniques deviennent possibles après une amélioration de la technologie , notamment de ses méthodes de codage et la baisse de cout des équipements .

Cependant, déjà à cette époque , une question restait sans réponse à savoir l'utilité réelle de la visiophonie. Quel est l'avantage de voir son interlocuteur quand un simple coup de téléphone devrait suffire ? En vérité, le besoin de cette technologie se fait de plus en plus ressentir sur le marché. L'internationalisation des entreprise nécessite un contact fréquent avec des personnes positionnées en des lieux géographiquement éloignés et les couts de déplacement d'un employé a la participation d'une réunion peuvent vite devenir onéreux. C'est entre autres pour ces raison que la visioconférence peut s'avérer utile si elle est utilisée à bon escient.

Cependant, durant de nombreuses années, la visioconférence est restée une technologie attendue mais non-exploitable. A l'heure actuelle, grâce à l'amélioration du système, les entreprises peuvent désormais l'utiliser et découvrir peu à peu ses bénéfices et surtout son retour sur investissement.

Dans cette optique, notre travail consiste à implémenter une conférence sous un logicielle spécifique de Cisco (Jabber Vidéo). Ce travail à été proposé par Algérie Télécoms, où nous avons effectué un stage de 2 mois.

Nous avons réparti ce mémoire en 4 chapitres, le 1er concerne l'étude du système existant : nous parlerons des différent services et équipements proposés pour une plateforme visioconférence au sein des Directions de l'éducation nationale et ensuite nous aborderons le sujet des interconnexions et la sécurité utilisée pour ces derniers.

Le second chapitre présente le fonctionnement de la visioconférence : nous aborderons les différents modes de diffusion, les différents protocoles utilisés, et nous ferons une comparaison entre ces protocoles. Nous parlerons aussi des différentes normes de compression pour les signaux audio et vidéo et aussi des cryptages, puis nous parlerons de la Qualité de services et de la résolution optique, ainsi que de proxy et firewalls utilisés pour la partie sécurité.

Le chapitre 3 présente l'optimisation du QoS et de la bande passante, nous parlerons des caractéristiques et ordonnancements du QoS et des mises en forme du trafic et surtout des problèmes de la qualité de services et des solutions proposés. Nous aborderons aussi les problèmes de l'optimisation de la bande passante pour une meilleure transmission de données.

Le chapitre 4; qui concerne la réalisation de ce projet, présente la mise en place de la plateforme visioconférence, à travers les différentes étapes mises en œuvre pour avoir une conférence simple et multiple.

Chapitre 1 :
Etude du système existant

I. Introduction

Dans ce chapitre 1 nous allons voire le système existant au niveau d'Algérie Télécoms, nous parlerons des différents services proposés par le NGN (Next Génération Network), comme le RMS d'Algérie télécoms pour la voix IP, la visioconférence et les différents équipements ainsi que les interconnexions dont la sécurité utilisées pour le bon fonctionnement de ces derniers proposer par la technologie Cisco.

II. SERVICES

1) Voix ip :

La voix sur IP, ou « VoIP » pour *Voice over IP*, est une technique qui permet de communiquer par la voix (ou via des flux multimédia: audio ou vidéo) sur des réseaux compatibles IP, qu'il s'agisse de réseaux privés ou d'Internet, filaire (câble/ADSL/optique) ou non (satellite, Wifi, GSM, UMTS ou LTE) . Cette technologie est notamment utilisée pour prendre en charge le service de téléphonie sur IP (« ToIP » pour *Telephony over Internet Protocol*).

Le terme « VoIP » est en général utilisé pour décrire des communications « point à point ». Pour la diffusion de son ou de vidéos sur IP en multipoints, on parlera plutôt de *streaming* pour une simple diffusion, comme les radios Web par exemple. Le terme multipoints sera réservé à des visioconférences dont le nombre de participants est plus grand que deux.

La voix ou le son sur IP peut se faire en mode *Unicast*, *broadcast* ou *Multicast* sur les réseaux, c'est-à-dire en mode « point à point », en mode « une émission et plusieurs réceptions » (comme un émetteur TV, par exemple) et en mode « une émission pour plusieurs réceptions » (mais le signal n'est routé que s'il y a des récepteurs) comme les radios Web.

Services de voip

- Collecte et terminaison de trafic sur IP (Voix, données) : Mutualiser la ressource réseau pour supporter le trafic Data (IP) et Voix (téléphonie).
  + VoIP : Transport de la Voix sur IP (numérisation et acheminement de la voix, transposition de la signalisation)
  + ToIP : Service de téléphonie s'appuyant sur la VoIP.

Inclut :

Services de base (téléphone, fax, …).
Services à valeur ajoutée offerts par un PABX (filtrage, renvoi, conférence, messagerie vocale, …), centre d'appels.

- Interconnexion de réseaux PABX : Cette solution permet à l'entreprise d'adopter la VoIP progressivement. L'infrastructure existante est maintenue (PABX et téléphones) et les différents sites de l'entreprise sont reliés à l'aide de passerelles IP.
- Interconnexion de réseaux d'opérateurs de téléphonie fixe type RTC et mobile type GSM, PRS, EDGE et UMTS.

- Interconnexion de serveurs audiotel.
- Interconnexion de Centres d'Appel : Grâce à la technologie de la VoIP qui permet aux entreprises d'interconnecter leur sites distants ou d'unifier leur standard téléphonique(un seul numéro mis à la disposition des clients pour joindre tous les sites).

2) Visioconférence :

On nomme visioconférence la combinaison de deux techniques :

- La visiophonie ou vidéo téléphonie, permettant de voir et dialoguer avec son interlocuteur .
- La conférence multipoints ou conférence à plusieurs, permettant d'effectuer une réunion avec plus de deux terminaux.

Dans la pratique, le terme reste toutefois utilisé même lorsque les interlocuteurs ne sont que deux.

Les premières applications de visioconférence se faisaient en utilisant des lignes RNIS. En 1995, les premières vidéoconférences publique eurent lieu comme celle entre l'Amérique du Nord et l'Afrique, liant un 'techno-fair' à San Francisco avec une 'techno-rave' à Cape-Town. Dans la même année une collaboration entre Intel, Microsoft et RADVISION lancèrent des systèmes de communications VoIP afin de les standardiser.

On leur préfère aujourd'hui pour des raisons de coût les supports d'Internet classiques : ADSL, câble pour les particuliers ou ligne dédiée pour les professionnels. L'ATM se prêterait bien aussi à ce genre d'applications, puisqu'il a été conçu dès le départ pour combiner les transports de voix, d'images et de données, ce qui n'était pas le cas de TCP/IP (qui a heureusement évolué pour le permettre partiellement depuis).

La Tendance Mondiale dans les Réseaux Télécoms c' est le NGN (Next Génération Network), comme le RMS en Algérie qui est un nouveau réseau de commutation de données à large bande d'envergure nationale, est de type IP/MPLS. Il est conçu afin de supporter et fédérer tous les types de protocoles et permettre l'interconnexion et l'inter fonctionnement des réseaux existants. Le backbone IP/MPLS s'inscrit dans le cadre de la modernisation du réseau d'Algérie Télécom et de sa tendance vers le monde du NGN notamment avec un réseau d'accès à large bande et un système unique de supervision et de maintenance.

Les différents services supportée sont :

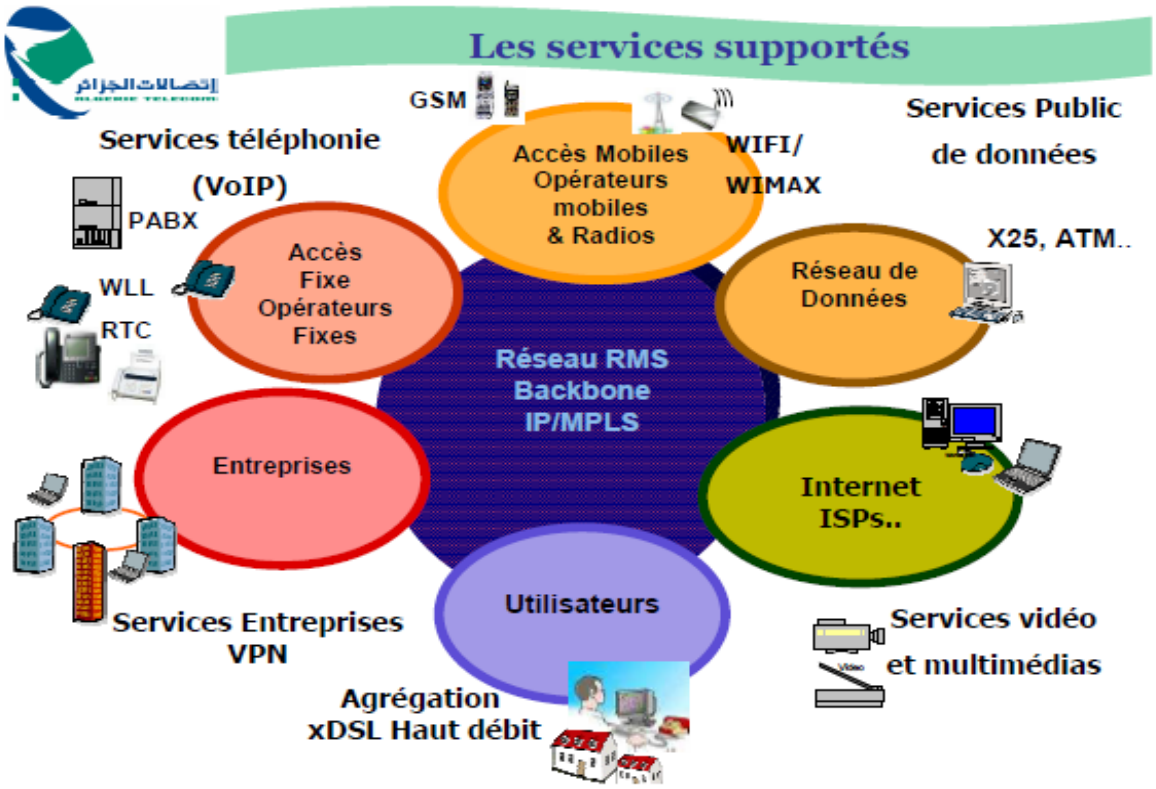


Figure 1.1:Différents services supportés par le backbone d'Algérie Télécoms

Services de données

- Services à haut Débit (ADSL…).
- Transport de données (x25, IP,…)
- Services de Réseaux Virtuels Privés (VPN) : Les réseaux VPN/MPLS assurent des livraisons multi-sites pour une entreprises selon plusieurs niveaux de hiérarchie, en garantissant la sécurité et une qualité de service (QOS).
- Interconnexion des sites (réseaux locaux LAN) : Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Dans ce cas, des équipements spécifiques sont nécessaires. Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les trames de l'un sur l'autre. Dans le cas contraire, c'est-à-dire lorsque

les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à une conversion de protocole avant de transférer les trames. Ainsi, les équipements à mettre en œuvre sont différents selon la configuration face à laquelle on se trouve.

Services multimédias (Ce service n'est pas utiliser dans ce projet.)

- Interconnexion des réseaux TV(CATV,IPTV).
- Services multimédias (vidéo, télémédecine, centre de contact).
- Interconnexion des serveurs vidéo.
- Interconnexion de futurs réseaux (WAP, UMTS).

III. EQUIPEMENTS

a) Data :

Architecture globale d'un data center (DC) :

L'architecture SAN (*Storage Area Network*) est apparue il y a quelques années. Elle avait pour objectif d'offrir une approche différente (augmentation des performances des serveurs, augmentation des débits réseaux) aux problèmes de l'explosion de la volumétrie des données. Cette architecture est basée sur la constitution d'un réseau performant et dédié à l'échange de données avec les périphériques de stockage.

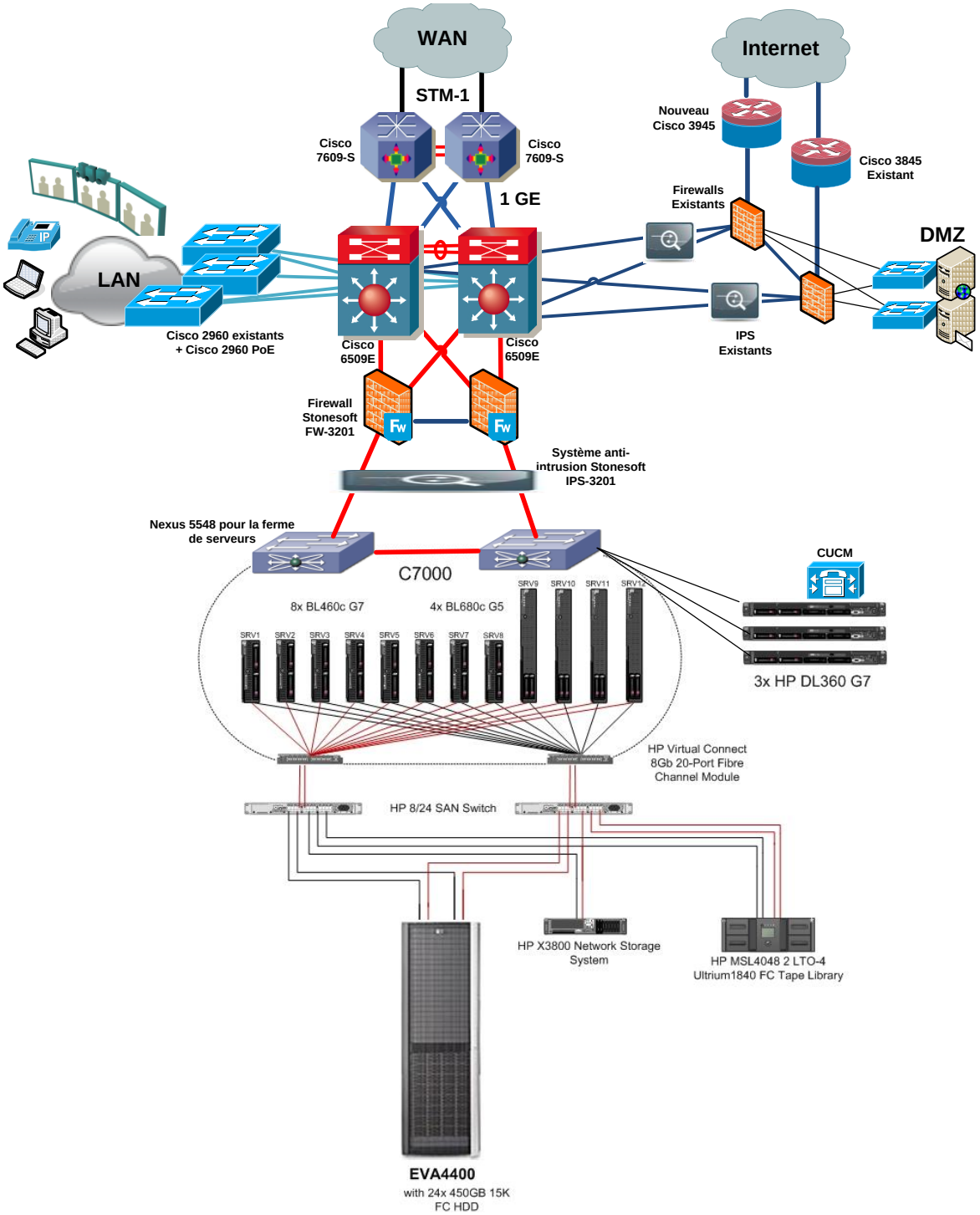


Figure1.2 : Architecture du Data Center

1) Routeurs :

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. Il y a habituellement confusion entre routeur et relais, car dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 de l'OSI.

Le Site Central sera doté de deux retours Cisco 7609-S équipés de la même configuration mis en partage de charge qui seront raccordés au Backbone d'Algérie Telecom via deux liaisons en Fibre Optique à 155 Mbps sur un châssis de transmission de 2,5Gbps.

Le Routeur Cisco 7609-S : Un routeur modulaire a 9 slots de hautes performances destiné à être placé au cœur des grands réseaux ou dans les Data Center là ou les besoins en puissance et en connectivité WAN sont nécessaires.

Le routeur Cisco7609 proposée comprend :

- Une carte de supervision **RSP720-3CXL-P**, et est caractérisée par :

- deux ports de un giga (Un port en 10/100/1000, un port en SFP ou /10/100/1000)
- jusqu'a de 400 **M**illion de **P**aquets **P**ar **S**econde en IPv4
- jusqu'a de 200 **M**illion de **P**aquets **P**ar **S**econde en Ipv6
- Produit capacité de bande de 40 Gbps par Slot
- Mémoire RP (Route processor) 2GB
- Mémoire SP (Switch processor) 1GB
- 512 de mémoire Flash
- 4MB NVRAM
- Supporte 256 000 routes en IPv4 et 128 000 en IPv6

Les Directions d'Education principales seront raccordé au Backbone d'Algérie Telecom via des liaisons Fibre Optique Channalizées STM1, exploité a 34Mbps (8 Mb pour le site Central et le reste en plusieurs E1 pour connecter les institutions sous-tutelles et DE secondaires).

Des routeurs Cisco ASR 1006 sont proposés pour ces DE Principales, ils sont de nouvelle génération de la famille des ASR 1000 (Agregate Service Router). Modulaires, intégrant de multiples services en hardware et conçu avec la flexibilité autorisant des performances de 10 Gbps.

Le Routeur Cisco ASR 1006 proposé est composé de :

- 01 module RP (Route Processor), qui possède un disque intégré de 40GB HDD et une mémoire 4GB DRAM.
- 01 module ESP (Embedded Services Processor), d'une capacité de 10GB.
- 01 module SIP10 (*SPA Interface Processor*), ce module est extractible. possède 04 slots pour modules SPA.
- 2 boitiers d'alimentation (1600W), en redondance.
- le package software utilisé est le Cisco IOS-XE Advenced Entreprise Services (SASR1R1-AESK9-31S), supporte toutes les fonctions existantes dans les routeurs actuels, l'encryptions IPSEC en 3DES, AES, SSH, SBC, et supporte aussi les protocoles classiques (IPX, Decnet…).

03 ports en connecteur RJ45 (Auxiliaire, Consol, de management) et deux ports USB.

Algérie Telecom propose Des Routeurs Cisco 3945 *Integrated Services Router* (ISR G2), qui offrent bien plus qu'une simple connexion de données au réseau.

Pour les sites de taille moyenne, Cisco 3945 ISR-G2, offre une performance de communication WAN avec des services tels que la sécurité, la mobilité, l'optimisation WAN, les communications unifiées et la vidéo.

La configuration matérielle du routeur Intranet **C3945-CME-SRST/K9** proposé est :

- 1 GB de mémoire DRAM
- 256 MB de mémoire Compact Flash
- 3 ports 10/100/1000 ports Ethernet (RJ-45)
- 4 emplacements pour Service module.
- 4 emplacements pour Module de type EHWIC, HWIC, ou VWIC
- 1 slot Service Module interne pour les services d'application
- Double alimentations AC
- License IP Base
- License Unified Communication pour la série 3900
- License Cisco SRST (*Survivable Remote Site Telephony*) pour 25 poste.
- Module PVDM3 pour 64-Channel
- Carte HWIC a 4 Ports E1/T1 clear channel
- 2 Cartes VWIC-2 MultiFlex Trunk a 2 port E1/T1

2) Switch :

En informatique, un *switch* désigne un commutateur réseau, un équipement qui permet l'interconnexion d'entités réseau appartenant à un même réseau physique. Contrairement au concentrateur (ou *hub*), il fractionne le réseau en domaines de collision indépendants.

HP et Algérie Télécom sont en mesure d'élaborer et de prendre en charge une infrastructure robuste et adaptative qui donnera les moyens d'atteindre ses objectifs. En particulier, la solution proposée permettra d'améliorer sa souplesse ,et d'atteindre ses objectifs de niveau de service et d'accroître son efficacité opérationnelle tout en atténuant les risques inhérents aux projets.

2.1) HP Virtual Connect

Les Switch Ethernet proposés sont des Virtual Connect Flex 10 qui permettent de découper chaque port réseau de 10GB à 4 Flex NIC ajustable à raison de 100MB se qui permettra de palier à tous goulet d'étranglement sur la partie réseau.

HP Virtual Connect est le moyen le plus simple pour connecter des serveurs Blade aux réseaux LAN et SAN.

La connexion d'un serveur est classiquement une opération compliquée, qui demande la configuration de paramètres de connexion et de sécurité et l'intervention de plusieurs administrateurs.

Le HP Virtual Connect Flex-10 apporte une flexibilité et des fonctions de qualité de service inédites. Disponible avec les ports Flex-10 intégrés dans les derniers ProLiant BL ou les cartes réseau Flex-10, connectés au module HP Virtual Connect Flex-10, Flex-10 permet de multiplier les ports réseau sans avoir à ajouter de cartes ni de modules de connexion et de choisir le débit des ports serveurs suivant la vraie demande des applications.

- Flex-10 permet de créer jusqu'à 4 ports « FlexNIC » par port Ethernet 10 Gb, avec le choix du débit de 100 Mb à 10 Gb par incréments de 100 Mb.

- Les ports Flex-10 sont créés par le matériel, dans le BIOS du serveur. Ils sont totalement transparents pour les systèmes d'exploitation : chaque FlexNIC possède sont identificateur PCI et son adresse MAC ou WWN.

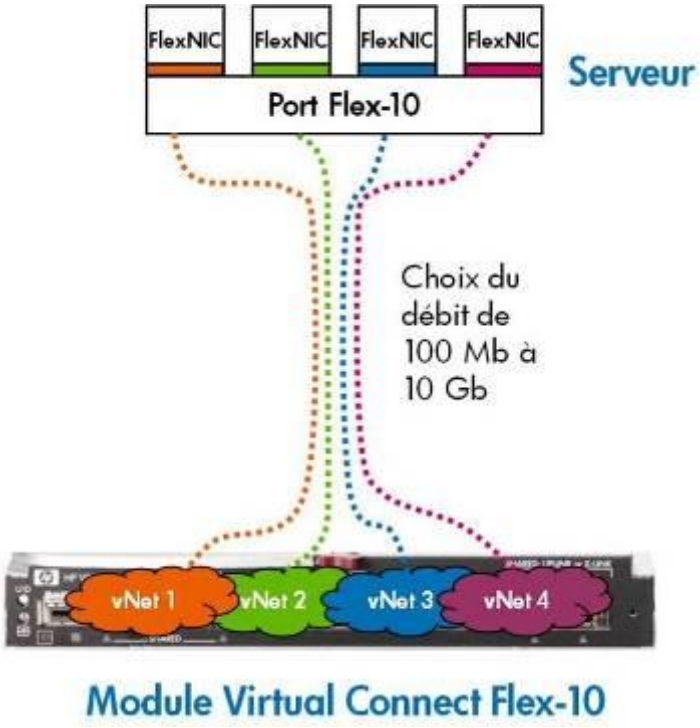


Figure 1.2: Switch HP Virtual Connect Flex 10

2.2) HP Switch SAN

Le HP Storage Works 8 / 24 commutateur SAN répond aux besoins des PME ainsi que les grandes entreprises en fonctionnant comme un commutateur central autonome ou comme commutateur de périphérie à faible coût dans les grands réseaux de base à bord de stockage hiérarchisé.

Le 8 / 24 commutateurs SAN offre une protection d'investissement sans précédent. Auto-détection des ports qui prennent en charge la compatibilité descendante avec 1, 2, 4 et 8 Gbit / sec dispositifs réduire considérablement la complexité de déploiement et les coûts, tout en assurant la compatibilité avec les périphériques installés.

Le 24/08 SAN Switch 24 ports peut être déployé comme un full-fabric switch ou en mode Access Gateway, qui fournit une connectivité dans toutes les SAN (le réglage du mode par défaut est un commutateur).

Access Gateway mode utilise NPIV interrupteur normes de présentation des connexions Fibre Channel en tant que dispositifs logique SAN.

Haute performance

• Comprend simultanément une grande vitesse d'interface pour tous les ports afin de fournir un système de haute performance avec une bande passante allant jusqu'à 384 Gbit/s en duplex intégral

• Fournit les meilleures performances disponibles, complète en amont et en protection.

Haute Evolutivité

• Livré avec 16 ports activés "pay-as-you-grow" évolutivité à 24 ports activés
• Offre une connectivité transparente aux environnements serveur multifournisseurs, et permet à un grand nombre de serveurs de se connecter à un SAN sans augmenter le nombre de domaine switch

• Permet jusqu'à huit ports (à 2, 4 ou 8 Gbit/s) entre une paire d'interrupteurs à être combinés pour former un ISL logique unique avec une vitesse allant jusqu'à 64 Gbit/s (128 Gbit/s en duplex intégral) pour utilisation de bande passante optimale et l'équilibrage de charge.

Amélioration de TCO

• Optimise les performances à l'échelle équilibrage de charge en acheminant automatiquement les données à toutes les voies disponibles

• Supprimer / éviter les goulets d'étranglement de performance à forte densité environnements de serveurs virtualités

• Des services avancée à la performance SAN et optimise l'utilisation des ressources

Les switchs sont diviser en plusieurs niveaux dont le L2 et L3 (level 2 et level 3) font référence aux couches de l'OSI.

- Le niveau 1 correspond au physique, la transmission des octets sur un media de propagation (lumière pour la fibre, une ddp sur cuivre, ou air pour les ondes radio).

- Le niveau 2 correspond au niveau des adresses hardwares locales des cartes réseau.

- Le niveau 3 correspond au niveau des adresses IP et du routage.

Au niveau du matériel réseaux on trouve des équipements pour ces catégories :

- Au niveau 1 : le hub ou répéteur multiport (qu'il répéte un signal optique comme avec une étoile optique, ou un boitier multi RJ45).

- Au niveau 2 : le Switch ou commutateur ou pont multiport ; A la différence du hub qui répète "bêtement" tout ce qu'il voit arriver sur un port, le Switch maintient par découverte une table d'adresse hardware (hexadécimales) des cartes réseau qu'il voit sur ses ports ; à l'arrivée d'une trame, il envoie a bon escient sur le bon port ou se trouve la destination et n'inonde pas les autres ports.

- Au niveau 3 : le routeur ou le commutateur L3 (= un Switch L2 + un module de routage L3).

Le flux de données peut être soit une agglomération de VLAN (on dit du flux "taggé" 802.1Q) ou être un flux d'un seul VLAN, d'un seul plan d'adressage. On peut faire des VLAN (réseau virtuels logiques) dans les Switch L2 ou L3 , Il y a plusieurs sortes de VLAN...

Le plus courant étant le VLAN par port : Cela revient a affecter des ports spécifiques a un VLAN. Ces groupes de ports réalisent alors logiquement la même fonction que s'il on reliait ces groupes de ports chacun à un switch dédié. Par exemple sur un switch 16 ports on affecte les ports 1 à 8 dans un VLAN1 et les ports 9 a 16 dans un VLAN2, cela revient a réaliser alors la même fonction que s'il on avait deux switchs 8 ports séparés. En général dans ces VLAN circulent des plans d'adressages séparés(des réseaux séparés).

On comprend alors que pour faire communiquer deux VLAN entre eux, deux plans d'adressages entre eux il faut passer par un niveau L3. Pour gérer les VLAN dans un switch, bien sur, il faut que celui ci soit mangeable. Il existe un autre mode de fonctionnement au niveau des VLAN, c'est le mode VLAN par mac (adresse hardware) ; assez pratique au niveau sécurité mais il implique une gestion rigoureuse, dans ce principe les adresses mac sont recensées dans une table et un VLAN particulier affecté a chacune de ces adresses, il peut y avoir un VLAN par défaut. Exemple de ce dernier mode, les adresses des PC de l'entreprise sont recensées et chaque fois qu'un portable reconnu se connecte sur le réseau de l'entreprise il sera automatiquement mis dans le VLAN intranet, si un PC inconnu se présente, alors il sera mis dans le VLAN externe qui a juste l'accès internet par exemple et ainsi ne pourra pas accéder aux ressources de l'entreprise.

La encore ces réseaux étanches ne peuvent communiquer que par du niveau L3 en général filtré (sinon il n'y a pas d'intérêt) de telle sorte que le réseau intranet peut être routé vers l'externe qui a l'internet, mais on bloque les retours pour que le réseau externe ne puisse rentrer, ceci avec un pare-feu .

Le VLAN par port est relativement aisé a faire et présent sur la gamme ng qui est, il faut le dire relativement bon marché, le vlan par mac est par contre les équipements les plus "pro".De même, sur des switchs L2 de milieu de gamme, il peut y avoir quelques fonctions L3 basiques (routage statique - dynamique) sur les vrais switchs L3 pro qui commutent les trames a hautes performances il y aura une vraie fonction L3 complète avec des fonctions étendues et performantes tant au niveau de la configuration que du fonctionnement. Par exemple les commutateurs L3 de haut de gamme travaillent en mode "cut-throught" c'est a dire que les trames sont commutées vers le bon port de destination alors juste que l'entête a été lue par des microprocesseurs (nommés ASIC) qui étudient chacun et de façon dédiée le flux de chaque port.

Dans les autres commutateurs c'est a dire des modèles les plus courants ils travaillent en mode "store and forward" c'est a dire que la trame quelque soit le port d'ou elle vient, est lue complément en mémoire, puis analysée par un seul et unique processeur central qui l'orientera ensuite. Entre les deux modèles la différence est une quantité considérable de puissance de commutation par seconde, et le temps de latence (= le temps de traversée du switch). Tout cela pour dire que des switchs, il y en a pléthore sur le marché, du L2 "grand public" non mangeable (donc sans possibilité de gérer les VLAN), le L2 mangeable, le L2 avec quelques fonctions "L3" de routage.

A retenir et en synthèse :

- Les switchs travaillent au niveau L2 de l'OSI celui des adresses hexadécimales Ethernet.

- On peut faire des VLAN dans certains switchs mangeables.

- Pour communiquer entre VLAN, il faut remonter au niveau L3 (de routage), celui des adresses IP.

b) Voix ip :

Les collaborateurs d'aujourd'hui exigent d'être connectés en permanence et de pouvoir accéder à tout moment aux modes de communication les plus efficaces. Grâce aux solutions de communications unifiées et aux réseaux IP, les entreprises peuvent faciliter la collaboration de leurs utilisateurs, quel que soit le lieu, l'heure ou le type de connexion.

L'explosion de la téléphonie IP a engendré une première source créatrice de valeur pour les entreprises et institutions. En fusionnant les réseaux voix, vidéo et données sur un seul réseau IP, ils sont parvenues à réduire le coût de leurs communications, en exploitant des capacités réseau jusque-là sous-exploitées et en posant les fondations de systèmes de communications unifiées.

Grâce à une suite complète de solutions de communications et de terminaux IP, vous avez la possibilité d'offrir des services de communication homogènes à l'ensemble de vos employés, quel que soit leur espace de travail (site principal, filiales ou sites distants) :

Cisco Unified Communications Manager : en adoptant ou en migrant vers la version actuelle, on peut bénéficier des avantages d'un espace de travail unifié et offrir à ses employés un large choix d'options de communication totalement indépendantes du système d'exploitation, du périphérique ou du support utilisés.

Cisco Unified Survivable Remote Site Telephony (SRST) : intégrée au logiciel Cisco IOS, la solution Cisco Unified SRST est utilisée conjointement à Cisco Unified Communications Manager ou à Cisco Unified Communications Manager Business Edition afin de permettre aux sites distants (DE secondaire dans le cas du Ministère de l'Education) d'accéder à une téléphonie IP haute disponibilité.

Téléphone IP Cisco Unified 7900 & 9900 : une gamme d'appareils robustes de nouvelle génération, avec un large éventail de téléphones IP adaptés à toutes applications : accueil de l'entreprise, bureau de responsables, bureaux de la direction, mais aussi à la maison, en déplacement ou dans une filiale.

Passerelle VOIX IP : Basées sur les routeurs ISR G2 (Integrated Service Routeurs - deuxième génération), les passerelles Voix sur IP de Cisco ont une architecture modulaire et utilisent le logiciel embarqué Cisco IOS. En face arrière, les passerelles offrent des slots pour accueillir les interfaces voix. Sur la carte mère des emplacements sont prévus pour insérer les processeurs de compression appelés DSP (Digital Signal Processor), permettant ainsi la communication entre le monde paquets et le monde circuits.

Switch Catalyst PoE : Des commutateurs CISCO de niveau 2 sont proposées afin d'alimenter en électricité tous les postes IP qui seront installés au niveau des sites .

connexion entre 2 site :

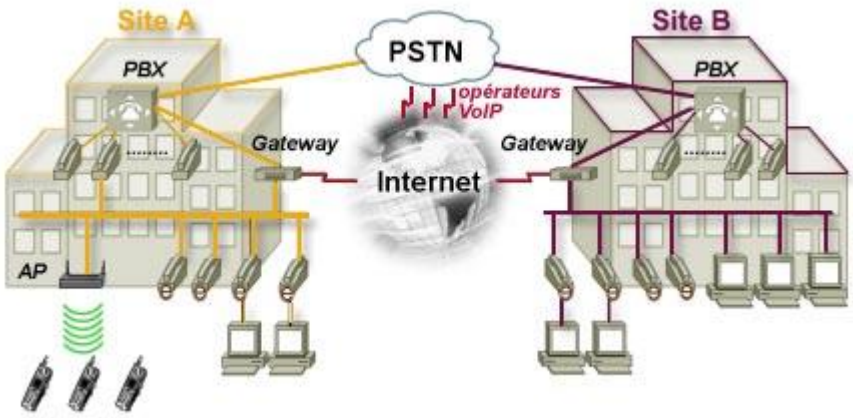


Figure 1.3: connexion entre différents sites.

PBX : central téléphonique actuel permettant d'accéder au réseau commuté.

IP PBX : central téléphonique IP se raccordant à IP ou Internet directement.

PSTN : Réseau commuté.

Gateway (ou passerelle) : équipement physique (boîtier) permettant de relier un équipement de technologie "commutée" au monde "IP".

AP : Access point (borne) Wifi ou DECT pour les combinés sans fils compatibles IP.

Opérateur VoIP : Opérateur vous permettant d'acheminer vos télécommunications vers le monde extérieur (VoIP ou non).

Serveurs Call manager

Ce matériel de traitement d'appels, Cisco Call Manager fournit des fonctions de téléphonie aux réseaux locaux et aux équipements réseau de téléphonie par paquets, tels que les téléphones IP, les équipements de traitement des médias, les passerelles de voix sur IP (VoIP) et les applications multimédia, [Serveur Cisco UCS C210 M1, Serveur Cisco L-UCSS-UCM].

