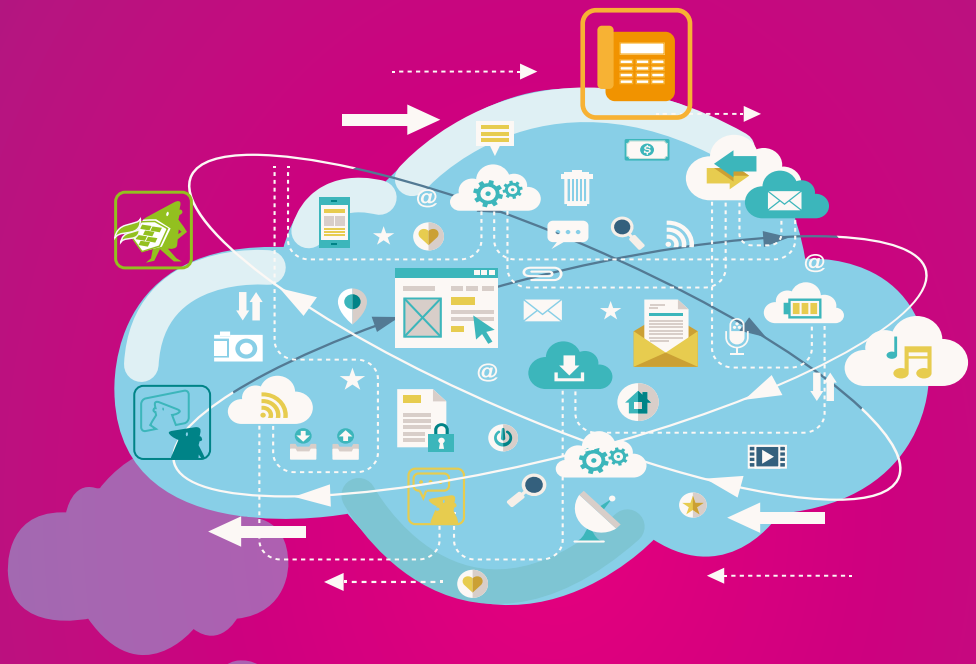
WHITE PAPER

Communications Unifiées et Private Cloud



QUANT ICT

Telic
Infinite Connections

TABLE DES MATIÈRES

- le signe indique l'endroit où vous trouverez un tableau pratique
- le signe indique l'endroit où vous trouverez un graphique explicatif
- le signe expert indique le niveau le plus élevé d'expertise

Georges Ataya

Contact :

be.linkedin.com/in/ataya/fr

PRÉFACE : GEORGES ATAYA

Les Communications Unifiées tendent à se généraliser et apportent une véritable valeur ajoutée aux entreprises sachant les exploiter. Elles correspondent à plusieurs besoins qu'impose la croissance.

Pour les entreprises leaders dans leurs domaines, l'externalisation des outils éloignés de leur métier de base est devenue une pratique fréquente.

Les technologies des communications virtualisées dans le «Private Cloud» offrent l'accès permanent aux ressources indépendamment du lieu géographique de son utilisateur. Celui-ci bénéficie de façon continue de l'ensemble des services et de leurs évolutions quel que soit le terminal employé.

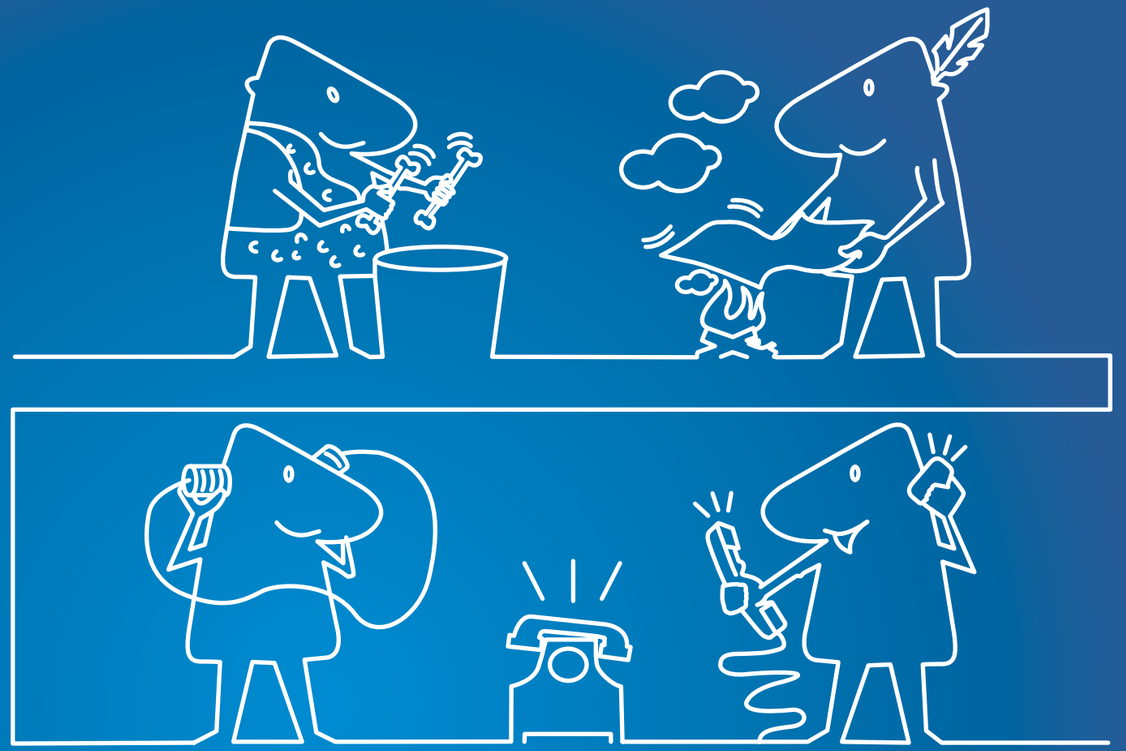
Cependant, face à ces développements rapides, il est de moins en moins admissible d'accepter une faiblesse de sécurité, de continuité de service ou un manque dans la maîtrise du coût. De même, il n'est pas plus tolérable de se lier à une solution ou un service sans avoir une garantie raisonnable d'une évolutivité permanente garantissant l'accès aux fonctionnalités potentiellement disponibles ailleurs.

Il est donc vital de s'assurer que le fournisseur maîtrise la technologie, la qualité du service, le suivi de l'évolution ainsi que les avantages fonctionnels et économiques qui l'accompagnent. Le bon fournisseur se doit d'offrir des liaisons avec les différentes offres de couches architecturales de plates-formes ou de services à valeur ajoutée.

Les générations se succèdent de plus en plus rapidement. En conséquence, chaque nouvelle couche nécessitera rapidement des compétences nouvelles. Il me semble primordial de bâtir sur de telles technologies pour rattraper à chaque génération le saut technologique ou fonctionnel nécessaire pour rester acteur dans la partie qui se joue.

Les services rendus et l'évolution de la Communication Unifiée en Private Cloud sera fonction de la capacité du prestataire à investir dans les technologies adéquates. Le succès de celui ou celle qui externalisera la gestion, l'évolution et l'exploitation de son outil reposera dès lors sur la capacité du partenaire qu'il choisit.

TÉLÉPHONIE LES «BASICS»



1. TÉLÉPHONIE LES «BASICS»

1.1. La téléphonie analogique

La téléphonie analogique est destinée à un usage simple du téléphone, qui se raccorde sur les ports analogiques du standard téléphonique.

1.1.1. Les lignes analogiques publiques

Elles permettent de faire transiter la voix d'un utilisateur analogiquement jusqu'au destinataire via le réseau commuté (PSTN). Ce type de connexion est limité à une communication par ligne.

La téléphonie analogique reste encore largement utilisée aujourd'hui dans les entreprises pour le branchement en direct sur le réseau public d'une alarme ou d'une ligne fax.

Dans la téléphonie analogique, le téléphone est généralement composé de deux circuits : un circuit de conversation qui est chargé de la voix et un circuit de signalisation, qui concerne la saisie des numéros et les appels.

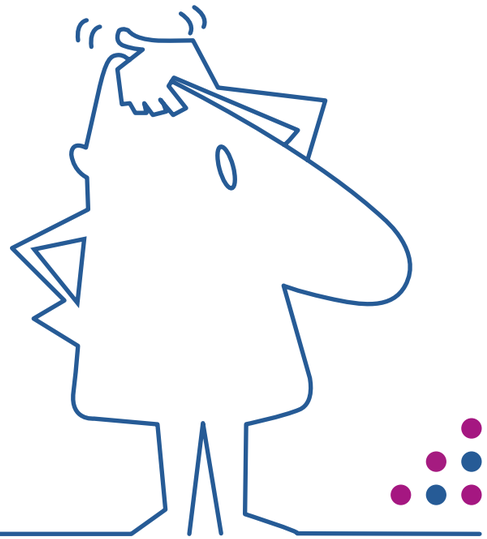
En 2012, la Belgique comptait **4,63 millions de raccordements à la téléphonie fixe** (3,13 millions pour les particuliers et 1,5 million pour le marché professionnel)[1]

1.1.2. Les lignes analogiques internes

La téléphonie analogique reste encore largement utilisée aujourd'hui dans les entreprises pour le branchement d'une alarme, d'un poste d'ascenseur ou d'une ligne fax au travers d'un central téléphonique. Ce type de raccordement offre l'avantage d'être compatible avec toutes les marques de centraux ; en cas de remplacement du central, ces postes ne doivent pas être remplacés, par contre, ils sont pauvres en termes de fonctionnalités.

Ces postes sont encore parfois utilisés pour les appels d'urgence. En effet, en cas d'urgence (une coupure de courant, par exemple), ils sont directement reliés à une ligne extérieure via un circuit de relais. La ligne extérieure fournit alors la puissance et l'appareil peut encore être opérationnel.

Les anciens postes analogiques utilisaient la signalisation DECADIC ou PULSE (numérotation par impulsion mécanique). On peut encore trouver ces appareils, mais la plupart du temps, ils ne fonctionnent plus. La signalisation DECADIC ou «numérotation par impulsions» a été principalement développée pour fonctionner sur les anciens centraux téléphoniques avec circuit de relais.



1. Institut belge des Services postaux et des télécommunications, Situation du secteur des communications électroniques, 2012.

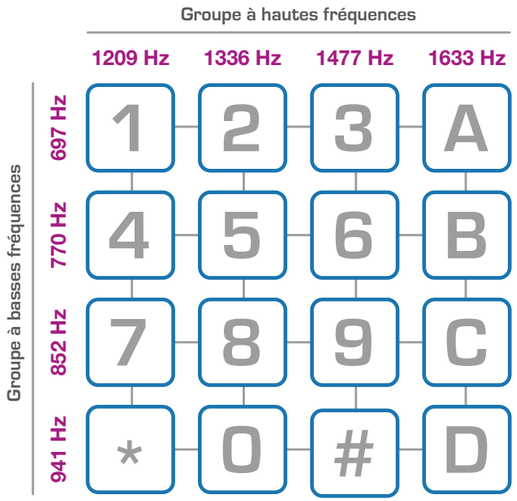
1.1.3. Dual-Tone Multi-Frequency (DTMF)

Le DTMF est l'ensemble des sons qui permet aux appareils d'émettre des appels. Chaque touche du cadran émet sa propre tonalité, celle-ci est identique quel que soit l'appareil. C'est cette tonalité qui permet de composer un numéro. En cours de communication, ces signaux émis seront également utilisés, par exemple, lors d'une consultation de boîte vocale, d'un service clientèle ou bancaire.

Le code DTMF est donc une combinaison de fréquences. Ces codes **(MultiFrequency)** sont additionnés **(Dual-Tone)** et émis lors de la pression sur une touche du clavier téléphonique.

Les fréquences ont été choisies pour éviter les harmoniques : aucune fréquence n'est un multiple d'une autre, la différence entre deux fréquences n'est jamais égale à l'une des fréquences de base, et la somme de deux fréquences n'est jamais égale à une troisième.

1.1.4. Groupe à hautes fréquences / Groupe à basses fréquences



1.2. Integrated Services Digital Network (ISDN / RNIS)

ISDN est un ensemble de standards de communication permettant la transmission numérique simultanée de la voix, la vidéo, les données et autres services réseaux au travers des lignes traditionnelles du réseau public (PSTN).

ISDN n'est pas un standard normalisé au niveau mondial. Il existe diverses normes de ce réseau qui ne sont pas compatibles entre elles. Aux Etats-Unis et au Canada, les canaux B ont des débits de 56 kbps. Les connexions ISDN sont disponibles en deux interfaces : Basic Access (BA) et Primary Rate Access (PRA).

La vitesse est cruciale pour le transfert des données. La qualité de la connexion au central téléphonique détermine le degré de fluidité des appels téléphoniques ou vidéo. Traditionnellement, ISDN a été utilisé pour établir des liaisons entre centraux téléphoniques et pour la transmission rapide de données.

Cette technologie est limitée à deux (BA) ou trente (PRA) communications par ligne.

1.2.1. Basic Access (BA)

En Europe, une connexion BA comprend deux canaux B (porteurs) pour le transfert de données à 64 kbps et un canal D (données) pour la signalisation à 16 kbps.

Cette connexion utilise donc 144 Kb.

Ce type de connexion est appelé BA, BRA, BRI ou T_0.

1.2.2. Primary Rate Access (PRA)

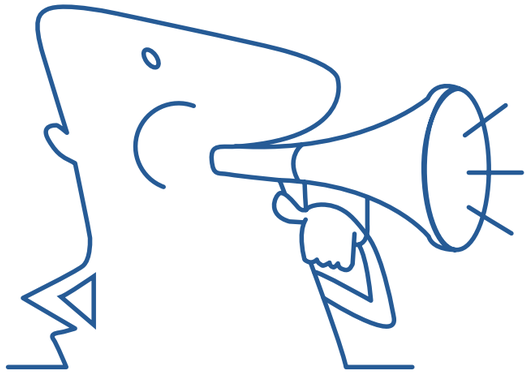
En Europe, une connexion PRA comprend trente canaux B (porteurs) pour le transfert de données à 64 kbps, un canal D (données) pour la signalisation à 64 kbps et un canal pour les alarmes et la synchronisation également à 64 kbps.

Cette connexion utilise donc 2.048 kbps. D'où le nom connexion de 2Mb.

Ce type de connexion est appelé PRA, PRI ou T_2 ou E_1.

BA et PRA utilisent toutes deux une technique appelée Multiplexage par répartition dans le temps **(MRT)**, qui permet, par synchronisation, d'avoir plusieurs communications sur une même ligne.

Le Multiplexage par répartition dans le temps (MRT) est un procédé consistant à placer plusieurs flux de données dans un seul signal en le décomposant en nombreuses tranches de temps, chacune d'une courte durée. Chaque flux de donnée individuel est alors réordonné à l'autre extrémité de la réception en fonction de la durée.



1.3. Les lignes digitales

Les lignes digitales reposent sur une technologie à deux fils de cuivre qui constitue le réseau téléphonique interne. Celles-ci ne peuvent recevoir que des postes téléphoniques digitaux.