Terminaux IP

CISCO nous propose plusieurs types de terminal IP dans : Cisco UC Phone 7911G (figure1) et

aussi de la haut gamme Cisco UC Phone 9971 (figure 2).

Figure 1

Figure 2

Gateway voix pour Site Central

Le terme ***gateway*** désigne un dispositif permettant de relier deux réseaux distincts présentant une topologie différente.

c) Visioconférence :

- Les différents systèmes :

Il existe plusieurs outil pour faire de la visioconférence sous différentes formes avec pour chacun d'entre eux des avantages et inconvénients. Le choix de leur utilisation va dépendre du besoin . il est clair qu'une réunion professionnelle est plus importante qu'un simple appel vidéo et que cela nécessite des équipements plus sophistiqués .

1. Les salles équipées .

Ces salles spécialement aménagées pour faire de la visioconférence sont équipées d'un ou plusieurs écrans et d'une caméra (HD). La caméra filme les interlocuteur ainsi qu'une partie de la table afin de donner l'impression que ces tables, bien qu'éloignées en réalité, ne font plus qu'une . Ces installations couteuses permettent d'obtenir un niveau de réalisme proche de la réalité. D'ailleurs, certains équipement permettent également de voire la personne distante à une échelle de

1 :1. Avec ce procédé, les interlocuteurs ont l'impression d'être en réunion face à face , ce qui facilite la communication et la rend plus agréable.

2. Les équipements sur pc .

Faire de la visioconférence à l'aide d'un pc est très facile et peu couteux. Il suffit d'avoir a sa disposition une webcam, un micron un logiciel permettant de faire des appels vidéo, et d'être connecté à internet avec une connexion haut débit. C'est le système le plus accessible pour une utilisation simple.

3. Les téléphones adaptes à la visiophonie (visiophones).

Beaucoup de constructeurs proposent des solution de bureau intégrées pour faire de la visiophonie. Certains périphériques comme des téléphones incluant un écran commencent peu à peu à voir le jour dans le milieu professionnel. Les appels sont de bonne qualité et leur utilisation est aussi simple qu'un téléphone ordinaire. L'ergonomie pour des appels vidéo à l'internet comme à l'externe reste leur points fort face au autres solutions. Bien entendu, ces périphériques restent à l'heure actuelle réservés à un usage professionnel et ne sont pas ou peu utilisés dans le privé.

4. Les périphériques mobiles .

La visiophonie mobile commence lentement à faire son apparition. Il est aujourd'hui possible de passer des appels vidéos depuis un appareil mobile de passer des appels vidéo depuis un appareil mobile de type Smartphone ou tablette pc sur différents réseaux.

La plupart doivent être connectés en wifi pour pouvoir fonctionner et d'autre peuvent se contenter d'un réseau 3G. cependant , un appel vidéo sur le réseau 3G reste d'une qualité médiocre et particulièrement instable.

5. Equipements proposer.

La gamme TANDBERG de Cisco privilégie l'innovation et les solutions à technologie avancée et développe des produits de visioconférence de pointe à haute valeur ajoutée. Ainsi, les solutions TANDBERG garantissent un retour sur investissement optimal. TANDBERG apporte la solution aux principales préoccupations des clients, à savoir la sécurité, la compatibilité totale, la communication de professionnel à professionnel et la convergence accélérée de la télé présence et des communications unifiées.

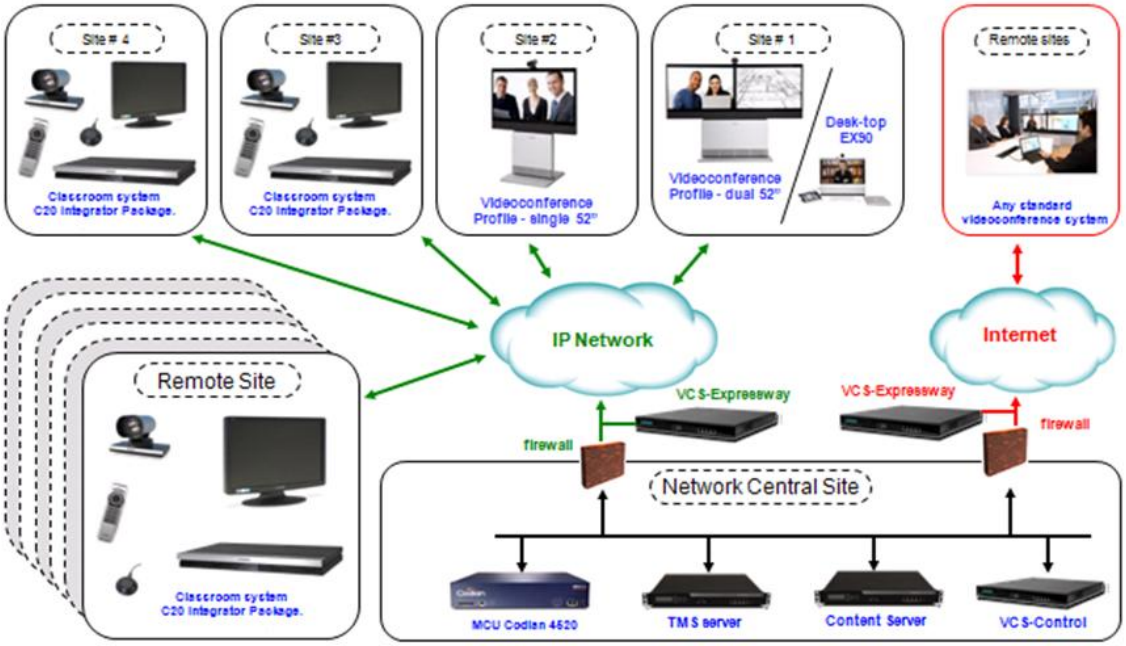


Figure1. 4:Architecture de connexion.

UNITES DE CONTROLE MULTIPOINT (MCU)

Les conférences multipoint permettent à plusieurs participants de participer à une seule et même visioconférence. TANDBERG propose plusieurs MCU afin de répondre aux besoins de votre entreprise. Des meilleures MCU HD du marché à présence continue au moteur de service hautement évolutif capable de s'adapter aux besoins de votre activité, TANDBERG possède la solution qu'il vous faut en matière de visioconférence

EXPRESSWAY

Une communication simplifiée et sécurisée au travers des Firewalls

La solution Expressway a pour but de faciliter la traversée des Firewalls. C'est une technologie innovante et unique sur le marché.

Jusqu'à maintenant, les terminaux de vidéoconférence pouvaient communiquer en IP soit en interne avec un respect de la sécurité du réseau, soit en externe mais au détriment de la sécurité du réseau (nécessité d'ouverture de plages de ports sur le firewall).

Au cours des dernières années, la technologie IP a rapidement évolué et son utilisation se généralise dans les entreprises.

TANDBERG a développé la solution Expressway qui permet de simplifier l'usage de la vidéoconférence sous IP, réduisant ainsi les coûts de communication.

En effet, Expressway permet de créer un accès sécurisé à travers n'importe quel firewall et respectant toutes les fonctionnalités des terminaux de vidéoconférence (H235, H264, H239…). Il devient alors possible pour les entreprises de communiquer entre elles en IP en toute sécurité, ce qui n'était pas possible jusqu'alors.

VIDEO COMMUNICATION SERVER (VCS)

Si la Vidéo Communication Server (VCS) a été récompensé pour ses performances et reconnu produit de l'année en 2008 par Internet Téléphonie c'est qu'il est le cœur de la technologie TANDBERG. Le Vidéo Communication Server relie l'ensemble des systèmes d'infrastructure et de gestion avec les terminaux et assure l'interopérabilité avec les réseaux de communication unifiées et de téléphonie IP, ainsi que les dispositifs VoIP.

Aujourd'hui ce produit garantit encore plus d'interopérabilité et plus de facilité dans l'administration du réseau vidéo de l'entreprise grâce à de nouvelles fonctionnalités :

Le Multiway™ permet de transférer à la volée une vidéoconférence point-à-point vers un pont multi-sites de façon transparente pour l'utilisateur. Cela apporte la fonctionnalité multi site à un terminal qui ne la possédait pas grâce à l'association avec les MCU Codian. Comme en téléphonie, le VCS apporte au monde de la vidéoconférence les fonctions de transfert d'un appel et de mise en attente d'un appel vidéo.

La compatibilité avec Microsoft Office Communicator: pour une interopérabilité totale avec les terminaux utilisant le standard H.323 (IP) en environnement Microsoft

Redondance : il est désormais possible d'installer jusqu'à 6 VCS en clusters afin d'éviter les pannes. La vidéoconférence étant devenue une application critique dans nombre d'entreprises, ce service doit être assuré quelles que soient les circonstances

Par ailleurs, le VCS de TANDBERG intègre une multitude de fonctionnalités dans un seul boîtier, là où les concurrents en auraient besoins de 3 ! Petit rappel de ses atouts :

FindMe : crée un numéro d'appel unique pour un utilisateur qui possède plusieurs moyens de communication (terminal individuel, logiciel de Visio, téléphone 3G…). Cette fonctionnalité permet ainsi d'appeler une personne et non un terminal

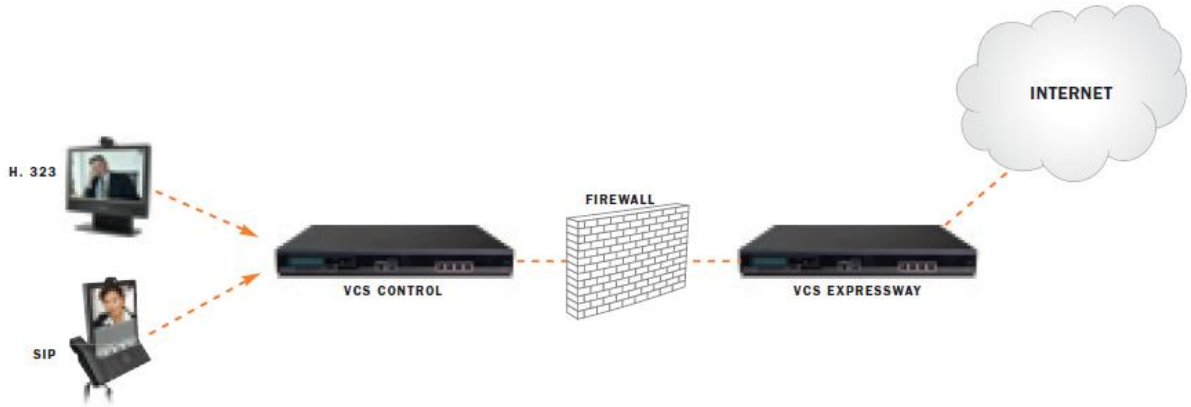
VCS Control : assume la fonction de passerelle entre les terminaux SIP et H.323

Expressway : facilite la communication avec le monde extérieur en permettant la traversée de pare-feu, idéale dans les communications vidéo via ordinateur portable par exemple. TANDBERG a été à l'origine de cette fonctionnalité, devenue depuis le standard H460

Gestion de la bande passante : facilite le contrôle des communications et l'authentification des terminaux

VCS Expressway :

Deux boitiers Vidéo Communication Server avec l'application Expressway seront mis en place entre les firewalls et les deux réseaux (Intranet et Internet), à l'aide de cette application, le VCS intègre la fonction de traversée de pare-feu pour des unités SIP et H.323. Grâce à la prise en charge des protocoles SIP et H.323, le VCS facilite la communication avec le monde extérieur



TANDBERG CONTENT SERVER

Les solutions d'enregistrement et de streaming de TANDBERG permettent le partage des connaissances et améliorent la communication en capturant et en diffusant les enregistrements de télé présence ou de visioconférence

GESTION

Une plateforme de gestion pour tous vos besoins en vidéo communications. TANDBERG Management Suite (TMS) est un outil évolutif et facile à utiliser, qui s'intègre avec les applications existantes. Il fournit une visibilité complète, un contrôle centralisé des systèmes sur site et hors site. TMS prend en charge la gestion, le déploiement et la programmation de l'ensemble du réseau vidéo.

EX90

Intuitif et élégant, l'EX90 est conçu pour communiquer mais aussi pour collaborer. Sa caméra vidéo haute définition Précision HD pivote de 90 degrés pour partager des esquisses, plans, radiographies et autres documents. Solution de collaboration puissante, l'EX90 peut recevoir d'autres caméras, moniteurs, appareils multimédias et périphériques.

En outre, l'EX90 dispose de la fonction Multi Site pour ajouter deux autres participants à un appel. Grâce à son écran HD 24 pouces grand format, la qualité des échanges reste optimale. TANDBERG intègre enfin un combiné audio pour faciliter les communications et faire gagner de la place sur le bureau. L'EX90 est compatible avec n'importe quel système de vidéo ou de Télé présence standard.

SERIE PROFIL 52"

La gamme Profile de TANDBERG est composée de systèmes de vidéoconférence haute définition, simples à utiliser et pleinement compatibles avec tous les systèmes de télé présence ou de vidéoconférence conformes aux standards actuels, ainsi qu'avec les plates-formes de communications unifiées telles que Microsoft Office Communicator. Chaque système est conçu pour apporter un rendu homogène, avec une vidéo HD 1080p, des écrans grand format de haute qualité et une interface conviviale et intuitive.

La sensation de contact direct est accentuée par le son full duplex et une caméra Précision HD™ 1080p. Tous les produits Profile Séries sont dotés d'un Codec TANDBERG, qui permet de partager aisément des présentations et des contenus multimédias lors d'une conférence. À l'exception du système d'entrée de gamme Profile 42" équipé du codec C20 plus, tous les systèmes Profile intègrent la fonction multi site permettant à plusieurs sites de se connecter et de collaborer en même temps.

La gamme Profile Séries utilise des composants en aluminium recyclables, conformément aux objectifs de développement durable de TANDBERG. En outre, elle s'inscrit dans l'offre Total Solution de TANDBERG, conçue pour apporter aux entreprises une approche et une administration globale du parc vidéo.

Pour le ministère de l'Education, nous proposons :

- La version Profile 52" single, un système simple écran, basé sur le Codec C60 et

idéal pour les bureaux d'équipes et les salles de réunion.

- La version Profile 52" Dual qui est fournie avec un écran 52''supplémentaire qui peut être dédié au partage de fichiers multimédias.

Quick Set C20

Transformez tout espace de réunion en hub de communications vidéo. Le TANDBERG Quick Set C20 offre, dans un système simple à déployer, à gérer et à utiliser, la qualité exceptionnelle d'une vidéo 1080p. Que vous veniez d'acquérir votre premier poste, ou que vous soyez en train de déployer la visioconférence à grande échelle, le Quick Set C20 vous offre les performances que vous attendriez d'un système plus important — dans un package compact et riche en fonctionnalités.

Le Quick Set C20 est un système complet qui se compose:

- d'un Codec C20

- d'une caméra 1080p30 haute résolution

- d'une télécommande et d'un microphone.

Simple d'utilisation, il se connecte à n'importe quel écran haute définition pour bénéficier immédiatement des fonctions de vidéoconférence.

Concrètement, il suffit de relier la caméra, l'écran, le cordon d'alimentation, le câble réseau et le microphone pour communiquer en vidéo avec ses collègues à distance, clients ou fournisseurs dans le monde entier.

Le Quick Set C20plus, fournie avec une caméra dotée d'un zoom 12x et offrant le choix entre les modes 1080p30 et 720p60.

Chacun des deux modèles, Quick Set C20 et Quick Set C20plus, peut être connecté à deux écrans pour améliorer le partage multimédia. Ils sont par ailleurs compatibles avec le TANDBERG

Management Suite, pour une meilleure gestion du parc vidéo, et avec le MCU HD pour organiser des conférences multipoints (une mise à niveau du logiciel est prévue pour le début du troisième trimestre).

MOVI

Associé au TANDBERG Vidéo Communication Server, Movi permet de convertir n'importe quel PC en un système vidéo de qualité professionnelle, capable de connecter son utilisateur à n'importe quel autre système de Télé présence ou de vidéo conforme aux standards H.323 et SIP.

Depuis un aéroport, une chambre d'hôtel, un café ou de chez soi, Movi 3 renforce considérablement les atouts de la collaboration mobile en permettant le partage du contenu PC. Ainsi, les sessions de vidéoconférence sont enrichies, plus efficaces et la communication unifiée prend tout son sens.

En outre, lorsqu'il est utilisé avec la caméra USB Précision HD de TANDBERG, Movi permet une vidéo haute définition en 720p30, garantissant la meilleure résolution pour un appel dans d'excellentes conditions. Ainsi lors d'un appel dans une salle de Télé présence ou une salle de réunion équipée en vidéoconférence, Movi fonctionne en qualité HD, apportant à tous les participants la qualité visuelle optimum. Cette solution peut être déployée grâce à la fonction « large scale provisioning » qui assure à l'administrateur un déploiement de masse simplifié et automatique sur le parc d'ordinateurs.

CAMERA

La caméra USB Précision HD utilise des composants et des technologies de la plus haute qualité. Elle ne demande ni pilote ni installation de logiciels. Il suffit de la connecter à un port USB pour voir les autres participants grâce au logiciel vidéo installé sur le PC. En outre et grâce à la gestion de nombreuses résolutions standard, la caméra assure les meilleures conditions possibles de communication avec les participants qui ne disposent pas de la vidéo HD.

IV. INTERCONNEXION

a) Network :

Dans cette partie, nous allons aborder, la manière dont un signal visiophonique est transmis à l'intérieur d'un réseau. Passer un signal transportant du son et de la vidéo nécessite une certaine organisation et un matériel adapté. Pour cela, plusieurs critères sont à prendre en compte tel que :

- La bande passante
- Les différents protocoles à utiliser

- Les algorithmes de compression

La bande passante disponible à l'envoi du message sera déterminante quant à la qualité de ce dernier. En effet, avec une bande passante élevée il es possible de faire transmettre plus d'informations relatives à la vidéo pour terminer au final avec une qualité d'image améliorée.

Cependant , la bande passante n'est pas le seul facteur déterminant. Les algorithmes de compression ont leur importance, car ils permettent de réduire le champ d'information d'un signal alors que la qualité d'image et de son n'aura pas ou peu changé. Aujourd'hui, ces algorithmes de compression sont devenus indispensables à la transmission de données qu'utilise la visioconférence, car ils améliorent la fluidité tout en gardant une qualité élevée si désiré.

Malheureusement , tout cela n'est pas suffisant car, même si l'on dispose du matériel nécessaire, une communication entre deux dispositifs ne peut pas avoir lieu s'ils ne <<parlent>> pas la même langue . pour remédier à ce problème, des normes ont été développées par l'ITU qui permettent d'assurer la compréhension du message entre les points. Il en existe plusieurs qui varient en fonction du type de matériel utilisé. Elles ont pour objectif principal de respecter une comptabilité matérielle et logicielle entre des équipements de marques différentes. C'est pour cette raison qu'il est impératif que les constructeurs suivent des normes établies afin que les utilisateurs n'aient pas à se soucier du type d'équipement qu'ils emploient.

a.1) Les types de réseaux

Même si aujourd'hui tout, ou presque ,passe par le réseau internet en utilisant le protocole IP, cela n'a pas toujours été le cas et il a fallu adapter des protocoles à des technologies utilisant d'autres systèmes comme le réseau téléphonique par exemple. Des nouveaux protocoles ont été développés tout au long de l'histoire de la visioconférence pour correspondre aux équipements de leur temps.

Il existe plusieurs types de réseaux différents sur les quelles il est possible de faire de la visioconférence. Ci-dessous, les réseaux , encore utilisés de nos jours, seront décrits afin de démontrer les différentes méthodes utilisées permettant de transmettre des flux vidéo/audio.

1) Réseaux RNIS

Le réseau RNIS est une évolution des réseaux téléphoniques et permet un accès à de multiples canaux servant à faire passer des informations en format numérique. Ce réseau peut être utilisé pour faire de la visioconférence mais aujourd'hui remplacé par des réseaux IP en raison de son faible débit.

2) Réseaux IP

Réseau à commutation de paquets , a la particularité d'être flexible et d'offrir une bande passante très rapide. L'indépendance par rapport au matériel le rend compatible avec bon nombre

d'équipements différents. Utilisé depuis déjà de nombreuses années, son évolution a fait de luis le réseau le plus utilisé aujourd'hui dans les foyers comme dans les entreprises.

3) Réseaux UMTS

Réseau de téléphonie mobile appelé aussi 3G, permettant la transmission de données sans fils. Son débit élevé offre de nouvelles possibilités d'application telle que la visioconférence en plein air. C'est le premier réseau non-câblé étant capable de fournir un tel services et a l'avantage d'être bien répandu à travers le monde. Son successeur, le réseau 4G, est déjà en service dans quelques pays et fera ses apparitions dans d'autre en 2013.

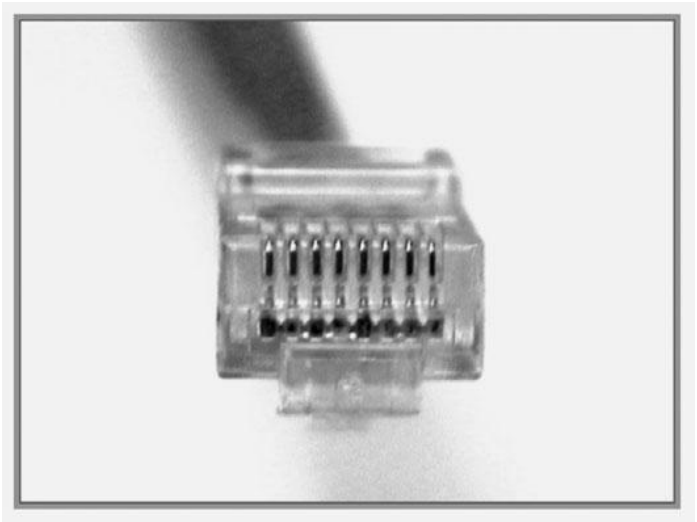
4) Le réseau ATM

L' ATM (Asynchronous Transfer Mode) est un réseau large bande à intégration de services qui est idéal pour la visioconférence. Il fonctionne en effet en haut débit et permet de garantir aussi bien la fluidité que la haute définition des images. Il est cependant en voie de disparition, car peu disponible (sauf pour les universités et centres de recherche). Nous le citons ici pour information sans y revenir dans la suite de l'exposé.

a.2) Les types de connexion réseaux

1) RJ.45

RJ-45 Connector



Si vous regardez le connecteur RJ-45 transparent-end, vous pouvez voir huit fils de couleur, tordu en quatre paires. Quatre d'entre les fils (deux paires) portent la tension positive ou vrai et sont considérés comme "pointe" (T1 à T4), les quatre autres fils portent l'inverse de fausse tension la terre et sont appelés "ring" (R1 à R4). Pointe et la bague sont des termes qui proviennent en les premiers jours du téléphone. Aujourd'hui, ces termes désignent les fils positifs et négatifs

dans une paire. Les fils de la première paire dans un câble ou d'un connecteur sont désignées en tant que T1 et R1, la seconde paire en tant que T2 et R2, et ainsi de suite.

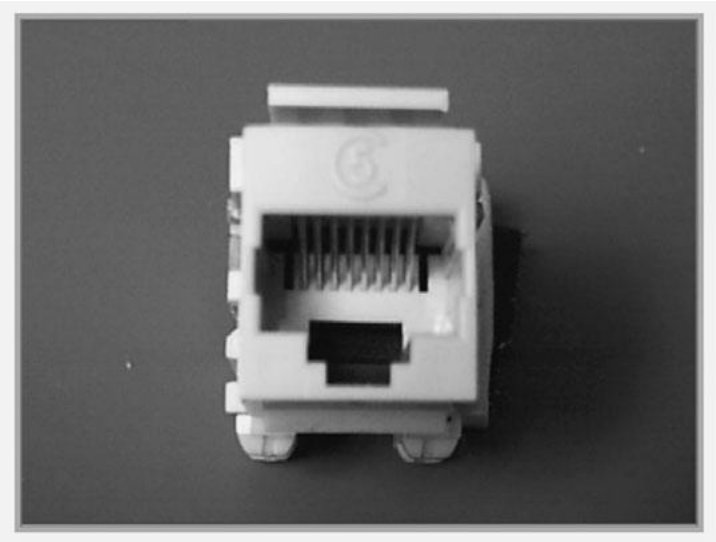
Le connecteur RJ-45 est le composant mâle, serti à l'extrémité du câble. Quand vous regardez la Connecteur mâle de l'avant, les emplacements de broche sont numérotés de 8 à gauche à une sur la droit. Figure dessus montre une prise RJ-45.

Le vérin est le composant femelle dans un dispositif de réseau, de mur, sortie de cloison de douche, ou panneau de brassage. En plus d'identifier l'EIA / TIA bonne catégorie de câble à utiliser pour une connexion appareil (selon la norme est utilisée par la prise du dispositif de réseau), vous nécessaire de déterminer lequel des énoncés suivants à utiliser:

■ Un câble droit (T568A OU T568B à chaque extrémité)

■ un câble croisé (T568A, à une extrémité, à l'autre T568B)

RJ-45 Jack :



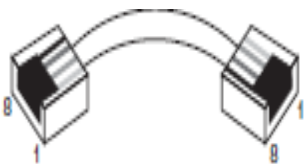
Dans la Figure si dessus, les connecteurs RJ-45 aux deux extrémités du câble Afficher tous les fils dans le même ordre. Si les deux connecteurs RJ-45 extrémités d'un câble sont maintenus côte à côte dans la même orientation, les fils de couleur (ou des bandes ou des épingles) peuvent être vus à chaque extrémité du connecteur. Si l'ordre de fils de couleur est le même à chaque extrémité, le type de câble est droit.

Cable droit:

Cable 10BASE-T / 100BASE-TX Straight Through

Pin Label		Pin Label
1 TX+	◄► 1	TX+
2 TX–	◄► 2	TX–

Straight-Through Cable



3 RX+	◄►	3	RX+
4 NC		4	NC
5 NC		5	NC
6 RX–	◄►	6	RX-
7 NC		7	NC
8 NC		8	NC

Fils sur les extrémités de câbles ont en ordre.

Avec les câbles croisés, les connecteurs RJ-45 aux deux extrémités montrent que certains des fils sur un côté du câble se croisent sur un axe différent de l'autre côté du câble. Plus précisément, pour Ethernet, la broche 1 à une extrémité RJ-45 doit être relié à la broche 3 à l'autre bout. Pin 2 à une extrémité doit être connectée à la broche 6 à l'autre extrémité, comme indiqué dans la Figure suivante.

Cable croisés

Cable 10BASE-T /

100BASE-TX Straight-Though

Croisés Cable

Pin Label		Pin Label
1 TX+	1	TX+
2 TX–	2	TX–
3 RX+	3	RX+
4 NC	4	NC
5 NC	5	NC
6 RX–	6	RX-
7 NC	7	NC
8 NC	8	NC

Fils sur les extrémités de câbles croisés.

Figure suivante montre les lignes directrices pour le choix du type de câble à utiliser lorsque équipements Cisco d'interconnexion. En plus de la vérification de la spécification de catégorie sur le câble, vous devez déterminer quand utiliser un câble droit ou croisé.
Utilisez des câbles de bout en bout pour le câblage suivant:

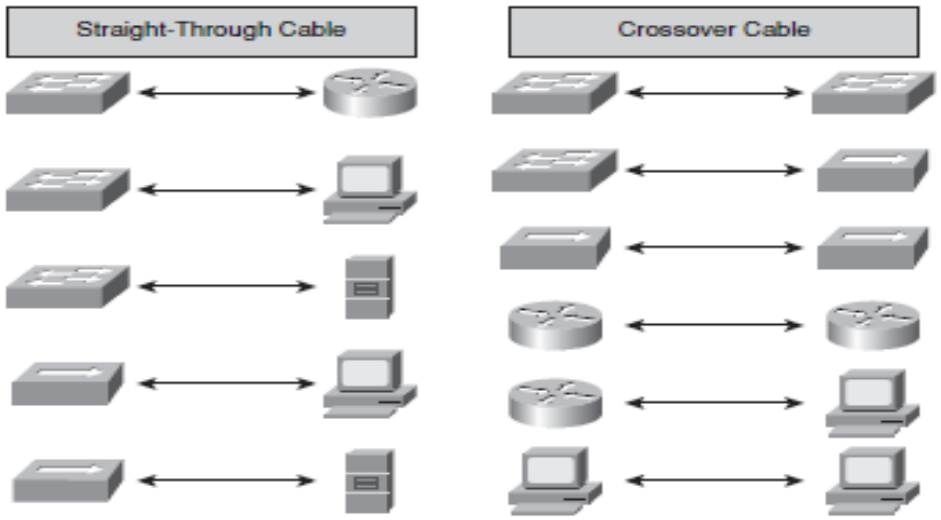
- Switch au routeur
- Switch au PC ou serveur
- Hub pour PC ou serveur

Utilisez des câbles croisés pour le câblage suivant:

- Switch à Switch
- Switch au hub
- Hub au hub
- routeur à routeur

■ Le port Ethernet routeur au PC NIC
■ PC à PC

Quand utiliser un câble droit et un câble croisés :



2) Fibre Optique

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de la lumière et sert dans la transmission de données. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et supporte un réseau « large bande » par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques. Le principe de la fibre optique a été développé au cours des années 1970 dans les laboratoires de l'entreprise américaine Corning Glass Works (actuelle Corning Incorporated).

Entourée d'une gaine protectrice, la fibre optique peut être utilisée pour conduire de la lumière entre deux lieux distants de plusieurs centaines, voire milliers, de kilomètres. Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'information. En permettant les communications à très longue distance et à des débits jusqu'alors impossibles, les fibres optiques ont constitué l'un des éléments clef de la révolution des télécommunications optiques. Ses propriétés sont également exploitées dans le domaine des capteurs (température, pression, etc.), dans l'imagerie et dans l'éclairage.

Un nouveau type de fibres optiques, fibres à cristaux photoniques, a également été mis au point ces dernières années, permettant des gains significatifs de performances dans le domaine du traitement optique de l'information par des techniques non linéaires, dans l'amplification optique ou bien encore dans la génération de supercontinuum utilisables par exemple dans le diagnostic médical. Dans les réseaux informatiques du type Ethernet, pour la relier à d'autres équipements, on peut utiliser un émetteur-récepteur.

3) Les lignes louées

On appelle lignes "louées" des lignes spécialisées (notées parfois **LS**) qui permettent la transmission de données à moyens et hauts débits (64 Kbps à 140 Mbps) en liaison point à point ou multipoints (service Transfix).

En Europe, on distingue cinq types de lignes selon leur débit :

- E0 (64Kbps)
- E1 = 32 lignes E0 (2Mbps)
- E2 = 128 lignes E0 (8Mbps)
- E3 = 16 lignes E1 (34Mbps)
- E4 = 64 lignes E1 (140Mbps)

Aux Etats-Unis la notation est la suivante :

- *T1* (1.544 Mbps)
- *T2* = 4 lignes T1 (6 Mbps)
- *T3* = 28 lignes T1 (45 Mbps)
- *T4* = 168 lignes T1 (275 Mbps).

a.3) Modules de connexion

1) SFP et SFP+

Le small form-factor pluggable (SFP) est un transceiver compact, insérable a chaud utilisé dans les réseaux de télécommunications et les réseaux informatiques. Le format physique et l'interface électrique sont définis par un accord multi-source (MSA). Il interface la carte mère d'un équipement réseau (par ex., un switch, un routeur, un convertisseur de média, etc.) à une fibre optique ou à un câble en paire de cuivre. C'est un format populaire dans l'industrie, développé et supporté par de nombreux vendeurs de composants. Les SFP sont conçus pour supporter SONET, Gigabit Ethernet, Fibre Channel, et d'autres standards de communication. En raison de sa petite taille, le SFP rend obsolète l'ancien et très répandu Gigabit Interface Converter (GBIC), et il est parfois appelé mini-GBIC, bien qu'aucun dispositif de ce nom n'ai jamais été défini dans les MSAs. Les modules optiques permettent une souplesse dans le type de signal souhaité, car ils sont interchangeables à chaud et ils permettent de changer le type de signal optique en changeant uniquement le module optique (petit et pas cher), plutôt que la carte d'interface elle-même (complexe et chère). Son faible encombrement permet d'obtenir une densité de ports importante, ce qui réduit le coût par port et explique en grande partie son succès.

Les transceiver SFP sont disponibles avec de nombreux types d'émetteurs et de récepteurs, ce qui permet aux utilisateurs de sélectionner le transceiver approprié pour chaque lien a fournir en fonction de la distance optique a atteindre et du type de fibre optique disponible (par exemple de la fibre multi-mode ou monomode). Les modules SFP Optiques sont généralement disponibles dans plusieurs catégories différentes:

- Pour les fibres multi-mode, avec un levier d'extraction noir ou beige.
    - **SX** - 850 nm, pour un maximum de 550 m a 1.25 Gbit/s (Gigabit Ethernet) ou 150m a 4.25 Gbit/s (Fibre Channel)
- Pour les fibres mono-mode, avec un levier d'extraction bleu.
    - **LX** - 1310 nm, pour une distance jusqu'a 10 km
    - **EX** - 1310 nm, pour une distance jusqu'a 40 km
    - **ZX** - 1550 nm, pour une distance jusqu'a 80 km
    - **EZX** - 1550 nm, pour une distance jusqu'a 120 km
    - **BX** - 1490 nm/1310 nm, SFP gigabit sur un brin de fibre Bi-Directionelle , sur deux brins fibre avec BS-U et BS-D pour respectivement la montée et la descente, avec une distance jusqu'à 10km.
    - 1550 nm 40 km (XD), 80 km (ZX), 120 km (EX or EZX)
    - CWDM et DWDM, transceivers à plusieurs longueurs d'ondes permettant d'atteindre les distances les plus élevées.
- Pour câblage en paire de cuivre torsadées.
    - **10Base-T** - ce module permet d'atteindre 10 Mb/s sur 2 paires de cuivre.
    - **100Base-TX** - ce module permet d'atteindre 100 Mb/s sur 2 paires de cuivre.
    - **1000Base-T** - ce module permet d'atteindre 1 Gigabit/s sur 4 paires de cuivre.
    - **1000Base-TX** - ce module permet d'atteindre 1 Gigabit/s sur 2 paires de cuivre de catégorie 6. Échec commercial.

Le enhanced small form-factor pluggable (SFP+) est une version améliorée de SFP. Il garde le même format, mais il supporte un débit de données plus élevé, jusqu'à 10 Gigabit/s. La norme SFP+ a été publiée pour la première fois le 9 Mai 2006 et la version 4.1 a été publiée le 6 Juillet 2009. SFP+ supporte le Fibre Channel jusqu'à 8 Gigabits/s, 10 Gigabits/s Ethernet et le standard Optical Transport Network OTU2. Un slot SFP+ peut être conçu de façon à accepter un module SFP standard. Il y a donc possibilité de rétrocompatibilité entre SFP+ et SFP. Cela en fait un format populaire dans l'industrie et il est supporté par beaucoup de vendeurs de composants.