Les appareils digitaux utilisent toujours un protocole spécifique au constructeur (protocole propriétaire). Ce type de postes offre l'avantage d'être riche en fonctionnalités, par contre n'étant compatible qu'avec sa propre marque de central, en cas de remplacement par un central d'une autre marque, ils ne pourront être réutilisés. Bien que l'on parle d'appareils digitaux, ils ne peuvent pas être connectés via Ethernet.

1.4. Voice over IP (VoIP)

Pourquoi déployer une solution VoIP sur son réseau local ?

L'avantage le plus évident est d'ordre économique. Il s'agit de déployer et entretenir un seul réseau. La suppression du réseau téléphonie traditionnel n'implique pas systématiquement l'installation de nouvelles prises. En effet, la plupart des postes téléphoniques disposent d'une ou deux prises Ethernet permettant de connecter un ordinateur ou tout autre périphérique sur celui-ci. Même s'ils sont connectés à partir d'une seule prise, ces éléments seront perçus et gérés de façons parfaitement distinctes par le réseau. De plus, ces «micro switches intégrés» sont disponibles avec des vitesses pouvant atteindre le Gigabit/sec., ce qui dans la plupart des cas ne ralentit pas les applications fonctionnant sur l'ordinateur.

Comme nous le verrons plus loin, même s'il s'agit d'un seul réseau physique de manière virtuelle et pourtant hermétique, le réseau voix sera séparé du reste du réseau.

D'un point de vue de la gestion du réseau, les postes téléphoniques seront considérés comme tout autre périphérique, ce qui permettra d'effectuer des vérifications ou des tests à partir d'une seule console de management.

Si le réseau intègre plusieurs sites distants, l'ensemble de l'infrastructure sera considérée comme un seul et unique réseau téléphonique permettant la gratuité des communications internes, et ce également sur les réseaux non-filaires, où les utilisateurs sont reconnus en passant d'un site à l'autre.

Un réseau téléphonique traditionnel reconnait l'utilisateur suivant la connexion qu'il emploie. En VoIP, c'est le poste qui est identifié. Par exemple, en cas de déménagement, il suffira à l'utilisateur de connecter son poste sur une prise réseau pour qu'il retrouve ses fonctions.

Dans les pages suivantes, nous allons examiner les préalables au déploiement d'un réseau VoIP.

1.4.1. Bande Passante

L'origine du terme provient du nombre maximal d'oscillations par seconde qu'un signal peut effectuer dans un câble sans s'atténuer.

Aujourd'hui, plus généralement, la bande passante détermine la quantité de données qu'une connexion est en mesure de traiter en une unité de temps, il s'agit du débit. Elle est généralement exprimée en bits par seconde (bps) ou bytes par seconde (Bps). Si l'on souhaite se référer à des valeurs plus élevées on parlera en Kilo, Mega, Giga ou Tera bits par seconde.

- 8 bits = 1 byte (B)
- 1024 bytes = 1 Kilobyte (KB)
- 1024 Kilobytes = 1 Megabyte (MB)
- 1024 Megabytes = 1 Gigabyte (GB)
- 1024 Gigabytes = 1 Terabyte (TB)

1.4.2. Quality of Service (QoS)

La **QoS** ou **Qualité de Service** définit la capacité d'un réseau (interne ou public) à transmettre un type de trafic, en garantissant la disponibilité, le débit, les délais de transmission et le taux de perte de paquets.

C'est un des éléments déterminants pour le transport de la voix, qui est sensible au temps de transmission. Suivant le nombre de communications simultanées souhaitées, on affectera donc une bande passante suffisante à la voix ainsi que la classe de service la plus élevée afin de garantir une communication de qualité.

Dans le cadre d'un réseau local, il est possible, après analyse, de s'assurer par un monitorage qu'il concentre les critères nécessaires pour assurer une bonne qualité des communications.

En ce qui concerne les appels vers le réseau public, le critère de qualité est incompressible. Il suffit de voir la qualité peu convaincante liée à l'utilisation de logiciels s'appuyant exclusivement sur Internet pour communiquer. Dans le cadre d'appels longue distance à titre privé, le facteur économique est souvent tel que l'on peut se contenter d'une certaine lenteur ou d'écho. Par contre, dans le cadre de communications professionnelles ou de services, opter pour un opérateur garantissant la QoS est un critère incontournable.

La QoS peut être réalisée de manières différentes suivant l'opérateur, mais on utilise en général le marquage DSCP/ToS, tant pour la signalisation que pour les flux de données (audio et/ou vidéo).

Afin d'appliquer la Qualité de Service, tous les composants du réseau entre la source et le destinataire doivent supporter la QoS. Il faut signaler que la QoS n'est pas garantie sur Internet, car tous les fournisseurs de services n'offrent pas ce service. Dans une configuration de Cloud privé, les réseaux IP-VPN (Virtual Private Network) et VPLS (Virtual Private LAN Service) permettent d'implémenter la QoS.

La Qualité de Service constitue une bonne alternative pour les entreprises dont les filiales sont trop éloignées pour être reliées par des liens WAN coûteux. En donnant la priorité à certaines données (ex. téléphonie IP) vous vous approchez au plus près de la connexion qualitative d'un réseau filaire.

La Qualité de Service existe sous différentes formes, le DSCP (Differentiated Services Control Point), étant la technologie la plus courante et performante dans ce domaine. Le DSCP est très granulaire, car il peut attribuer jusqu'à 64 niveaux de priorité.

Les paquets de données sont marqués par une étiquette QoS, précisant s'ils peuvent être prioritaires ou pas par rapport à d'autres paquets transitant sur votre réseau de données. Un paquet peut recevoir son étiquette QoS de l'appareil où il est généré (ex. téléphone IP), ou du commutateur auquel l'appareil est connecté.

La Qualité de Service est particulièrement intéressante lorsque la bande passante disponible sur votre réseau est limitée. Vous pouvez ainsi donner la préférence à la voix, pour qu'elle soit sensiblement plus performante, par rapport à la navigation ou aux e-mails.

Et même si vous disposez d'une bande passante suffisante, nous vous recommandons la QoS pour la cohabitation «du trafic en temps réel» de la voix et notamment de la vidéo.

Vous éviterez de cette façon les problèmes dans un cas de charge de CPU élevée sur un commutateur (Switch), lorsque par exemple un technicien analyse un problème de switch. Si les paquets de voix n'ont pas une priorité de QoS élevée, ils devront attendre que le switch ait terminé le debugging (débogage).

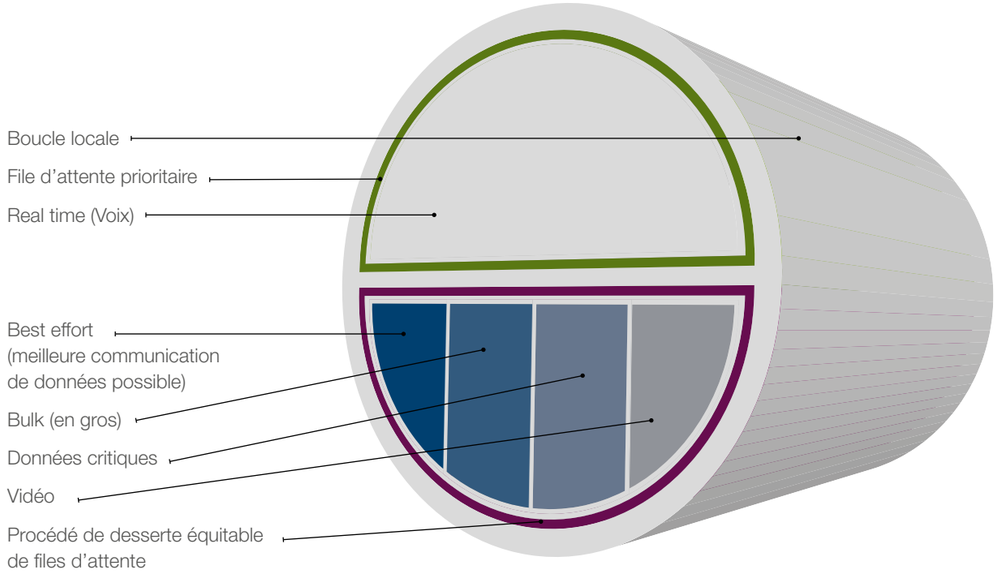
Pour un fonctionnement optimal, le réseau qui supportera le trafic voix devra offrir un niveau de performance suffisant sur 3 critères :

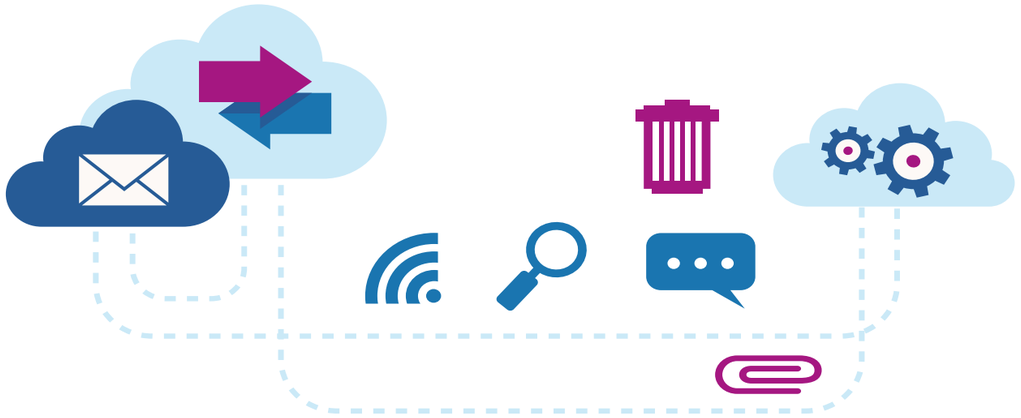
- Le «Delay» (Délai de transit) et la latence sont des termes similaires qui font référence à la quantité de temps qu'il faut à un bit pour être transmis de la source à la destination.
- Le Jitter (Gigue de phase) est la variation du délai de transfert de l'information.
- Packet Loss (Perte de paquets de données) est la défaillance d'un ou plusieurs paquets lors de la transmission. Cet événement peut provoquer des effets notables dans tous les types de communications numériques.

1.4.3. Niveaux de performances

	Mauvais	Moyen	Bon
Delay	D > 400 ms	150 ms > D < 400 ms	D < 150 ms
Jitter	J > 50 ms	20 ms > J < 50 ms	J < 20 ms
Packet Loss	P > 3%	1% > P < 3%	P < 1%

1.4.4. Classe de Service





1.4.5. Power over Ethernet (PoE & PoE+)

Power over Ethernet (PoE) est un système qui permet d'alimenter des appareils via le câblage Ethernet. Ce système est similaire à celui de la téléphonie analogique : la ligne analogique transporte 48 VDC (Direct Current ou Courant Continu) pour faire fonctionner le téléphone et activer la sonnerie. Dans le PoE on retrouve la même tension (48 VDC), de telle sorte que dans les data centers, les batteries de sauvegarde de la téléphonie classique puissent être réutilisées dans les réseaux de données actuels.

En 2003, l'IEEE a ratifié la norme standard 802.3af garantissant l'injection de 15,4 W DC par la source PoE (minimum 44 VDC à 350 mA). Compte tenu de la déperdition d'énergie sur le câble, un périphérique peut recevoir une puissance de 12,95 W. Le courant est transmis sur au moins deux paires de câbles Ethernet Cat 5 ou un câble supérieur.

En 2009, l'IEEE a approuvé la norme 802.3at assurant une puissance de 25,2 W aux équipements raccordés. Un standard mieux connu sous l'appellation PoE+.

Certains switchs intègrent directement la technologie PoE, le PoE alimente ainsi directement les équipements. L'autre option est de passer par des injecteurs intermédiaires placés entre un switch non PoE et un périphérique d'extrémité.

Certains fabricants offrent aujourd'hui des appareils et des injecteurs qui permettent de fournir 60 W de PoE, et ceci au profit de terminaux distants pour une solution d'infrastructure de bureau virtuel (Virtual Desktop Infrastructure - VDI).

Grâce à l'utilisation du PoE, il n'est pas nécessaire d'avoir des prises distinctes pour chaque téléphone IP ou point d'accès sans fil afin de se raccorder à une source de courant.

De l'électricité via votre câble Ethernet :

Les technologies sont en constante évolution, et aujourd'hui un nombre croissant d'appareils sont connectés à Internet. Mais disposez-vous de suffisamment de prises de courant, au bon endroit, pour pouvoir alimenter tous ces périphériques en électricité ?

Grâce au Power over Ethernet, vous n'avez plus besoin de prises de courant pour chaque téléphone IP ou point d'accès sans fil. Cela représente une solide économie tant en termes de câblage que d'alimentation individuelle.

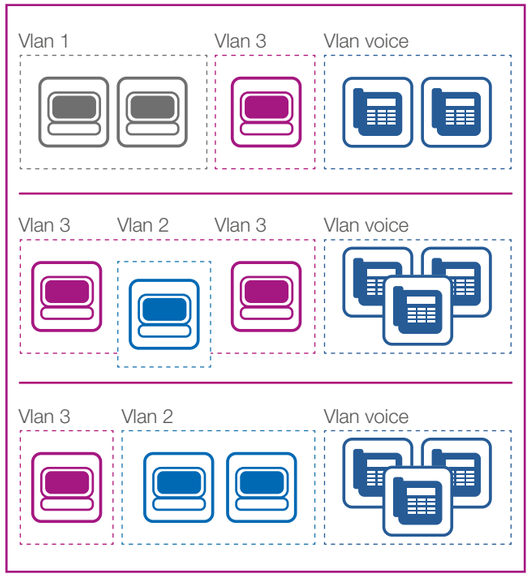
1.4.6. Virtual Local Area Network (VLAN)

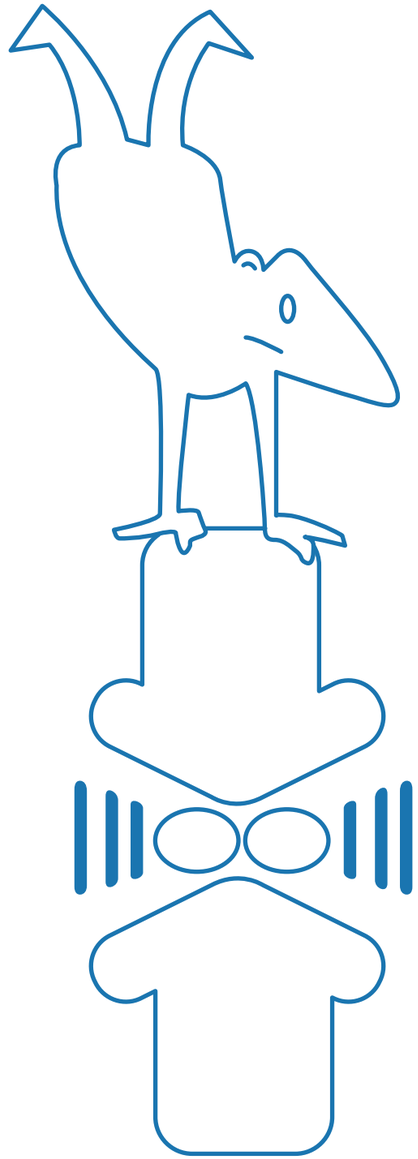
Un VLAN est un réseau local regroupant de manière logique (virtuelle) les éléments qui y sont connectés.