- Types :
    - **SR** - 850 nm, pour un maximum de 300 m a 10 Gbit/s
    - **LR** - 1310 nm, pour une distance jusqu'a 10 km
    - **ER** - 1550 nm, pour une distance jusqu'a 40 km
    - **ZR** - 1550 nm, pour une distance jusqu'a 80 km

2) XFP

L'XFP est un standard de télécommunication pour les modules optiques à la vitesse de transmission de données de 10 gigabits/seconde. Ces modules optiques sont utilisés dans les équipements réseaux tel que les commutateurs (switches) ou les routeurs (routers).

Le standard XFP (10 Gigabit Small Form Factor Pluggable) a été défini en 2002.

Il existe de nombreux types[2] de modules optiques XFP pour :

- Différentes *distances* optiques tel que :

  - SR (Short Reach/Courte Distance) jusqu'à 500 mètres.

  - LR (Long Reach/Longue Distance) jusqu'à 10 Km.

  - ER (Extended Reach/Très Longue Distance) jusqu'à 40 Km et plus (ZR).

  - ZR jusqu'à 80 Km et plus.

  - DWDM (différentes fréquences c'est-à-dire différentes couleurs).

- Différents *types de fibres optiques* tel que les fibres optique :

  - MMF (Multi Mode Fiber) de couleur orange pour les courtes distances (longueur d'onde de 850 nm).

  - SMF (Single Mode Fiber) de couleur jaune pour les grandes distances (longueur d'onde entre autres de 1310 nm ou 1550 nm).

- Différents types de *connecteurs optiques* :

  - LC : Les XFP sont toujours de type LC.

  - SC : Pour les GBIC.

  - RJ45 : Pour les câbles en cuivre (jusqu'à 1GE donc pas utilisé pour les XFP).

L'XFP est indépendant du protocole utilisé par la carte d'interface sur laquelle il est inséré. Les cartes d'interfaces peuvent utiliser différents protocoles comme par exemple : Ethernet, Fiber Channel ou SDH/SONET.

b) Sécurité

Une grande partie de l'équipement de vidéoconférence est connecté à Internet sans pare-feu et est configuré pour répondre automatiquement aux appels vidéo entrants. Cela permet à un intrus distant de contrôler l'information audio et vidéo, souvent avec peu ou pas d'indication sur la cible. La partie intéressante de cette étude est de savoir qui affecte, ces unités peuvent coûter de quelques centaines de dollars (utilisés) à des dizaines de milliers de dollars pour les systèmes de salle haut de gamme. Il est rare de trouver un système de visioconférence haut de gamme dans un endroit sans importance. Exemples identifiés par cette recherche comprennent les conseils d'administration, des aires de consultation détenu-avocat, les sociétés de capital-risque, et les installations de recherche.

Des chercheurs en sécurité ont réussi à s'introduire dans les réseaux de téléconférence de grandes entreprises et à manipuler les caméras vidéo pour espionner les réunions. H.D. Moore et Mike Tuchen ont rendu public leurs recherches réalisées pour le compte de l'entreprise de sécurité Rapid7. Ceux-ci expliquent la facilité avec laquelle des attaquants éventuels pourraient secrètement espionner des salles de réunion équipées de systèmes de conférence configurés pour recevoir des appels de n'importe qui par défaut. De leur côté, les vendeurs doivent trouver un juste équilibre entre sécurité et convivialité.

Le problème vient de la réponse automatique, une caractéristique que l'on trouve dans des produits de Cisco, Polycom et LifeSize. Cette fonction permet de connecter automatiquement des appels audio ou vidéo entrants. H.D Moore, directeur de la sécurité chez Rapid7, a écrit un programme capable de repérer les systèmes de téléconférence où cette fonction, qui présente un risque de sécurité majeur, a été activée par les administrateurs. Cette recherche a couvert environ 3% de l'Internet adressable et mis l'accent sur l'équipement qui a parlé le protocole H.323. Sur les 250.000 systèmes identifiés à ce service, un peu moins de 5.000 ont été configurés pour recevoir automatiquement les appels entrants. On estime à 150.000 systèmes sur l'Internet dans son ensemble affecté par ce problème. Cela ne compte pas les centaines de milliers de systèmes de visioconférence exposés sur les réseaux internes des grandes entreprises.

La problématique de la sécurité se pose à partir du moment ou on passe d'une technologie IP à une technologie ISDN. La visioconférence dans un environnement ISDN est sécurisée par nature : Intercepter une communication sur ISDN est très difficile, l'intrus doit d'abord accéder à un des commutateurs ISDN pendant l'acheminement de l'appel. Puis, il doit identifier les multiples canaux B concernés par la communication, sachant qu'une même communication peut utiliser entre 2 et 6 canaux pouvant emprunter des chemins différents donc des commutateurs différents. Une fois tous les canaux B identifiés, ils devraient être réunis par l'intrus pour reconstituer la communication interceptée.

A l'inverse, la visioconférence dans un environnement IP peut poser des problèmes de sécurité si certains points essentiels ne sont pas pris en compte.

Le matériel servant à faire de la visioconférence doit fonctionner correctement sans compromettre les autres dispositifs sur le réseau IP déjà existant.

Il est nécessaire également d'adapter la politique de sécurité appliquée dans le réseau LAN de l'entreprise afin de prendre en compte les nouveaux types de flux qu'apporte la visioconférence IP. Cela passe généralement par le Firewall.

Les Firewalls sont la base d'un réseau d'entreprise sécurisé, il est donc nécessaire de les prendre en compte lors du déploiement d'une solution de visioconférence IP avec tout ce qu'elle génère comme nouveaux flux et ce qu'elle rajoute comme éléments au réseau.

H.323 utilise des ports statiques et des ports dynamiques. Ces derniers sont des ports UDP ou TCP choisis aléatoirement entre 1024 et 65535 lors de l'appel :

Port TCP : 1503	T.120
Port TCP : 1720	Q.931
Port TCP : 1731	Audio call control
Port TCP : [1024-65535]	H.245
Port UDP : [1024-65535]	RTP/RTCP (audio/vidéo)
Port TCP : 1718, 1719	Gatekeeper RAS

Lors de communications en dehors de l'Intranet et nécessitant le franchissement de Firewalls, ces ports doivent être ouverts à l'ensemble du trafic, car on ne peut pas prédire tous les ports ouverts dynamiquement. Le Firewall devient, par conséquent, inefficace, car il ne filtre rien sur une large plage de ports et un éventuel intrus pourrait exploiter cette faille pour s'introduire dans l'Intranet de l'entreprise.

Pour éviter cette situation, le Firewall doit pouvoir :

• Détecter la valeur des ports dynamiques utilisés au moment de l'établissement de l'appel H323.

• Autoriser le trafic uniquement sur les canaux choisis et seulement pendant la durée de l'appel.

Certains Firewall supportent le contrôle d'accès dynamique en examinant les messages du canal de contrôle H323.

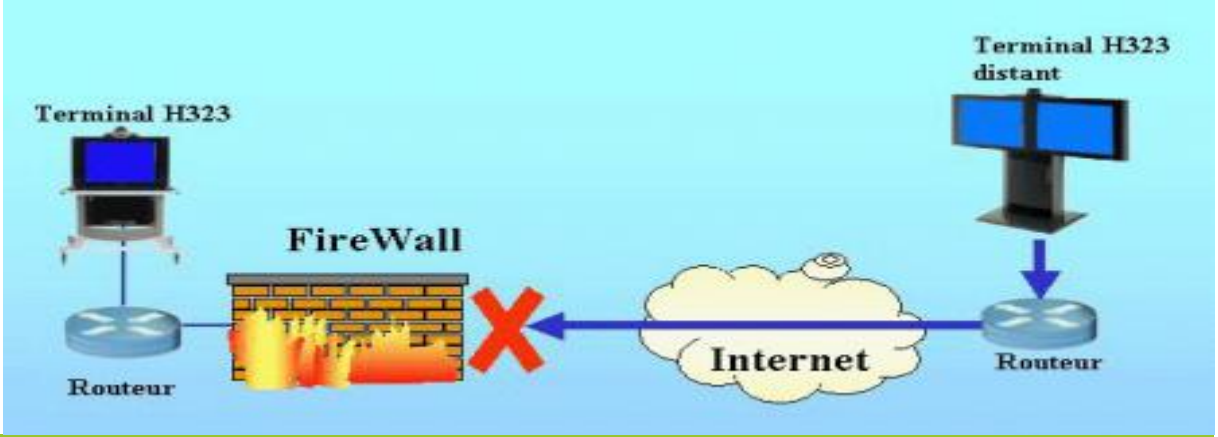
S'il n'y a pas de contrôle d'accès dynamique ou si la sécurité doit être renforcée, la solution consiste à utiliser un proxy dans le Firewall. Seul, le Proxy et le Gatekeeper pourront alors interagir avec l'extérieur. Les terminaux H323 à l'intérieur du réseau deviennent « invisibles ». Si le Firewall ne

peut pas translater les adresses avec NAT (Network Address Translation), il faut également utiliser un Proxy.

Il est à noter que certains terminaux permettent de fixer les valeurs des ports UDP et TCP pour pouvoir traverser les Firewall en limitant les problèmes de sécurité.

1. Firewall

Un Firewall (pare feu dans la littérature française) est un dispositif de sécurité placé à la jonction entre deux réseaux distincts, le réseau informatique interne à un établissement et le réseau extérieur, Internet en l'occurrence. Organe de sécurité destiné à protéger le réseau interne, sa tache principale est d'interdire les activités malveillantes en provenance de l'extérieur. La contrainte du firewall est d'être le plus transparent possible pour les activité à l'intérieur de l'entreprise et d'être à la fois le plus efficace possible en offrant un niveau maximum de sécurité. C'est essentiellement un outil de filtrage destiné au contrôle de la circulation des paquets, et qui doit assurer le blocage de toutes les données qui ne doivent pas passer d'un côté à l'autre. Il va généralement interdire toutes les « entrées » de données qui ne répondraient pas à une requête préalable de l'un des postes du réseau local. Comment dès lors, répondre à une demande d'initialisation pour une session de visioconférence lorsqu'elle est sollicitée depuis l'extérieur ?



Les firewalls bloquent la plupart des paquets non sollicités, ici une tentative de connexion pour une visioconférence. Pour que la communication s'établisse, de nombreux ports doivent être ouverts sur le FireWall, à commencer par le port 1720 qui est utilisé lors de l'initialisation de la liaison.

Figure 1.5: Architecture générale.

Un firewall va également assurer la surveillance des « ports » qui sont utilisés. Sur un micro-ordinateur, chaque application logicielle se voit attribuer un port (le port est en quelque sorte « l'adresse » d'une application). Lors d'une connexion « classique » à Internet la majorité des ports sont fermés sur le firewall, seuls les quelques uns qui correspondent aux applications directement concernés sont ouverts. Dans le cadre de la visioconférence, de nombreuses connexions doivent être simultanément maintenues entre les terminaux, et de nombreux ports doivent y êtres ouverts, certains aléatoirement (c'est à dire sans que l'on puisse prévoir préalablement leur numéro). Cette notion de ports dynamiques ne facilite pas la configuration des firewall : pas question de laisser tous les ports entre 1024 et 65535 ouverts ! Sauf mise en place de dispositifs particuliers, l'ouverture de tous ces ports sont autant de failles dans la sécurité globale d'un réseau local. A l'inverse, du fait des

dispositifs de protection adoptés par les administrateurs de réseau, la mise en place de séances de visioconférence peut se révéler difficile, parfois même impossible.

Sur un micro-ordinateur, chaque application logicielle se voit attribuer un port (le port est en quelque sorte« l'adresse » de l'application). Pour des données en provenance de l'extérieur, le numéro de port indique à quelle application sont destinées les données. Les ports sont codés sur 16 bits, 65535 ports sont théoriquement disponibles, pratiquement moins, car 1024 sont réservés. Lors d'une connexion « classique » sur Internet la majorité des ports sont fermés, seuls les quelques uns qui correspondent aux applications directement concernés sont ouverts pour permettre les échanges de données (port 80 pour HTTP, ports 25 et 110, respectivement pour les échanges SMTP et POP3 de la messagerie...). Bloquer l'utilisation d'un port, c'est interdire le transit des données correspondant à certaines applications. Dans le cadre de la visioconférence, certains de ces ports sont spécifiés d'une manière définitive (ports statiques) par la norme H263, par exemple, port 1720 pour l'appel initial, port 1719 en cas d'utilisation d'un gatekeeper, port 1503 pour le partage d'applications via la norme T120... D'autres (ports dynamiques) sont attribués aléatoirement au moment de l'établissement de l'appel (ports compris entre 1024 et 65535). Ce sont par exemple ceux utilisés pour le transfert des données vidéo et audio (flux RTP et RTCP). Suivant le type de données, les transferts pourront s'effectuer en utilisant les protocoles TCP ou UDP.

Pour protéger les Données et applications contre tout accès non-autorisé et intrusion, on propose un cluster de Firewall StoneGate en haute disponibilité (Actif/Actif) qui représente un deuxième mur de protection pour la plateforme Intranet, et une sonde anti intrusion IPS- StoneGate soit complémentaire à l'existant (Firewall et IPS de Stonesoft) pour bien bloquer les menaces traversant le réseau.

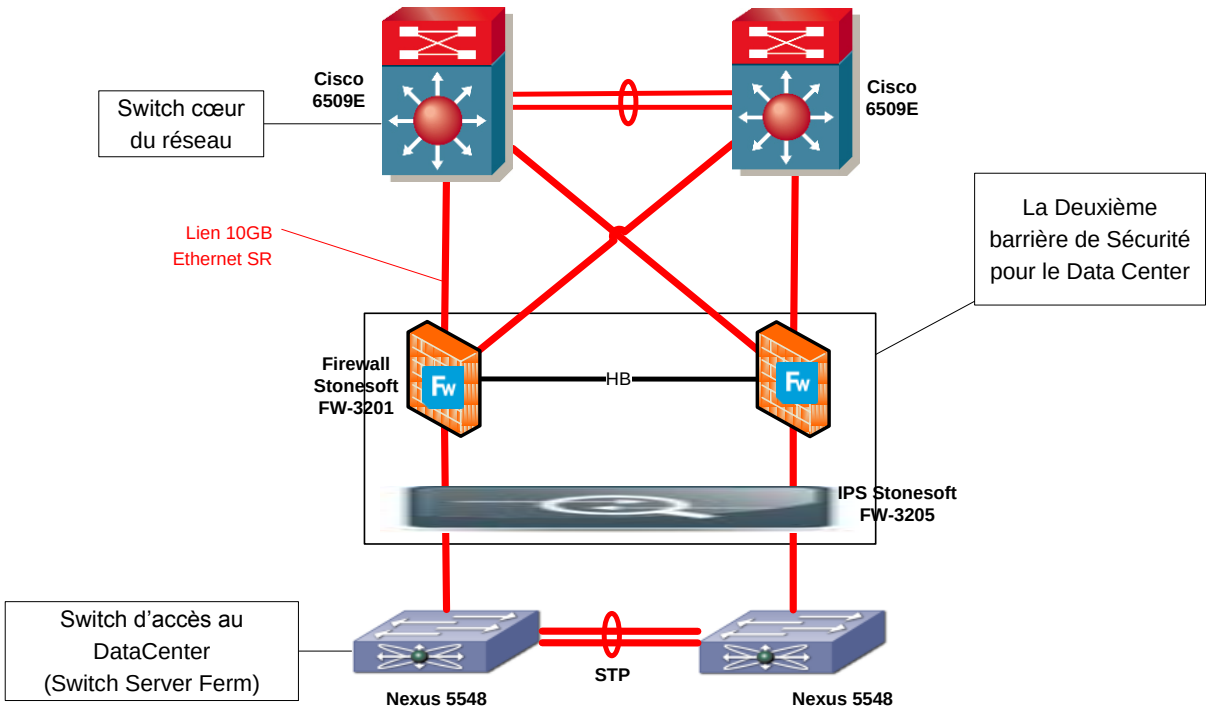
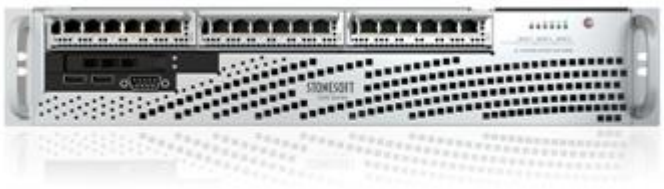


Figure 1.6: Architecture utilise



Le Firewall FW-3201 est proposé en cluster afin de répondre aux besoins de disponibilité nécessaire pour le Data Center, offre des performances Firewalling de 10 Gbps. Le FW-3201 est un équipement modulaire qui possède 3 Slots pour carte d'interface.

Pour la protection en profondeur contre les menaces, une (01) sonde anti-intrusion StoneGate **IPS-3205** est prévue pour sécuriser les flux d'informations entrent et sortent a la zone d'applications.

La sonde anti-intrusion IPS StoneGate est un équipement transparent sur le réseau. Il est par conséquent facile à déployer n'importe où sur le réseau pour sécuriser les zones jugées les plus importantes sur le réseau.

Ce type de configuration permet d'inspecter et d'arrêter toutes les attaques entrantes et sortantes sur les segments les plus sensibles du réseau du ministère. En plus la sonde peut inspecter et monitorer les communications entre les serveurs dans le même segment, une autre interface peut être configurée pour envoyer un **RESET** pour terminer les connections jugées malhonnête.

2. IDS/IPS

Avec l'émergence de nouvelles menaces sans fin et des ressources de l'entreprise sous pression constante, il peut être difficile de concilier toutes les tâches stratégiques et opérationnelles nécessaires à un programme efficace de sécurité de l'information. Détection des intrusions sur le réseau et la prévention (IDS / IPS) appareils peuvent fournir une couche très efficace de sécurité conçu pour protéger les actifs critiques contre les menaces cybernétiques. Les entreprises peuvent détecter les tentatives par des attaquants afin de compromettre les systèmes, applications et données en déployant IDS réseau, mais en gardant les appareils réglés et mis à jour afin qu'ils soient efficaces est un défi pour de nombreuses organisations.

Gestion des IDS et IPS appareils nécessite un ensemble de compétences spécialisées, parce que les appareils ne sont efficaces que s'ils sont bien réglés sur les menaces actuelles et le réseau dans lequel ils sont déployés. Dispositifs IDS peut générer des milliers d'alertes chaque jour et sont très sujettes à des faux positifs, ce qui rend difficile l'identification des véritables menaces et de prendre rapidement des mesures pour protéger les actifs. Pour cela nous allons avoir besoin de connaître tous les détails essentiels de configuration et le dépannage du système de prévention des intrusions de Cisco (IPS), à la fois à partir de la ligne de commande et via Security Device Manager (SDM). Nous devons d'abord établir une distinction claire entre le fonctionnement du système de prévention des intrusions et le système de détection d'intrusion (IDS). Ces termes semblent similaires, mais ils sont très différents en fonction.

Un IDS fait exactement ce que son nom l'indique - il détecte les intrusions réseau. Assez simple! Cependant, l'IDS est essentiellement un «crieur public» en ce qu'elle avisera les autres

périphériques réseau de l'attaque, mais ne défend pas directement contre l'attaque elle-même. L'IDS ne reçoit pas directement les flux de trafic. Au lieu de cela, les flux de trafic sont reflétés à l'IDS. Lorsque le trafic infecté n'a frappé le réseau, les IDS ne verront cela et prendre les mesures appropriées. Le problème est que cette action appropriée n'est pas une action directe; depuis l'IDS n'est pas dans le flux de la circulation, il doit en informer un périphérique réseau qui se trouve dans ce flux que des mesures doivent être prises. Au moment où l'IDS détecte un problème et informe les périphériques réseau appropriés, le début de l'écoulement du trafic infecté est déjà dans le réseau.

En revanche, notre système de prévention des intrusions (IPS) ne s'asseoir au milieu de la circulation - dans ce cas, les IPS seront effectivement notre routeur Cisco. Lorsque l'IPS détecte un problème, l'IPS lui-même peut empêcher le trafic d'entrer dans le réseau. Le site Web de Cisco décrit les IPS comme une «restructuration» de l'IDS. Alors que vous verrez plus d'IPS de IDS dans le monde réel articles de fitness networksHealth d'aujourd'hui, nous devons être très clair sur les différences entre les deux pour l'examen ISCW. Assurez-vous que vous êtes à l'aise avec la configuration IPS à partir de la ligne de commande et en utilisant SDM ainsi.

Les différents système de détection d'intrusion :

Les systèmes de détection et de prévention d'intrusions		
Editeur/ solution	**Type**	**Description**
Arkoon ***Arkoon IDS en coupure***	**Appliance IPS**	Cet IPS combine à la fois les fonctions de décodage applicatif temps réel et de détection d'intrusion à base de signatures contextuelles. - Décodage applicatif temps réel : décodage des protocoles applicatifs utilisés, vérification de la conformité de la communication par rapport à la norme du protocole applicatif (RFC), respect des règles d'utilisation de ces protocoles définies par l'administrateur sécurité. - Détection à base de signatures : plus de 500 signatures répertoriées.
Cisco ***NetRanger***	**Appliance IDS**	Cisco propose deux produits distincts : un IDS réseau et un IDS host. - Les capteurs réseau comprennent un appareil de sécurité réseau et un module de sécurité qui permet d'exécuter des fonctions de surveillance et de commutation à partir d'un même châssis. La détection des intrusions se fait en temps réel, notamment en environnement Gigabit et sur des liaisons 802.1q. - La solution Cisco IDS Host Sensor, développée par Entercept, permet de protéger les serveurs d'entreprise. Elle permet notamment le déploiement d'un grand nombre d'agents afin d'assurer une couverture de sécurité des environnements réseau étendus contre certains vers (type Code Red ou Nimda).
Computer Associates ***eTrust Intrusion Detection***	**Logiciel IPS**	Solution intégrant à la fois protection réseau, gestion des sessions réseau et arrêt des contenus Internet. Une console de gestion centrale, un moteur anti-virus, l'automatisation des mises à jour sont fournies.
Enterasys Networks ***Dragon 6.0***	**Appliance IDS**	Protège à la fois les serveurs (Dragon Host Sensor) et les réseaux (Dragon Network Sensor). Permet également la surveillance de pare-feu, de routeurs et d'IDS d'autres marques. Une gestion par interface Web est proposée ainsi qu'une mise à jour quotidienne des signatures.
ISS ***RealSecure et Proventia***	**Logiciel et appliance IDS - IPS**	Destiné aux réseaux et aux systèmes, la gamme RealSecure propose RealSecure Network Sensor, qui s'installe sur une station dédiée pour contrôler le trafic réseau à la recherche de signatures d'attaques et RealSecure Server Sensor, qui protège les serveurs stratégiques par l'analyse des événements au niveau du noyau du système d'exploitation, des journaux de connexions et de l'activité réseau de ces serveurs. Une console de management - RealSecure Workgroup Manager - offre un reporting de type graphique et une base de données d'assistance en ligne en réponse aux incidents. L'éditeur a récemment lancé une gamme d'appliances IDS (Proventia A Series) et IPS (Proventia G Series : en mode coupure). La gamme Proventia M Series regroupe les technologies d'antivirus, pare-feu, réseaux privés virtuels et protection contre les intrusions au sein d'un seul moteur.

Netasq ***IPS-Firewall***	**Appliance IPS**	Société du nord de la France, Netasq propose une gamme de boîtiers IPS/ pare feu pour PME et grands comptes. Le moteur de sécurité ASQ (Active Security Qualification) de Netasq associe à l'identification contextuelle des paquets suspects (stateful inspection) l'analyse des techniques d'attaque jusqu'aux couches applicatives, ainsi qu'une observation de l'historique multi-session, le traitement des dénis de service et buffer overflow, le repérage des comportements anormaux, signes d'intrusions ou d'attaques même inconnues.
NetScreen ***NetScreen Intrusion Detection and Prevention (IDP)***	**Appliance IPS**	Le spécialiste des pare-feu propose une méthode de détection et de prévention en plusieurs points : signatures d'attaques connues, détection d'anomalies de protocoles et de trafic, mais aussi de portes arrières (backdoor) et de pots de miel (honeypots) de réseau.
Network Associates ***Mcafee Entercept et IntruShield Network IDS Sensor***	**Appliances et logiciel IDS/IPS**	Les rachats respectifs d'Intruvert et d'Entercept Security Technologies (en avril 2003) permettent à Network Associates de proposer deux produits distincts. IntruShield pour la prévention d'intrusions réseau (en appliance) et Entercept pour la prévention d'intrusions système. - IntruShield Network IDS Sensor est une gamme de boîtiers permettant d'identifier une large gamme d'attaques. L'éditeur met en avant les IDS virtuels qui permettent de segmenter un capteur en capteurs virtuels dont les règles de sécurité sont adaptées au composant protégé. - Entercept fonctionne selon des règles de comportement et de signatures d'attaques. Prévention des attaques en dépassement de tampon (buffer overflow), prévention des élévations de privilèges et protection des ressources système critiques. Disponible en version desktop et serveurs de données
NFR Security ***Sentivist 4.0***	**Logiciel IPS**	NFR Security s'appuie sur un algorithme de corrélation des alertes dénommé `Meta Alert'. L'éditeur applique un processus de discrimination au niveau de chaque élément de la solution : la sonde, le serveur et l'interface d'administration. Ce processus est constitué par des algorithmes relatifs à la suppression des mêmes alertes répétées en permanence ou encore l'empreinte des systèmes d'exploitations et applications, établie selon le profil de vulnérabilité du réseau de l'entreprise. Cette version intègre le support d'IPv6 et est compatible avec les environnemens Ethernet 1 Giga-bit saturés.
Snort ***Snort***	**Logiciel IDS**	Solution issue du monde du logiciel libre, Snort offre un moteur de détection, une analyse des flux HTTP, une surveillance des protocoles et des anomalies de trafic, pour le réseau. (lire notre interview)
Symantec ***Symantec Host IDS et Symantec ManHunt***	**Logiciel IDS**	Le leader mondial de la sécurité se positionne à la fois au niveau des serveurs (Symantec Host IDS) et du réseau (Symantec ManHunt). Ces solutions s'intègrent à Symantec Security Management System pour optimiser la hiérarchisation et l'identification des attaques. - Symantec Host IDS : fournit un accès aux données granulaires des processus, permet aux administrateurs de définir une grande diversité de configurations de sécurité et de limiter les capacités des serveurs grâce à des politiques définies - Symantec ManHunt protège les réseaux à des vitesses pouvent aller jusqu'à 2 giga-bits par seconde. Prend en charge le système d'exploitation Red Hat Linux.
TippingPoint Technologies ***UnityOne Intrusion Prevention***	**Appliance IPS**	TippingPoint combine la détection d'intrusion à la protection par pare-feu et à l'évaluation des vulnérabilités d'un système au sein d'appliances uniques qui utilisent des composants ASIC et reposent sur un processeur appelé Threat Suppression Engine (TSE) supportant des vitesses multigigabit. La protection peut se faire sur serveur ou sur réseau.
TopLayer ***Attack Mitigator IPS***	**Appliance IPS**	Boîtier stoppant les attaques de type HTTP, déni de service, SYN Flood, spoofing IP, de protocole et qui détecte les anomalies de trafic. Peut, en raison d'une architecture basée ASIC, fonctionner en environnements de 100 megabits à plusieurs gigabits. Mécanismes de détection de SYN flood et de blockage brevetés.
Watchguard ***Gamme Firebox***	**Appliance IPS**	Spécialisé dans les pare-feu sous forme de boîtiers, Watchguard intègre la prévention d'intrusion au sein de ces matériels. L'éditeur utilise une base de signatures d'attaques, les anomalies de protocoles et de comportements.
Editeur/ solution	**Type**	**Description**

Architecture :

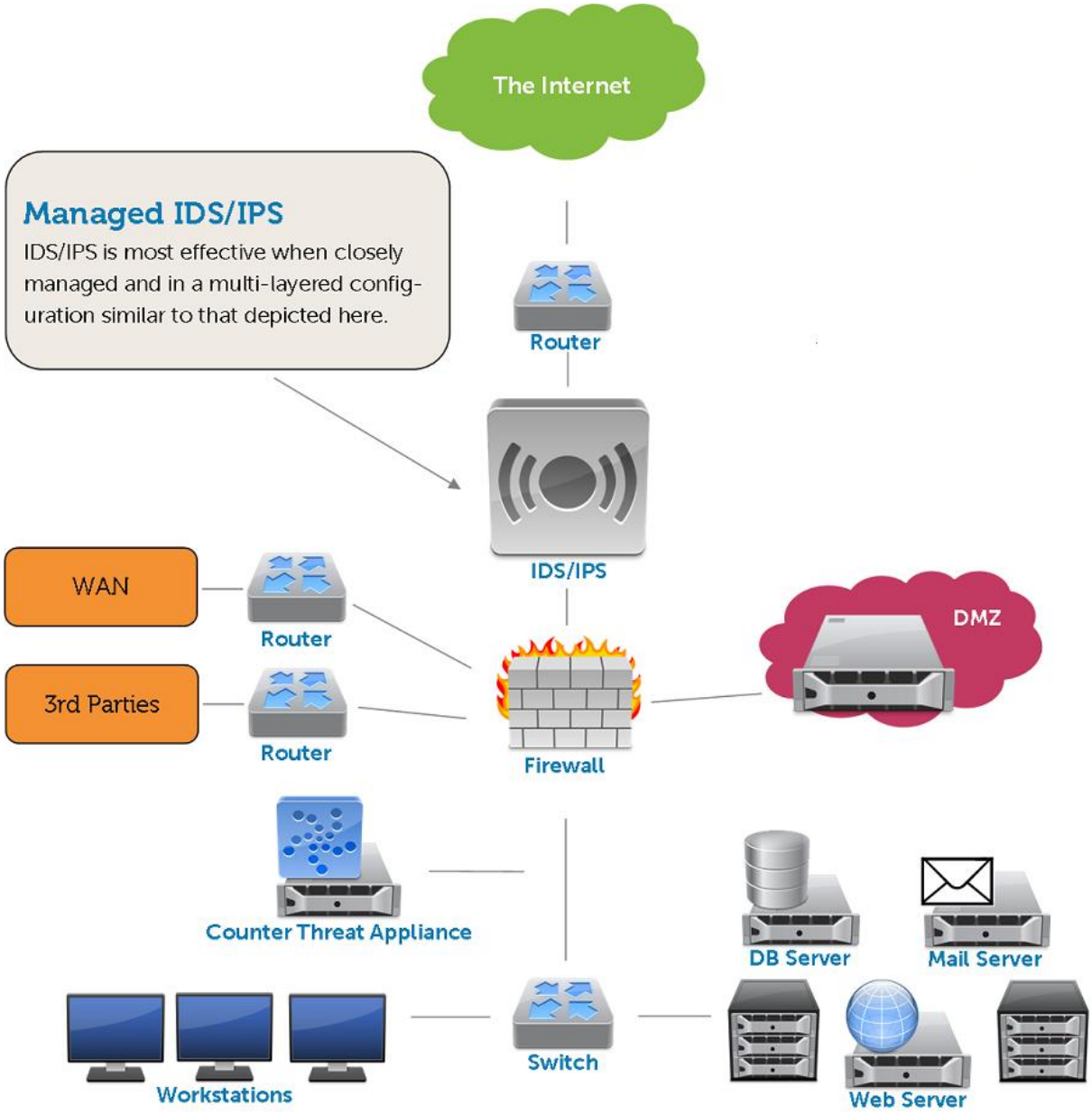


Figure 1.7: Architecture globale de sécurité

3. Deep Packet Ispection

En informatique, le Deep Packet Inspection (DPI), en français Inspection des Paquets en Profondeur, est l'activité pour un équipement d'infrastructure de réseau d'analyser le contenu (au-delà de l'en-tête) d'un paquet réseau (paquet IP le plus souvent) de façon à en tirer des statistiques, à filtrer ceux-ci ou à détecter des intrusions, du spam ou tout autre contenu prédéfini. Le DPI peut servir notamment à la censure sur Internet ou dans le cadre de dispositifs de protection de la propriété intellectuelle.

Le DPI mêle les fonctions d'un IDS et d'un IPS à celles d'un pare-feu à état : cette combinaison permet de détecter certaines attaques que les IDS/ISP et le pare-feu ne peuvent révéler à eux seuls.

Si le pare-feu à état peut voir le début et la fin d'un flux de paquets réseau, il ne peut pas remarquer des évènements inadéquats pour une application en particulier. Les IDSs peuvent détecter les intrusions, mais sont peu utiles pour les bloquer ; enfin les DPIs sont employés pour prévenir les attaques par virus ou vers, et s'avèrent plus spécifiquement utiles contre des attaques par dépassement de tampon, par Déni de service (DoS), ou par l'emploi de vers qui tiennent dans un seul paquet. Le DPI permet de lire les couches 2 et 3 du Modèle OSI, voire dans certains cas jusqu'à la couche 7, ce qui inclut à la fois les *headers* (en-têtes), les structures des protocoles et la charge, le contenu du message lui-même. Il peut par ailleurs identifier et classer le trafic à partir d'une base de données de signatures, c'est-à-dire à partir des données contenues dans le paquet lui-même (ce qui permet un contrôle plus efficace que s'il était uniquement basé sur les informations des en-têtes) ; un chiffrage des points de sortie est donc généralement nécessaire pour échapper à une inspection de type DPI. Un paquet classifié peut être redirigé, marqué, bloqué, voir son débit limité, et bien sûr être rapporté à un agent du réseau : dans ce genre de cas, plusieurs types d'erreurs HTTP peuvent être identifiées et transférées pour une analyse ultérieure. Beaucoup de dispositifs DPI peuvent analyser des flux de paquets (plutôt que procéder à une analyse paquet par paquet), ce qui permet un contrôle sur des flux cumulés d'informations.

V. CONCLUSION

Dans ce chapitre nous avons vu tous les équipements proposés par Algérie télécoms en routeur, Switch, gatekeeper, Gateway, et tous équipements proposés par «Tandberg » ainsi que par « HP ». Nous avons aussi vu les différents services proposés, et les différents moyen de sécuriser la connexion en firewall et deep packet et ainsi que le IDS/IPS. Nous avons enfin, vu les différents modules de connexion entre les réseaux.