Chaque VLAN pourra être déterminé suivant des critères propres à l'activité, par exemple pour isoler de manière étanche la partie réseau sur laquelle l'on retrouve des données confidentielles, comme celles des ressources humaines. Ils pourront être segmentés sur base de différents critères tels que l'adresse MAC des appareils, le numéro de port sur lequel il est raccordé, le protocole (TCP/IP), etc.

Tout en partageant la même infrastructure physique, le réseau voix sera placé dans un VLAN distinct pour l'isoler très simplement et efficacement de phénomènes parasites.

1.4.7. Infrastructure VLAN





1.4.8. Compression et codecs

Le terme codec vient de COder DECoder ou encore de COmpresser ou DECompresser.

Un codec est donc le logiciel ou le matériel qui met en œuvre un procédé capable de compresser ou décompresser des données dans un format normalisé.

Chaque codec est un compromis entre :

- La qualité de la voix
- La puissance de calcul
- La bande passante
- La latence

Il existe des codecs pour l'audio, mais aussi pour la vidéo.

En détails

La latence doit rester minimale dans le cadre d'un appel en voix sur IP. Elle correspond au décalage entre le temps écoulé entre l'émission de la parole et son écoute par le correspondant. Elle est la somme des différents délais introduits lors de la transmission :

- Capture par le micro du correspondant
- Conversion en signal numérique
- Compression par le codec
- Encapsulation en paquets RTP
- Transmission sur le réseau
- Somme des délais pour réaliser les opérations inverses à l'autre bout.

Il est donc nécessaire, si on souhaite conserver une conversation de qualité, de minimiser la latence introduite par la compression/décompression, tout en minimisant la bande passante, la puissance de calcul, mais en conservant la meilleure qualité audio possible.
(Voir 4.4.3 QoS)

Les codecs audio les plus répandus sont G.711, G.722 et G.729 :

- La norme G.711 est la base du transport de la voix sur le réseau téléphonique commuté (RTC, PSTN en anglais) ou sur l'ISDN. Ce codec est également utilisé pour le transport de la voix avec peu de compression dans les réseaux IP, plus généralement sur un LAN et rarement sur Internet à cause de la bande passante nécessaire.
- La norme mondiale de codage G.722 normalisée par l'UIT-T en 1987 permet d'obtenir en voix sur IP une qualité de voix «haute définition» (dite téléphonie large-bande). Cette qualité est obtenue par doublement de la bande de fréquence codée (50-7.000 Hz) par rapport à la qualité téléphonique usuelle dite bande étroite (300-3.400 Hz) produite par le format de codage G.711 utilisé en téléphonie «classique» sur les réseaux RTC. L'utilisateur bénéficie donc d'une sensation de présence de son interlocuteur, d'un confort d'écoute et d'une intelligibilité fortement améliorés.

De nombreux téléphones IP, bien que labellisés «HD Voice» ne font que supporter ce type de signalisation sans pour autant pouvoir le restituer en haute définition réelle. G.722 est rarement utilisé sur les connexions Internet à cause de la bande passante nécessaire.

- Le codec G.729 est moins consommateur en bande passante que G.711. Il est utilisé pour obtenir une téléphonie de qualité.

De nombreux autres codecs existent, tant pour la voix que pour la vidéo.

Le tableau suivant indique les différents codecs VoIP les plus répandus, ainsi que leur bande passante sur un réseau Ethernet, et leur score MOS.

Le score MOS, obtenu par expérimentation, ou «note d'opinion moyenne» (Mean Opinion Score) est une note donnée à un codec audio pour caractériser la qualité de la restitution sonore. La note varie entre 1 et 5 (excellent).

1.4.9. VOIP-SIP.ORG Codec and Bit Rate

VOIP-SIP.ORG Codec and Bit Rate	Sample Size (Bytes)	Sample Rate (ms)	MOS Quality	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Brandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80	10	4.3	160	20	50	87.2
G.729 (8 Kbps)	10	10	3.7	20	20	50	31.2
G.723.1 (6.3 Kbps)	24	30	3.9	24	30	33.3	21.9
G.723.1 (5.3 Kbps)	20	30	3.8	20	30	33.3	20.8
G.726 (32 Kbps)	20	5	3.85	80	20	50	55.2
G.726 (24 Kbps)	15	5	–	60	20	50	47.2
G.728 (16 Kbps)	10	5	3.61	60	30	33.3	31.5
G.722 (64 Kbps)	80	10	4.13	160	20	50	87.2
iLBC (15.2 Kbps)	38	20	4.14	38	20	50	38.4
iLBC (13.33 Kbps)	50	30	–	50	30	33.3	28.8

1.5. Session Initiation Protocol (SIP)

SIP est un protocole standard ouvert de télécommunications multimédia qui a été normalisé et standardisé par l'IETF (The Internet Engineering Task Force). Il a été défini dans sa version 2 dans le RFC (Request for Comments) 3261 datant de 2002. Dans le monde de la voix sur IP, ce protocole définit comment établir un appel, le terminer, renvoyer des codes d'erreur, etc. Il est devenu progressivement la norme du secteur des télécoms pour les communications multimédia, remplaçant peu à peu le H323 qui posait entre autres des problèmes de sécurité.

SIP a été conçu de manière suffisamment générique afin de permettre d'initier différents types de sessions en temps réel, qu'il s'agisse d'initier un appel, des sessions de messagerie instantanée ou encore une conférence audio ou vidéo multicast.

Il faut noter que certaines fonctionnalités supplémentaires, qui ne sont pas relatives à l'établissement de sessions, font partie de RFC additionnels. Par ailleurs, SIP ne réinvente pas la roue et se base sur la réutilisation de protocoles classiques d'Internet tels que DNS, UDP, TCP, ou encore RTP pour le transport des flux audio et vidéo et SDP pour la description des codecs supportés.

1.5.1. L'architecture SIP et ses composants

SIP définit donc les composants d'une infrastructure et leurs interactions. Les composants principaux sont les suivants :

- User Agent (UA) : de type «Client» ou «Serveur» selon qu'il émet ou reçoit des requêtes SIP. Il s'agit en général des terminaux SIP tels que softphones (téléphone sous forme de logiciel PC, tablette, smartphone), téléphones et certains types de serveurs.
- Redirect Server : la composante d'un serveur ou d'un user agent qui permet de rediriger un appel d'un point A à un point B.
- Proxy server : composant principal d'un réseau SIP. Il agit comme un interprète pour les demandes des clients qui recherchent des ressources d'autres serveurs. Il surveille et facilite les échanges.
  Le concept a été imaginé pour :
  - Être le plus «agnostique» possible afin de supporter de manière transparente les extensions de SIP ;
  - Conserver aussi peu d'informations que nécessaire afin de contrôler plus finement l'utilisation des ressources mémoire et CPU et ainsi être facilement évolutif.
- Registrar : il s'agit d'un autre concept fondamental de tout réseau SIP. Ce composant traite un type de requête SIP spécifique et permettra d'associer à une URI SIP (URI : chaîne de caractères identifiant une ressource sur un réseau) l'emplacement spécifique du terminal sur le réseau. L'association entre URI SIP et adresse IP se fera au sein d'un «Location Service» également défini dans le RFC et qui consiste en une base de données virtuelle.
- Back-to-Back User Agent (B2BUA) : entité logique qui reçoit des requêtes SIP et les traite comme le ferait un user agent en mode serveur. Ensuite, pour déterminer comment répondre à la requête, il se comportera comme user agent en mode client. Dit plus simplement, chaque appel entrant génère automatiquement un appel sortant. C'est ainsi que les infrastructures SIP reposant sur un B2BUA auront un contrôle plus fin sur les appels avec des possibilités additionnelles de transcodage des flux audio et vidéo et de manipulation de ces derniers (annonces de pré-décrochage, temporisation, …). Si le contrôle est plus fin, l'évolutivité sera pourtant bien moins importante que pour une infrastructure reposant sur un proxy server.

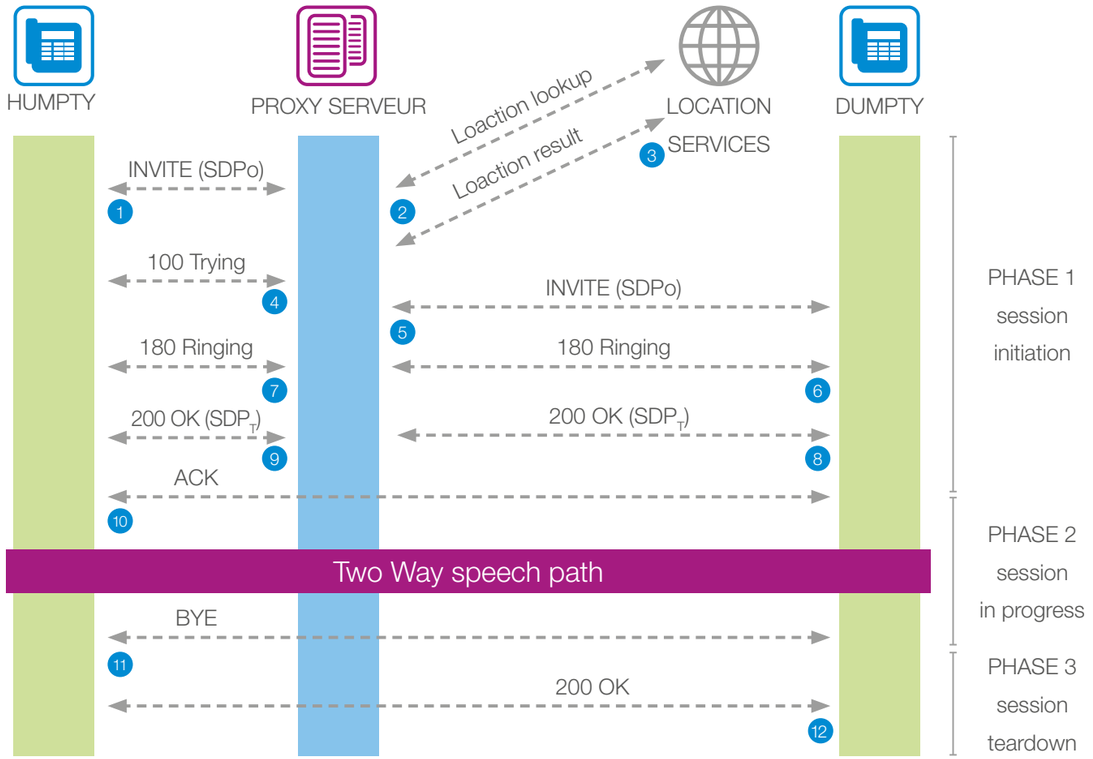
On retrouvera donc sur le marché de nombreux serveurs SIP construits autour d'un proxy server, et de nombreux serveurs SIP reposant sur un back-to-back user agent. Certains même combinant les deux approches afin d'en tirer le meilleur parti.

1.5.2. Mécanisme d'un appel SIP

Le protocole SIP, qu'il permette à des téléphones de communiquer entre eux ou encore de se connecter à un fournisseur de minutes SIP, sera identique et repose sur deux types de messages dont certains sont inspirés du fameux protocole HTTP :

- Les requêtes : un UA enverra une requête INVITE afin, par exemple, d'établir un appel. Les requêtes définies par le RFC 3261 sont au nombre de 6. D'autres RFC définissent d'autres requêtes ayant d'autres objectifs, mais tout en conservant les mêmes règles de construction et de routage que celles édictées par le RFC 3261. Cela permet donc à un proxy server n'ayant pas la connaissance de ces requêtes de les router d'un UA à un autre sans perte de fonctionnalité.
- Les réponses : ce sont des réponses à une requête reçue, générées par l'entité distante. Elles sont divisées en 6 classes. Par exemple, une requête d'appel envoyée à un utilisateur SIP inconnu générera une réponse de type «404 Not Found», réponse que l'on retrouvera également au niveau HTTP.

1.5.3. Un appel SIP



Exemple de flux d'appel sur base d'une architecture articulée autour d'un simple proxy server. Les étapes sont simples :

1. Humpty appelle Dumpty et envoie une requête INVITE au proxy server
2. Le proxy server regarde au sein du Location Service quelle est l'adresse IP réelle du poste appelé
3. Le proxy server reçoit la réponse du Location Service, et génère une réponse «100 Trying» indiquant qu'il va tenter de joindre le poste distant
4. Le proxy server relaie l'INVITE vers le poste distant maintenant qu'il connaît sa localisation exacte
5. Le poste distant accepte l'appel entrant et se met à sonner. Il en informe le proxy via une réponse «180 Ringing»
6. Le proxy server relaie la réponse à l'appelant
7. Le poste distant est décroché par l'utilisateur, l'appel est pris. Il génère une réponse «200 OK»
8. Le proxy server relaie la réponse «200 OK» au poste appelant
9. Le poste appelant envoie une requête «ACK» directement au poste appelé (elle peut passer par le serveur ou pas, suivant la négociation préalable et la configuration)
10. Le flux audio est établi directement entre les deux postes
11. Quand l'appelant raccroche, il envoie une requête «BYE» au poste appelé (qui peut également passer par le proxy server ou pas)
12. La réception de la requête «BYE» est confirmée par l'émission d'un message «200 OK» par le poste qui la reçoit

Il est à noter que le flux audio ne passera jamais par le proxy server car un proxy server ne gère que les messages SIP (la signalisation) et pas les flux audio. Il peut en aller autrement dans le cas d'un appel émis à travers un Back-to-Back User.

1.5.4. Signalisation et flux des communications

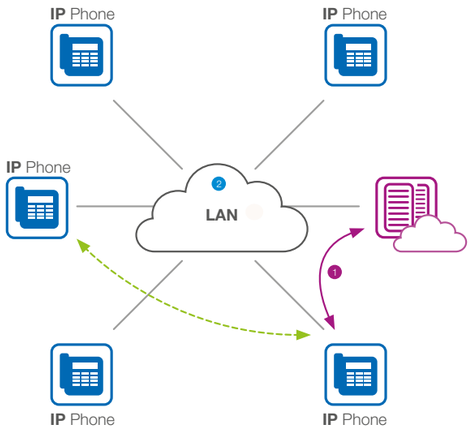
La signalisation échange les informations concernant l'appel, tels que les identifiants des postes, l'état, l'initialisation ou la libération de l'appel.

Qu'il s'agisse d'une architecture sur site ou dans le «Private Cloud», il est important de comprendre le cheminement des flux de communication. La signalisation en SIP utilise très peu de bande passante, alors que le transport des flux est consommateur.

Comme décrit précédemment, il existe plusieurs types d'architectures SIP. Parmi celles-ci, relevons les architectures basées sur un B2BUA, celles qui reposent sur un proxy pur qui ne gèrent que la signalisation ou encore celles s'appuyant sur un mélange des deux composants précédents.

Dans le cas d'un proxy, les flux de média transiteront directement en mode point-à-point, d'un terminal à un autre ou d'un terminal à une passerelle.

Dans le cas d'un B2BUA, les flux de média transiteront par le serveur. Cependant, certaines solutions disposent de mécanismes permettant de basculer les flux directement et dès que possible entre les deux terminaux impliqués dans l'appel. C'est ainsi que bien souvent seul l'enregistrement d'appels, les applications spécifiques de type menu vocal, boîte vocale, etc. nécessiteront de faire transiter les flux par le serveur.



Ce schéma illustre une architecture typique où les flux ne remontent pas par le serveur dans le Cloud, même en cas d'appel entre deux postes de sites différents. Lors d'un appel sortant vers un numéro public, et dans le cas de l'utilisation d'un SIP trunk, l'appel remontera par contre par l'infrastructure serveur.

En cas de solution multi-sites, il n'est pas rare que les bandes passantes disponibles et réservées à la voix diffèrent d'un site à l'autre. Il est dès lors important que la solution IP dispose d'un mécanisme de Call Admission Control afin de garder le contrôle sur les flux média au sein de votre architecture. Chaque site aura une sortie réseau limitée en bande passante. Le lien privé vers le data center hébergeant le serveur de communications sera également limité. Il est donc nécessaire que la solution de communications garde le contrôle sur les flux.

Le mécanisme de Call Admission Control aura dès lors deux rôles importants pour une qualité de communication irréprochable :

- La compression des appels transitant en inter-sites et vers le DataCenter afin d'économiser la bande passante.
- Le comptage des appels au niveau de chaque site. Tout appel qui pourrait potentiellement surcharger la bande passante allouée garantie sera refusé avec, par exemple, une tonalité de congestion, tout comme cela serait le cas lorsqu'on essaye de faire passer plus d'appels sur une ligne traditionnelle que ce qu'elle ne permet de transporter.

1.5.5. SIP providers

Migrer vers la VoIP et utiliser le protocole SIP pour établir des sessions d'appel permet en toute logique de se passer de la connectivité traditionnelle, tels les accès ISDN et analogiques.

Vous utilisez dès lors la connexion vers Internet afin de faire transiter les messages et requêtes SIP jusqu'à un serveur idéalement placé, qui ressortira sur le réseau classique à un tarif plus avantageux puisque l'appel aura transité par le réseau informatique avant de ressortir. De plus, il est possible d'obtenir des numéros «traditionnels» indépendamment de la localisation géographique de l'entreprise.

Des fournisseurs d'accès permettent d'établir et de recevoir des appels vers et/ou à partir de numéros «traditionnels» en utilisant le protocole SIP. On les appelle ITSP (Internet Telephony Service Provider ou Fournisseur de Services de Téléphonie sur Internet). Connus aussi sous le nom de fournisseur VoIP, ils proposent des SIP trunks à cet effet.

1.5.6. SIP trunk

Si on prend l'exemple d'une société belge appelant fréquemment aux États-Unis, on peut imaginer l'appel transiter via SIP jusqu'à un serveur SIP situé aux États-Unis et ressortant sur les lignes locales directement là-bas. Ceci permettant donc d'appeler au tarif local américain plutôt qu'au tarif international belge. Cet exemple est bien entendu volontairement simplifié.

En détails

Il existe en pratique deux types de fournisseurs de SIP trunking :

- Les opérateurs qui permettent un accès à leur infrastructure à partir de n'importe où dans le monde. Ils ne peuvent toutefois pas garantir la qualité de la communication voix. En effet, les paquets SIP et RTP transiteront par un certain nombre de routeurs IP et de lignes sur lesquels le fournisseur n'a pas de contrôle. En outre, la qualité de ces lignes pourrait être aléatoire en fonction des pannes, du trajet réellement emprunté par les paquets IP et de la charge du réseau.
- Les opérateurs qui offrent un accès à leur infrastructure à partir de leurs liens. Ils contrôlent la qualité du transport de la voix depuis votre entreprise jusqu'à leur infrastructure SIP. Il leur incombe par la suite d'obtenir les bons accords afin de pouvoir acheminer avec qualité la voix, de la manière la moins coûteuse depuis leur infrastructure jusqu'à la destination réelle de l'appel.

Plus de possibilités et de flexibilité

Le remplacement d'une connexion ISDN au profit d'une connexion SIP comporte quelques avantages comme profiter d'une plus grande flexibilité et de capacités étendues.

- Réduction des coûts de connectivité.
- Une bande passante plus large peut être mise à disposition pour intégrer à la fois voix, vidéo et données.
- La limitation à 2 ou 30 canaux par connexion est abolie au profit d'un dimensionnement plus précis et plus souple.

1.5.7. Session Border Controller (SBC)

Session : Communication entre deux parties ou l'appel téléphonique

Border : Point de démarcation entre 2 réseaux différents

Control : Capacité à manipuler les flux de données

Un Session Border Controller (SBC) est un équipement hardware ou une application software qui gère la façon dont les communications téléphoniques SIP sont initiées, acheminées et clôturées dans un réseau Voice over Internet Protocol (VoIP). Dans la littérature professionnelle, les communications téléphoniques sont habituellement désignées comme des sessions.

Un SBC fonctionne comme une sorte de pare-feu entre deux réseaux, où seules les sessions autorisées peuvent transiter via le point de raccordement (la frontière). Parallèlement, le SBC peut assurer l'adaptation des protocoles SIP et donc l'interopérabilité. Par la normalisation et la médiation des flux SIP, on peut adopter une connectivité multi-vendeurs et multi-protocoles. Le SBC définit et contrôle le niveau de la Qualité de Service (QoS) pour toutes les sessions, de telle sorte que les appels d'urgence, par exemple, arrivent directement au bon endroit et reçoivent en outre la priorité sur les autres appels. Les SBC sont généralement configurés comme des SIP back-to-back user agent (B2BUA). Un back-to-back user agent opère entre les deux extrémités d'une communication, divise le canal de communication en deux «call legs» et effectue la médiation de toutes les signalisations SIP entre les deux extrémités de l'appel, depuis son initiation jusqu'à la fin.

1.5.8. Pourquoi un SBC est-il nécessaire ?

Flexibilité

En séparant son réseau Cloud privé du réseau du fournisseur de services, l'utilisateur possède une totale indépendance. Ainsi, des changements peuvent être rapidement effectués dans un Cloud privé, sans devoir préalablement négocier avec le fournisseur de services.

Les flux de signalisation et RTP peuvent être normalisés entre les différents réseaux en interne et en externe, complétés par la traduction de protocole, le transcodage média et la QoS.

De plus en plus de SIP trunks venant de différents fournisseurs de réseaux peuvent être reliés au Cloud privé.

Dans des cas exceptionnels, un soutien peut même être offert pour des flux d'appel qui ne sont pas, en temps normal, pris en charge par le réseau du fournisseur d'accès.

Sécurité

La politique de sécurité du Cloud privé peut être fortement étendue sans devoir tenir compte de la politique de sécurité appliquée au réseau du fournisseur de services.

La topologie du réseau Cloud privé est totalement cachée du monde extérieur.

Le SBC offre une protection contre les vulnérabilités du protocole SIP.

Une protection également contre les attaques DoS (Denial-of-Service/par déni de service) en provenance du réseau public.

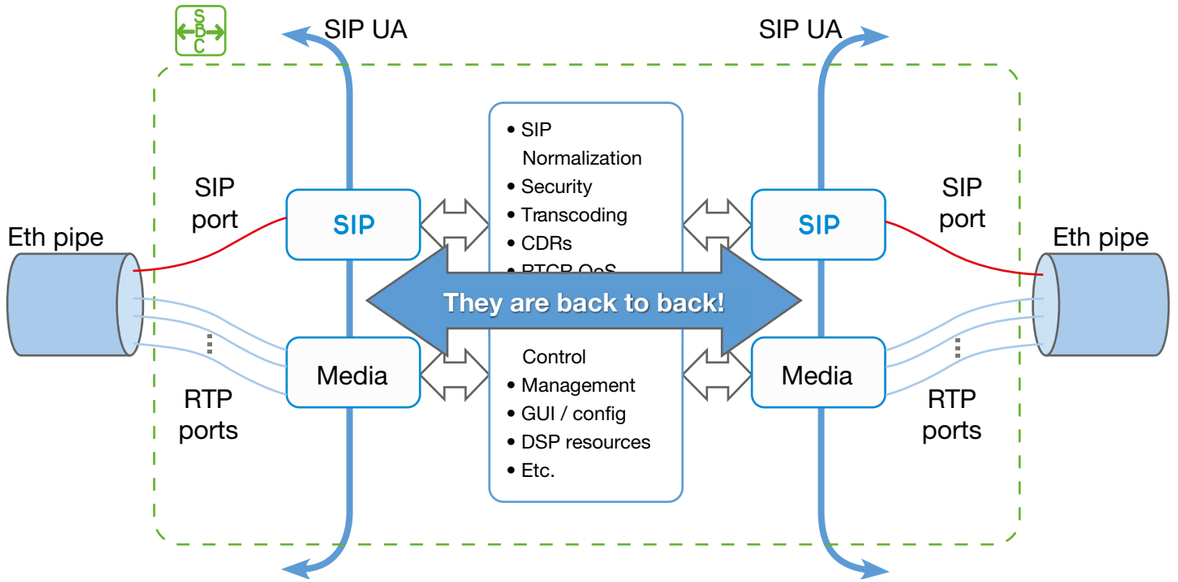
Logging & Reporting

Enregistrement de chaque statut d'appel, QoS et monitorage SLA

Enregistrement des tentatives d'intrusion

Enregistrement des sessions

Facturation



http://www.moythreads.com/congresos/empowered-bogota-2014/empowered-bogota-sbc-workshop-2014.pdf

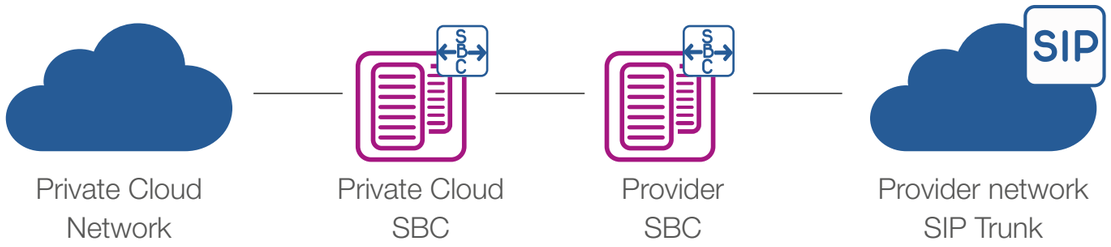
1.5.9. Où placer le SBC ?

Pour des raisons de sécurité, le SBC peut être placé tant du côté opérateur que de l'entreprise, voire des deux.

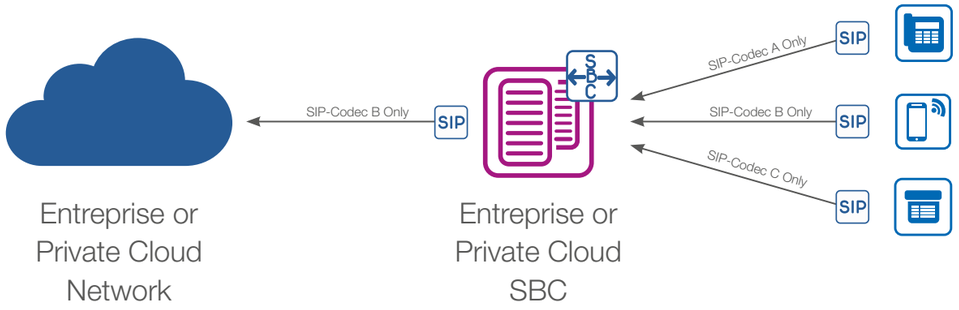
Le SBC est souvent installé au point de démarcation, entre une partie du réseau et une autre. La plupart des SBC sont placés entre les réseaux peering des fournisseurs d'accès, entre le réseau de l'entreprise et le réseau du fournisseur de services, ou entre le réseau du prestataire de services et les utilisateurs privés.

Les schémas ci-dessous permettent de voir où un SBC peut être installé.

Entre le Cloud privé et le réseau du fournisseur d'accès. Le SBC agit comme un dispositif de sécurité et comme régulateur des flux SIP entrants et sortants.



Un SBC placé du côté de l'entreprise est généralement considéré comme un E-SBC (Entreprise Session Border Controller). Le SBC fonctionne ici essentiellement comme un dispositif de sécurité et normalise les connexions SIP des appareils du côté public.



1.6. Mobilité

La mobilité de la téléphonie au sein d'un ou plusieurs sites peut être assurée de différentes façons.

- Généralement, les entreprises souhaitent pouvoir bénéficier de l'ensemble des fonctionnalités du central téléphonique sur un appareil portable et pouvoir en même temps circuler dans un bâtiment, un entrepôt ou un parking, tout en maintenant une communication ininterrompue.
- Que l'on parle de DECT ou de WiFi, il est nécessaire de garantir des fonctions de type Handover pour que la communication soit relayée d'une antenne à l'autre lorsqu'on se déplace.
- Pour pouvoir utiliser l'ensemble des fonctionnalités d'un central téléphonique spécifique, aujourd'hui encore, beaucoup de ces appareils sont dits «propriétaires» et donc rarement interchangeables.
- Le déploiement d'une solution DECT passera par l'installation de stations de base, qui seront placées en nombre plus ou moins important selon le volume de communications désiré et la nature des matériaux du bâtiment.
- En milieu professionnel, le déploiement de solutions basées sur le DECT est aisé vu qu'il dispose de sa propre bande de fréquence, contrairement au WiFi.
- Qu'il s'agisse d'antennes WiFi ou de stations de bases DECT, estimer le nombre d'antennes nécessaires est le préalable à toute installation. Il est possible de procéder soit par estimation, pour des espaces simples, soit par simulation, sur base de plans tenant compte ou pas des matériaux.
- Enfin, la méthode la plus fiable consiste à effectuer des mesures sur place, avec un équipement permettant de calculer précisément le niveau de réception et la qualité de couverture. Cette dernière méthode – qui a généralement un coût – offre l'avantage d'un engagement contractuel de résultat par l'entreprise mandatée. Le plan ainsi généré, intègre la répartition des zones selon la force du signal. On pourra renforcer certaines zones en fonction de la densité des utilisateurs ou prévoir des antennes supplémentaires pour des secteurs critiques, afin de parer à toute panne.

Il existe plusieurs types de stations de base «spécialisées» d'intérieur, d'extérieur ou conçues pour fonctionner en environnement explosif (ATEX).

Il existe différents types de postes DECT, des plus traditionnels à ceux répondant aux normes ATEX, souvent plus onéreux. D'autres appareils encore sont équipés d'un système permettant de réagir à une perte de verticalité, une propriété utile notamment pour des personnes effectuant des rondes de garde, vu que ce système permet de signaler une chute ou une agression.

Marquage ATEX pour les équipements électriques certifiés pour atmosphères explosives

1.6.1. Digital Enhanced Cordless Telecommunications (Dect)

Le DECT (télécommunication numérique sans fil) est une norme de téléphonie sans fil, originaire d'Europe, qui remplace les normes téléphoniques précédentes CT1 et CT2. DECT est une technologie cellulaire qui utilise la gamme de fréquence 1.800/1.900 MHz.