Chapitre 2 : Fonctionnement de la visioconférence

I. INTRODUCTION

Contrairement à la visiophonie, la visioconférence permet de faire dialoguer plus que deux personnes simultanément et donc de simuler une conférence à plusieurs lorsque tous les membres ou une partie d'entre eux sont éloignés géographiquement.

Pour arriver à cela , il existe plusieurs façons de s'organiser. Ce que nous détaillerons dans ce chapitre. Nous allons voire tous les utilitaires, mode de diffusion et aussi les différents protocoles permettant la relation, ainsi que les cryptages de sécurité utilisés.

II. Mode de diffusion.

La mise en place d'une réunion par visioconférence peut différer selon les outils que l'on dispose. Cette mise en place est appelée <<mode de diffusion>>. Elle représente l'organisation d'une visioconférence. Elle peut être constituée de plusieurs personnes disposant chacune de son propre système pour interagir dans la conférence, ou alors, d'un seul système dédie à plusieurs personnes en même temps.

a) Le mode point à point

Une simple visiophonie est en mode point à point. C'est-à-dire que seul deux interlocuteurs sont en relation avec chacun leur dispositif nécessaire. A ce niveau, il est encore trop tôt de parler de visioconférence.

b) Le mode broadcast ou mode diffusé

Dans ce mode de diffusion, plusieurs point écoutent un seul point. Ce système est utilisé lorsqu'un message important doit être diffusé à plusieurs endroits et que les autres points n'ent aucune raison d'interagir entre eux.

c) Le mode multipoints

Le dernier mode de diffusion appelé <<multipoints>> va faire interagir tous les points entre eux. Dans ce mode , le partage de la conférence est complet et égal pour tous. Chaque interlocuteur pourra ainsi s'exprimer et se faire entendre par tous les autres. Ce mode est celui qui correspond le mieux à une situation réelle.

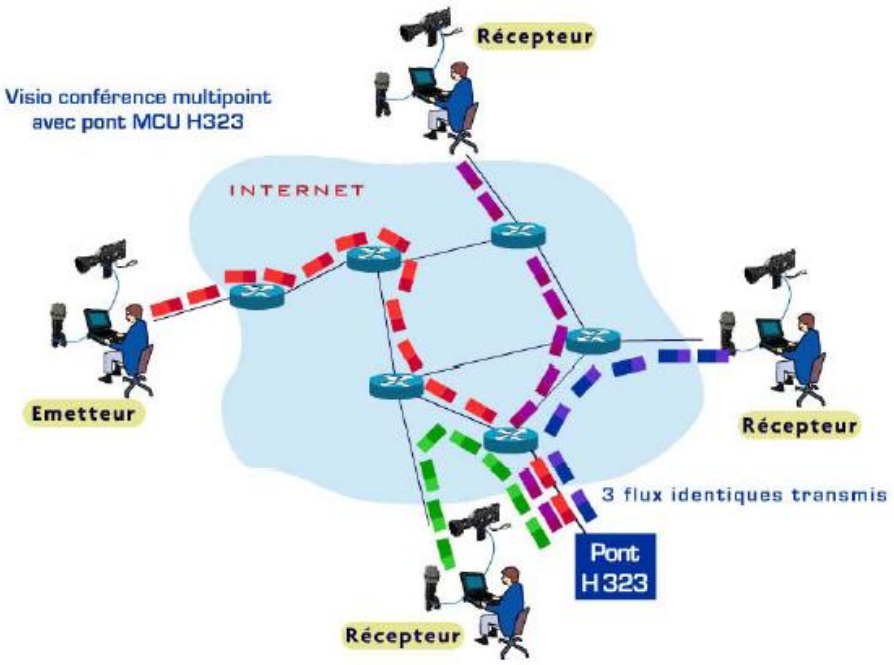


Figure 2.1 : Architecture du mode multipoints.

La visioconférence multipoint permet la communication de plus de 2 sites distants simultanés en vidéo, audio et éventuellement données informatiques. Pour cela, vous devez utiliser au moins un système de visioconférence multipoint ou un pont multipoint de visioconférence.

NB : chaque émetteur et aussi un récepteur et vis versa.

Pendant vos visioconférences multipoint, vous pouvez :

- Visualiser un seul site à la fois (celui qui prend la parole)
- Visualiser plusieurs sites en simultané
- Faire intervenir des participants
- Travailler en temps réel sur vos documents informatiques.

Une communication unicast signifie qu'il y a un et un seul destinataire, et qu'il n'y a qu'un et un seul émetteur. L'un comme l'autre sont identifiés par leur adresse IP respective. De cette manière, quand le paquet de données arrive à un routeur, il sait globalement quoi en faire : soit il sait où l'envoyer pour atteindre la cible, soit il l'envoie à son routeur par défaut qui devrait savoir quoi faire.

Le mode Unicast, peut être utilisé avec les classes A,B,C d'adresses, et il n'envoie un message qu'à un seul pc (une seule adresse ip).

Une communication multicast ne diffère que très peu. En effet, il y a aussi une adresse d'émission, et une de destination. Seulement, l'adresse de destination n'identifie pas un ordinateur, elle identifie un groupe. Pour pouvoir faire la distinction, cette adresse est choisie dans la classe D, en

IPv4 et dans une plage d'adresse spécifique en IPv6. Et le routeur effectue la même opération : soit il sait vers où envoyer le paquet de données (il est possible que ce soit sur une ou plusieurs interfaces), soit il remet le paquet à son routeur par défaut, si il existe.

Le multicast correspond à la classe D c'est à dire utilisant les adresses 224.0.0.1 à 239.255.255.255, il permet d'envoyer le même message à tout un groupe d'utilisateur (sur le même réseau).

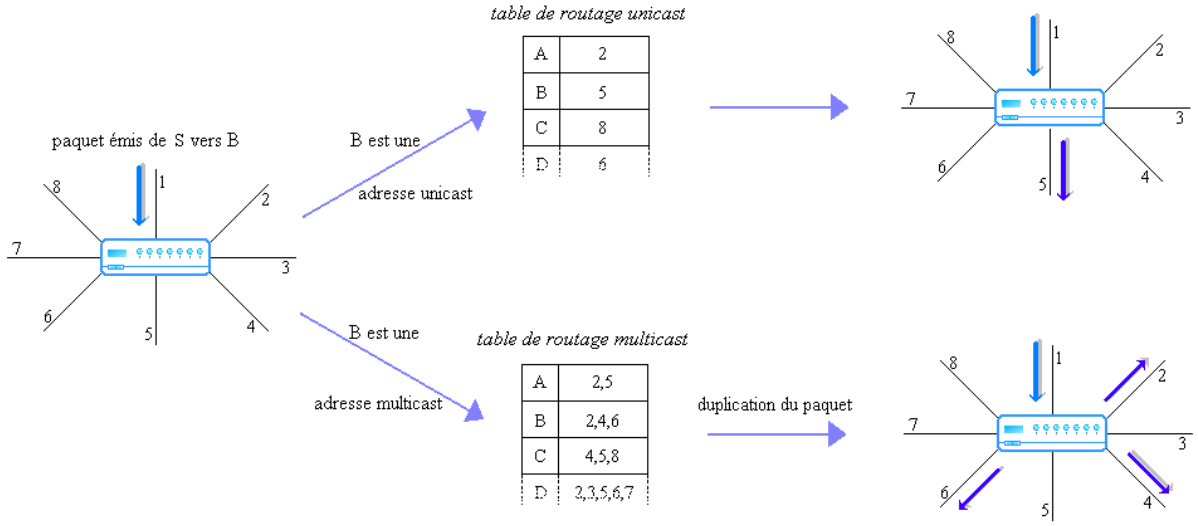


Figure 2.2 : Schéma du fonctionnement d'un routeur en unicast et multicast.

A priori, il n'y a pas d'autres différences que le fait de devoir dupliquer le paquet sur certains routeurs au lieu de le passer directement au routeur suivant. Mais si l'on veut envoyer trois fois la même information vers trois destinataires différents, en unicast, il faudra envoyer trois fois le même paquet de donnée. Et si on l'étend au cas général, c'est à dire, vouloir envoyer la même donnée à n destinataires, on s'aperçoit très vite que l'on va saturer la bande passante entre l'émetteur et le premier routeur, et sans doute entre ce premier routeur et d'autres.

D'où l'idée du multicast. Il est en effet nécessaire d'envoyer la donnée seulement une fois pour qu'elle arrive à tous les destinataires. Comme les routeurs dupliqueront l'information au bon moment, on se retrouve avec la manière la plus optimale de distribuer une information à un groupe. De plus, il n'est pas nécessaire que la source des données soit unique. En effet, une autre source pourrait tout aussi bien émettre vers ce même groupe. L'information serait, elle aussi, dupliquée par les routeurs, aux mêmes endroits que pour la donnée précédente.

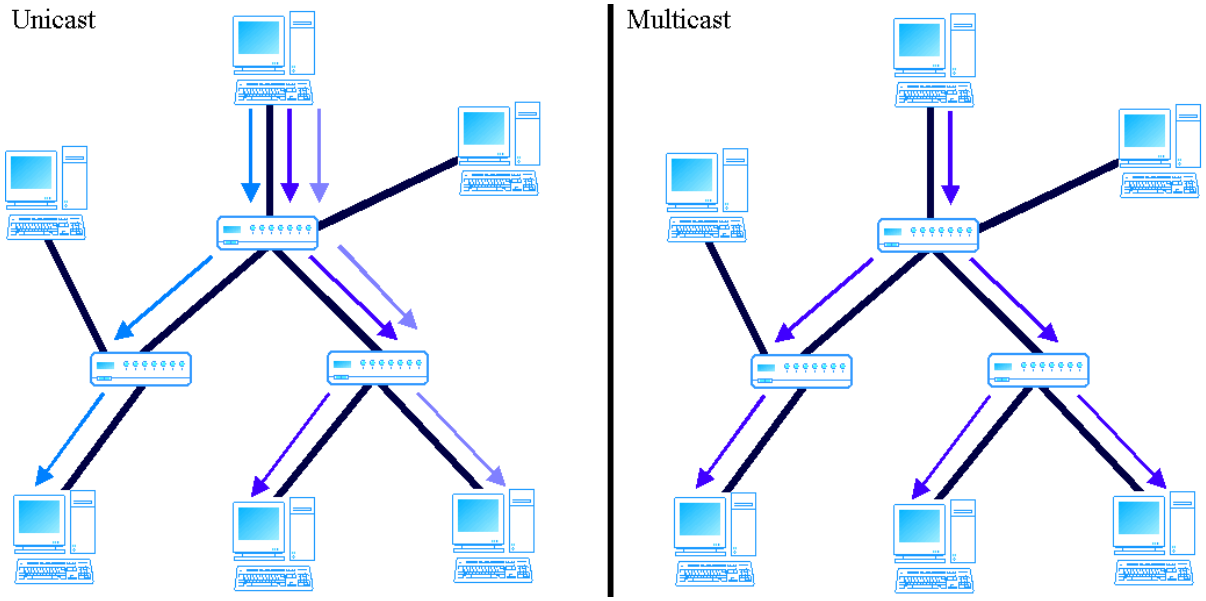


Figure 2.3 : Envoi d'une même donnée à trois récepteurs en unicast/multicast

On a parlé plus haut de broadcast. En fait, ce n'est pas vraiment une technique de communication dans l'Internet, mais plutôt dans les réseaux locaux. En théorie, le broadcast est l'envoi d'une information vers tous les ordinateurs. Toujours en théorie, un routeur, à la réception d'un paquet adressé à une adresse de broadcast (dernière adresse du sous-réseau), est censé dupliquer le paquet, et l'envoyer sur toutes ses interfaces, hormis l'interface sur laquelle il a reçu le paquet. On pourrait donc se dire que cela aurait pu s'instaurer à la place du multicast, puisqu'il n'y a aussi qu'un seul paquet qui est envoyé à plusieurs destinataires. Mais la différence fondamentale, c'est qu'on l'envoie à tout le monde, et non pas aux seuls intéressés. Et tous les ordinateurs qui reçoivent un paquet vérifient en premier lieu que le paquet leur est destiné. Or dans le cas d'une adresse de broadcast, l'ordinateur accepte le paquet, et cela l'oblige à le traiter par la suite.

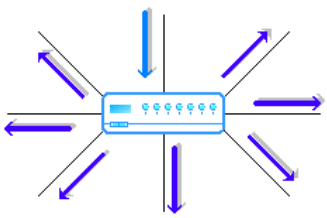


Figure 2.4 : Schéma d'une diffusion broadcast

Et là, on commence un peu à comprendre pourquoi ce mode de communication n'existe pas dans l'Internet. Car en fait, cela signifie en théorie que si j'envoie un paquet avec une adresse de broadcast, tous les ordinateurs de l'Internet vont recevoir ce paquet et vont devoir le traiter. Ce qui est bien sûr impensable. C'est pour cette raison que les messages avec une adresse de ce type ont une durée de vie très courte, et ne sortent pas de leur sous-réseau. La grande majorité du temps, le routeur ne donne pas suite au paquet. Il sera donc reçu par tous les ordinateurs du lien, et ne sera pas diffusé plus loin. Ce qui règle d'ailleurs un autre gros problème, mis à part le traitement du paquet par tous les ordinateurs : les boucles de routage.

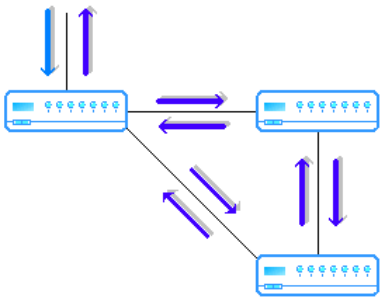


Figure 2.5 : Schéma d'une boucle de routage

III. Protocoles

Il existe à l'heur actuelle plusieurs protocoles différents servant à faire communiquer des machines, ou des logiciels ensemble. Ces protocoles, parfois normalisés, regroupent plusieurs normes qui seront décrites par la suite.

Il est important de bien comprendre que le message transmis est un regroupement de plusieurs normes avec pour chacune des fonctions bien distinctes. On y retrouve notamment des normes dédiées à la vidéo, à l'audio ainsi qu'au contrôle et à la signalisation.

Cependant un protocole n'utilise pas seulement forcément qu'une seule de ces normes par catégorie mais plusieurs. Ex : si dans une communication entre deux machines l'une d'elles ne reconnait pas une norme vidéo, le protocole va alors en choisir une autre, reconnue par les deux, afin d'assurer la communication.

H .323 et SIP

Pour comprendre le fonctionnement, le détail de deux de ces protocoles, H323 et SIP, sera décrit dans ce chapitre. Ils ont été choisis en fonction de leur importance sur le marché et comportent chacun leurs spécificités. Ces deux protocoles, bien que différents, ont le même objectif : faire passer des informations audio/vidéo sur un réseau en maximisant la qualité tout en utilisant le moins de bande passante possible. Pour assurer une interopérabilité entre des équipements ou logiciels, ils ont recours à des techniques différentes et présentent chacun des avantages et inconvénients.

A) Le protocole H.323

H.323 est un regroupement de plusieurs normes et sert à encapsuler un signal de visioconférence sur des réseaux IP. Il se présente comme un des premiers protocoles adaptés dans le transfert de données multimédias sur un réseau.

Il regroupe, entre autre les normes suivantes :

Types de normes	Normes
Normes vidéo	H.261, H.263, H.263+, H.264
Normes audio	G.711, G.722, G.723, G.726, G.728, G.729
Normes contrôle et signalisation	H.225, H.245

Architecture du H.323 :

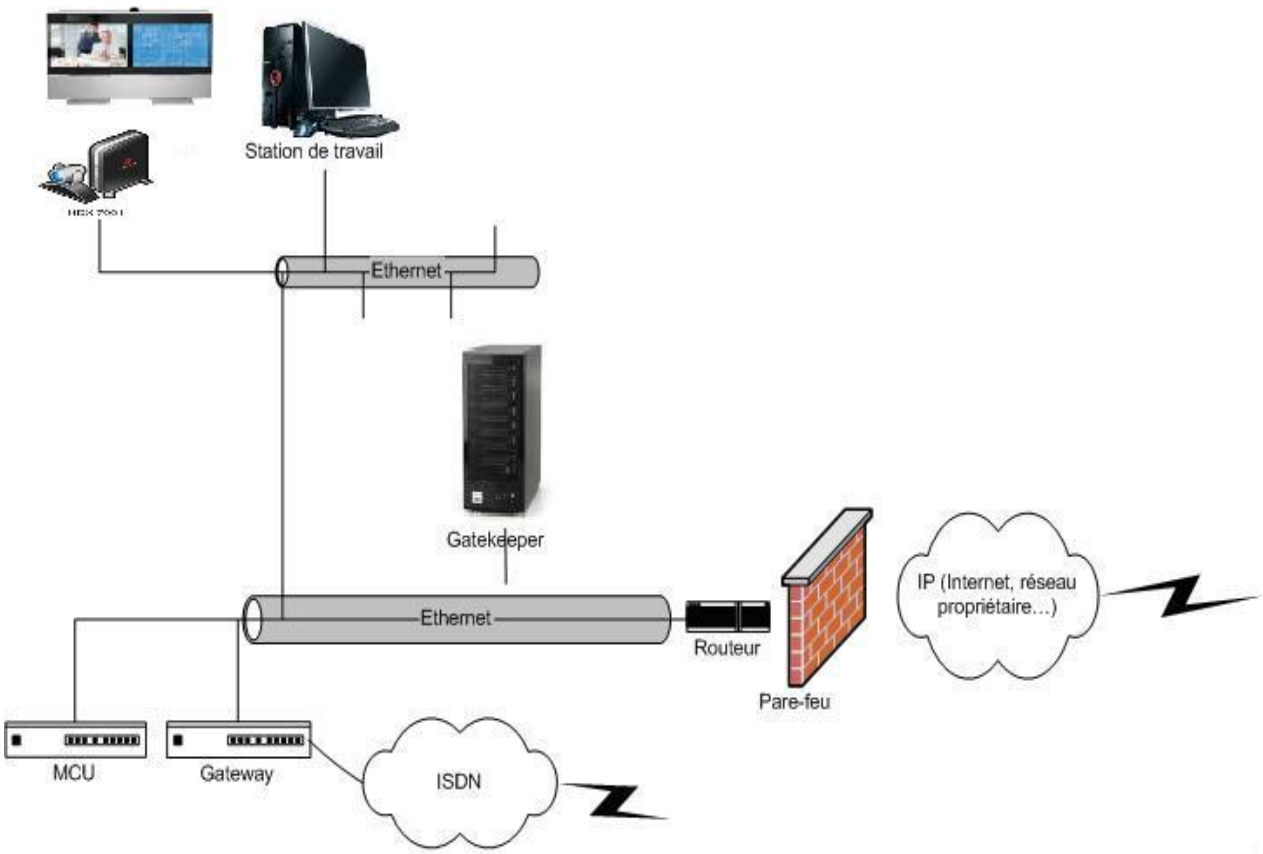


Figure 2.6 : Architecture du protocole H.323

Fonctionnement :

Le fonctionnement du protocole H323 diffère selon les cas d'utilisation (le nombre d'interlocuteurs ou de la structure utilisée). Par exemple : dans un schéma simple comme le point à point ou les deux points sont directement connectés entre eux, l'utilisation d'autres éléments servant à la multi connexion ne sont pas requis.

Cas d'utilisation n°1 : le fonctionnement point à point

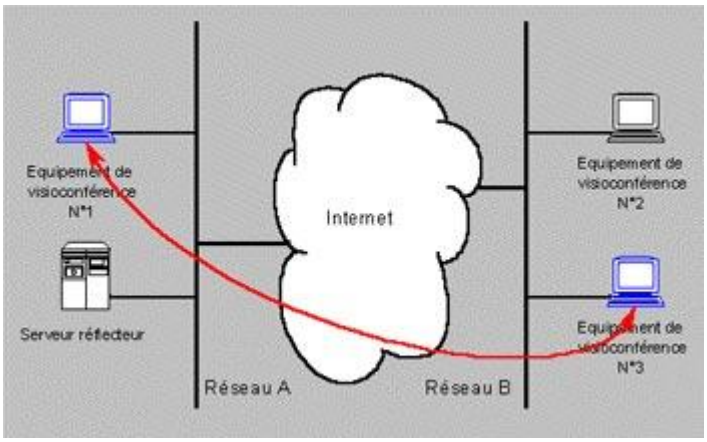


Figure 2.7 : Connexion en point à point

Dans ce premier cas, l'appelant va entrer l'adresse IP du destinataire pour pouvoir entrer en connexion. Le destinataire répond en fonction de son état <<libre>> ou <<occupé>>. En cas de réponse <<libre>> à l'appelant, les deux point se mettent d'accord sur le codecs audio et vidéos qu'ils vont utiliser et la connexion s'établit .

Une fois la connexion établie, les données seront transmises sur des ports différents, En effet , l'information audio et vidéo passera sur des ports UDP et les données utiles à la connexion sur des ports TCP. Mais pourquoi cela ?

Les données importantes relatives à la connexion, sont envoyées avec le protocole TCP car celui-ci va s'assurer qu'elles arrivent à destination. Cela coute plus cher en terme d'information à passer sur le réseau dû aux données de vérification qui doivent voyager. Contrairement aux données sensibles, les données audio et vidéo peuvent se permettre de la perte. En effet, une perte d'audio ou de vidéo de quelques millisecondes ne représente pas un gros problème pour la compréhension du message au sens humain. Ces données passent donc avec un protocole UDP qui s'occupe de transporter les données sans vérifier qu'elles arrivent à destination afin d'éviter l'engorgement du réseau.

Cas d'utilisation n°2 : utilisation de << Gatekeeper>>

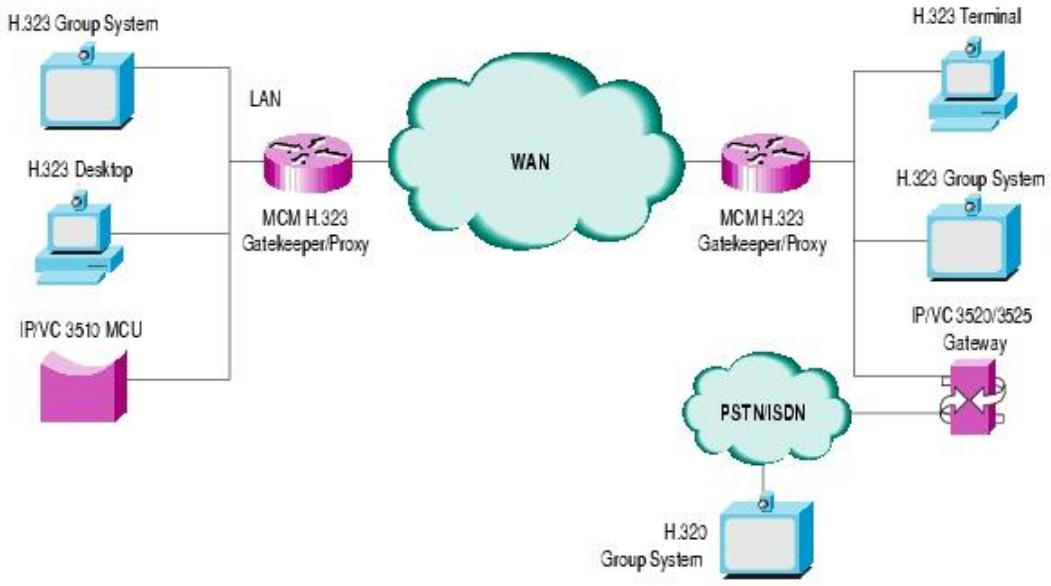


Figure 2.8 : Architecture avec gatekeeper

Un autre cas d'utilisation est l'ajout d'un Gatekeeper entre les points, qui a pour rôle de traduire les numéros de téléphone en adresses IP ainsi que de gère les autorisation. Il sert de passerelle d'accès pour pouvoir se connecter ensuite directement au destinataire

Tout d'abord, l'appelant doit demander une autorisation au Gatekeeper pour se connecter avec le destinataire. Si le Gatekeeper lui donne l'autorisation et que le destinataire n'est pas occupé, le Gatekeeper transmet l'adresse du destinataire à l'appelant. La suite des opérations se passe comme dans le premier cas où une fois mis en relation , les deux points communiquent indépendamment sans passer par le Gatekeeper. Cependant , ce dernier est informé lorsque la conversation prend fin et rétablit les états des intervenants à <<libre>>.

Cas d'utilisation n°3 : utilisation de MCU

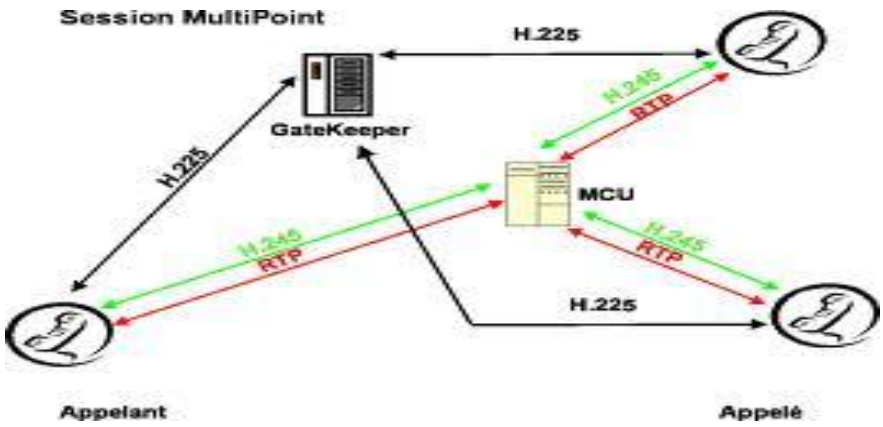


Figure 2.9 : Architecture de l'utilisation de MCU

Lors d'une utilisation multipoints, l'utilisation de MCU est requise. Ils peuvent être sous forme de logiciel ou machine et ont pour rôle d'établir plusieurs communications simultanément. Lors de la vidéoconférence ce sont les MCU qui vont permettre aux utilisateurs de se retrouver dans la même conversation. Ces MCU sont prévus pour les modes « diffusé » et « multipoints ».

Ils ont également l'avantage de servir de passerelle entre deux points dont les codecs sont incompatibles, ce qui leur permet d'élargir les possibilités de connexion entre les équipement.

Par rapport au cas précédent, les points ce seront plus directement connectés entre eux après la demande de résolution d'adresse par les Gatekepper, mais seront en relation directe avec le MCU. Il peuvent être plus que deux connectés à ce dernier ce qui représente une salle virtuelle de communication.

Les problèmes relatif au protocole H.323

Bien que ce protocole reste encore utilisé sur divers équipement et logiciels , il présente certain problèmes techniques dans son utilisation.

Ce protocole est un mélange de ses prédécesseurs avec à son bord de nouvelles fonctions prévues pour faire de la visioconférence. Malheureusement ce « mélange » le rend complexe à mettre en place, ce qui a pour cause de réduire la compatibilité matérielle. Elle a d'ailleurs pour défaut de ne pas respecter le modèle OSI et mélange les couches « Application » et « Transport » ce qui modifie la structure des paquets TCP /IP. De plus, l'ouverture de ports de façon dynamique, peut poser problème à des pare-feux car elle complique la gestion de la sécurité des informations entrantes et sortantes.

H.323 un protocole bientôt obsolète

Malgré une utilisation encore élevée par certains équipements et logiciels, ses contraintes dont qu'il tend à être remplacé peu à peu au profit d'autre systèmes. En effet, depuis quelques années d'autres protocoles permettant de faire de la vidéoconférence sont en train de se développer et deviennent des concurrents de plus en plus sérieux faisant de l'ombre au protocole H.323. il n'est pas improbable que dans un futur proche il se range du coté des protocoles historique utilisé pour faire de la visioconférence.

B) Le protocole SIP

SIP (Session Initiation Protocole) est un protocole destiné à établir, modifier ou fermer des sessions multimédia. Il a été conçu spécifiquement pour la VoIP et permet son utilisation dans d'autres domaines tels que la messagerie instantanée, les jeux vidéo et bien d'autres. Etant indépendant du transport d'information, il n'est pas chargé de faire passer des données vidéo ou audio, mais il offre une compatibilité élargie avec d'autres protocoles. En effet, il a la particularité d'être flexible et peut fonctionner avec bon nombre de codecs vidéo, audio ainsi que des protocoles de transport différents.

Architecture SIP :

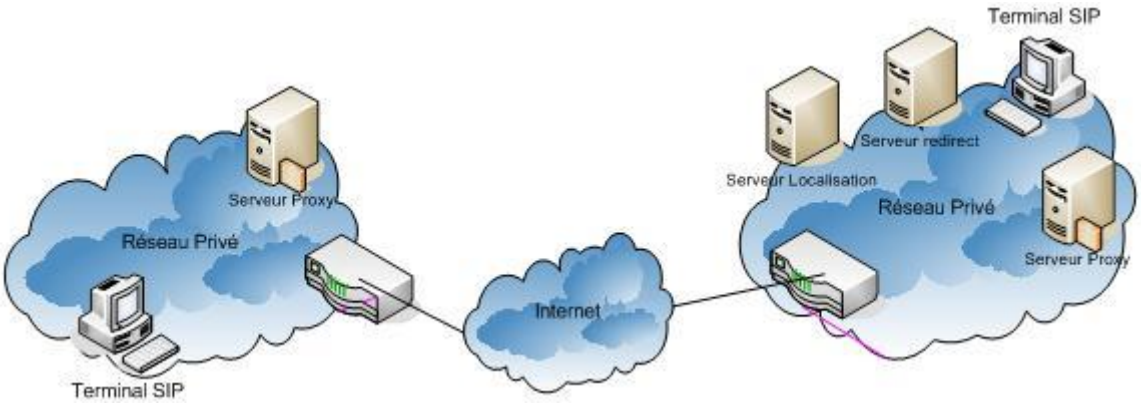


Figure 2 .10 : Architecture globale du protocole SIP

L'architecture de SIP comporte les entités principales suivantes:

- Les agents SIP (UAC) : Application du visiteur qui lance et envoie des demandes de SIP.
- Les serveurs SIP (UAS) : Reçoit et répond aux demandes de SIP au nom des clients : accepte, réoriente ou refuse des appels.
- Serveur Proxy : Entre en contact avec un ou plusieurs clients ou serveurs du prochain saut et passe les demandes d'appel plus loin. Contient UAC et UAS.
- Serveur redirect : Accepte des demandes de SIP, trace l'adresse dans des adresses zéro ou plus récentes et renvoie ces adresses au client.

- Serveur localisation : Fournit des informations au sujet des endroits possibles d'un visiteur pour le réorienter aux serveurs Proxy. Peut Co-être placé avec un serveur de SIP.
- Terminal SIP : Soutient la communication en temps réel et bidirectionnelle avec une autre entité de SIP.

Ces entités interagissent entres elles afin de localiser un usager au sein d'un réseau et permettre des services qui sont définis dans les extensions de SIP.

Fonctionnement

SIP fonctionne sur la base d'un échange de requête serveur-client contenant des demandes, des réponses, ainsi que des requêtes spécifiques au protocole SIP.

Les requêtes d'envoi sont les suivantes :

• Libellé de la requête	• Description
• INVITE	• Demande d'une nouvelle session
• ACK	• Confirmation d'ouverture de la session
• CANCEL	• Annulation de la demande en cours
• BYE	• Termine la session
• OPTION	• Demande de capacité d'un server
• REGISTER	• Envoie de l'adresse de l'argent au serveur

Requêtes de réponse :

• Libellé de la requête	• Description
• 100 Trying	• Essai d'établissement de connexion
• 180 Ringing	• Réponse provisoire
• 200 OK	• Réponse finale
• 404 Not Found	• Erreur
• 486 Busy	• Occupé

Exemple de communication avec le protocole SIP :

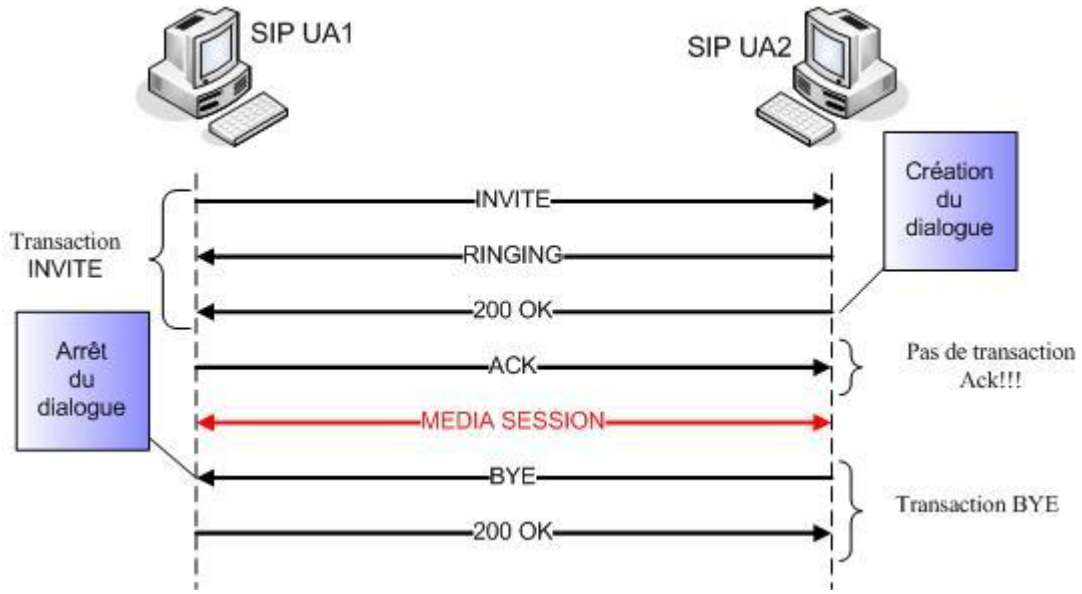


Figure 2.11 : Exemple de communication SIP

Une source appelle son destinataire qui répond d'abord par une réponse provisoire. Une fois que les deux agents ont répondu positivement, une session est ouverte et laisse place à un échange de données, entre autres les flux vidéo et audio, qui se fera grâce à l'aide du protocole de transport choisi. Quand l'un des deux raccroche, un signale est envoyé à l'autre de façon à l'avertir que la communication a été arrêtée.

L'utilisation de Registrar :

Afin de signaler leur emplacement, les équipements, téléphone, ordinateurs ou autres, peuvent s'inscrire auprès d'un Registrar qui s'occupera d'enregistrer leur adresse. Ces adresses sont enregistrées sous forme d'IP associées à une courte chaine de caractères qui sert d'identifiant unique. Une fois reçues par serveur Registrar, elles sont stockées dans une base de données chargée de récolter toutes les adresses des équipements connectés afin de simplifier l'acheminement des informations .

Inconvénients et avantages

Le protocole SIP, tout comme le H.323, contient certaines faiblesses dans sa structure. En effet , les login et mot de passe, lors de la gestion de sessions passent en clair sur le réseau. Il existe cependant des solutions permettant de crypter les données qui sont indépendantes du protocole. De plus, comme le SIP est basé sur les adresses IP, cela pose problème à l'entrée d'un local car il ne traverse pas les NAT(Network Address Translation).

Malgré ces inconvénients, le protocole SIP est en pleine croissance et dépasse peu à peu le protocole H.323. sa flexibilité et son utilisation moins complexe le rend plus adapté dans bien des domaines, notamment dans la visioconférence. Il reprend quelques fonctionnalités de protocole H.323 en y améliorant certains aspects, comme le renforcement de l'interopérabilité qui aujourd'hui a son importance étant donné le nombre d'équipements différents existants sur le marché.

Comparaison de H.323 et SIP

• Critères	• H.323	• SIP
• Comité	• ITU	• IETF
• Origines	• Issu du monde de la téléphonie	• Développé pour internet (réseaux IP)
• Flexibilité	• Fonctionne avec un nombre de normes et protocoles limités.	• Flexible pouvant fonctionner avec bon nombres de normes et protocoles différents
• Complexité de la communication	• Entre 6 et 7 échanges nécessaires à l'établissement d'une connexion	• Entre 1et 5 échanges nécessaires à l'établissement d'une connexion
• Latence	• Latence pouvant aller jusqu'à 8 secondes	• Latence minime
• Evolution	• Doit tenir compte de ses versions précédentes pour évoluer	• Evolue avec moins de complications pour s'adapter à de nouveaux codecs

IV. Compressions /Décompression

Dés les débuts de la visioconférence, la quantité d'informations demandées pour un appel a vite été le premier problème des constructeurs et la simple amélioration des équipements ne permettait pas d'y remédier. Il a fallu se pencher sur des solutions logicielles pour alléger la quantité d'informations transmises.

Afin de décharger les réseaux de cette quantité de données, l'utilisation de codecs est nécessaire. Un codec est un procédé servant à compresser et décompresser le signal afin de respecter certaines normes, et est utilisé de façon à ce que le flux vidéo ou audio puisse être lu dans un format plus léger. Il exister plusieurs codecs avec pour chacun une méthode de

compression/décompression différente. Cependant , deux machines désirant communiquer doivent utiliser les mêmes codecs des deux cotés afin de coder et décoder le signal de la même manière. Sans cela, le signal ne serait pas lisible par le receveur.

Les normes

La transmission d'un flux d'informations à travers un réseau requiert l'utilisation de plusieurs normes afin de faciliter la communication entre plusieurs machines. La visioconférence fait l'usage de plusieurs d'entre elles qui se regroupent en catégories distinctes. Ces catégories ont une fonction propre à elles-mêmes et contiennent plusieurs normes plus ou moins récentes. Afin de faciliter la compréhension de ce chapitre, seules 3 catégories contenant quelques unes leurs normes seront abordées dans l'ordre suivant.

- Audio
- Vidéo
- Contrôle et signalisation

Les normes audio

• Norme	• Description
• G.711	• Norme de compression audio pour la vidéoconférence en H.323 et H.320
• G.722	• Norme permettant d'obtenir une qualité de voix haut définition
• G.723	• Norme de compression audio pour la visioconférence ainsi que la téléphonie IP
• G.726	• Modulation par impulsions et codage différentiel adaptatif allant de 40, 32, 24, 16 kbit/s
• G.728	• Norme obsolète à faible débit. Ne correspond pas aux nouvelles technologies
• G.729	• Norme définissant un codage de la voix sur 8kbit/s

Les normes vidéo

• Norme	• Description
• H.261	• Norme pour l'audiovisuel à 64 Kbits/s
• H.263	• Norme obsolète notamment utilisée par les consoles de jeux
• H.261	• Norme dédiée aux réseaux RNIS

• H.263	• Norme vidéo pour les lignes à bas débits (à l'origine)
• H.264	• Norme vidéo flexible plus efficace que ses prédécesseurs
• MPEG-2	• Norme développée pour le transport sur des réseaux pour la tv numérique
• MPEG-4	• Evolution de la MPEG-2 en ajoutant de nouvelles applications multimédia

Les normes de contrôle et signalisation

• norme	• Description
• H.225	• Sous norme de H.323 servant à la gestion des appels (établissement et contrôle d'un appel)
• H.245	• A pour but de négocier les codecs communs et de décrire l'ouverture/fermeture des canaux media

V. Qualité de service

Les paramètres de qualité de service (QoS) sont divisés en deux types on à : les paramètres dynamiques qui viennent d'être vus et qui influent sur les mécanismes de l'application, et les paramètres statiques qui n'influent pas sur son comportement dynamique. Le tableau suivant présente tous les paramètre de QoS du point de vue de l'utilisateur.

•	• Paramètres dynamiques de QoS	• Paramètres statiques de QoS
• Vidéo	• Nombre d'images/s • Gigue vidéo max • Nombre max de discontinuités	• Dimensions de l'image • Qualité de l'image
• Audio	• Gigue audio max • Nombre max de discontinuités	• Qualité du son
• synchronisation	• Type de synchronisation • Dérive inter flux max	•
• Retard de présentation	• Délai max	•

La QoS est négociée entre les deux interlocuteurs à l'établissement de la connexion. Cette négociation prend en compte, d'une part la qualité souhaitée par les utilisateurs (qui est fonction de leurs besoins mais qui peut aussi être fonction du coût de communication), et d'autre part de la puissance de traitement disponible sur la machine, la qualité du/des réseaux interconnectant les deux machines, et les formats d'échanges de données supportés par ces machines(généralement ces formats dépendent des cartes multimédia qui équipent les stations). Si les deux interlocuteurs sont d'accord sur une QoS que peuvent assurer les deux machines et les le réseau de communication, alors la connexion est établie. Dans le cas contraire, l'application de visioconférence proposera aux utilisateurs une QoS plus faible qu'ils pourront accepter ou refuser.

Cependant, cette qualité ne peut pas être que statique. Elle doit être renégociable, c'est-à-dire qu'elle doit pouvoir être modifiée à tout moment, suite à un problème qui apparait (surcharge due au lancement d'une nouvelle application par exemple) à l'émetteur ou au récepteur, ou suite à une demande explicite de l'un des deux utilisateurs. La nouvelle qualité de service est négociée entre l'émetteur et le récepteur, de la même manière qu'au début de la visioconférence. Il faut noter que pendant toute la durée de la négociation, qui se fait sur un canal de signalisation annexe, la visioconférence continue de fonctionner avec la synchronisation en cours.

VI. Résolution et qualité (HD)

La résolution Haute Définition (HD) en visioconférence améliore tous les processus de communication. En effet, la visioconférence HD à travers une meilleure qualité d'image et de son vous rapproche le plus précisément possible de la réalité. La résolution HD séduit aujourd'hui les professionnels et les systèmes de visioconférence HD deviennent indispensables dans tous les processus de collaboration à distance.

La visioconférence HD se révèle être très performante, les images HD projetées sont très proches de la réalité que l'œil perçoit.

De plus, la résolution HD entraine la réduction de la sensation de fatigue liée au temps passé devant les écrans. Ce qui se révèle être un élément prioritaire à prendre en compte par les professionnels. La visioconférence HD offre aussi la possibilité d'avoir une bonne qualité d'image à haut débit mais en exclusivité mondial chez LifeSize également à bas débit grâce aux 55 résolutions supportées . DWPro, grossiste en visioconférence, offre, à travers la gamme de visioconférence HD de LifeSize, la possibilité d'expérimenter la visioconférence HD et ainsi de réaliser la différence fondamentale qui existe entre la visioconférence en Définition Standard (DS) et la visioconférence en Haute définition (HD). En effet, la différence qui existe entre une visioconférence en résolution standard (SD) et une visioconférence en Haute Définition (HD) n´est pas négligeable :

La visioconférence en résolution standard (SD)

La visioconférence en Haute Définition (HD)

- En Haute Définition (HD) deux formats de résolution existent : La résolution 1280 X 720
- La résolution 1920 X 1080

- La qualité de la vidéo pour la visioconférence dépend selon : Le nombre de pixel à transmettre

Sa définition (clarté de l'image) : Plus l'image est claire, plus la bande passante sera augmentée son rafraîchissement (nombre d'images par seconde)

Plus le nombre d'images par seconde est grand, plus la bande passante sera augmentée

- La bande passante augmente proportionnellement à ces facteurs.
- Normalement plus la bande passante est grande mieux est la qualité de la vidéo.

VII. Proxy/ Firewall et visioconférence

Quelques exemples des ports utilisés pour une visioconférence :

• Port	• Type	• Protocoles	• Description
• 1719	• Statique	• UDP	• Gatekeeper RAS
• 1720	• Statique	• TCP	• Q.931 (Call Setup)
• 1024-65535	• Dynamique	• TCP	• H245 (Call parametrers)
• 1024-65535	• Dynamique	• UDP	• Video and audio Data Stream
• 1024-65535	• Dynamique	• UDP	• Control Video and audio Stream
• Ports optionnels	•	•	•
• 389	• Statique	• TCP	• ILS Registration (LDAP)
• 1503	• Statique	• TCP	• T.120

Différentes solutions techniques ont été développées pour contourner ces obstacles et permettre un fonctionnement correct des protocoles H323 à travers les firewalls :

Utiliser des firewalls intégrant H323 :

C'est sans doute la meilleure solution, et celle qui offre la meilleure sécurité. Beaucoup des firewalls récents intègrent désormais H323 (sous l'appellation Application Level Gateways ou ALG dans certains textes). Ces équipements ont la faculté de scruter les communications qui sont établies en amorce à une visioconférence afin de détecter les numéros de ports qui seront effectivement utilisés. Ils pourront alors autoriser l'ouverture de ces ports spécifiques et permettre le trafic entre appelé et appelant pendant une durée qui restera limitée à celle de la session. Ces ports sont refermés ensuite. On utilise parfois le terme de « pinholing » pour désigner cette méthode qui consiste à n'ouvrir que les quelques ports nécessaires (des « trous d'épingle ») dans le firewall. Certains modèles intègrent également la fonction NAT. Lors de la translation d'adresses, ils sont capables, non seulement de remplacer une adresse privée par une adresse publique dans l'entête des paquets, mais également de réaliser cette opération dans le corps même de la charge utile, permettant de ce fait le fonctionnement correct de toute session de visioconférence.

Utiliser des proxys : Un proxy est une passerelle spécialisée qui va permettre à des flux H323 de contourner dans certaines conditions les firewalls, sans affaiblir les conditions de sécurité. Il va agir comme un intermédiaire. C'est lui qui va assurer la gestion de tous le trafic H323 en lieu et place des terminaux de visioconférences qui seront ainsi totalement isolés d'Internet (ils seront invisibles de l'extérieur, y compris pont et passerelle). Lors de l'établissement d'une liaison, ce n'est plus un appel qui sera généré mais deux. Le premier sera initié par l'équipement de visioconférence situé à l'intérieur du réseau local en direction du proxy qui à son tour en générera un second sur le réseau public (et en utilisant sa propre adresse) en direction de l'équipement distant. Seul le proxy peut interagir avec l'extérieur. Le Firewall devra être correctement configuré pour pouvoir fonctionner lui. Ce mode de fonctionnement impose l'utilisation d'un gatekeeper . Différentes configurations sont possibles pour le proxy : il pourra être intégré au gatekeeper ou au firewall.

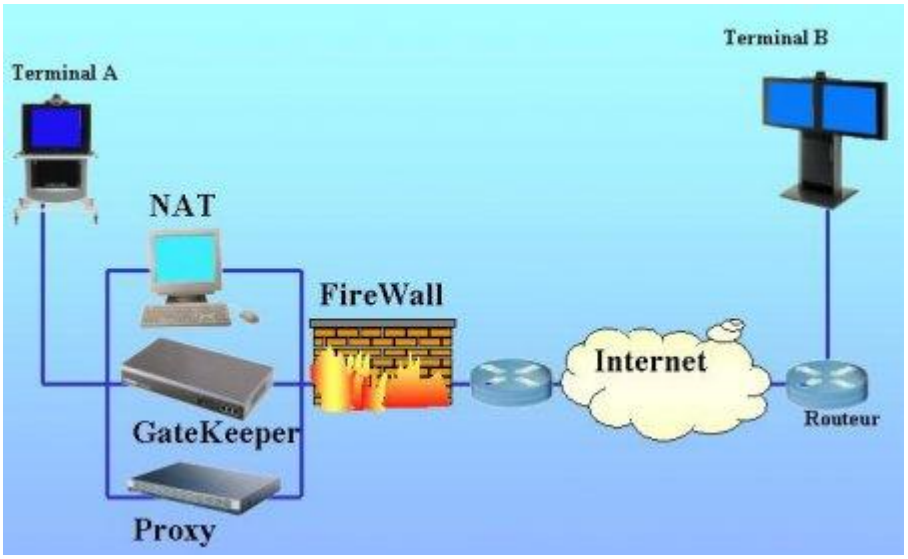


Figure 2.12 : Architecture d'utilisation d'un proxy

Un proxy est une passerelle spécialisée qui va permettre à des flux H323 de traverser dans certaines conditions un firewall.

S'appuyer sur une « zone démilitarisée » ou DMZ :

Une DMZ est une zone particulière du réseau informatique d'un établissement ou d'une entreprise. C'est une zone séparée qui ne va héberger que les équipements qui doivent être accessibles depuis l'extérieur, non seulement les serveurs (serveurs Web, serveurs FTP, serveurs Email....) mais également éventuellement des dispositifs de visioconférence. Elle est située, sur le plan des risques, entre le réseau local privé (qui doit être totalement protégé) et Internet (qui est une zone à très fort risque). La DMZ doit être également accessible depuis le réseau privé. Les adresses pourront y être privées ou ce qui est beaucoup mieux, publiques pour permettre des accès sans translation d'adresse. Les règles de communications entre les trois entités - le réseau local, la DMZ et Internet - seront différentes et gérées par un FireWall.

Proxy derrière un FireWall

- FireWall laisse passer le trafic entre le Proxy et l'extérieur .
- Tous les trafics passent par le Proxy.
- Inconvénient : le Proxy, même si il a la capacité de réduire la gamme de ports dynamiques, doit rester ouvert sur une grande plage de ports UDP et TCP.

FireWall statefull inspection qui intègre H.323:

- Par exemple : Netscreen, Check Point, Cisco PIX .
- Le FireWall détecte dès la signalisation d'appel les ports TCP et UDP négociés.
- Il ouvre dynamiquement les ports concernés uniquement pour la durée de connexion.

VIII. Cryptage

Lorsqu'une visioconférence strictement confidentielle est requise ou quelle est effectuée sur internet, le système de communication vidéo active une vidéoconférence avec des signaux audio, vidéo et données cryptés produits par l'unité de solution de données. Une visioconférence qui utilise cette fonction est appelée visioconférence cryptée .

Le système de communication vidéo est équipé du cryptage standard, conforme aux recommandation ITU-T H.233, H.234 et H.235, et du cryptage de propriétaire, méthode de cryptage d'origine Sony.

Le H.233 : est pris en charge dans un large éventail de services standards, y compris H.320, H.323, et H.324.

H.234 : qui précise comment le chiffrement et les clés sont manipulées.(Voir H.320, H.323, H.324). Ainsi le H.234 est le gestionnaire de clés de chiffrement et d'authentification pour l'audiovisuel services.

Trois méthodes de gestion de clé de chiffrement sont certifiés ISO 8732,Diffie-Hellman, RSA. Elles sont applicables à l'encryptage de l'audiovisuel ,au signaux transmis numériquement en utilisant la structure de trame H.221. à la gestion des messages définis qui sont transmises dans le signal de commande de cryptage (ECS) canal de H.221, et dont la structure est définie à l'utilisation H.233.

La méthode de cryptage de propriétaire est disponible uniquement entre des systèmes de communication vidéo PCS-1/1P ou entre le PCS-1/1P et des correspondants (récepteurs) qui utilisent les systèmes de communication vidéo PCS-11/11P, PCS-G70/G70P, PCS-G50/G50P, PCS-TL50 ou PCS-TL30.

Vous ne pouvez pas effectuer de visioconférence par cryptage de propriétaire avec des systèmes de communication Sony différents de ceux répertoriés ni avec des systèmes de visioconférence d'autre fabricants.

Lorsque vous utilisez le cryptage standard, une visioconférence cryptée entre deux points ou plusieurs points (y compris une connexion en cascade) est disponible via un réseau LAN et/ou RNIS. Une visioconférence cryptée entre plusieurs points via une connexion mixte LAN et RNIS est également possible. Lorsque vous utilisez le cryptage de propriétaire, une visioconférence cryptée entre deux ou plusieurs points est disponible via LAN ou SIP.

Disponibilité de la méthode de cryptage :

En mode point a point

• Interface réseau • Protocole de cryptage	• LAN	• RNIS	• SIP
• Méthode de propriétaire	• O	• X	• O
• Méthode standard (H.233, H.234, H.235)	• O	• O	• X

En mode multipoint

• Interface réseau • Protocole de cryptage	• LAN	• RNIS	• SIP	• LAN et RNIS mélangés	• LAN et SIP mélangés	• RNIS et SIP mélangés
• Méthode de propriétaire	• O	• X	• O	• X	• O	• X
• Méthode standard	• O	• O	• X	• O	• X	• X

O : visioconférence cryptée disponible.

X : visioconférence cryptée indisponible .

Priorité de connexion :

Connexion avec cryptage à un correspondant avec la connexion cryptée standard activée. Connexion sans codage aux correspondants ne pouvant se connecter avec le cryptage standard ou aux correspondants ayant le cryptage désactivé.

Priorité de cryptage

Connexion aux correspondants avec connexion cryptée standard activée uniquement.

Si le message suivant apparait lorsque vous appelez un correspondant, il n'est pas possible d'effectuer une visioconférence cryptée.

• Message d'erreur	• Causes
• La fonction de cryptage du système distant est désactivée	• La fonction de cryptage d'un système distant est désactivée, ou les réglages du protocole de cryptage sur le système distant sont différents de ceux sur le système local.
• Le mot de passe entré pour la fonction de cryptage n'est pas correct.	• Le mot de passe entré sur le système distant est différent de celui du système local.
• La visioconférence cryptée n'est pas disponible si un terminal est connecté sur le réseau RNIS.	• Lorsque la visioconférence est exécutée via une connexion RNIS, vous ne pouvez connecter aucun terminal via la connexion LAN.
• La conférence n'a pas pu commencer parce que la fonction de cryptage du système local est désactivée.	• La fonction de cryptage du système local est désactivée.
• La conférence n'a pas pu commencer parce que la fonction de cryptage du système distant est désactivée.	• La fonction de cryptage du système distant est désactivée.
• Commence une conférence. (La fonction de cryptage est désactivée.)	• La fonction de cryptage est désactivée.
• La visioconférence par cryptage standard n'est pas disponible avec la connexion SIP.	• Votre système est connecté aux système distant via SIP.
• La visioconférence par cryptage de propriétaire n'est pas disponible avec la connexion RNIS.	• Votre système est connecté aux système distant via ISDN.

Cryptage utiliser :

IP-Sec :

IP-sec (Internet Protocol Security), défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques, est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. IP-sec se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme

et c'est la raison pour laquelle il est considéré comme un cadre de standards ouverts. De plus IP-sec opère à la couche réseau (couche 3 du modèle OSI) contrairement aux standards antérieurs qui opéraient à la couche application (couche 7 du modèle OSI), ce qui le rend indépendant des applications, et veut dire que les utilisateurs n'ont pas besoin de configurer chaque application aux standards IP-sec.

Le protocole IP-sec est l'une des méthodes permettant de créer des VPN (réseaux privés virtuels), c'est-à-dire de relier entre eux des systèmes informatiques de manière sûre en s'appuyant sur un réseau existant, lui-même considéré comme non sécurisé. Le terme sûr a ici une signification assez vague, mais peut en particulier couvrir les notions d'intégrité et de confidentialité. L'intérêt majeur de cette solution par rapport à d'autres techniques (par exemple les tunnels SSH) est qu'il s'agit d'une méthode standard (facultative en IPv4, mais obligatoire en IPv6), mise au point dans ce but précis, décrite par différentes RFCs, et donc interopérable. Quelques avantages supplémentaires sont l'économie de bande passante, d'une part parce que la compression des en-têtes des données transmises est prévue par ce standard, et d'autre part parce que celui-ci ne fait pas appel à de trop lourdes techniques d'encapsulation, comme par exemple les tunnels PPP sur lien SSH. Il permet également de protéger des protocoles de bas niveau comme ICMP et IGMP, RIP, etc...

IP-sec présente en outre l'intérêt d'être une solution évolutive, puisque les algorithmes de chiffrement et d'authentification à proprement parler sont spécifiés séparément du protocole lui-même. Elle a cependant l'inconvénient inhérent à sa flexibilité : sa grande complexité rend son implémentation délicate. Les différents services offerts par le protocole IP-sec sont ici détaillés. Les manières de les combiner entre eux que les implémentations sont tenues de supporter sont ensuite présentées. Les moyens de gestion des clefs de chiffrement et signature sont étudiés et les problèmes d'interopérabilité associés sont évoqués. Enfin, un aperçu rapide de quelques implémentations IP-sec, en s'intéressant essentiellement à leur conformité aux spécifications est donné.

Les services offerts par IP-sec :

Les deux modes d'échange IP-sec :

IP-sec peut fonctionner dans un mode transport hôte à hôte ou bien dans un mode tunnel réseau.

Mode transport : Dans le mode transport, ce sont uniquement les données transférées (la partie *payload* du paquet IP) qui sont chiffrées et/ou authentifiées. Le reste du paquet IP est inchangé et de ce fait le routage des paquets n'est pas modifié. Néanmoins, les adresses IP ne pouvant pas être modifiées sans corrompre le *hash* de l'en-tête AH généré par IP-sec, pour traverser un NAT il faut avoir recours à l'encapsulation NAT-T. Le mode transport est utilisé pour les communications dites hôte à hôte (*Host-to-Host*).

Mode tunnel : En mode tunnel, c'est la totalité du paquet IP qui est chiffré et/ou authentifié. Le paquet est ensuite encapsulé dans un nouveau paquet IP avec une nouvelle en-tête IP. Au contraire du mode transport, ce mode supporte donc bien la traversée de NAT. Le mode tunnel est utilisé pour créer des réseaux privés virtuels (VPN) permettant la communication de réseau à réseau

(e.g. entre deux sites distants), d'hôte à réseau (e.g. accès à distance d'un utilisateur) ou bien d'hôte à hôte (e.g. messagerie privée.)

Les protocoles à la base d'IP-sec :

1) AH (authentication header) :

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

L'authentification : les datagrammes IP reçus ont effectivement été émis par l'hôte dont l'adresse IP est indiquée comme adresse source dans les en-têtes.

L'unicité (optionnelle, à la discrétion du récepteur) : un datagramme ayant été émis légitimement et enregistré par un attaquant ne peut être réutilisé par ce dernier, les attaques par re jeu sont ainsi évitées.

L'intégrité : les champs suivants du datagramme IP n'ont pas été modifiés depuis leur émission : les données (en mode tunnel, ceci comprend la totalité des champs, y compris les en-têtes, du datagramme IP encapsulé dans le datagramme protégé par AH), version (4 en IPv4, 6 en IPv6), longueur de l'en-tête (en IPv4), longueur totale du datagramme (en IPv4), longueur des données (en IPv6), identification, protocole ou en-tête suivant (ce champ vaut 51 pour indiquer qu'il s'agit du protocole AH), adresse IP de l'émetteur, adresse IP du destinataire (sans source routing).

En outre, au cas où du source routing serait présent, le champ adresse IP du destinataire a la valeur que l'émetteur a prévu qu'il aurait lors de sa réception par le destinataire. Cependant, la valeur que prendront les champs type de service (IPv4), indicateurs (IPv4), index de fragment (IPv4), TTL (IPv4), somme de contrôle d'en-tête (IPv4), classe (IPv6), flow label (IPv6), et hop limit (IPv6) lors de leur réception n'étant pas prédictible au moment de l'émission, leur intégrité n'est pas garantie par AH. L'intégrité de celles des options IP qui ne sont pas modifiables pendant le transport est assurée, celle des autres options ne l'est pas. Attention, AH n'assure pas la confidentialité : les données sont signées mais pas chiffrées. Enfin, AH ne spécifie pas d'algorithme de signature particulier, ceux-ci sont décrits séparément, cependant, une implémentation conforme à la Rfc 2402 est tenue de supporter les algorithmes MD5 et SHA-1.

2) ESP (encapsulating security payload)

ESP est le second protocole de protection des données qui fait partie de la spécification IP-sec. Il est détaillé dans la Rfc 2406. Contrairement à AH, ESP ne protège pas les en-têtes des datagrammes IP utilisés pour transmettre la communication. Seules les données sont protégées. En mode transport, il assure :

La confidentialité des données (optionnelle) : la partie données des datagrammes IP transmis est chiffrée.

L'authentification (optionnelle, mais obligatoire en l'absence de confidentialité) : la partie données des datagrammes IP reçus ne peut avoir été émise que par l'hôte avec lequel a lieu l'échange IP-sec, qui ne peut s'authentifier avec succès que s'il connaît la clef associée à la

communication ESP. Il est également important de savoir que l'absence d'authentification nuit à la confidentialité, en la rendant plus vulnérable à certaines attaques actives.

L'unicité (optionnelle, à la discrétion du récepteur).

L'intégrité : les données n'ont pas été modifiées depuis leur émission.

En mode tunnel, ces garanties s'appliquent aux données du datagramme dans lequel est encapsulé le trafic utile, donc à la totalité (en-têtes et options inclus) du datagramme encapsulé. Dans ce mode, deux avantages supplémentaires apparaissent:

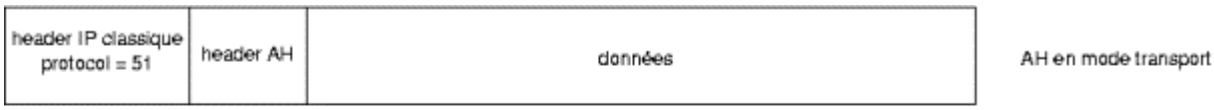
Une confidentialité, limitée, des flux de données (en mode tunnel uniquement, lorsque la confidentialité est assurée) : un attaquant capable d'observer les données transitant par un lien n'est pas à même de déterminer quel volume de données est transféré entre deux hôtes particuliers. Par exemple, si la communication entre deux sous-réseaux est chiffrée à l'aide d'un tunnel ESP, le volume total de données échangées entre ces deux sous-réseaux est calculable par cet attaquant, mais pas la répartition de ce volume entre les différents systèmes de ces sous-réseaux.

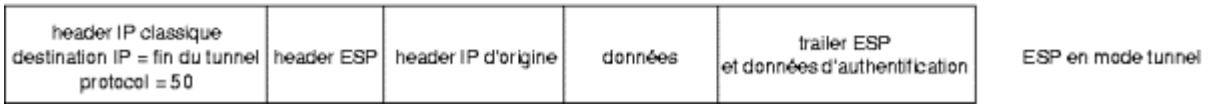
La confidentialité des données, si elle est demandée, s'étend à l'ensemble des champs, y compris les en-têtes, du datagramme IP encapsulé dans le datagramme protégé par ESP).

Enfin, ESP ne spécifie pas d'algorithme de signature ou de chiffrement particulier, ceux-ci sont décrits séparément, cependant, une implémentation conforme à la Rfc 2406 est tenue de supporter l'algorithme de chiffrement DES en mode CBC, et les signatures à l'aide des fonctions de hachage MD5 et SHA-1.

Implantation d'IP-sec dans le datagramme IP

La figure si dessous montre comment les données nécessaires au bon fonctionnement des formats AH et ESP sont placées dans le datagramme IPv4. Il s'agit bien d'un ajout dans le datagramme IP, et non de nouveaux datagrammes, ce qui permet un nombre théoriquement illimité ou presque d'encapsulations IP-sec : un datagramme donné peut par exemple être protégé à l'aide de trois applications successives de AH et de deux encapsulations de ESP.





AES :

Advanced Encryption Standard ou AES (soit « standard de chiffrement avancé »), aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il à étai lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il a été également approuvé par la NSA (National Security Agency) pour les informations top secrètes.

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(2^8) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

DES :

Le Data Encryption Standard (DES) est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable. Quand il est encore utilisé c'est généralement en Triple DES, ce qui ne fait rien pour améliorer ses performances. DES a notamment été utilisé dans le système de mots de passe UNIX. Le premier standard DES est publié par FIPS le 15 janvier 1977 sous le nom FIPS PUB 46. La dernière version avant l'obsolescence date du 25 octobre 1999 FIPS PUB 46-3.

L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits. Il manipule des clés individuelles de 56 bits, représentées par 64 bits (avec un bit de chaque octet servant pour le contrôle de parité). Ce système de chiffrement symétrique fait partie de la famille des chiffrements itératifs par blocs, plus particulièrement il s'agit d'un schéma de Feistel (du nom de Horst Feistel à l'origine du chiffrement Lucifer).

D'une manière générale, on peut dire que DES fonctionne en trois étapes :

- permutation initiale et fixe d'un bloc (sans aucune incidence sur le niveau de sécurité).
- le résultat est soumis à 16 itérations d'une transformation, ces itérations dépendent à chaque ronde d'une autre clé partielle de 48 bits. Cette clé de ronde intermédiaire est calculée à partir de la clé initiale de l'utilisateur (grâce à un réseau de tables de substitution et d'opérateurs XOR). Lors de chaque ronde, le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre selon un schéma de Feistel. Le bloc de 32

bits ayant le poids le plus fort (celui qui s'étend du bit 32 au bit 64) subira une transformation.

- le dernier résultat de la dernière ronde est transformé par la fonction inverse de la permutation initiale.

DES utilise huit tables de substitution (les S-Boxes) qui furent l'objet de nombreuses controverses quant à leur contenu. On soupçonnait une faiblesse volontairement insérée par les concepteurs. Ces rumeurs furent dissipées au début des années 1990 par la découverte de la cryptanalyse différentielle qui démontra que les tables étaient bien conçues.

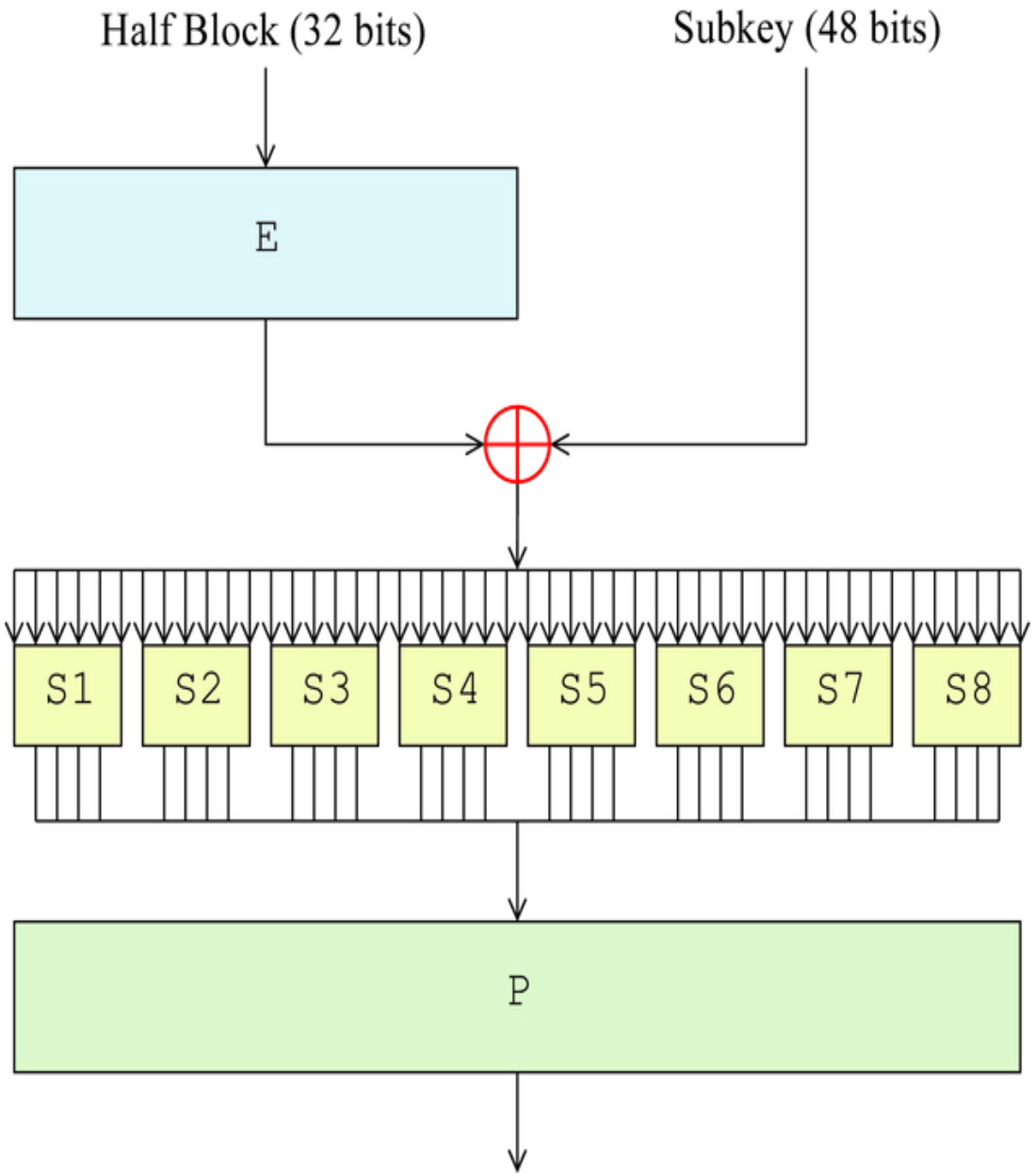


Figure 2.13 : Algorithme DES

Triple DES :

Le Triple DES (aussi appelé 3DES) est un algorithme de chiffrement symétrique par bloc, enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes.

Cette utilisation de trois chiffrements DES a été développée par Walter Tuchman (chef du projet DES chez IBM), il existe en effet d'autres manières d'employer trois fois DES mais elles ne sont pas forcément sûres. La version de Tuchman utilise un chiffrement, suivi d'un déchiffrement pour se conclure à nouveau par un chiffrement.