Le standard DECT est conçu pour fournir des services de mobilité dans des environnements à forte intensité d'utilisateurs, tels que les grands immeubles ou les campus : 10.000 Erlang/km2 (GSM 200 Erlang/km2, DCS 500 Erlangs/km2). L'Erlang mesure le taux d'occupation d'un équipement de communication sur une période donnée.

Cette norme, basée sur la technologie numérique, offre une communication de haute qualité, avec des capacités de roaming et d'itinérance (sans fil).

Le CDCS (Continuous Dynamic Channel Selection) est une fonctionnalité unique qui assure à chaque téléphone mobile d'opérer sur le meilleur canal radio disponible. En outre, aucune planification des fréquences n'est nécessaire lors de l'ajout d'une station radio de base. Toutes les stations de base peuvent émettre sur n'importe quel canal.

Les stations de base DECT sont reliées à un dispositif de commande ; elles peuvent également être directement connectées au central téléphonique. Certains constructeurs proposent des stations de base DECT couplées à une carte digitale. Les stations de base DECT les plus courantes sont raccordées via un câblage distinct.

La norme DECT inclut un profil standard d'interopérabilité appelé GAP ou Generic Access Profile (ETSI standard 300.444), qui permet la compatibilité des stations DECT avec les appareils d'autres constructeurs.

Le «call recovery» est un plus de la téléphonie DECT. Si un utilisateur quitte la zone de couverture radio ou en cas panne de liaison radio, un appel en cours est automatiquement mis en attente. Dès que l'utilisateur revient dans une zone de couverture, son combiné est rappelé et il/elle peut récupérer l'appel. Si par contre, l'usager ne revient pas dans une zone de couverture endéans une durée prédéfinie, les appels internes sont abandonnés et les appels externes redirigés vers le standard.

1.6.2. IP Dect

Les stations de base IP DECT peuvent se connecter directement au réseau Ethernet existant. Leur avantage est de pouvoir utiliser la même infrastructure de réseau que pour les données. Ces stations de base peuvent dans la plupart des cas être alimentées via la technologie PoE (Power over Ethernet), conforme à IEEE 802.1af ou PoE+, conforme à IEEE 802.1at. Elles offrent également la possibilité d'être raccordées via un adaptateur externe sur le secteur.

1.6.3. Voice over WiFi (VoWiFi)

Téléphoner sans fil via WiFi

Nombreuses sont les entreprises qui sont équipées d'un réseau WiFi sur leur site. Pourquoi dès lors ne pas également utiliser cette infrastructure pour la téléphonie sans fil ? Dans le monde de la téléphonie IP, VoWiFi est une alternative aux appareils sans fil DECT.

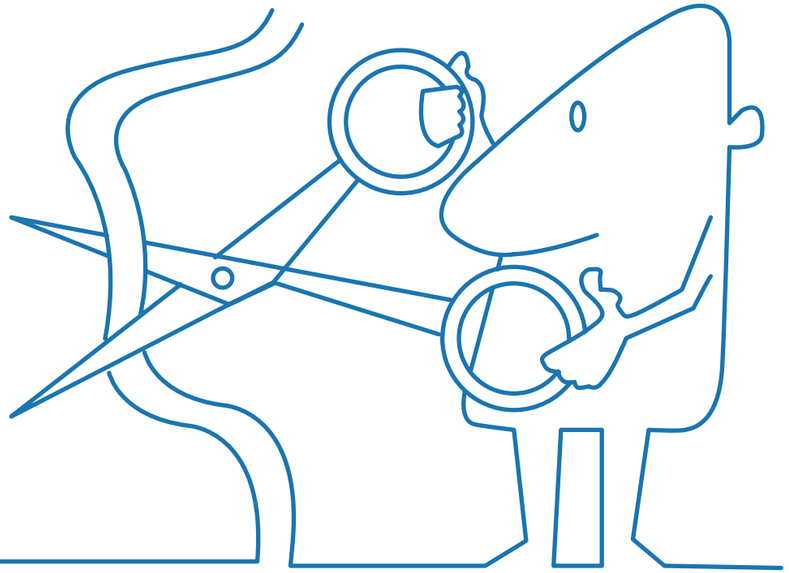
La téléphonie sans fil WiFi, appelée VoWiFi, est particulièrement adaptée aux grandes implantations, dans lesquelles un nombre important de collaborateurs doivent communiquer entre eux. Les utilisateurs peuvent ainsi se déplacer librement sans jamais perdre le contact. En outre, il n'est pas nécessaire d'investir dans un réseau distinct.

Tout comme dans la téléphonie IP où il n'est plus nécessaire de maintenir deux réseaux câblés (un pour la voix et un pour les données), VoWiFi n'a plus besoin non plus de deux réseaux radio. Au lieu de la norme DECT pour la téléphonie sans fil, vous utilisez le réseau WiFi pour la téléphonie IP.

Si votre entreprise ne dispose pas encore de solution de téléphonie sans fil, nous vous recommandons le déploiement de VoWiFi, vu que vous avez déjà un réseau WiFi en interne. VoWiFi fonctionne sur les ordinateurs portables, les PDA, les GSM et sur les appareils téléphoniques portables WiFi.

Spécifications techniques

L'impact de la VoWiFi sur le réseau WiFi (IEEE 802.11) ne doit pas être sous-estimé. Pour garantir une bonne qualité, la force du signal WiFi doit être beaucoup plus élevée (-65 dBm au lieu de -70 dBm). Il est donc essentiel de prévoir suffisamment de points d'accès sans fil afin de bénéficier partout d'une couverture radio suffisante.



COMMUNICATIONS UNIFIÉES

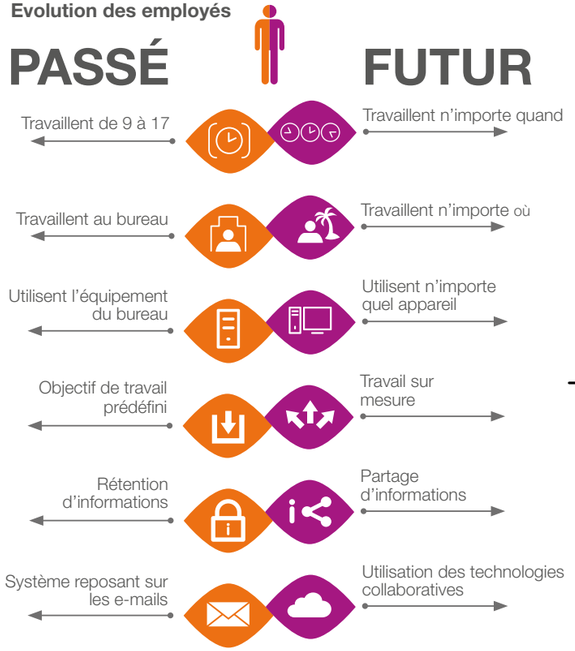
2. COMMUNICATIONS UNIFIÉES (UC)

Les Communications Unifiées visent à rassembler un ensemble de services en un minimum d'outils : appels téléphoniques fixes ou mobiles, systèmes de conférences, messagerie instantanée, gestion de la présence, agendas, vidéo conférence, partage de documents, présentations, e-mail, fax, messagerie vocale, etc.

En unifiant les communications, les constructeurs cherchent à ce que l'expérience reste la plus similaire possible quel que soit l'appareil (device) employé par l'utilisateur : poste téléphonique, smartphone, ordinateur, tablette…

L'enjeu est complexe, car cette approche ne répond pas à une simple mode mais bien à une demande réelle des utilisateurs qui, désormais habitués à retrouver la même expérience sur l'ensemble des supports dont ils disposent, ne peuvent plus concevoir qu'un appareil ne soit pas en mesure d'offrir un contexte simililaire d'un dispositif à un autre.

Evolution des employés



SOURCE : @ Chess Media Group

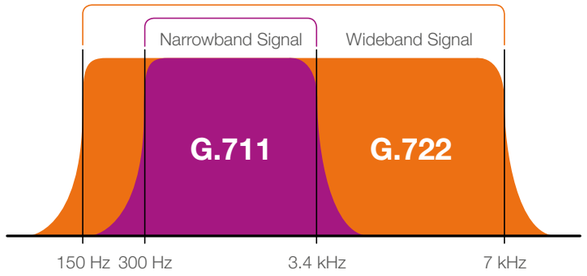
2.1. Média et services

2.1.1. Audio

Face à l'émergence des Communications Unifiées, le paysage de la téléphonie traditionnelle a profondèment changé. Les nouveaux appareils tirent parti du protocole IP ou SIP, ce qui permet d'obtenir une meilleure qualité audio qu'avec des appareils analogiques classiques ou numériques. L'utilisation de la norme G.722 permet d'obtenir une qualité de voix de téléphonie large-bande, en comparaison de la norme G.711, sans optimiser la bande passante via une connexion Ethernet. Du côté de l'Ethernet, les deux protocoles utilisent des débits de 64 Kbps sans compter l'Overhead (Surcharge provoquée par le découpage du fichier et l'ajout d'adresses de contrôle). Avec celui-ci on arrive à un bit rate théorique d'un peu moins de 100 Kbps.

L'audio est disponible sur les appareils téléphoniques, smartphones, tablettes, PC.

2.1.2. Frequency response



G.711, G.722 Frequency response

2.1.3. Vidéo

En ce qui concerne la vidéo sur IP, il est très important de pouvoir compter sur la bande passante. Une conversation vidéo haute définition de 720p peut rapidement utiliser jusqu'à 1 Mbps. Aujourd'hui, ce n'est pas un problème au niveau LAN car les vitesses dans ce cas peuvent souvent s'élever à 100 Mbps ou 1Gbps. Dans le domaine WAN, c'est toujours un facteur qu'il faut prendre en compte. Il existe différents codecs pour envoyer de la vidéo sur IP.

En voici quelques exemples:

- H.261 est un standard de compression vidéo, développé initialement pour la transmisson via des lignes ISDN à des débits de 64 kbit/s.
- H.263 est une norme de codage vidéo développée pour la transmission de visioconférences sur des lignes à bas débits. Elle a d'abord été mise au point pour une utilisation dans les systèmes H.324 (RTC et autres réseaux à commutation de circuits de visioconférence et vidéotéléphonie), mais elle a ensuite été intégrée dans des protocoles de visioconférence du type H.323 (visioconférence sur RTP/IP), H.320 (norme de visioconférence sur ISDN), RTSP (média en mode streaming) et SIP (systèmes de conférence par Internet).
- H.264 est également connue sous le nom MPEG4 AVC (Advances video coding). Les appareils de visioconférences les plus récents utilisent le codec H.264.

2.1.4. Chat

Un outil de chat classique fournit en général trois fonctionnalités majeures :

- La messagerie instantanée, c'est-à-dire la possibilité de s'envoyer des messages textuels longs ou courts d'un utilisateur à l'autre ;
- Une liste de contacts, c'est-à-dire que les contacts les plus courants sont en général repris au sein d'une liste affichant le nom du contact, son état de présence (en ligne, absent, occupé, …), et éventuellement sa photo de profil ;
- La possibilité de publier un état de présence personnel qui sera relayé aux utilisateurs ayant votre contact dans leur liste de contact.

D'autres fonctionnalités telles que le partage de bureau ou encore le transfert de fichiers peuvent venir s'y ajouter.

Il existe de nombreux protocoles autour desquels différents produits de «chat» sont articulés, sans pour autant être compatibles entre eux, de l'ancêtre ICQ aux plus populaires qui ont été entretemps intégrés dans la gamme de grands producteurs de logiciels.

Dans le monde des standards, deux protocoles permettent au moins la messagerie instantanée, les listes de contacts avec notion de présence et la publication d'état de présence dominent le marché.

D'une part XMPP (Jabber®) et d'autre part son alternative articulée autour de SIP : SIP/SIMPLE.

L'avantage de XMPP est que le protocole est largement éprouvé, complet et fonctionnel.

L'avantage de SIP/SIMPLE est qu'il est également pensé «téléphonie» et est donc parfaitement intégré à ce monde tout en fournissant l'essentiel des fonctionnalités.

C'est ainsi qu'un simple softphone ou un téléphone compatible SIP pourra indiquer l'état de présence des collègues, permettant ainsi de savoir s'il est utile de tenter de joindre un collègue en particulier ou s'il est en rendez-vous.

De manière similaire, un serveur SIP pourra router les appels différemment suivant l'état de présence.

2.1.5. One Number et Rapid Session Shift

Le One Number permet de joindre tout utilisateur à partir d'un seul numéro quel que soit le dispositif employé et ce de manière totalement transparente pour l'appelant. Ce sera à l'appelé de définir préalablement soit l'appareil sur lequel il voudra être joint, soit un ensemble d'appareils qui sonneront simultanément ou une stratégie, l'ordre dans lequel ses appareils sonneront.

Lorsque la communication est établie, grâce au Rapid Session Shift, la communication ou la vidéoconférence glissera de manière continue d'un autre appareil sans rompre la conversation ou envoyer une musique d'attente. L'utilisateur appuie sur une touche ou sélectionne dans un menu le dispositif cible. Le changement de session peut être activé par l'utilisateur tant sur un appel sortant ou qu'entrant.

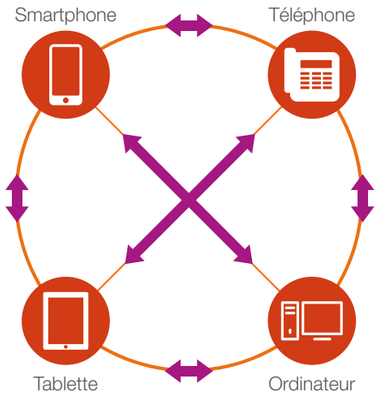
2.1.6. Ad hoc Conferencing

Une conférence «ad hoc» est une conférence téléphonique qui a été initiée «à la volée». Cela signifie qu'en partant d'une conversation normale vous évoluez vers une conférence multipartite en ajoutant des utilisateurs. En utilisant la fonction Rapid Session Shift telle que décrite ci-dessus, il est possible de passer d'un téléphone fixe à un PC par exemple. Ensuite, il est également possible d'y ajouter, par exemple, la vidéo ou le partage de documents.

2.1.7. Reserved Conferencing

Lorsque la conférence est planifiée, une invitation est envoyée à tous les participants. Cette invitation peut être un e-mail ou une invitation dans le calendrier. Cette invitation contiendra une URL (adresse web) un login et un mot de passe. La plupart du temps cette invitation contient en outre un numéro de téléphone qui peut être utilisé pour suivre la conférence. Une fois connecté dans le pont de conférence, les possibilités telles que la messagerie instantanée, le partage de bureau, le partage de documents, le partage de présentation sont désormais disponibles. Il est également possible d'établir en parallèle une session de messagerie instantanée avec un ou plusieurs participants à la conférence.

2.1.8. Communication muti-device ininterrompue



2.1.9. Web Real-Time Communication (WebRTC)

L'idée du WebRTC est de faire de tout appareil connecté un dispositif de communication et pouvoir partager en temps réel un maximum d'informations (appels, messages instantanés, partage de fichier, partage d'écran) entre navigateurs (browsers).

Les applications WebRTC offrent par exemple la possibilité d'appeler en ligne un conseiller d'un magasin dont nous sommes en train de consulter le site en cliquant sur le bouton « appel », faire appel à de l'assistance en ligne ou créer un réseau social dynamique interne à l'entreprise.