Le Triple DES est généralement utilisé avec seulement deux clés différentes. Le mode d'usage standard est de l'utiliser en mode EDE (*Encryption, Decryption, Encryption*, c'est-à-dire *Chiffrement, Déchiffrement, Chiffrement*) ce qui le rend compatible avec DES quand on utilise trois fois la même clé. Dans le cas d'une implémentation matérielle cela permet d'utiliser le même composant pour respecter le standard DES et le standard Triple DES. Dans le mode proposé par Tuchman, 3DES s'écrit plus formellement de cette manière :

$$C = E_{DES}^{k3}\left(D_{DES}^{k2}\left(E_{DES}^{k1}(M)\right)\right)$$

Une autre variante de Triple DES est celle de Carl Ellison, mais elle ne fait pas partie du standard défini pour 3DES :

$$C = E_{DES}^{k3}\left(T\left(E_{DES}^{k2}\left(T\left(E_{DES}^{k1}(M)\right)\right)\right)\right)$$

où T est une fonction de transposition destinée à augmenter la diffusion. Cette fonction prend en entrée un bloc de 8192 octets, remplit la graine d'un générateur de nombres pseudo-aléatoires avec l'histogramme des octets, et mélange les octets du bloc grâce à la sortie du générateur. L'histogramme n'est pas changé par les permutations et donc l'opération inverse est possible. David Wagner a proposé une attaque sur le schéma d'Ellison en 1997.

Même quand 3 clés de 56 bits différentes sont utilisées, la force effective de l'algorithme n'est que de 112 bits et non 168 bits, à cause d'une attaque *rencontre au milieu*. Cette attaque reste cependant peu praticable, en effet elle nécessite un stockage de données de l'ordre de 2^{56} mots de 64 bits, de plus ce stockage doit être « interrogeable » en un temps très court. C'est pour éviter ce genre d'attaque que le Double DES est simplement proscrit et que l'on passe directement à du Triple DES, le Double DES n'assure en effet qu'une force effective moyenne de 57 bits.

Bien que normalisé (par exemple par le NIST), bien connu, et assez simple à implémenter, il est assez lent, et appelé à être remplacé par des algorithmes plus modernes tels qu'AES, également reconnu via le NIST aux États-Unis comme sûr pour tout échange d'information.

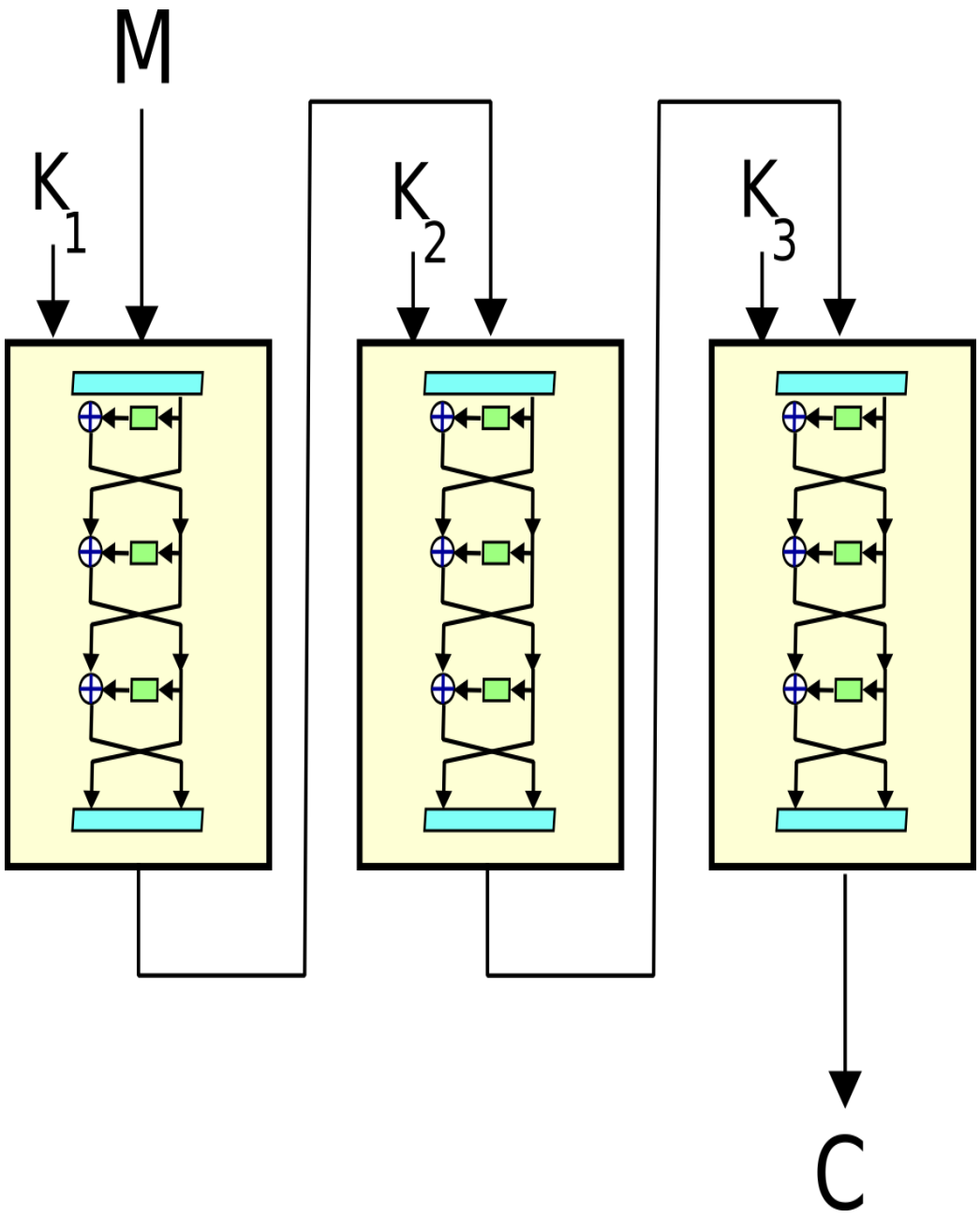


Figure 2.14 : Architecture du Triple DES

IX. CONCLUSION

Dans ce chapitre on a vu tous les différents utilitaire utiliser comme les modes de transmission (Multicast et Broadcaste) ainsi que les protocoles de communication utilisés (SIP et H323). Nous avons aussi vu les différents protocoles de compression utilisés pour tout types de données envoie a travers le réseau et aussi les cryptages (IP-sec, AH, AES, DES et 3DES). Enfin on a vu l'utilisation de proxy et firewall pour la visioconférence .

Chapitre 3 : Optimisation du QoS et de la bande passante

I. Introduction

Dans les chapitres précédent nous avons vu tous les équipements a utilisés ainsi que les programmes et protocoles de sécurité, de cryptage et tous les moyens utiles pour avoir une bonne transmission de données en toute sécurité. Dans ce chapitre nous allons parler de la qualité de service et de la bande passante et de ces optimisations pour avoir une meilleure qualité de transmission sur la voix sur IP et la visioconférence .

II. Qualité de service

La **qualité de service (QDS)** ou **Quality of service (QoS)** est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, gigue, débit, délais de transmission, taux de perte de paquets…

La qualité de service est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau (en management du système d'information) ou d'un processus (en logistique) et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par applications (ou activités) suivant les protocoles mis en œuvre au niveau de la structure. Elle permet ainsi aux fournisseurs de services (départements réseaux des entreprises, opérateurs…) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leurs infrastructures IP.

La qualité de service se réalise au niveau de la couche 3 du modèle OSI. Elle doit donc être configurée sur les routeurs ou la passerelle reliée à Internet. Il existe deux types de paramètre de QoS : les paramètres dynamiques qui influent sur les mécanismes de l'application, et les paramètres statistiques qui n'influent pas sur son comportement dynamique.

	Paramètres dynamiques du QoS	Paramètres statistiques du QoS
vidéo	Nombre d'images /s Gigue vidéo max Nombre max de discontinuités	Dimensions de l'image Qualité de l'image
audio	Gigue audio max Nombre max de discontinuités	Qualité du son
synchronisation	Type de synchronisation Dérive inter flux max	
Retard de présentation	Délai max	

-Définition de la QoS utilisateur-

La QoS est négociée entre les deux interlocuteurs à l'établissement de la connexion. Cette négociation prend en compte, d'une part la qualité souhaitée par les utilisateurs (qui est fonction de leurs besoins mais qui peut aussi être fonction du cout de communication), et d'autre part de la puissance de traitement disponible sur la machine, la qualité des réseaux interconnectant les deux machines, et les formats d'échanges de données supportés par ces machines (généralement ces format dépendent des cartes multimédias qui équipent les stations). Si les deux interlocuteurs sont d'accord sur une QoS que peuvent assurer les deux machines et le réseau de communication, alors

la connexion est établie. Dans le cas contraire, l'application de visioconférence proposera aux utilisateurs une QoS plus faible qu'ils pourront accepter ou refuser.

a) Caractéristique :

Dans un réseau, les informations sont transmises sous la forme de paquets, petits éléments de transmission transmis de routeur en routeur jusqu'à la destination. Tous les traitements vont donc s'opérer sur ces paquets.

La mise en place de la qualité de service nécessite en premier lieu la reconnaissance des différents services. Celle-ci peut-se faire sur la base de nombreux critères :

- La source et la destination du paquet.
- Le protocole utilisé (UDP/TCP/ICMP/etc.).
- Les ports source et de destination dans le cas des protocoles TCP et UDP.
- La date et l'heure.
- La congestion des réseaux.
- La validité du routage (gestion des pannes dans un routage en cas de routes multiples par exemple).
- La bande passante consommée.
- Les temps de latence.

En fonction de ces critères, différentes stratégies peuvent ensuite être appliquées pour assurer une bonne qualité de service.

b) Ordonnancement :

La méthode par défaut gérant l'ordre de départ des paquets est définie selon le principe du "Premier arrivé, premier servi", ou FIFO "First In, First Out". Celle-ci n'appose aucune priorité sur les paquets, et ceux-ci sont transmis dans l'ordre où ils sont reçus. D'un point de vue technique, cette méthode est toujours utilisée par défaut sur les interfaces dont le débit est supérieur à 2 Mb/s. Sur les produits Cisco, il est possible de la configurer via la commande d'interface *tx-ring-limit*.

L'ordonnancement désigne l'ensemble des méthodes visant à modifier cet ordre, en remplacement de la règle précédente. Une de ses applications les plus courantes, le *Priority Queuing*, consistera ainsi à donner la priorité à certains types de trafic, de façon sommaire en ne laissant passer le trafic de faible priorité que s'il n'y a plus de trafic de forte priorité, ou de façon plus fine avec des algorithmes de *Round-Robin* pondérés (devenant alors le *Custom Queuing*), visant à faire passer des paquets des différentes connexions tour à tour, en laissant plus de temps aux paquets prioritaires.

Une autre application, le *Fair Queuing* consiste à séparer nettement les connexions, et à leur attribuer successivement et équitablement une possibilité de faire passer leurs paquets : cela permet de s'assurer qu'aucune application, même très demandeuse de débit, a ne pas écraser d'autres. Une version générale de cette application existe, le *Weighted Fair Queuing*. Cette généralisation est effectuée en multipliant la taille du paquet concerné par l'inverse du poids de la file dans laquelle il se trouve (le FQ en est un cas spécial dans le sens où les files ont toutes le même poids). Une dernière version existe, le *Class-Based Weighted Fair Queuing* (autrement appelée *Class-Based Queuing*) qui utilisera des classes configurées selon différents critères (priorité, interface, application d'origine, ...) en lieu et place des connexions du *Fair Queuing*. Chacune de ces classes se voit ainsi allouée une partie de la bande passante en fonction de leur priorité globale.

Une dernière application, appelée le *Low Latency Queuing* concentre son action sur le trafic sensible au délai. Il prend comme base le CBWFQ en rendant les priorités plus strictes. Cette méthode est particulièrement adaptée à l'usage de VOIP et de visiophonie.

c) Mise en forme du Trafic :

Mettre en forme un trafic (*Trafic shaping* en anglais) signifie prendre des dispositions pour s'assurer que le trafic ne dépasse jamais certaines valeurs prédéterminées. Pratiquement, cette contrainte s'applique en délayant certains paquets pour forcer un certain trafic, selon divers algorithmes.

Le contrôle du trafic peut-être utile pour limiter l'engorgement et assurer une latence correcte. Par ailleurs, des limitations de débits séparément aux trafics permettent en contrepartie de leur assurer en permanence un débit minimum, ce qui peut être particulièrement intéressant pour un fournisseur d'accès par exemple, souhaitant garantir une certaine valeur du débit à ses clients.

Les deux algorithmes les plus utilisés sont :

- Le seau percé (*Leaky bucket*).
- Le seau à jetons (*Token bucket*).

d) Ressources réseau :

Le réseau doit être en mesure de transmettre les paquets IP avec un taux de perte faible (environ 1%), un délai de transmission inférieur à 200ms et une gigue (variation du délai de transmission) inférieur à 30ms. Ces trois paramètres peuvent être respectés si les liaisons IP disposent d'une bande passante suffisante et si les équipements réseau sont fiables (cartes interface, routeurs, commutateurs, supports physiques,…).

A travers un réseau IP (campus, régional, Renater ou Internet), il convient d'effectuer des mesures avant de déployer un service de visioconférence. La première solution, effectuée par l'utilisateur, consiste à appeler son correspondant et à évaluer soi même la qualité de transmission. La seconde, à la charge de l'administrateur réseau, consiste à mesurer le taux de perte, le délai et la

gigue entre les sites. Il existe beaucoup d'outils de mesure, on citera deux exemples déployés à travers Internet : SAA Cisco et la matrice Beacon pour le multicast.

SAA (Service Assurance Agent) :

Disponible sur IOS Cisco. Il permet à des sites de Renater et des réseaux régionaux d'effectuer des mesures en continue et de construire des graphes de mesure MRTG à partir des OID SNMP Cisco .

Multicast Beacon :

Permet d'effectuer des mesures relatives aux multicast. Les topologies multicast et unicast sont très souvent congruentes (les mêmes). On peut en déduire que les résultats fournis par la matrice Beacon peuvent être interprétés aussi pour le trafic unicast.

Un service a été mis en place sur Renater pour permettre à des clients de participer aux mesures.

Les mesures fournissent des informations utiles mais ne résolvent par les problèmes actuels inhérents à l'Internet : le best effort, c'est à dire l'absence d'une garantie de qualité de service entre l'appelant et l'appelé. Les réseaux académiques et recherche comme Renater, Géant, Internet2, disposent maintenant d'une certaine qualité de service : over-provisionning (sur débit). Les liaisons IP disposent de débits importants (Gigabit/s) permettant en général de respecter les critères relatifs aux délais et taux de pertes de paquets. Concernant l'Internet commercial et le raccordement des sites, la situation est très différente et diversifiée. Les liaisons ne sont pas toujours adaptées (raisons économiques), des congestions peuvent survenir entraînant une dégradation de la qualité de transmission. Afin de respecter les critères de qualité, une solution consiste à implémenter des mécanismes basés sur la différentiation des flux (Diff-Serv) .

Diff-serv :

Lors de la congestion d'une liaison, Diff-Serv différentie et donne une priorité aux flux identifiés et classifiés (par exemple marquage du champ TOS : Type Of Service). Il existe peu d'implémentation de classe de service aujourd'hui sur les réseaux IP.

En Europe, sur Géant, un service a été déployé, le service Premium IP.

Des expérimentations et services ont démarré sur des sites de Renater :

- Le projet du réseau régional Lothaire sur la mise en oeuvre de la QoS pour la téléphonie sur IP.
- L'expérimentation à travers Renater entre les réseaux régionaux Lothaire, Noropale, Vikman, Picardie et Syrhano.

Comme France Télécom dispose d'une offre de service CoS IP, et certains réseaux régionaux en bénéficient. Trois différenciations de flux ont été définies :

Prioritaire : réservé pour la voix sur IP ou la visioconférence, le champ ToS doit être marqué à 3,4 ou 5. En cas de congestion, 60% de la bande passante est réservée pour ces flux.

Privilège : réservé pour des données prioritaires, le champ ToS est marqué à 1 ou 2. En cas de congestion, 30% de la bande passante est réservée.

Standard : pour les autres flux, sans priorité, qui utilisent le reste de la bande passante.

Il n'y a pas de difficulté technique à mettre en œuvre la QoS, par contre l'activation nécessite de disposer de routeurs adaptés en CPU.

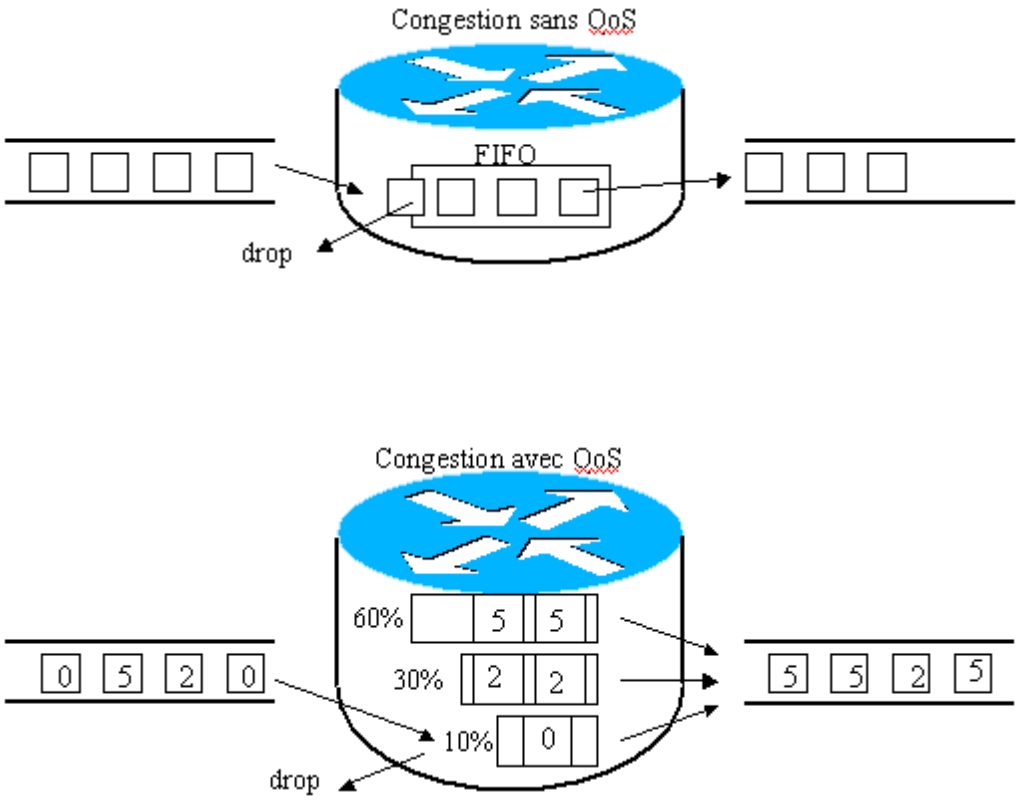


Figure 3.1 : Principe des classes de service

Les opérateurs de réseau sont capables de fournir un service de Classe de Service à leurs clients. La différentiation des flux ne concerne que les paquets en provenance et à destination du même réseau de collecte. Tous les paquets en provenance de l'Internet ne peuvent pas être privilégiés. La politique de marquage est donc propre à un seul client ou entreprise, en l'occurrence pour nous le réseau régional. Chaque site se doit de respecter une charte pour le réseau régional et ne pas privilégier des flux qui ne doivent pas l'être. Si on considère que la majorité des flux d'un réseau régional provient de Renater, un tel service a très peu d'intérêt. Les flux issus d'une visioconférence en provenance de Renater doivent être remarqués à zéro. Ces flux ne sont donc pas prioritaires. Pour réussir à mettre en œuvre la Qualité de service à travers Renater, et d'autres réseaux d'opérateur, il faudrait que tous les opérateurs et les sites concernés adoptent une même convention sur le marquage des paquets (par exemple celle du service IP Premium de Géant) et respectent une charte commune.

e) Les problèmes rencontré :

1- Latence

La maîtrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho (similaire aux désagréments causés par les conversations par satellites, désormais largement remplacés par les câbles pour ce type d'usage).

Or la durée de traversée d'un réseau IP dépend de nombreux facteurs:

- Le débit de transmission sur chaque lien.
- Le nombre d'éléments réseaux traversés.
- Le temps de traversée de chaque élément, qui est lui même fonction de la puissance et la charge de ce dernier, du temps de mise en file d'attente des paquets, et du temps d'accès en sortie de l'élément.
- Le délai de propagation de l'information, qui est non négligeable si on communique à l'opposé de la terre. Une transmission par fibre optique, à l'opposé de la terre, dure environ 70 ms.

Noter que le temps de transport de l'information n'est pas le seul facteur responsable de la durée totale de traitement . Le temps de codage et la mise en paquet de la voix contribuent aussi de manière importante à ce délai.

Il est important de rappeler que sur les réseaux IP actuels (sans mécanisme de garantie de qualité de service), chaque paquet IP « fait son chemin » indépendamment des paquets qui le précèdent ou le suivent: c'est ce qu'on appelle grossièrement le « Best effort » pour signifier que le réseau ne contrôle rien. Ce fonctionnement est fondamentalement différent de celui du réseau téléphonique où un circuit est établi pendant toute la durée de la communication.

Les chiffres suivants (tirés de la recommandation UIT-T G114) sont donnés à titre indicatif pour préciser les classes de qualité et d'interactivité en fonction du retard de transmission dans une conversation téléphonique. Ces chiffres concernent le délai total de traitement, et pas uniquement le temps de transmission de l'information sur le réseau.

Classe n°	Délai par sens	Commentaires
1	**0 à 150 ms**	**Acceptable pour la plupart des conversations**
2	**150 à 300 ms**	**Acceptable pour des communications faiblement interactives**
3	**300 à 700 ms**	**Devient pratiquement une communication half duplex**
4	**Au delà de 700 ms**	**Inutilisable sans une bonne pratique de la conversation half duplex**

En conclusion, on considère généralement que la limite supérieure "acceptable" , pour une communication téléphonique, se situe entre 150 et 200 ms par sens de transmission (en considérant à la fois le traitement de la voix et le délai d'acheminement).

2- Perte de paquets

Lorsque les buffers des différents élément réseaux IP sont congestionnés, ils « libèrent » automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrant, en fonction de seuils prédéfinis. Cela permet également d'envoyer un signal implicite aux terminaux TCP qui diminuent d'autant leur débit au vu des acquittements négatifs émis par le destinataire qui ne reçoit plus les paquets. Malheureusement, pour les paquets de voix, qui sont véhiculés au dessus d'UDP, aucun mécanisme de contrôle de flux ou de retransmission des paquets perdus n'est offert au niveau du transport. D'où l'importance des protocoles RTP et RTCP qui permettent de déterminer le taux de perte de paquet, et d'agir en conséquence au niveau applicatif.

Si aucun mécanisme performant de récupération des paquets perdus n'est mis en place (cas le plus fréquent dans les équipements actuels), alors la perte de paquet IP se traduit par des ruptures au niveau de la conversation et une impression de hachure de la parole. Cette dégradation est bien sûr accentuée si chaque paquet contient un long temps de parole (plusieurs trames de voix de paquet). Par ailleurs, les codeurs à très faible débit sont généralement plus sensibles à la perte d'information, et mettent plus de temps à « reconstruire » un codage fidèle.

Enfin connaître le pourcentage de perte de paquets sur une liaison n'est pas suffisant pour déterminer la qualité de la voix que l'on peut espérer, mais cela donne une bonne approximation. En effet, un autre facteur essentiel intervient; il s'agit du modèle de répartition de cette perte de paquets, qui peut être soit « régulièrement » répartie, soit répartie de manière corrélée, c'est à dire

avec des pics de perte lors des phases de congestion, suivies de phases moins dégradées en terme de QoS.

3- Gigue

La gigue est la variance statistique du délai de transmission. En d'autres termes, elle mesure la variation temporelle entre le moment où deux paquets auraient dû arriver et le moment de leur arrivée effective. Cette irrégularité d'arrivée des paquets est due à de multiples raisons dont: l'encapsulation des paquets IP dans les protocoles supportés, la charge du réseau à un instant donné, la variation des chemins empruntés dans le réseau, etc…

Pour compenser la gigue, on utilise généralement des mémoires tampon (buffer de gigue) qui permettent de lisser l'irrégularité des paquets. Malheureusement ces paquets présentent l'inconvénient de rallonger d'autant le temps de traversée global du système. Leur taille doit donc être soigneusement définie, et si possible adaptée de manière dynamique aux conditions du réseau.

La dégradation de la qualité de service due à la présence de gigue, se traduit en fait, par une combinaison des deux facteurs cités précédemment: le délai et la perte de paquets; puisque d'une part on introduit un délai supplémentaire de traitement (buffer de gigue) lorsque l'on décide d'attendre les paquets qui arrivent en retard, et que d'autre part on finit tout de même par perdre certains paquets lorsque ceux-ci ont un retard qui dépasse le délai maximum autorisé par le buffer.

Ainsi, les 2 problèmes majeure sont :

Le premier problème provient des pertes qui sont occasionnées par le support de communication. Ces pertes peuvent vraisemblablement être acceptées si elle restent exceptionnelles, toute fois , ces pertes sont souvent la source de fortes dégradations de la qualité de présentation de l'application , et a chaque perte engendre beaucoup plus qu'une simple discontinuité ; si une donnée est perdu par le réseau et si cette perte est tolérable par rapport à la qualité de service demandée par l'utilisateur, alors cette perte va conduire à une duplication de la donnée précédente, ce qui d'un point de vue présentation correspond à une discontinuité. Cependant , avec les algorithmes de présentation, comme les processus de présentation ne peuvent pas déterminer si cette donnée à été perdue ou si elle a seulement été retardée, ils attendent au maximum avant de lancer le traitement exceptionnel correspondant à une donnée perdue ou trop retardée. Ainsi , l'application n'a pas pu recouvrir l'erreur engendrée par la perte, et elle a de plus perdu du temps à attendre la donnée a traiter. A cause de cette perte de temps, ou à l'accumulation de ce type de pertes de temps, le retard de présentation de bout en bout augmente, ce qui peut conduire à l'intervention du mécanisme de contrôle du retard par perte, et peut donc provoquer de nouvelles pertes.

Le second problème est également un problème lié à des prises de retard, mais cette fois-ci au cours de la présentation des objets de l'un des flux audio ou vidéo. En effet, le paragraphe ci-

dessus montre combien les retard peuvent être préjudiciables à la qualité de présentation de l'application. Aussi , il faut éviter au maximum que les temps de présentation des objets dépassent leur temps, ou du moins faire en sorte qu'en moyenne, les temps de présentation des données soient égaux à leur temps.

f) Solution

Pour palier à ces problèmes, il faut pouvoir détecter au plus tôt les pertes, et cette détection ne peut être faite qu'au niveau du support de communication. Ainsi , si les pertes sont détectées au plus tôt , cela permettra au processus de présentation de l'application de réaliser le traitement exceptionnel correspondant à une perte sans attendre, et ainsi de ne pas perdre de temps, et donc de ne pas risquer de provoquer d'autre pertes par des mécanismes annexes. De même , comme la partie non déterministe de temps de traitement des processus de présentation consiste à attendre la délivrance de l'objet suivant, si le support de communication assure une délivrance au plus tot des objets reçus, cela permettra des gains temporels intéressants, car les processus de présentation ont toutes les chances de s'exécuter en un temps compris entre le temps minimal et nominale, et aucun retard ne sera pris par l'application par rapport à son scénario de synchronisation idéal.

En fait, la délivrance des objets et la détection des pertes au plus tôt doivent permettre d'améliorer la qualité de présentation des flux multimédias, car elles permettent d'optimiser l'utilisation de la ressource temporelle pour un scénario de synchronisation. Elles évitent donc que le mécanisme annexes pour le contrôle du retard et l'accélération de flux ne se mettent en marche. Ces deux mécanismes ne doivent être utilisés qu'en dernier ressort, par exemple lorsque la charge machine est élevée, au point de ne plus permettre à l'application de s'exécuter ; l'utilisation de ces deux mécanismes qui nuit à la qualité de la présentation finale de l'application doit rester exceptionnelle .

Une solution basée sur un transport à ordre partiel : plusieurs organismes internationaux (AME94a , CHA95a, CHA95b, DIA95) définissent un nouveau protocole de transport à ordre partiel comme un transport ayant pour but de délivrer à l'utilisateur les objets transitant sur une ou plusieurs connexions, en respectant un ordre donnée. Cet ordre est n'importe quel ordre compris entre un ordre total (TCP) et le non ordre (UDP), et il peut s'exprimer, en particulier, sous la forme de compositions séries et/ou parallèles des objets à transmettre. Il s'avère alors qu'un tel ordre peut en particulier être celui décrit par l'automate du TSPN de l'application (DIA94c). Ainsi (AME94a, CHA95a, CHA95b, DIA95) définissent cette délivrance suivant un ordre prédéfini comme une synchronisation logique définie par les informations multimédias.

De plus, cette nouvelle notion d'ordre partiel est complémentée par la notion de la fiabilité partielle. Par rapport aux problèmes rencontrés, la notion de fiabilité partielle est essentielle, car cette notion est étroitement liée à la notion de qualité de service transport qui définit une qualité de service nominale, et une qualité de service minimale en dessous de laquelle le service demandé par l'utilisateur ne sera plus rendu. Par rapport a la notion de fiabilité, cette qualité de service minimale peut s'exprimer par un nombre maximal de pertes sur une séquence, et par un nombre maximal de pertes consécutives. Ainsi , en cas de perte acceptable, détectée lors de la réception d'un objet ordonné logiquement après l'objet attendu, l'objet initialement attendu est déclaré perdu au plus tôt

(aucun essai de recouvrement n'est initié), et l'objet qui vient de parvenir à l'entité transport réceptrice est délivré à l'utilisateur le plus rapidement. Si par contre la perte n'est pas acceptable par rapport à la fiabilité définie par l'utilisateur, un certain nombre de retransmission peuvent être essayées, ce nombre de retransmissions pouvant être paramétré. Tout objet reçu par l'entité transport réceptrice est donc délivré au plus tôt en accord avec l'ordre et la fiabilité partielle ; si cet objet n'est pas dé livrable au regard de l'ordre partiel, il est vraisemblable qu'un problème a perturbé les objets qui le précèdent logiquement, et donc, si au regard de la fiabilité partielle les objets manquants peuvent être perdus, alors ils seront considérés comme perdus, et l'objet reçu ne sera pas retardé.

III. Bande Passante

La bande passante est définie comme la quantité d'informations qui peut transiter sur une connexion réseau en un temps donné. Il est important de comprendre le concept de bande passante pour les raisons suivantes.

La bande passante est finie. Quel que soit le média qui est utilisé pour construire un réseau, il y a des limites à la capacité du réseau à transporter des informations. La bande passante est limitée par les lois de la physique et aussi par les technologies utilisées pour placer des informations sur le média. Par exemple, la bande passante d'un modem conventionnel est limitée à environ 56 kbits/s, à la fois par les propriétés physiques des fils téléphoniques à paires torsadées et par la technologie du modem. La technologie DSL utilise les mêmes fils téléphoniques à paires torsadées. Cependant, elle délivre bien plus de bande passante que les modems conventionnels. Ainsi, même les limites imposées par les lois de la physique sont quelques fois difficiles à définir. La fibre optique possède le potentiel physique pour fournir une bande passante pratiquement illimitée. Malgré cela, la bande passante de la fibre optique ne pourra être pleinement exploitée avant que des technologies ne soient développées pour tirer pleinement parti de son potentiel.

La bande passante n'est pas gratuite. Il est possible d'acquérir des équipements pour un réseau local qui fourniront une bande passante quasiment illimitée sur une longue période. Pour les connexions WAN, il est généralement nécessaire d'acquérir de la bande passante auprès d'un fournisseur de services. Dans un cas comme dans l'autre, l'utilisateur individuel ou l'entreprise pourra faire des économies significatives en comprenant bien la notion de bande passante et l'évolution de la demande avec le temps. L'administrateur doit prendre les bonnes décisions sur les types d'équipement et de services à acheter.

La bande passante est un facteur important qui est indispensable pour analyser les performances du réseau, concevoir de nouveaux réseaux et comprendre Internet. Un professionnel des réseaux doit comprendre l'impact considérable de la bande passante et du débit sur la performance et la conception du réseau. Les informations circulent sous forme de chaîne de bits d'un ordinateur à l'autre à travers le monde. Ces bits constituent des quantités énormes d'informations qui transitent d'un bout à l'autre de la planète en quelques secondes à peine.

La demande en bande passante ne cesse de croître. Dès que des nouvelles technologies et infrastructures de réseau sont créées pour fournir une bande passante plus large, on voit apparaître de nouvelles applications qui tirent parti de cette capacité supérieure. La remise sur un réseau de contenus multimédias tels que la vidéo et l'audio en continu nécessite une quantité considérable de bande passante. Les systèmes de téléphonie IP sont à présent installés couramment à la place de systèmes vocaux traditionnels, ce qui augmente encore le besoin en bande passante. Tout professionnel de réseau digne de ce nom doit anticiper le besoin en bande passante accrue et agir en conséquence.

Exemples de bandes passantes

- Signal téléphonique : [300Hz - 3400Hz]
- Signal de télévision PAL pour 1 canal : [6Mhz]
- Signal de télévision SÉCAM pour 1 canal : [8Mhz]

Optimiser le WAN ou augmenter la bande passante

Les entreprises dont les sites géographiques sont dispersés doivent souvent faire face à une infrastructure informatique lente. Pour remédier à ce problème, deux possibilités s'offrent aux responsables informatiques: optimiser le réseau étendu, le WAN ou augmenter la bande passante.

Le fait que les entreprises soient par nature constituées de plusieurs sites a rendu complexe la gestion et l'accès aux fichiers et aux applications Quelle que soit sa taille, une entreprise dont les sites sont géographiquement distribués utilise de plus en plus les réseaux étendus (Wide Area Networks, ou WAN) pour donner à ses employés l'accès aux données. Toutefois, l'accès à ces données à travers le WAN se traduit souvent par des performances médiocres, ce qui impacte la productivité et mécontente les employés.

Lorsque les utilisateurs se plaignent d'applications léthargiques, la réponse de l'entreprise est souvent d'augmenter la bande passante des liaisons WAN. Mais les directeurs informatiques s'aperçoivent souvent qu'au lieu d'arranger les choses, le fait d'augmenter la bande passante des sites distants n'a que peu ou pas d'effet sur les performances. En effet, le problème vient bien souvent de la latence et du manque d'efficacité de l'utilisation des protocoles à travers le WAN.

Les vraies causes des problèmes de performance des applications via le WAN

En général, les connexions WAN ont une bande passante plus faible et une latence plus importante que les liaisons LAN (Local Area Networks, ou réseaux locaux). Comment ces contraintes affectent-elles les performances des applications ? Il existe quatre types de goulot d'étranglement : l'un est lié à la bande passante, les trois autres à la latence. Le premier est évident : il est impossible d'envoyer des données plus rapidement que ce que ne l'autorise la bande passante disponible. Les trois autres sont plus subtils et ne deviennent évidents que si la bande passante n'est pas une

contrainte : à cause des trois problèmes de latence, les applications ne parviennent pas à utiliser toute la bande passante disponible, même lorsqu'elle paraît largement suffisante.

Le premier problème de latence découle des accusés de réception du protocole TCP (Protocole de Contrôle de Transmission). Celui-ci utilise une fenêtre de paquets qui peuvent être en cours de transmission d'un bout à l'autre de la liaison (c'est-à-dire entre le client et le serveur). Lorsque la fenêtre est pleine, l'émetteur n'envoie pas de paquets supplémentaires tant que le récepteur n'accuse pas réception d'au moins une partie des paquets déjà envoyés. Si la fenêtre maximale est trop petite, le débit de la liaison peut être limité par la vitesse à laquelle chaque fenêtre pleine peut être envoyée et validée par l'autre extrémité.

Le second problème de latence est provoqué par l'algorithme de démarrage lent de TCP et par son mode de contrôle de la congestion. Nous avons vu que le problème de latence est lié à la taille maximale autorisée pour la fenêtre. Le deuxième tient à ce que le TCP n'utilise pas en permanence cette taille maximale (probablement car elle est inadaptée). En effet, le TCP augmente progressivement la taille de sa fenêtre lorsque la transmission semble se dérouler correctement, et la réduit subitement lorsqu'elle semble échouer. Sur un réseau avec une bande passante confortable mais avec une latence élevée, ce comportement entraîne de longues périodes pendant lesquelles une bonne partie de la bande passante disponible reste inutilisée. Toutefois, ce problème ne concerne principalement que ceux qui tentent de remplir de tels réseaux (nommés LFN, à latence et bande passante élevés).

Le troisième problème lié à la latence est dû aux protocoles des applications, qui fonctionnent au-dessus de TCP. Rappelons que pour le premier problème lié à la latence, la bande passante disponible n'était pas vraiment une limitation si le TCP était déjà limité par la taille de la fenêtre de données et la nécessité d'accuser réception. De même, il n'est pas utile de s'inquiéter de la bande passante disponible et des deux premiers problèmes liés à la latence (qui interviennent au niveau du TCP) si l'on est limité au niveau de la couche application par la taille des messages et par la nécessité d'accuser réception ou de répondre à ces données. Les protocoles applicatifs conçus d'emblée pour fonctionner via le WAN (comme HTTP et FTP) ne rencontrent généralement pas ce troisième type de problème de latence. À l'inverse, les protocoles d'application conçus à l'origine pour les réseaux locaux, comme le partage de fichiers Microsoft Windows via CIFS, sont souvent gravement affectés.

Réduire les goulots d'étranglement grâce à l'optimisation du WAN

Les solutions d'optimisation du WAN peuvent appliquer diverses approches pour réduire les goulots d'étranglement. Elles peuvent réduire la quantité de données, mettre en cache les données, les fichiers et les e-mails, éviter la réplication, optimiser le TCP, utiliser la qualité de service (QoS), compresser le réseau et utiliser l'accélération SSL. Cependant, chacune de ces approches n'est efficace que pour un éventail réduit de protocoles. Par exemple, la mise en cache remédie à la latence des applications mais pas à celle de TCP. Il faut donc envisager une solution d'optimisation du WAN qui associe plusieurs approches, pour déboucher simultanément plusieurs types de goulots d'étranglement.

La mise en œuvre d'une solution d'optimisation du WAN couvrant de nombreux protocoles, configurations et applications garantit de tirer au mieux les partis des réseaux, des infrastructures et

des applications. Cette approche en couches améliore les performances des applications fonctionnant au-dessus de TCP, mais en outre, elle applique des modules spécifiques à chaque application pour éliminer les inconvénients liés aux protocoles « bavards ». L'utilisation de solutions d'optimisation du WAN accélère généralement les applications d'un facteur 50, voire 100 dans certains cas, tout en réduisant de 65 à 95% la bande passante utilisée.

Ainsi, le réseau WAN en place peut servir bien plus d'utilisateurs et accepter de nouvelles applications, et l'entreprise peut éviter ou retarder la mise à niveau coûteuse de la bande passante, parfois jusqu'à cinq ans. Pour cela, il faut bien comprendre les quatre goulots d'étranglement du WAN décrits ci-dessus et savoir y remédier. Enfin, en investissant dans une solution d'optimisation du

WAN, une entreprise peut réaliser d'autres économies importantes :

- **Consolider l'infrastructure dans le centre de données** : en supprimant des bureaux distants une grande partie de l'infrastructure informatique (serveurs de fichiers, de courrier, de SMS et SharePoint, unités à bande, NAS et systèmes de sauvegarde en local), sans réduire les performances des applications.

- **Optimiser la reprise après sinistre** : en améliorant les performances d'un site de reprise, conduisant à des économies et à des sauvegardes plus fréquentes et plus fiables.

- **Renforcer la collaboration** : car les employés peuvent partager des fichiers volumineux où qu'ils soient, devenant ainsi plus productifs.

- **Améliorer les objectifs de point de reprise** : grâce aux sauvegardes et réplications possibles dans des délais plus courts via des liaisons WAN à longue distance, donc dans des fenêtres auparavant inaccessibles.

L'optimisation du WAN est ainsi un outil essentiel pour les entreprises distribuées. Elle permet de réduire le trafic circulant via le WAN, d'améliorer considérablement les performances des applications, de consolider l'infrastructure informatique, et de mettre en œuvre des initiatives de sauvegarde et de reprise. De nombreuses entreprises ont ainsi pu tirer le meilleur parti de leur infrastructure en place, évitant de procéder à des mises à niveau coûteuses de la bande passante.

Accélérer le trafic tout en garantissant la performance des applications critiques , sur les réseaux longue distance et les sites limités en bande passante, la fonction d'optimisation du WAN d'Ipanema réduit au minimum l'impact du délai de transfert sur la performance des applications générant beaucoup de trafic comme le protocole CIFS (Common Internet File System). Cette optimisation du WAN permet d'augmenter la bande passante disponible et de réduire ainsi le temps de transfert des applications.

L'optimisation du WAN réduit les temps de réponse, ce qui améliore la qualité d'expérience (QoE) délivrée aux utilisateurs. Elle associe plusieurs techniques dont des mécanismes de suppression des redondances (appelée également compression, cache de flux ou déduplication), d'accélération TCP et d'accélération des applications (avec notamment une procédure spécifique d'optimisation du protocole CIFS). L'optimisation du WAN est appliquée de manière dynamique dans le cadre des fonctions de QoS & contrôle afin d'attribuer prioritairement de la performance aux applications les plus critiques, définies par les objectifs de performance applicative.

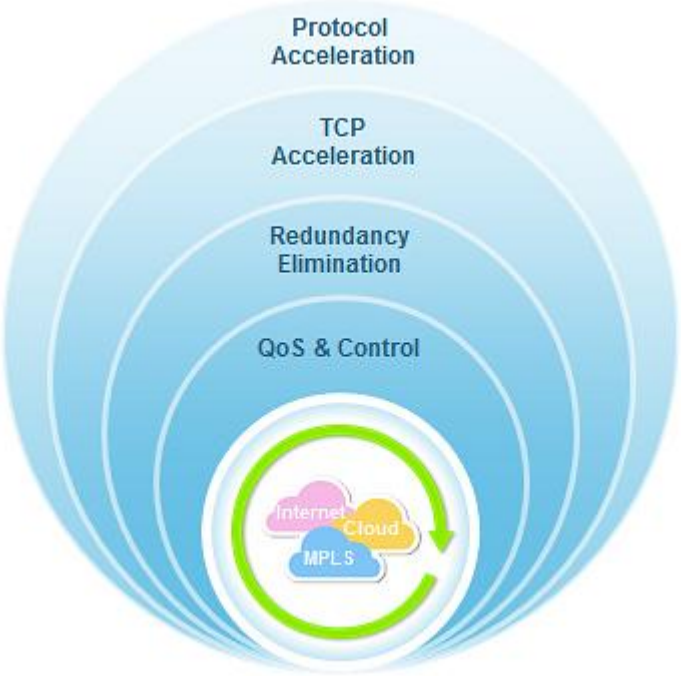


Figure 3.2 : Principe d'optimisation de la bande passante

L'approche d'Ipanema en matière d'optimisation du WAN avec l'ANS est :

Contrôlée : La fonction d'optimisation du WAN est étroitement intégrée à celle de QoS & contrôle. Cela évite que l'accélération des applications ne crée un engorgement qui perturbe les applications critiques et protège par là même les autres applications telles que la voix et la télé présence. De plus, la « bande passante virtuelle » créée par l'optimisation du WAN est allouée en fonction des priorités métier (pas forcément pour l'application qui a été mise en cache/compressée), ce qui renforce l'efficience business.

Transparente pour l'infrastructure IT et le réseau : L'optimisation du WAN d'Ipanema est entièrement transparente et n'exige aucune modification de la configuration de l'infrastructure IT ou des mécanismes de réseau (comme les classes de service MPLS).

Transposable à toutes les applications : L'optimisation du WAN porte sur les trois principaux points de blocage (la bande passante, le protocole TCP et le protocole applicatif) entraînant une dégradation de la performance des applications. Elle prend en charge tous les types d'applications : temps réel, transactionnelles et transfert de données.

À la carte/modulaire : La fonction d'optimisation du WAN doit être uniquement déployée à bon escient et non sur des sites bénéficiant déjà d'un accès à haut débit et de délais de transferts courts.

IV. Conclusion

Nous venons de voir les différents problèmes du QoS qui se résument à la perte de paquet qui est due au réseau IP congestionné, également à la prise de retard pour cause, d'encapsulation des paquets IP, ainsi qu'à la charge de réseau à un instant donné. La solution proposée est un transport de données à ordre partiel. Pour la bande passante la proposition faite pour son amélioration est l'optimisation du WAN.

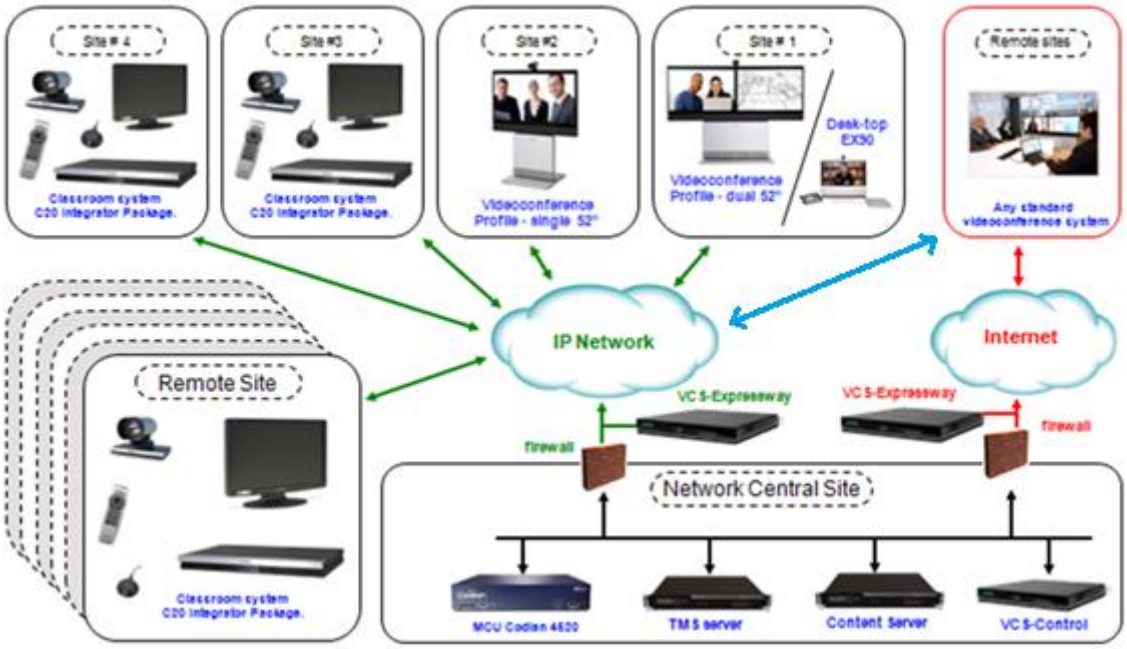
Chapitre 4 : Réalisation

Introduction

Dans tous les chapitres précédents nous avons vu les différents équipements ainsi que les moyens mis en œuvre pour avoir une plateforme visioconférence . Maintenant nous allons voir la partie pratique de ce projet qui se résume a créer un compte visant l'établissement d'un contact par le biais d'une visioconférence et cela grâce au logiciel spécifique de Cisco connu sous le nom de « Jabber Video » .

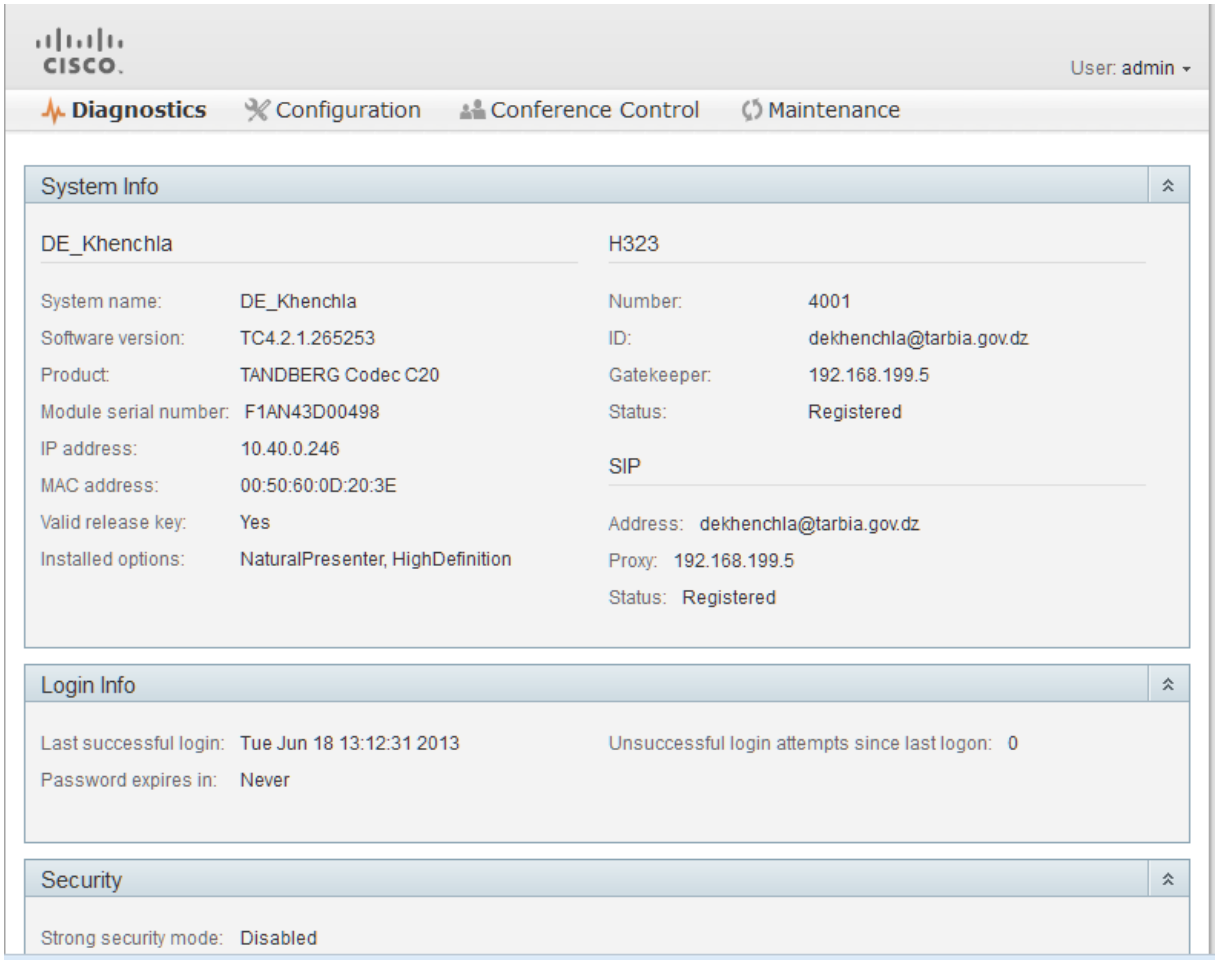
1- Architecture

Dans cette image nous avons représenté l'architecture globale du réseau pour effectuer des appels visio :



2- Paramètres du codec (CAMERA) :

En 1er lieu avant d'espérer faire un appel vidéo ou une conférence il faudra configurer le codec et cela que ce soit en H323 ou en SIP, et cela en attribuant un numéro d'appel et un identifiant pour le codec comme montré ci après :



3- Configuration du codec en H323

Pour la configuration du codec en H323, il faudra déjà donner l'identité du codec a configurer puis son digit , et préciser le chemin à suivre et cela en donnant l'adresse de gatekeeper central.

4- Configuration du codec en SIP

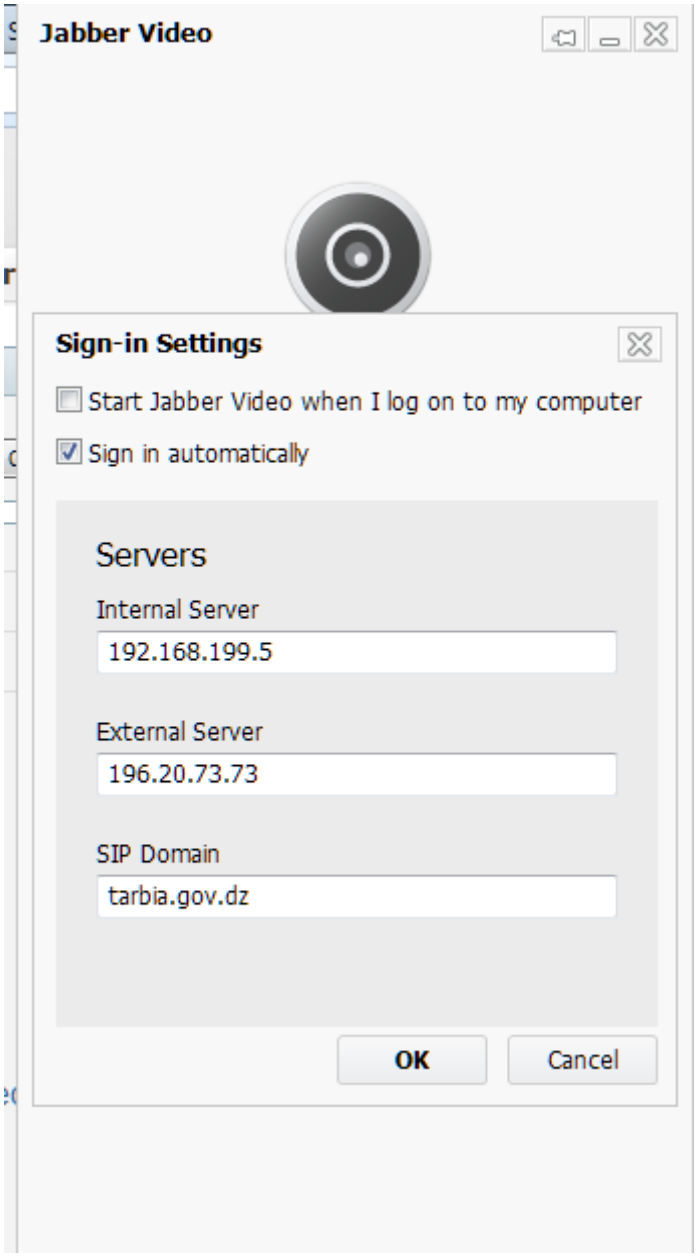
Pour la configuration en SIP, cela se fera de la même façon que pour le H323 sauf que pour le SIP, il n' y aura pas de digit car le SIP ne fonctionne qu' avec des noms de domaine comme on peut le voir ici en URI1, et aussi avec le nom de l'utilisateur.

5- Configuration du codec en mode conférence (H323 ou SIP) :

Configuration en mode conférence, cela se fait en précisant la taille de données à transmettre et à recevoir comme on le voit ci-dessous . Nous devrons préciser également le mode de protocole à utilisé. La bande passante ayant une relation avec la qualité HD devra être fixée .

6- Configuration du Movi en SIP :

Pour une éventuelle visioconférence à partir d'un ordinateur on utilisera ce que l'on appelle un movi qui est un logiciel défini pour cette utilité. Nous utiliserons un movi nommé Jabber Video conçu par CISCO. Une fois installé il faudra le configurer pour pouvoir l'utiliser, et cela on lui indiquant les chemins à suivre que ce soit en national ou international .

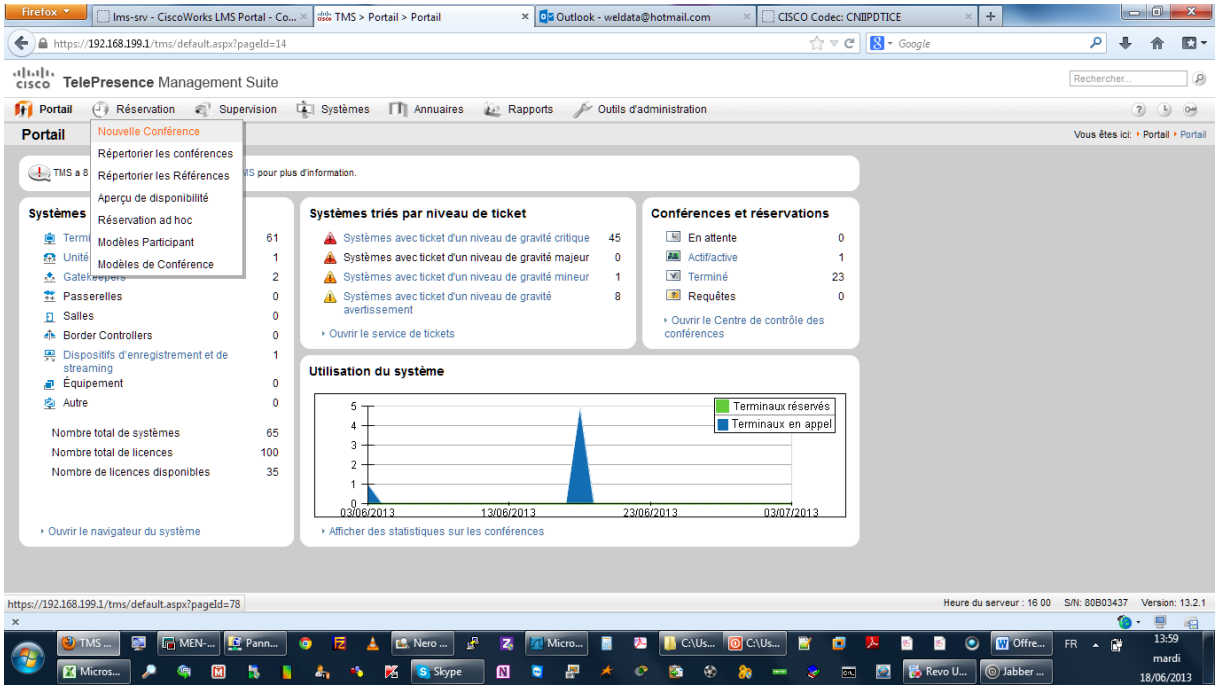


Une fois la configuration terminée, il faudra créer un compte de conférence, et cela ce fait à partir de cette adresse IP : 192.168.199.1

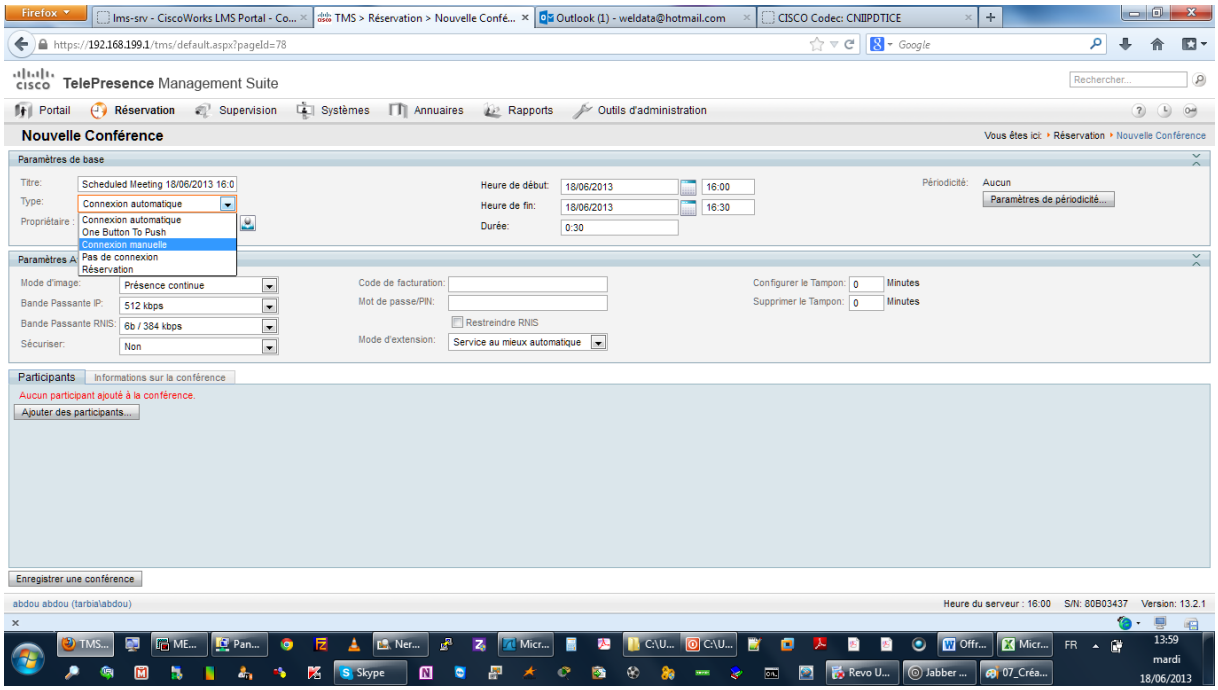
7- Création d'une conférence :

La création de compte terminée, nous pouvons maintenant créer une conférence comme suit :

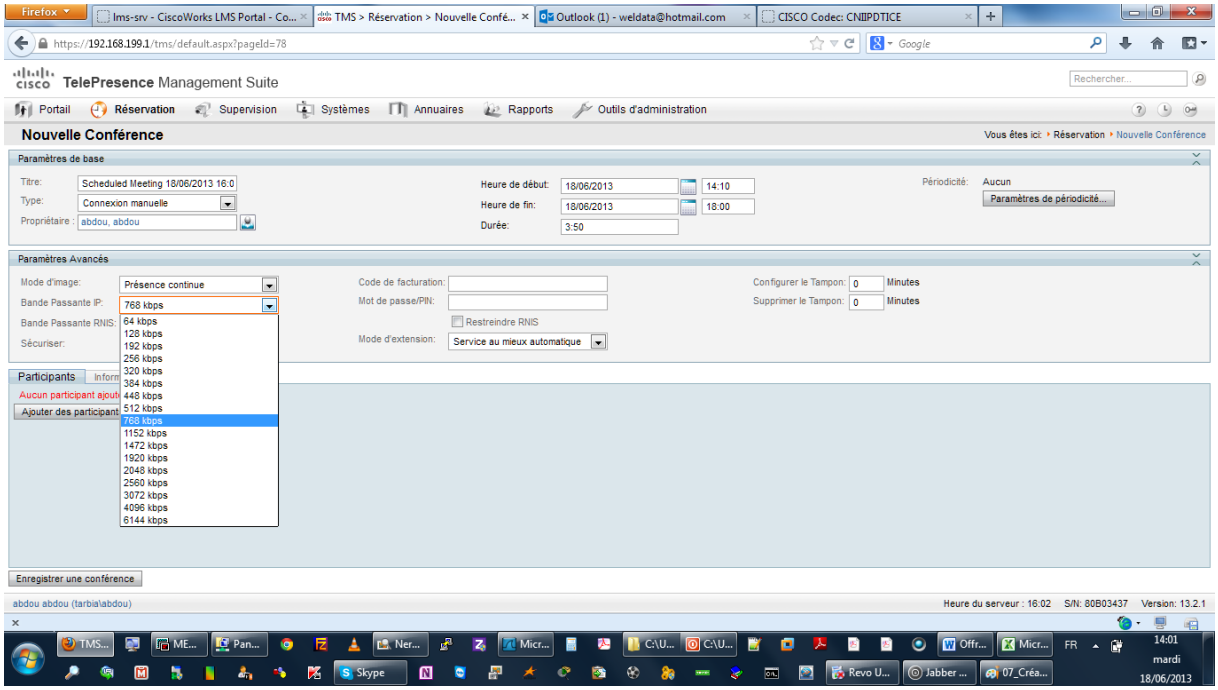
- Réservation de conférence.
- Nouvelle conférence.



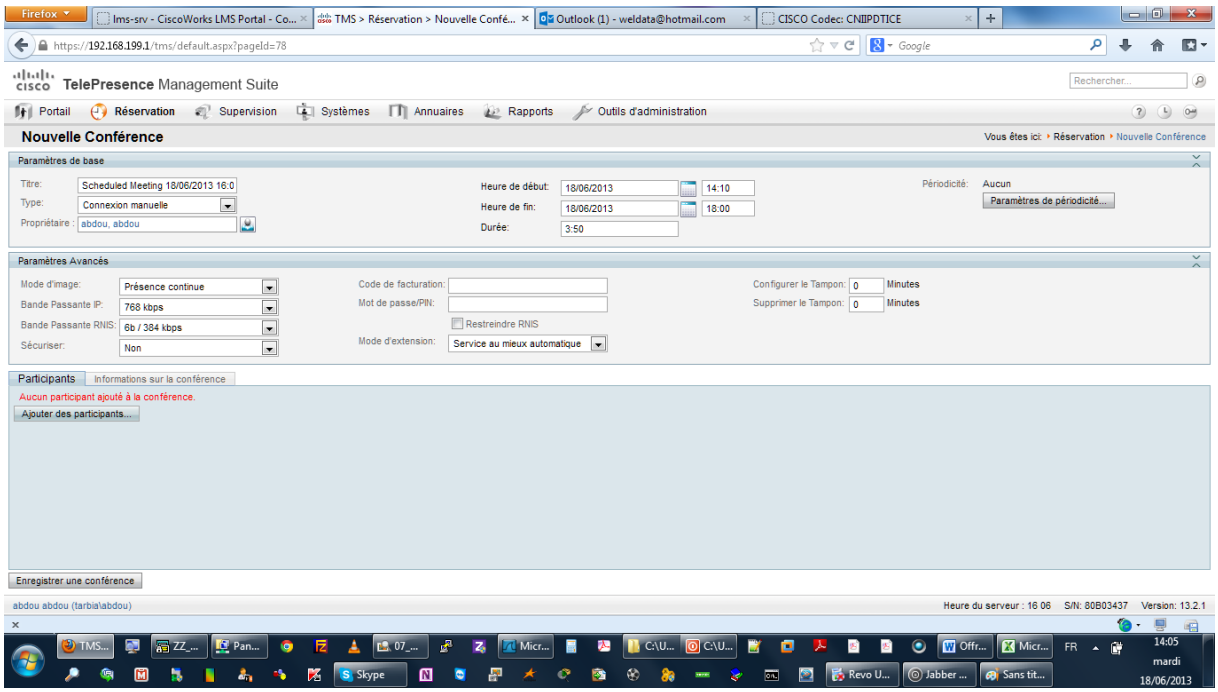
- Type de connexion : manuelle.



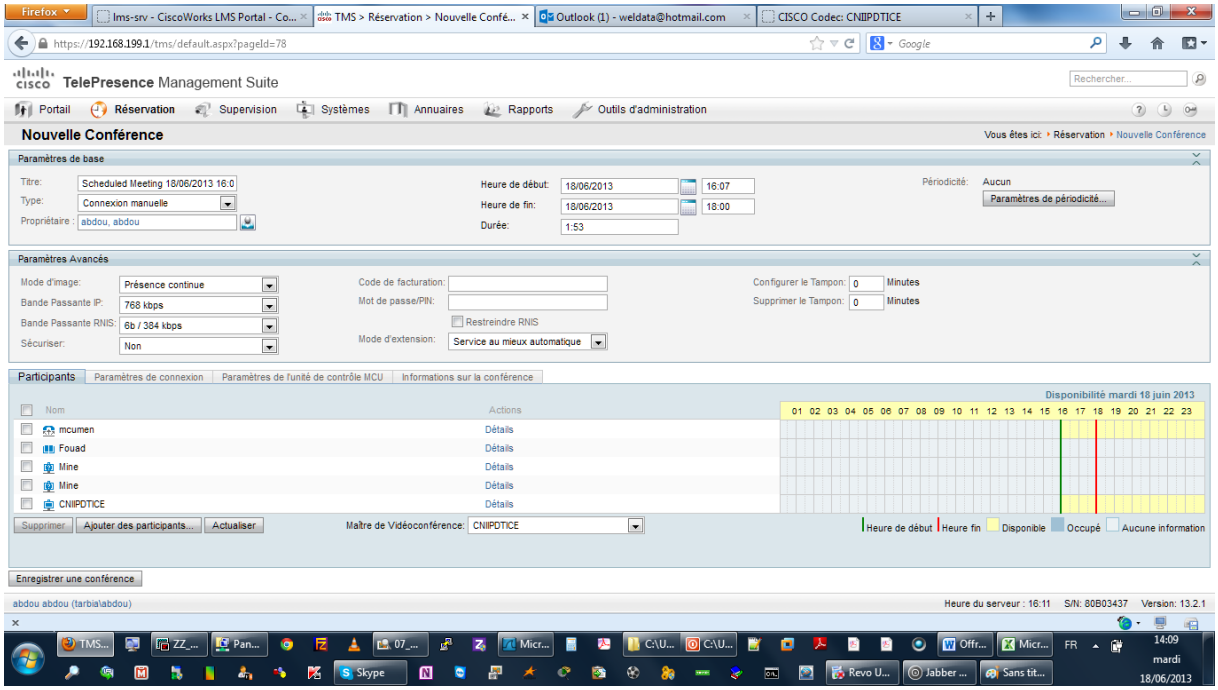
- On prédéfini la bande passante de notre conférence .