La richesse et les fonctionnalités dépendront de la fonction que l'on voudra donner à cette interface.

Avec les Communications Unifiées, c'est aussi l'avènement du numéro unique. L'approche WebRTC permettrait de se passer à la fois de l'installation d'applications, des circuits des opérateurs téléphonique et même à terme, du numéro de téléphone.

Ce nouveau standard s'avère en tout cas riche en possibilités et offrira aux entreprises de nombreuses nouvelles applications créatives.

CLOUD

3. CLOUD

3.1. Les Communications Unifiées en mode Private Cloud

Peut-on ignorer le nombre de nouveaux dispositifs de communications qui ont envahi notre environnement en moins de 10 ans ?

Peut-on affirmer connaître aujourd'hui tous les outils disponibles dans les 5 prochaines années ?

La génération née dans les années 80-90 ne nous laisse pas l'embarras du choix, elle est connectée et avec tout ce qu'elle trouve sous la main. Il y a fort à parier que la vague suivante sera encore plus exigeante et plus créative encore.

Investir dans un central téléphonique en espérant que celui-ci passera de longues et paisibles années est devenu illusoire à moins d'ignorer la demande des utilisateurs. Il faudra sans cesse l'adapter, à un rythme de plus en plus élevé et ces mises à jour ont un coût qu'il est impossible de prévoir au moment de sa mise en service.

Le Private Cloud déplace cette problématique chez le prestataire, celui-là même qui sera en charge d'offrir un service de téléphonie toujours en concordance avec la réalité des technologies.

Le Private Cloud a la vocation d'assurer cette évolutivité permanente et de réduire à sa portion congrue le financement du matériel nécessaire à communiquer qui représente le premier frein à l'évolutivité.

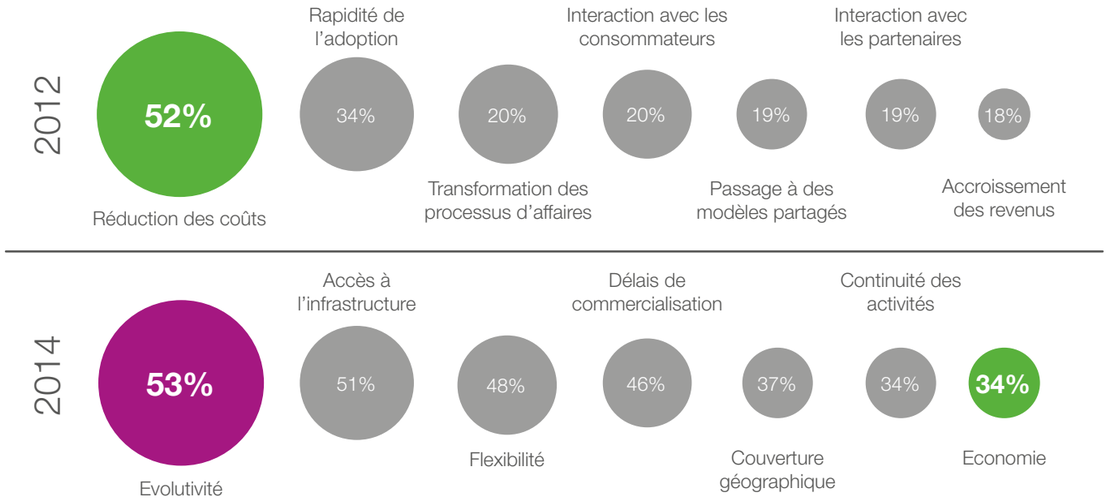
Le coût n'est plus représentatif de l'investissement à consentir mais bien du niveau de service et d'efficacité que l'on tient à garantir à ses collaborateurs. Grâce au Private Cloud, ce coût fixe est établi et permet de répondre avec précision avec un ensemble de fonctionnalités exigées, pour des utilisateurs dont le nombre et les attentes peuvent varier à tout instant.

En 2014, 53% des motivations d'adoption d'une solution Private Cloud est l'évolutivité [1], alors qu'en 2012 la réduction des coûts était la première pour 52 % des IT Executives [2]. Aujourd'hui, l'aspect coût ne constitue plus que 34% des motivations.

[1] Rightscale State of the Cloud Report 2014

[2] KPMG- Research- Global cloud surveys 2012

3.1.1. Les principales raisons pour adopter le Cloud



3.1.2. Caractéristiques du Private Cloud

Du point de vue de l'exploitation quotidienne, la solution externalisée ne diffère de la solution locale que par l'absence sur site de « l'intelligence » du système. Elle n'impose aucune restriction d'utilisation. La gestion et l'accès aux ressources reste rigoureusement identique ou peut être également confiée au partenaire.

Le système d'exploitation de la solution Private Cloud fait partie intégrante du réseau de l'entreprise, dans un environnement hermétiquement sécurisé dans une infrastructure dédiée.

Economies

Service facturé sur base de l'utilisation réelle, pour un coût unitaire fixé initialement.

Flexibilité

Ajout ou suppression d'utilisateurs ou de fonctionnalités en toute facilité.

Sécurité

Hébergement de la téléphonie dans un environnement redondant sécurisé jour et nuit.

Evolutivité

Le système bénéficie en permanence des mises à jour correctives et évolutives. Elles sont testées préalablement avant d'être distribuées. L'accès à ces mises à jour fait partie du service offert mais elles peuvent aussi être facultatives si des applications ou des équipements spécifiques au client l'exigeaient.

3.2. Cloud privé et public

La définition précise reste un vaste débat d'ordre plutôt commercial.

Dans cet ouvrage, nous sommes partis du postulat que la différence résidait dans la parfaite connaissance de l'ensemble de l'architecture ou non. Le Cloud privé serait dès lors la virtualisation de l'infrastructure auprès d'un fournisseur au travers d'un opérateur dont l'équipement, les mesures de sécurité et le parcours des données seraient parfaitement connus. D'une part, le design se doit de garantir un niveau de sécurité tel qu'il puisse être considéré comme une extension du réseau interne, pouvant afficher les mêmes garanties qu'une gestion en interne. D'autre part, et particulièrement en termes de communications, la connexion doit pouvoir offrir de bout en bout la Qualité de Service (QoS). Nous considérerons donc ici toute autre approche comme publique.

3.2.1. Internet Protocol - Virtual Private Network (IP-VPN)

Il s'agit d'un réseau privé virtuel, dans le sens « logique » du terme, établi dans un réseau public, celui d'un opérateur. Il fonctionne comme s'il s'agissait d'un réseau câblé interne.

Un IP-VPN, établi entre plusieurs bâtiments, permettra de considérer l'ensemble de ces bâtiments comme un seul réseau et donc, les appareils qui y seront connectés bénéficieront des mêmes ressources quelle que soit leur situation géographique.

L'authentification et l'encryption seront les mécanismes mis en œuvre pour assurer la sécurité et la confidentialité des données transmises. Seuls les utilisateurs autorisés pourront accéder au réseau virtuel.

Il permet l'étanchéité vis-à-vis des autres flux sur l'infrastructure publique ainsi que l'activation de la QoS.

Du point de vue de la Voix sur IP, cette approche permettra d'envisager la gratuité des appels inter-sites et la mutualisation des connexions vers le réseau public. En outre, l'ensemble des sites pourront être considérés et gérés comme un vaste central avec, par exemple, un plan de numérotation global.

3.2.2. Connexion au data center

La liaison au data center du fournisseur d'infrastructure Cloud privé se fait au travers du backbone d'un opérateur. La connexion à celui-ci se fait au travers d'une liaison fibre optique, cuivre (VDSL ou Ethernet sur cuivre) ou câble coaxial suivant les disponibilités locales de l'opérateur. Ce lien fera transiter la signalisation permettant de connaître l'état des communications, mais aussi éventuellement, suivant le constructeur et l'architecture de la solution Communication Unifiée, les conférences vocales, vidéos, la messagerie vocale, les guides vocaux, etc.

Cette liaison n'influence pas le choix de connexion vers le réseau public, toutefois, si l'option SIP est retenue pour la connexion vers le réseau public, elle pourra se faire également au travers de ce backbone.

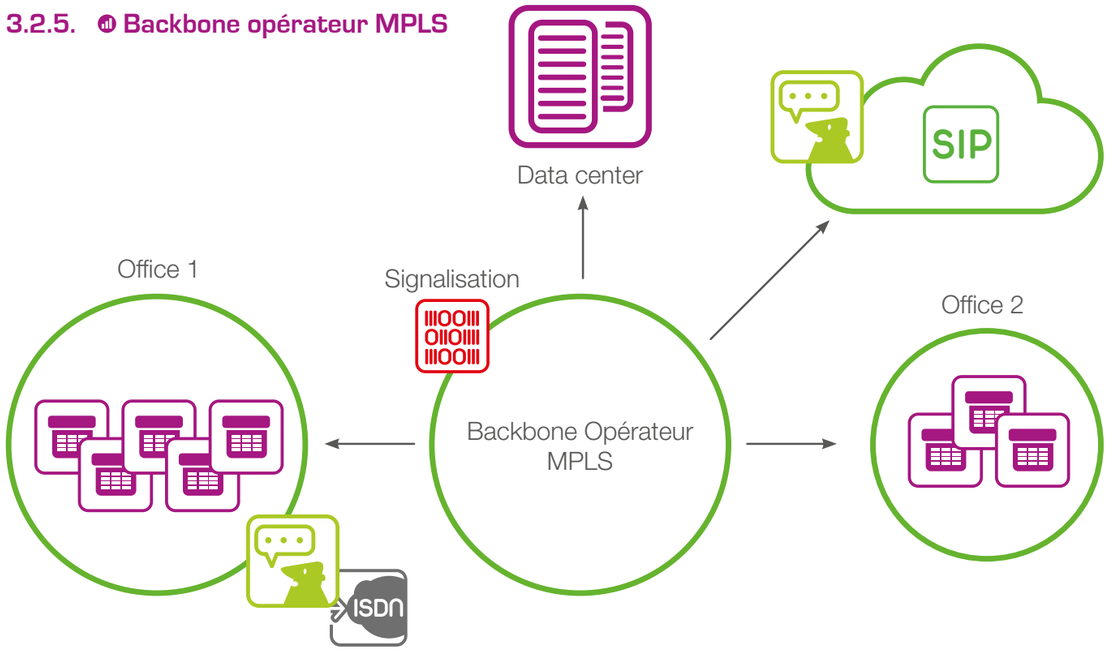
3.2.3. Multi-Protocol Label Switching (MPLS)

Il s'agit de l'un des principaux protocoles utilisés pour le trafic IP sur les backbones haut débit des opérateurs. Il rend les flux totalement étanches et isolés entre les clients et permet l'envoi des données vers un ou plusieurs sites distants spécifiques.

3.2.4. Very High Bit Rate Digital Subscriber Line (VDSL)

Cette technologie permet des vitesses de transmission très élevées avec des signaux transportés sur une paire de cuivre.

3.2.5. Backbone opérateur MPLS



3.3. Data Center

Les données : à tout moment, partout et en toute sécurité

Le Voice Private Cloud s'appuie sur des data centers professionnels, qui stockent les données en toute sécurité et offrent une accessibilité à tout moment. Et comme la solidité d'une chaîne se mesure à son maillon faible, la redondance doit s'étendre à chaque niveau : réseau, stockage, serveurs…

- **Des services hautement professionnels**
  Dans un Voice Private Cloud, les changements de configurations ne sont opérés que par des ingénieurs certifiés.

- **Vos données valent de l'or**
  La gestion qualitative des données et leur sécurisation sont des postes coûteux lorsqu'une entreprise en a la charge individuellement. Il suffit de penser aux équipements, aux licences, au personnel nécessaire, le niveau d'expertise requis, les mises à jour, la perte des données en cas de problème…

- **Gestion professionnelle**
  Les entreprises sont de plus en plus nombreuses à migrer leurs données vers un data center externe professionnel. Elles bénéficient de cette façon des dernières technologies, d'une redondance à la pointe et d'un soutien professionnel évolutif. Leur département IT peut dès lors se concentrer sur d'autres tâches.

  «Dans l'univers IT, le Cloud Computing est le changement le plus important, le plus radical et le plus durable de ces dernières décennies. Nous sommes à l'aube d'une révolution et nous pouvons en être les acteurs, à condition de s'adapter… » dit Joseph Reger, CTO de Fujitsu (Reger, 2012)

  Aujourd'hui, la technologie des data centers a évolué au point de pouvoir gérer conjointement le trafic voix et vidéo dans le Cloud. Il est clair que seul les data centers qui satisfont aux exigences les plus élevées en matière de redondance sont pris en considération dans ce cas-ci. Dans ces data centers, rien n'est laissé au hasard. Monitoring, sécurité et choix du hardware sont d'une importance cruciale ! C'est la seule manière d'atteindre le niveau requis afin de gérer la voix et la vidéo.

- **For your eyes only**
  Un Private Cloud suppose que l'utilisateur final dispose de son propre parc de serveurs, son propre PABX, son propre reverse proxy… sans devoir le partager.
  Il octroie de surcroît à l'utilisateur son propre pare-feu de telle sorte que l'environnement reste strictement privé.
  De même, la connexion de et vers le data center est entièrement privée et n'est jamais partagée. Il s'agit donc bien d'une infrastructure voix, données et vidéo dédiée à 100%.

- **Toujours accessible**
  Un Voice Private Cloud comprend toujours plusieurs data centers. Grâce à une technologie en real-time, les données sont créées en miroir entre deux data centers. Vos données sont donc toujours stockées en deux exemplaires (redondant) derrière un double pare-feu. Si l'un des data centers tombe en panne, l'autre est prêt à prendre le relais. Le temps d'immobilisation est ainsi quasiment nul.

  Chaque cluster de serveurs/PABX doit également pouvoir être installé, le cas échéant, au moins une fois dans chacun des data centers. Ainsi, les clusters PABX peuvent être accessibles dans des sites géographiques distincts.

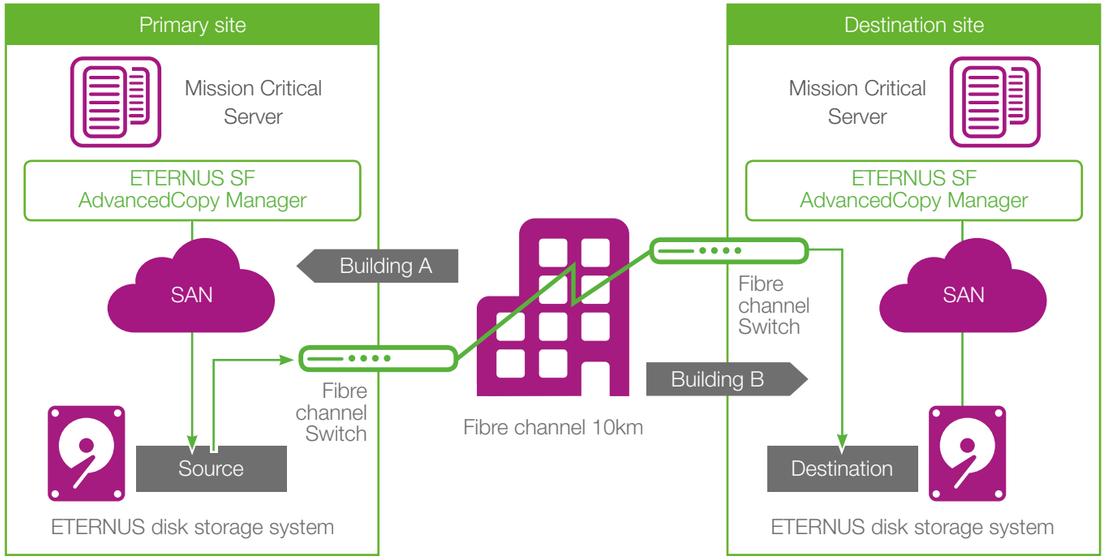
  Tous les serveurs privés doivent en outre être sauvegardés quotidiennement. Si jamais un des serveurs privés tombait en panne, une sauvegarde remontant à MAXIMUM 24 heures pourrait être restaurée.