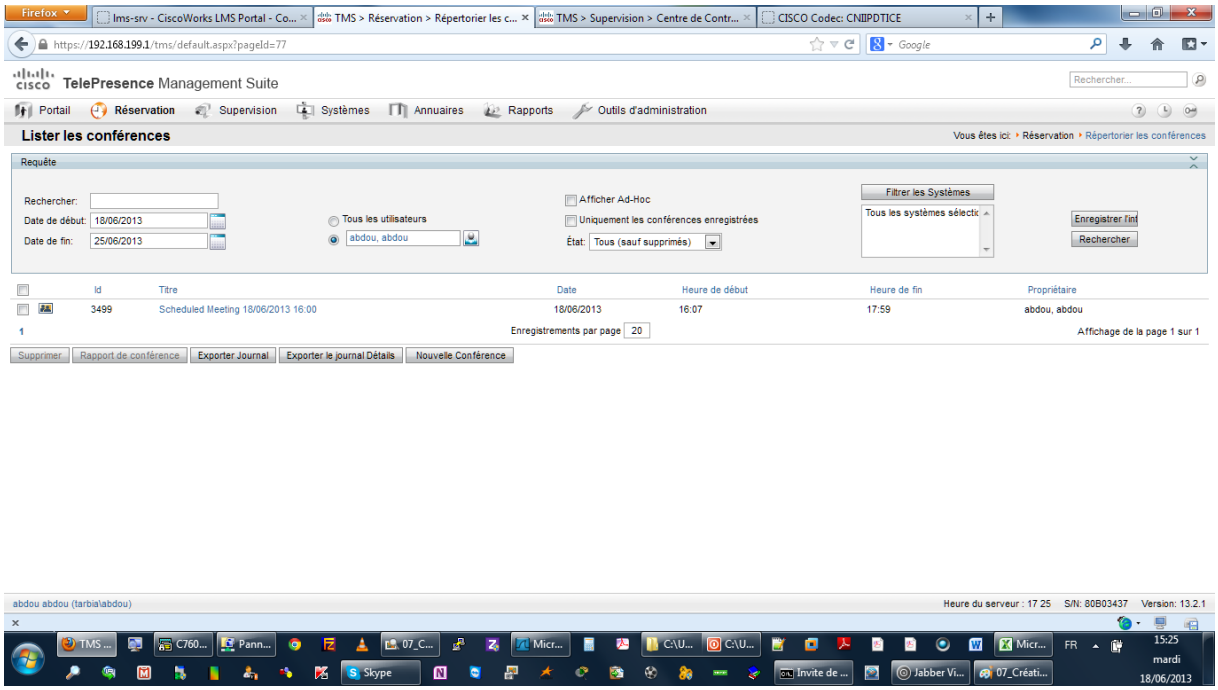
Une fois la création de la conférence terminée nous devons ajouter des participants à cette conférence.



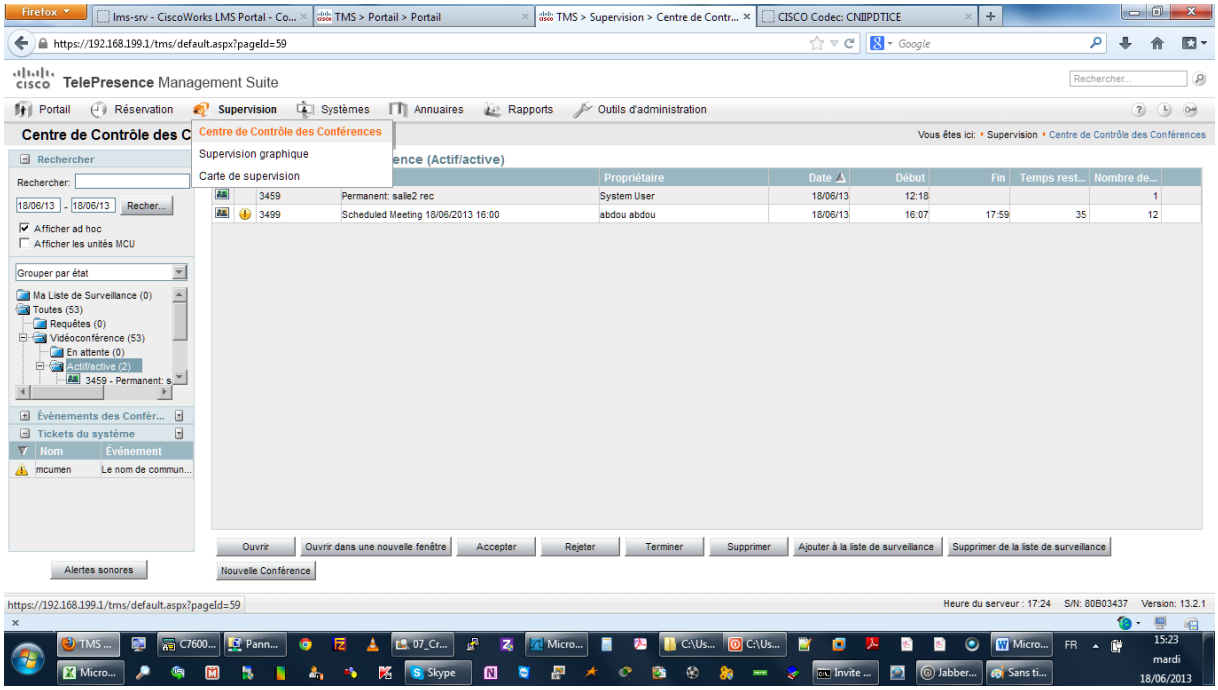
Pour l'ajout de participants une fois cliqué sur « Ajouter des participants » nous aurons une liste de participants et nous choisirons ceux avec lesquels nous établirons notre conférence .



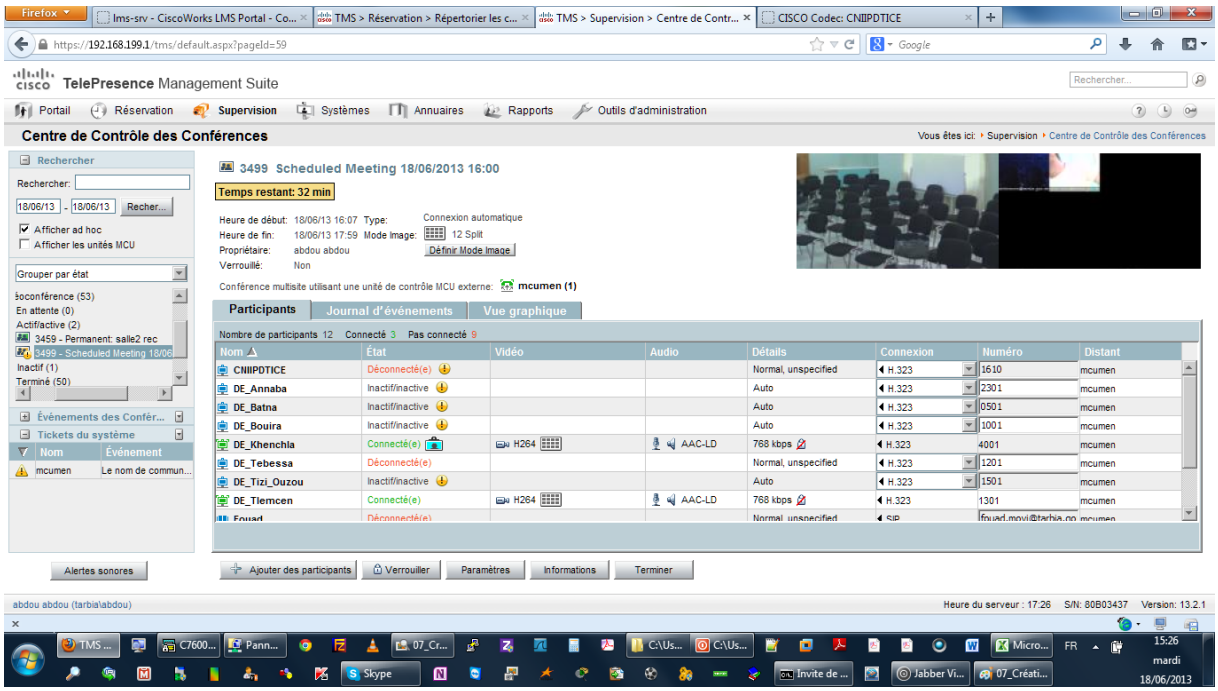
Une fois les participants ajoutés, nous allons lister les conférences existantes .



une fois les conférences listées nous choisirons notre conférence puis nous superviserons celle si et la contrôlerons comme suit :

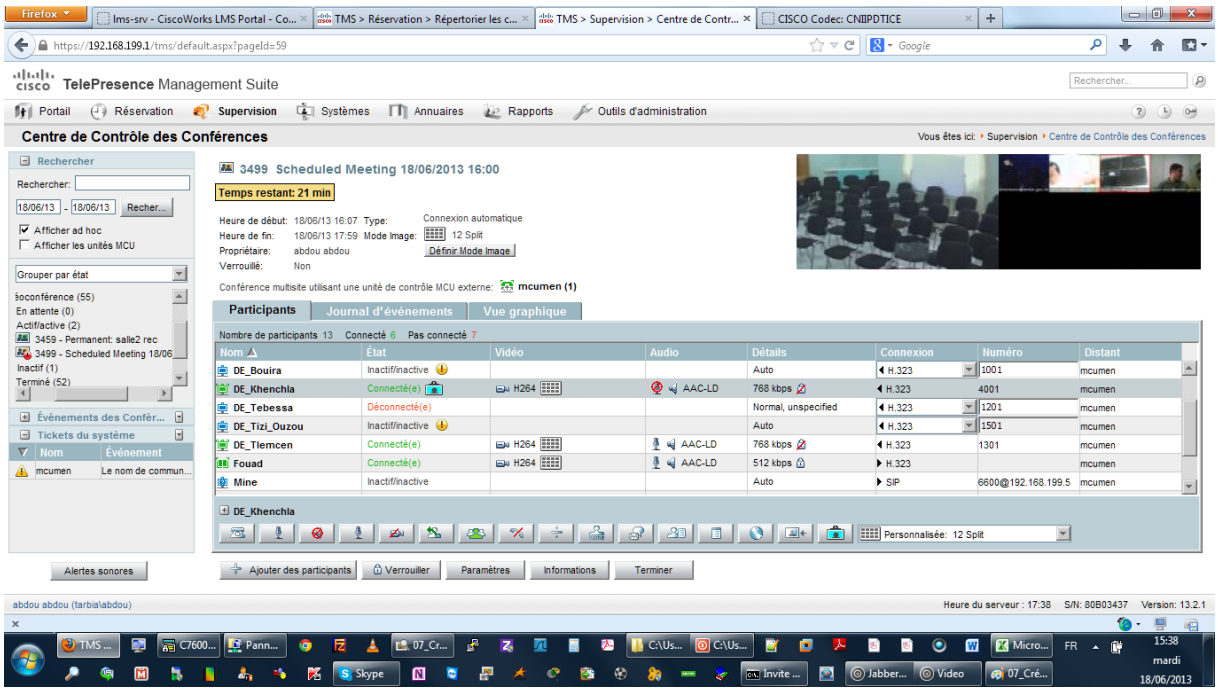


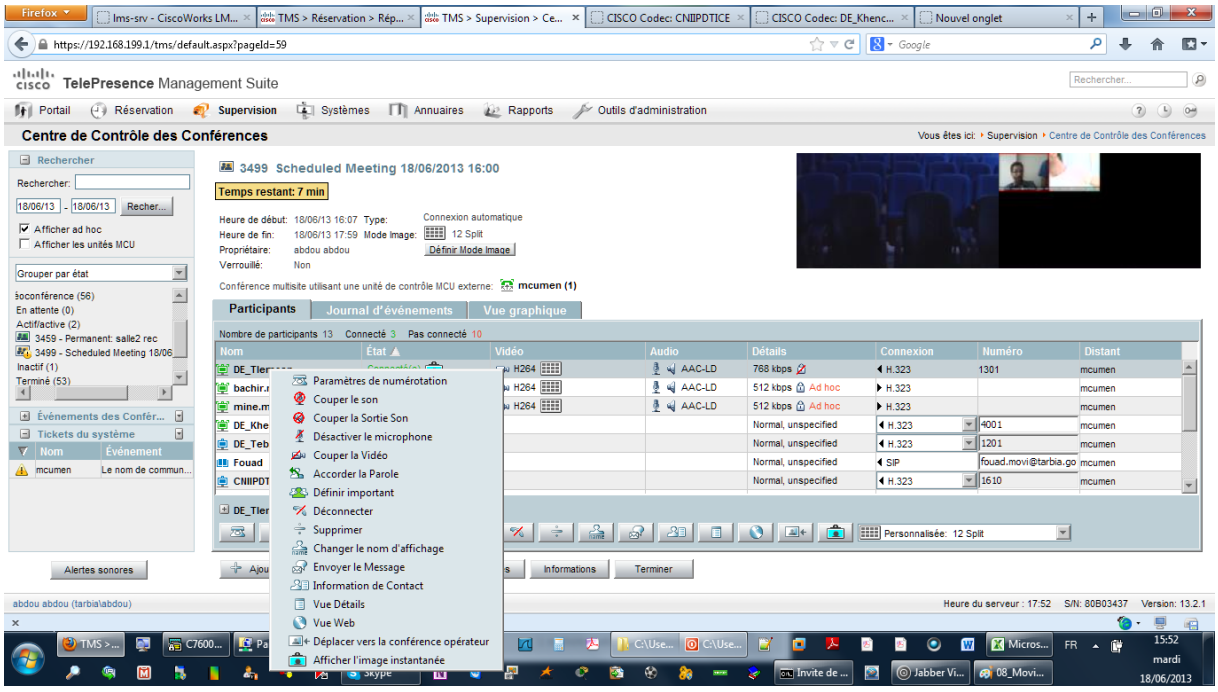
Maintenant nous avons le pouvoir de contrôle de toute la conférence .



8- Contrôle de conférence

Pour le contrôle d'une conférence on aura à choisir une des salles avec laquelle nous communiquerons. Nous voyons les exemples de contrôle qu'on peut faire .





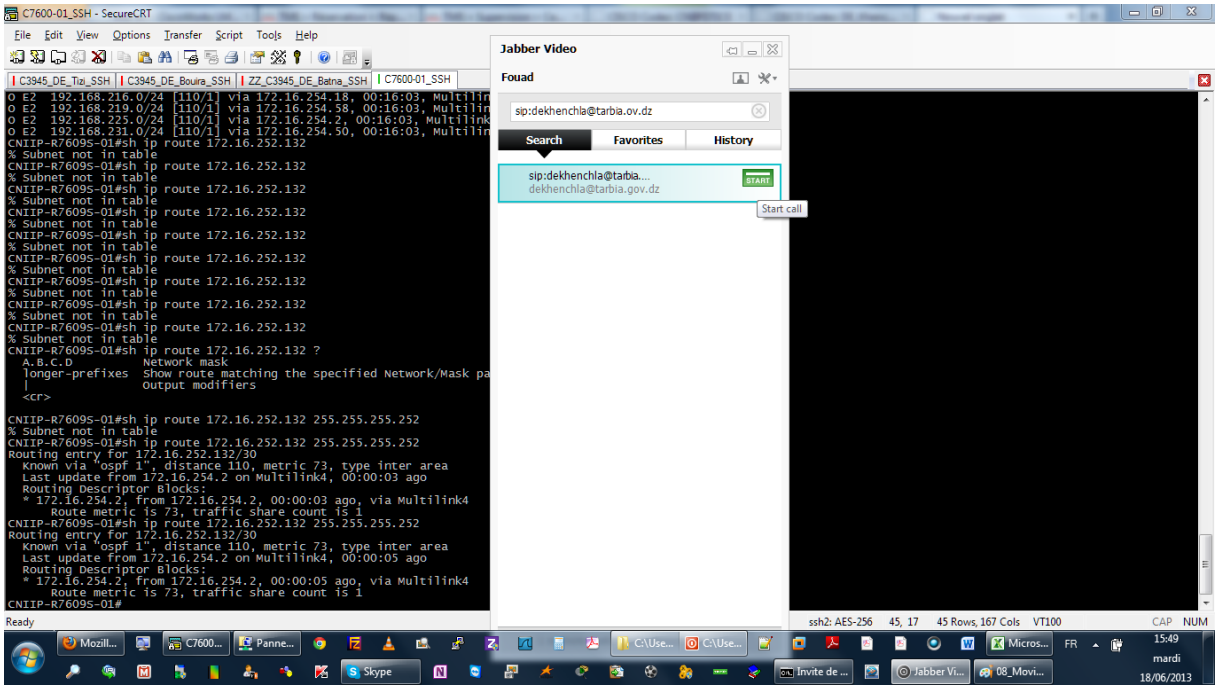
9- Appel de conférence Movi

Une fois toutes les configurations terminées nous pouvons effectuer maintenant l'appel pour lancer la conférence. Cela ce fait grâce a l'appel du 150 qui nous redirigera directement aux salles de conférences. Nous choisirons une salle de conférence, comme suis la 6600 (crée précédemment), la validation effectuée, nous pouvons alors commencer la conférence.

Dans ce type d'appel, nous distinguons les appels SIP et les appels H.323.

Appel SIP

On peut aussi faire un appel visio à une seule personne comme suit :

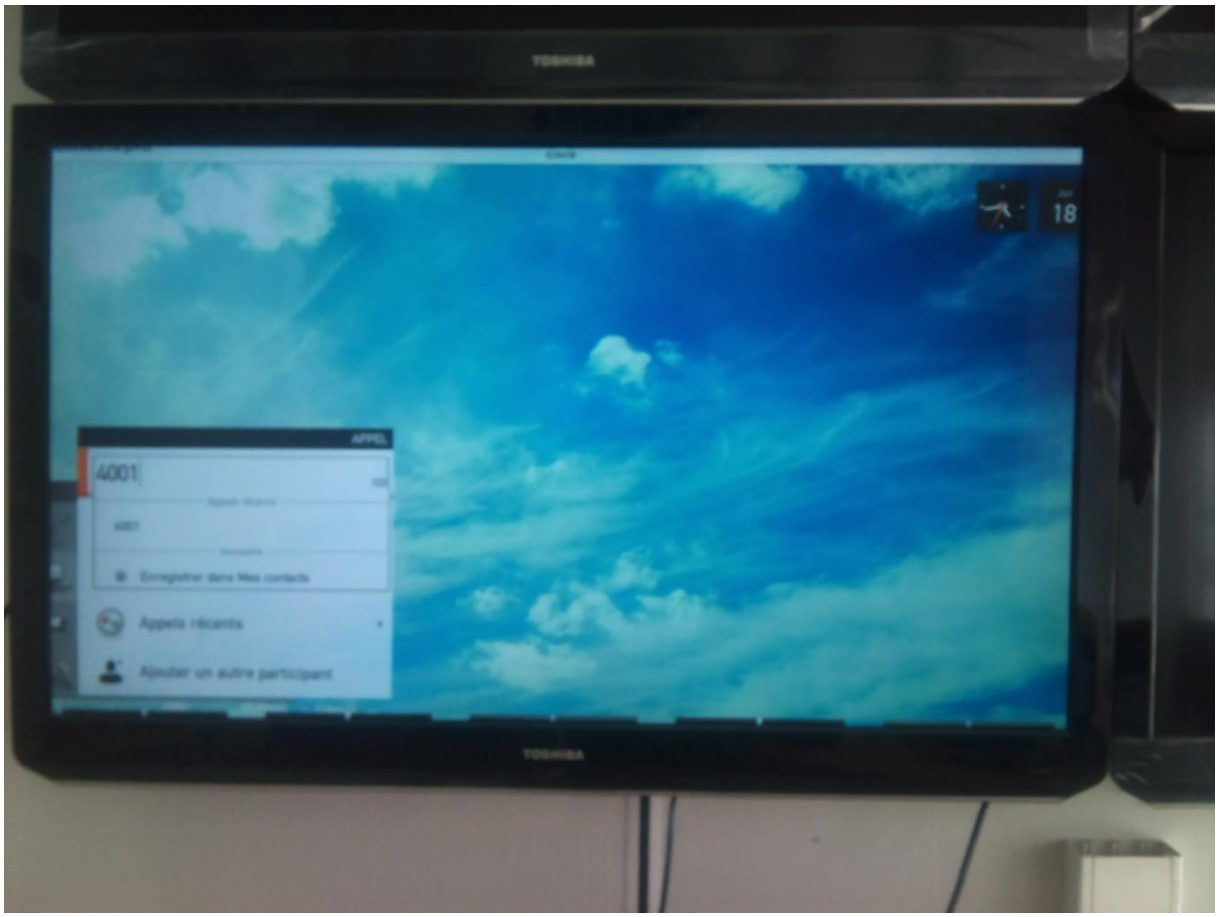


L' appel visio pour une seule personne se fait grâce à la procédure suivante:

Protocole : Nom de l'utilisateur@ Nom du domaine . (dz ou autre)

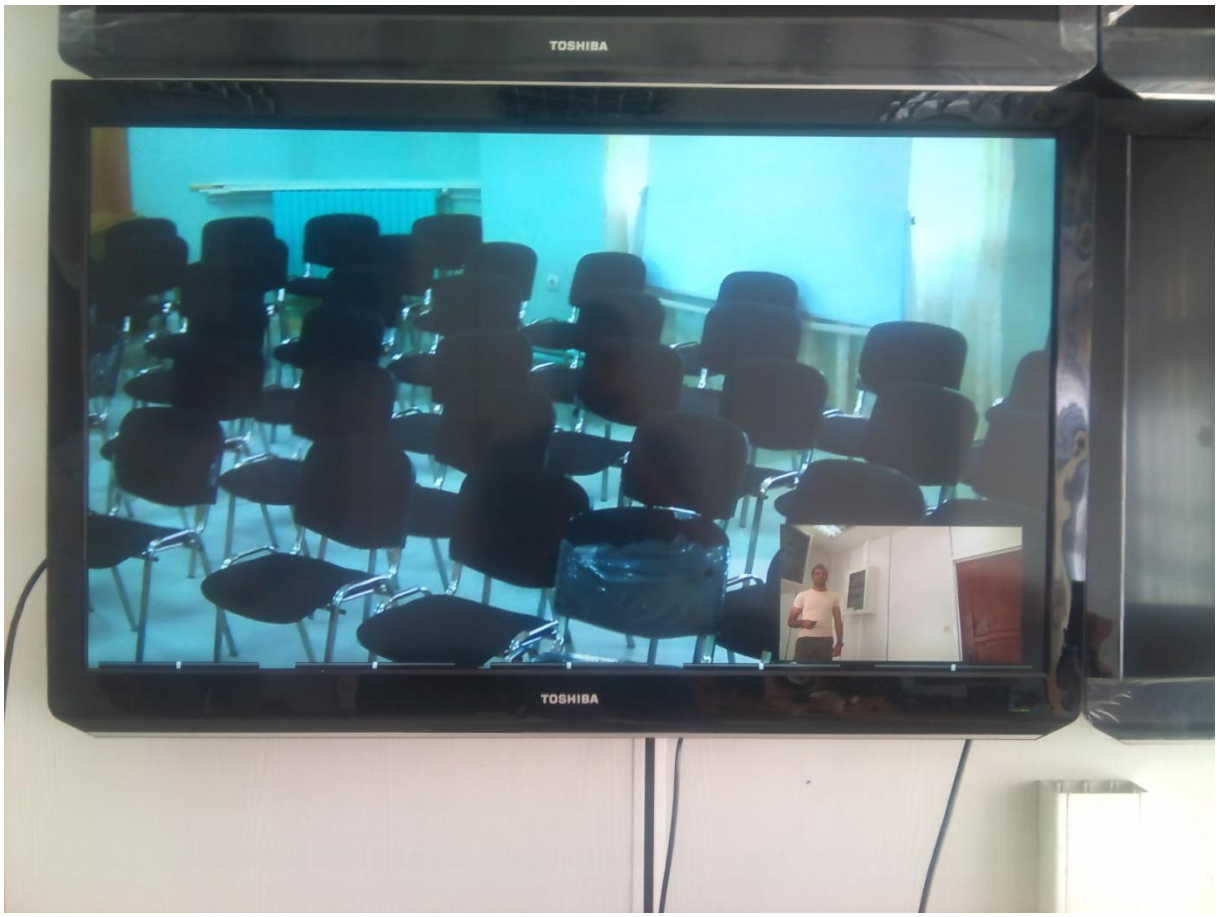
10- Appel du codec en H323

On peut aussi faire un appel visio en H323 qui est plus simple , avec le H323 on utilise simplement un appel a l'aide de chiffres appelés des digit en 4 chiffres .



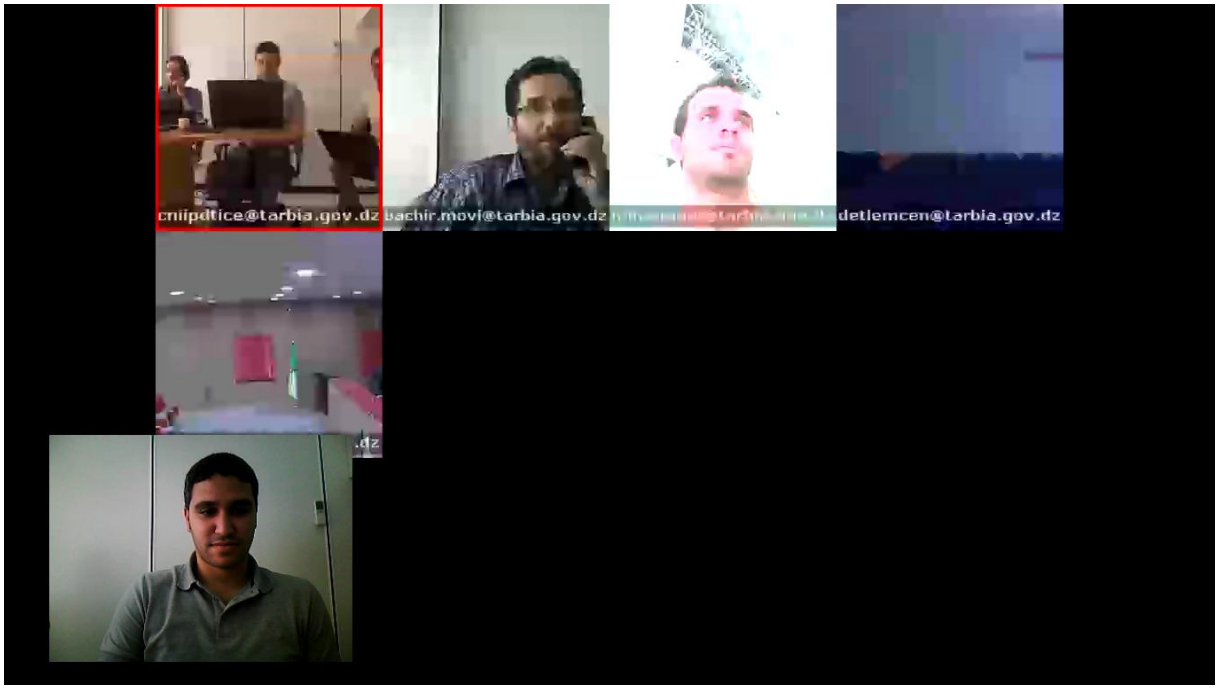
Conférence du codec en h323

Une fois l'appel lancé , et la réponse de l'autre codec obtenue qu'elle soit automatique ou manuelle la conférence peut être entamée.



11- Conférence

L'illustration suivante montre la conférence effectuée entre différents centres sur le territoire national.



Conclusion :

Nous venons de voir la manière de configuration du movi et aussi la création de conférence, ainsi que le contrôle de cette dernière, tout comme le lancement d'une conférence multiple. Au final nous nous sommes rendu compte que la qualité de la conférence ce différencie selon le taux de la bande passante choisie, plus elle est grande, plus la qualité et meilleure. Nous avons aussi vu les deux différentes manières d'effectuer ces appels. Pour la facilité de manipulation, le H.323 offre une utilisation plus simplifiée, contrairement au SIP. Pour la latence et la fluidité le SIP est recommandé, c'est une des raisons qui font que le protocole H.323 est délaissé.

Conclusion

Conclusion

Au cours de ce projet, l'objectif a été de voir tous les moyens mis en œuvre(en équipements, protocoles, cryptages, sécurité, connexion de réseau) pour une plateforme visioconférence, et l'amélioration de la qualité de service et de la bande passante pour une meilleure retransmission.

Durant ce stage effectué au sein d'Algérie Télécoms, nous avons remarqué que la qualité de service et aussi importante que les équipements utilisés. Pour une amélioration du QoS la technologie Cisco mise sur la norme H264 qui comprend de nombreuses techniques lui permettant des compressions plus efficaces que les normes précédentes. Le taux de bande passante choisie et aussi important, cela se répercute directement sur la qualité de transmission et d'images, pour la bande passante Algérie Télécoms propose une optimisation du WAN, qui réduit les temps de réponse.

En perspective un nouveau projet proposant une nouvelle solution visioconférence basée sur la technologie Polycom au sein de Djaweb /Algérie Télécoms , qui sera présentée prochainement.

La visioconférence semble constituer un enjeu de grande importance pour les années à venir. Quels que soient les domaines considérés(conférences, télémédecine,….). Elle semble être une solution très adaptée pour cela.

Glossaire

PABX : Dans l'industrie des télécommunications, on désigne par PABX IP (PBX IP ou encore IPBX) un système utilisé en entreprise qui assure l'acheminement de tout ou partie des communications en utilisant le protocole internet (IP), en interne sur le réseau local (LAN) ou le réseau étendu (WAN) de l'entreprise.

RTC : Réseau Téléphonique Commuté.

EDGE : Enhanced Data Rates for GSM Evolution.

UMTS : Universal Mobile Telecommunications System.

ATM: Asynchronous Transfer Mode.

NGN: Next Generation Network.

RMS: Réseaux Multi Services

IP/MPLS: Internet Protocol / Multiprotocol Label Switching.

VPN : Virtual Private Network

SAN: Storage Area Network.

OSI: Open Systems Interconnection.

SSH: Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé.

Port SFP: Small Form-factor Pluggable.

PCI: Peripheral Component Interconnect

Adresse **WWN**: World Wide Name.

TCO: Total cost of ownership

TCP: Transmission Control Protocol

NPIV: N port identifier virtualization.

VLAN: Virtual LAN.

ITU: International Télécommunication Union.

RNIS: Réseau Numérique à Intégration de Services.

UMTS: Universal Mobile Télécommunications System.

EIA/TIA: Electronic Industries Alliance/ Telecommunications Industry Association.

Supercontinuum: Est un phénomène d'optique non linéaire qui correspond à un élargissement de spectre très prononcé à partir d'une onde électromagnétique. Typiquement, on peut créer un supercontinuum en dirigeant un faisceau laser sur un matériau non linéaire : les effets non linéaires élargissent le spectre du faisceau de départ au cours de sa traversée dans le matériau.

SDH/SONET: Synchronous Optical NETwork/Synchronous digital hierarchy.

CWDM/DWDM: Wavelength Division Multiplexing (le CWDM pour 8 longueurs d'ondes, le DWDM pour 32 longueurs d'ondes).

XFP: est un standard de télécommunication pour les modules optiques à la vitesse de transmission de données de 10 gigabits/seconde.

LC : Lucent Connector (connecteur de fibre optique)

SC: Type de connecteur de fibre optique.

GBIC: Gigabit Interface Converter.

IDS/IPS: Intrusion Prevention System.

DPI: Deep Packet Inspection.

UDP: User Datagram Protocol.

UAC: User Account Control.

IETF: Internet Engineering Task Force.

NAT: Network Address Translation.

ISDN: Integrated Services Digital Network.

RFC: Requests For Comments.

ICMP : Internet Control Message Protocol.

IGMP : Internet Group Management Protocol.

RIP: extraction de données.

DES: Data Encryption Standard.

CBC: Cipher Block Chaining, est un mode de chiffrement cryptographique.

MD5: L'algorithme MD5, pour Message Digest 5, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier.

CBWFQ: Class Based Weighted Fair Queuing.

SSL : Secure Sockets Layer, un protocole de sécurisation des échanges sur Internet, devenu Transport Layer Security (TLS) en 2001

NAS: Network Attached Storage, serveur de stockage en réseau**.**

Gatekeepers: Sont des éléments optionnels dans une solution de réseau informatique H.323. Ils ont pour rôle de réaliser la traduction d'adresse (numéro de téléphone - adresse IP) et la gestion des autorisations. Cette dernière permet de donner ou non la permission d'effectuer un appel, de limiter la bande passante si besoin et de gérer le trafic sur le LAN.

NEXUS 5548 : Ces des switchs polyvalents multicouches peuvent être déployés à travers un ensemble diversifié tel que le routage de données traditionnel, virtuel, ainsi qu'à l'informatique de haute performance (HPC).

BIBLIOGRAPHIE

[1] : Algérie Télécom , « Fourniture, Installation et mise en service du réseau Intranet / Internet du Ministère de l'Education National », Octobre 2010.

[2] : Mr Amrane Raouli, « le Réseau RMS d'Algérie Télécom », année 2006 à Alger.

[3] : Philippe OWEZARSKI, « Conception et formalisation d'une Application de visioconférence », année 1996 à Toulouse.

[4] : Tandberg, « MCU Tandberg/Codian », Version 3.0, Mai 2009.

Site Internet

- http://tel.archives-ouvertes.fr/index.php?b_type=browse_domain&submit=1&which_domain=SPI%3ATRON&halsid=ukghu6iamoutbqaan0h126qfd5&begin_at=40
- http://bases-hacking.org/segmentation-memoire.html
- http://www.epitech.eu/vlvc-sct433.html
- http://www.framablog.org/index.php/post/2006/10/15/VLVC-video-conference-avec-VLC
- http://www.commentcamarche.net/forum/affich-2890980-logiciel-visio-conference
- http://www.linguee.fr/anglais-francais/traduction/multicast+to+unicast.html
- http://www.rap.prd.fr/pdf/technologie_multicast.pdf
- http://www.pfast.fr/?Visioconference-les-technologies-d&artpage=11-13
- http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2006-ttnfa2007/Hjibe-Dorville/SIP.htm
- http://www.testeur-voip.com/technologie-voip-explication.php?numpage=4
- https://community.rapid7.com/community/metasploit/blog/2012/01/23/video-conferencing-and-self-selecting-targets