- **Modulable selon les besoins de l'utilisateur**
  Un data center moderne dans le Private Cloud doit avoir la capacité de s'adapter à la croissance du client et offrir des options aisées d'extension ou de mise à jour. Les serveurs dans le Cloud doivent littéralement grandir au fur et à mesure des besoins des utilisateurs. (HD, CPU et mémoire)

- **Redondance**
  Un data center dans le Private Voice Cloud assure des technologies de redondance minimale afin d'offrir en continu voix, données et vidéo services aux utilisateurs.

Le stockage des data centers en miroir : un Voice Private Cloud comprend au minimum deux data centers ou au minimum deux bunkers distincts entre lesquels les données sont dupliquées en miroir. En cas de défaillance d'un data center, l'autre data center doit pouvoir reprendre l'activité sans perte de données. Sont utilisées dans ce processus des technologies spécialisées de duplication telles que Fujitsu REC (Remote Equivalent Copy).

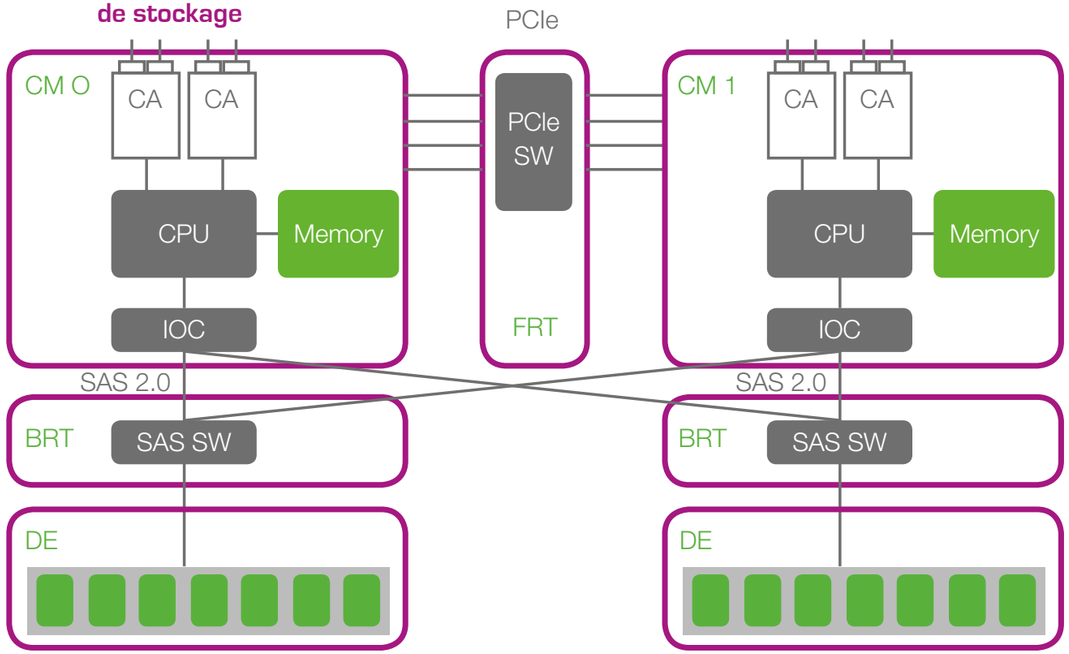
3.3.1. Duplication avancée à distance dans un environnement serveur Mission critical IA, UNIX ou Standard de l'industrie



SOURCE: http://www.fujitsu.com/global/products/computing/storage/disk/eternus-dx/feature/STRSYS_c01.html

Chaque data center se compose d'au moins un espace de stockage par site et deux sites au minimum sont prévus par Private Voice Cloud. Chaque unité de stockage doit posséder chacun de ses composants au moins deux fois. Plusieurs composants différents peuvent tomber en panne, mais lorsque deux composants similaires font défaut, tout doit commuter vers le site DR (Disaster Recovery). De la même façon, les contrôleurs de stockage peuvent être aisément mis à jour. Cette opération est totalement transparente pour l'utilisateur et ne nécessite pas de se connecter au site DR. Le schéma ci-dessous montre l'installation d'un contrôleur de stockage Fujitsu ETERNUS DX® tel qu'utilisé dans des data centers Private Cloud.

3.3.2. Installation d'un contrôleur de stockage



CA: Channel Adapter
IOC: I/O Controller
SAS SW: SAS Switch
BRT: Back-End Router
FRT: Front-End Router
PCIe SW: PCIe Switch

SOURCE : <<wp-eternus-dx-feature-set-ww-en.pdf P4 >>

- **RAID (Redundant Array of Independent Disks /Re-groupement redondant de disques indépendants)**
  Un contrôleur de stockage utilisé dans un Voice Private Cloud peut disposer d'une multitude de configurations RAID différentes sur la même plate-forme de virtualisation. La sélection du RAID s'effectuera en conséquence de l'application requise. Il est également possible de migrer d'un groupe RAID sélectionné vers un autre groupe RAID si les besoins ou les applications l'exigent.

3.3.3. RAID

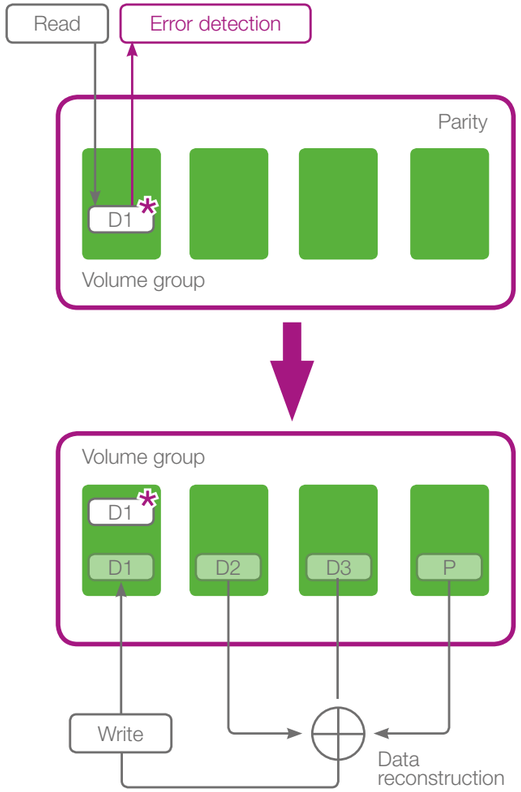
	Reliability	Data efficiency	Write performance
RAID 1	Good	OK	Good
RAID 1+0	Good	OK	very Good
RAID 5	Good	Good	Good
RAID 5+0	Good	Good	Good
RAID 6	Very Good	Good	Good

SOURCE : <<wp-eternus-dx-feature-set-ww-en.pdf P11 >>

- **Disk Drive Patrol**
  Cette technologie scanne en quelque sorte tous les disques du contrôleur de stockage. Si une erreur est détectée, celle-ci par cette information redondante est «réparée dans le groupe volume disponible» et retranscrite à un endroit plus fiable sur le disque.

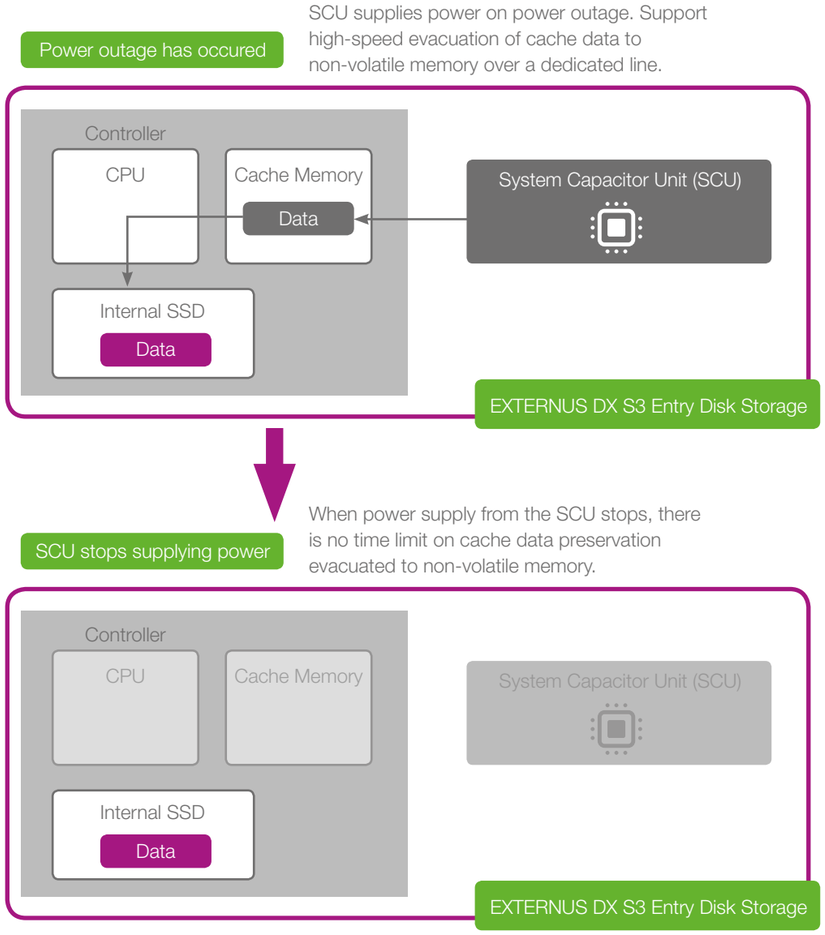
  Dans le cas d'une coupure d'alimentation ou d'un circuit électrique, même les données présentes dans le cache des contrôleurs de stockage ne seront pas perdues, grâce à une technologie telle que Cache Protector ®. En cas de coupure d'alimentation, une batterie interne peut retranscrire les données du cache sur un disque interne SSD. De cette façon, les données sont sécurisées en permanence. (Voir graphique 3.3.5)

3.3.4. Disk Drive Patrol



SOURCE : <<wp-eternus-dx-feature-set-ww-en.pdf P7 >>

3.3.5. Sécurisation des données Caches



SOURCE : <<wp-eternus-dx-feature-set-ww-en.pdf P8 >>

- **Spécifications techniques**
  Telic utilise les serveurs Fujitsu PRIMERGY X86 et ETERNUS DX storage afin de fournir des prestations de haute qualité. Ces équipements sont considérés comme les meilleures solutions « do more with less » du marché.

- **PRIMERGY X86**
  Les serveurs PRIMERGY ont une disponibilité moyenne du matériel de pas moins de 99,997%. Fujitsu a soumis ces serveurs à des tests exigeants afin de détecter le moindre défaut, réduisant au maximum le pourcentage de panne.

- En termes de vitesse de charge de travail, PRIMERGY bat également des records. Grâce à un traitement plus rapide, vous avez besoin de moins de systèmes pour la même charge de travail IT.

- La fonction Cool-safe Advanced Thermal Design permet à ces serveurs de tourner à des températures allant jusqu'à 40°C, ce qui permet d'économiser 27% d'énergie. Ces serveurs sont en outre les plus éco-énergétiques du marché (jusqu'à 20% de prestation supplémentaire par watt en comparaison des systèmes similaires). Ces serveurs sont non seulement moins chers à l'usage mais aussi plus respectueux de l'environnement.

- La gestion des ressources se déroule de façon dynamique, ce qui signifie que les serveurs physiques et virtuels reçoivent automatiquement la puissance de traitement dont ils ont besoin à tout moment. Et cela, pour une fraction du prix des méthodes traditionnelles de paramétrage.

- Cette génération de serveurs PRIMERGY peut facilement être intégrée à des environnements de gestion d'autres producteurs. Les coûts d'implémentation, d'adaptation et de formation peuvent par conséquent être réduits de 45%. Dans des environnements LAN et SAN, ces serveurs sont de surcroît très flexibles et faciles à gérer.

- PRIMERGY est la référence dans le domaine des solutions intégrées de stockage sur mesure pour votre entreprise. Le temps de mise en œuvre est réduit tout comme le risque d'échec de votre projet informatique.

- **Fujitsu ETERNUS DX**
  Le design unique et compact de ce système de stockage sur disque offre une architecture simplifiée et une totale compatibilité. L'ETERNUS DX est facilement extensible avec des disques ou des étagères supplémentaires sans devoir installer de logiciel additionnel.

- ETERNUS DX propose une plate-forme sécurisée grâce à :
  - Un Cache protector en combinaison avec un Cache Guard (sur SSD)
  - Un Data Block Guard & Oracle Database Data Guard
  - Une protection Raid, Hot-Spare, IO-Striping, IO-optimization et Fast Recovery

- La flexibilité de l'ETERNUS DX s'appuie sur des fonctionnalité logicielles telles que la virtualisation intégrée (ex. Thin-provisioning, Snapshot, Tiering, QoS, AQos…), l'intégration OS avec Windows 2012 et Unix (Linux, Suse, Solaris, AIX, HP…) et la virtualisation OS (ex. VMware, Hyper-V, Xen), Oracle VM (ex. VAAI, VASA, V-Vol, ODX).

- Il réalise des captures instantanées efficaces (snapshots) de votre système et des duplications à haute vitesse (gestion uniforme des captures instantanées pour Oracle, SQL, Exchange, DB2, MaxDB…). Il restaure vos données en cas de panne.

- ETERNUS DX est équipé pour le cryptage (avec des contrôleurs et des drives d'auto-cryptage) et peut offrir un accès sécurisé à des volumes sensibles (ex. Eternus Snap Manager, CommVault, Symantec…)

- Le système de stockage est optimisé pour éviter la latence dans le transfert de données et garantir un haut débit, tant pour les processus aléatoires en ligne que pour les longues lectures et écritures séquentielles. Un complément de capacité peut facilement être apporté dans les pools RAID, LUN et Thin-Provision.

- Le système d'exploitation est développé afin de minimaliser l'empreinte mémoire et laisser ainsi le plus de DRAM possible (Dynamic Random Access Memory) pour la mise en mémoire cache. Nous utilisons la Qualité de Service Automatique et la technologie Flash (dans les contrôleurs ou sur les disques SSD).

- **Moins de coûts pour plus de fiabilité**
  Garantir le même niveau de redondance et de prestations localement serait fastidieux et impliquerait des coûts élevés pour votre entreprise. Installer et maintenir des serveurs en interne représente en effet un investissement important tant en ressources humaines qu'en frais de maintenance. Résultat : votre infrastructure IT est plus chère que nécessaire. En outre, à côté du coût d'achat élevé des équipements s'ajoutent les tentatives incessantes de les maintenir à jour, sans mentionner le prix considérable des licences pour le software qui tourne sur votre parc de serveurs. L'investissement dans l'expertise requise et la formation du personnel représente également un poste non négligeable afin de garantir la gestion des données.

Dans un data center vous ne payez que les frais d'abonnement, la configuration et la formation de votre personnel IT à l'utilisation du data center, qui est de surcroît d'un usage convivial et très simple.

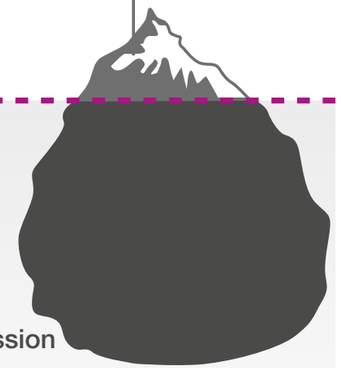
Dans la solution Private Cloud, la majeure partie de l'investissement est constitué par la configuration de l'installation et éventuellement, si un degré d'autonomie supérieure est souhaitée, par la formation du personnel, ce qui ne diffère pas beaucoup de la version locale. Dans la version locale, les coûts futurs sont plus difficiles à prévoir avec précision, tandis que dans la version Private Cloud les coûts doivent être précisés contractuellement au moment de la signature.

Central téléphonique Local

20%
Licences logicielles

Configuration & déploiement

Matériel



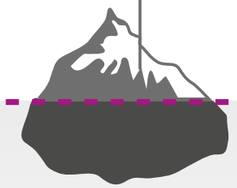
Coûts de possession
Total Cost of ownership (TCO)

- Personnel
- Maintenance
- Formations
- Application des correctifs, patches de mise à niveau
- Temps d'arrêt
- Reprogrammation des configurations
- Maintenance et mise à niveau de la sécurité
- Maintenance et mise à niveau de la redondance
- Usure des serveurs et du matériel

Communications Unifiées en Private Cloud

68%
redevances

Implémentation, configuration et formations



Coûts de possession
Total Cost of ownership (TCO)

- Formations
- Configuration

3.4. Virtualisation

Un Voice Private Cloud utilise la virtualisation pour pouvoir héberger le plus grand nombre de serveurs virtuels possible dans un minimum de serveurs physiques. En outre, la virtualisation offre les avantages suivants :

3.4.1. High Availability (HA)

Si un des serveurs physiques dans le cluster tombe en panne, les machines virtuelles reliées à cet hôte, redémarrent automatiquement sur d'autres serveurs physiques en activité. Ce processus se déclenche automatiquement.

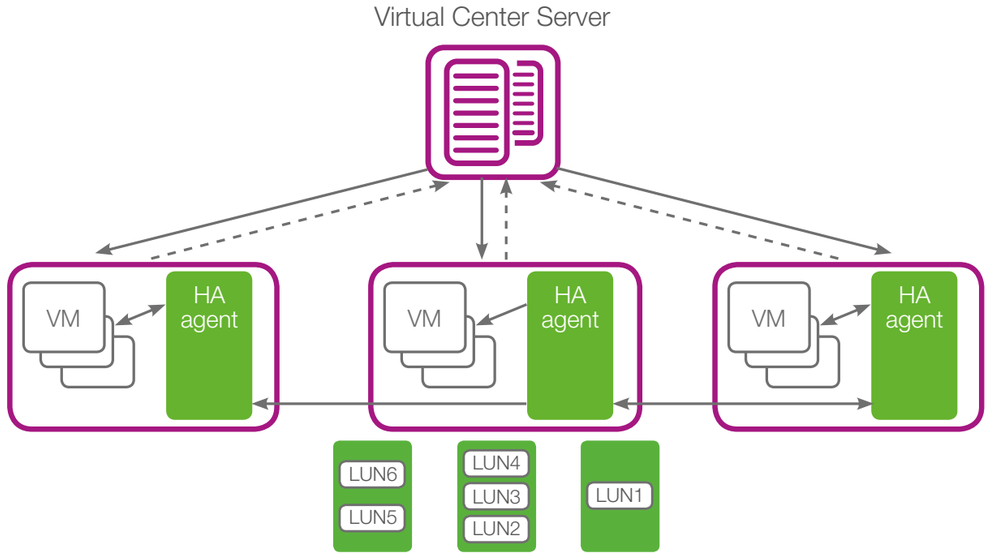
3.4.2. Clustering

Le cluster est un ensemble de serveurs homogènes organisés en grappe.

Les clusters présentent de nombreux avantages même durant les périodes de maintenance. Il est ainsi possible d'assigner un serveur physique pour la maintenance. Les serveurs virtuels, dans ce cas, basculent automatiquement vers d'autres serveurs physiques. Après l'opération de maintenance, les serveurs virtuels reviennent sur le serveur physique hôte. Cette fonctionnalité de migration automatique s'effectue via vmotion ®. Pour l'utilisateur final, la migration est complètement transparente. Les serveurs virtuels basculent vers d'autres serveurs physiques sans interruption de leurs activités.

3.4.3. Network Interface Cards / Cartes d'Interface Réseau (NIC Teaming)

VMware NIC teaming est une manière de regrouper plusieurs Cartes d'Interface Réseau (NIC) afin qu'elles se comportent comme une seule NIC logique. Par la virtualisation, plusieurs interfaces réseaux physiques peuvent être couplées au même switch physique ou à une superposition de switches. En cas de panne d'une interface réseau physique ou d'un switch, la plate-forme de virtualisation veille à ce qu'une autre interface réseau physique transparente prenne le relais. Ce processus se déroule automatiquement et est entièrement géré par la plate-forme de virtualisation. Aucune configuration n'est requise sur le switch physique.

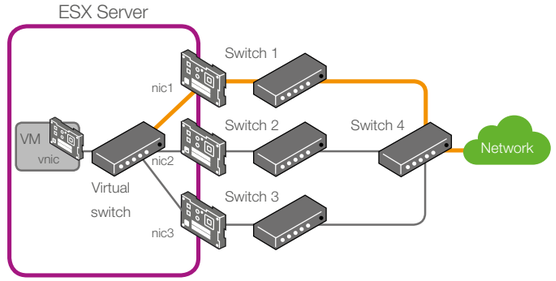


SOURCE : <<VMwareHA_twp.pdf P11>>

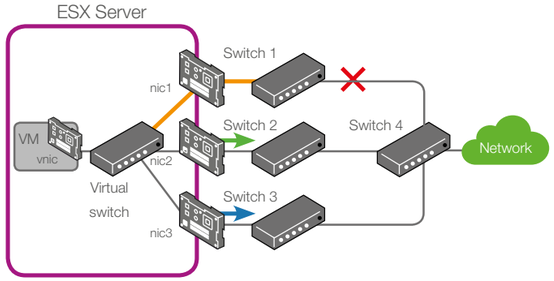
LUN : Logical Unit Number

3.4.4. Aperçu des possibilités de VMware®.

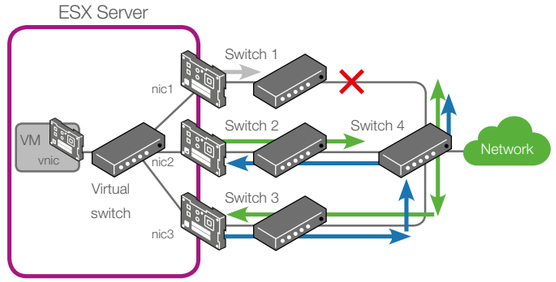
SOURCE : <<http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf P9>>



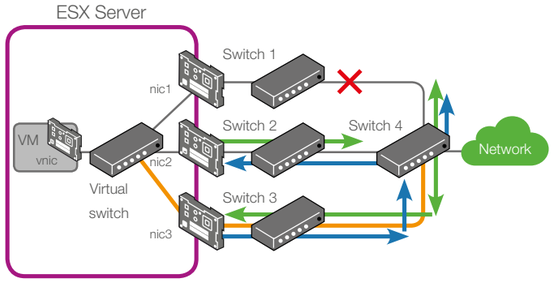
Trafic du réseau des machines virtuelles géré par nic 1



Echec de la connexion entre switch 1 et swtich 4
Chaque adaptateur Ethernet envoie un paquet balise



Les balises retournent sur nic 2 et nic 3, et non sur nic 1



Les données sont reroutées sur le réseau via nic 3

Les composants d'une infrastructure VMware pour la continuité des activités

	Protection en cas d'arrêts planifiés	Reprise rapide suite à une panne imprévue
Composant	NIC Teaming, Multipathing	
Serveur	VMotion, DRS + Maintenance Mode	VMware HA
Stockage	Storage VMotion	Encapsulation, VMware Consolidated Backup
Données	NA	Encapsulation, VMware Consolidated Backup
Site	VMware Site Recovery Manager	

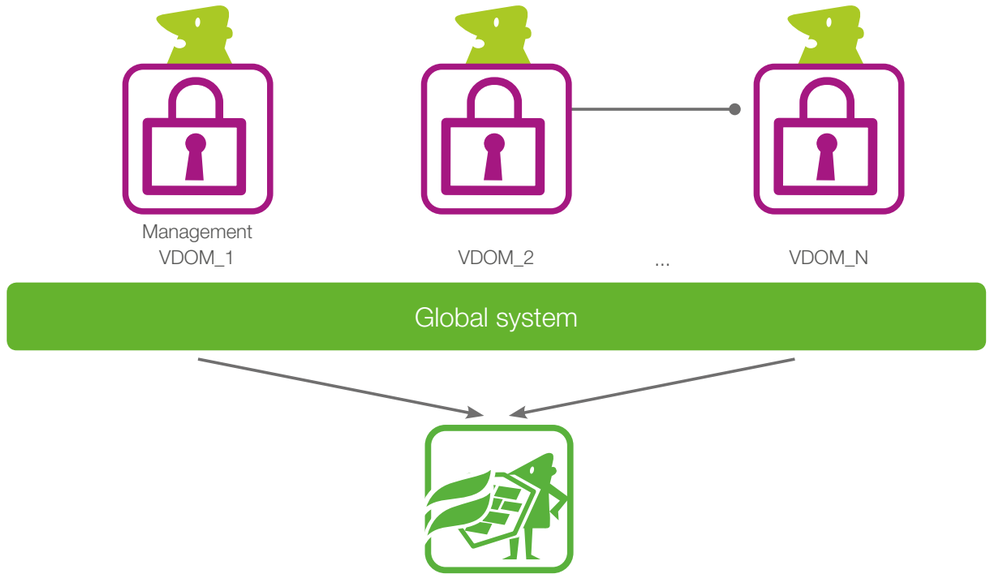
Source : vmware ® image vmware HA P10

3.5. Firewall / Pare-feu

Un Voice Private Cloud exige qu'il y ait le plus de redondance possible du côté du pare-feu. Pour commencer, il faut éviter à tout prix la défaillance du matériel physique (hardware). Ainsi, chaque pare-feu doit avoir au moins 2 alimentations séparées, reliées à 2 circuits électriques distincts. Pour éviter d'autres défaillances du pare-feu matériel, il est préférable de construire un cluster avec un autre pare-feu. Il est également recommandé de répartir ce cluster dans des zones géographiques distinctes.

Chacun des parcs de serveurs virtuels des utilisateurs finaux doit être toutefois protégé par son propre pare-feu. Pour atteindre cet objectif, une des meilleures solutions est l'utilisation de VDOM (Virtual Domains) ou plus petits pare-feu virtualisés à l'intérieur d'un même matériel redondant.

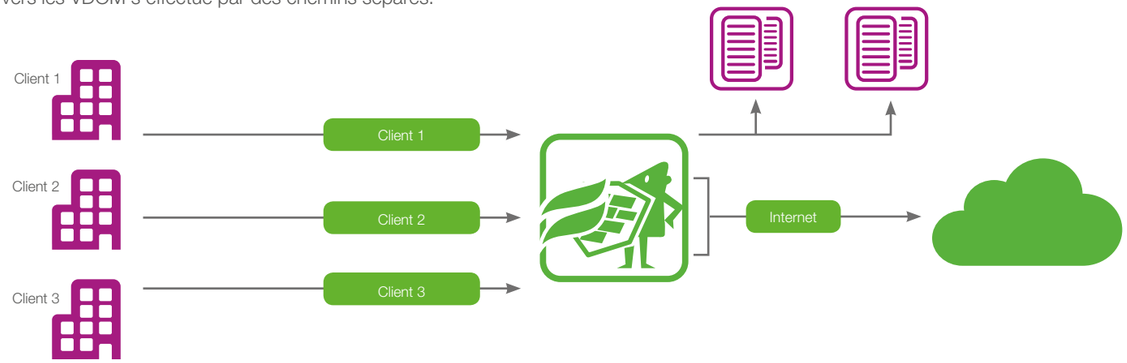
3.5.1. Domaines Virtuels (VDOM)



SOURCE : <<inside fortios ® vdoms 50 P1>

3.5.2. Pare-feu virtualisé

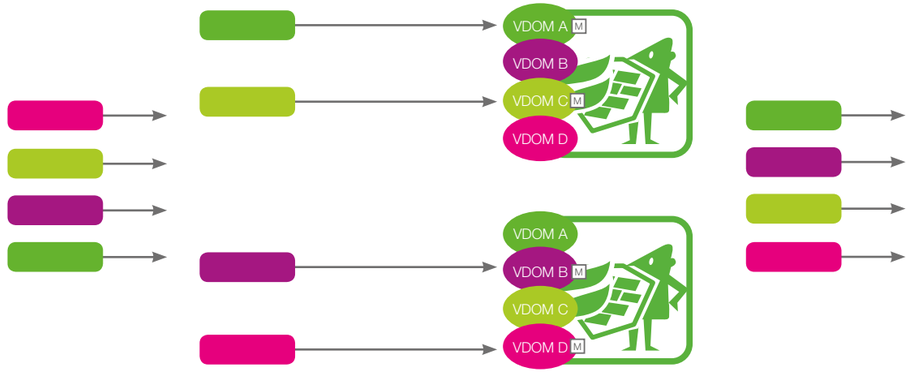
Chaque pare-feu virtualisé ou VDOM possède exactement les mêmes fonctionnalités qu'un pare-feu matériel individuel. Il dispose de sa propre table de routage, de sa propre politique, d'une table en mode NAT, de son propre VPN, etc. Le trafic réseau de et vers les VDOM s'effectue par des chemins séparés.



SOURCE : <<inside fortios ® vdoms 50 P2 >>

3.5.3. Virtual Clustering

Les VDOM peuvent être répliqués dans le cluster vers d'autres pare-feu matériels situés à des endroits différents.



SOURCE : << inside fortios ® vdoms 50 P3 >>

3.5.4. SBC et Pare-feu

- **Dans le réseau du fournisseur de services**
  Dans ce cas-ci, le fournisseur se protège lui-même de tout danger.

- **Chez l'utilisateur final**
  Ici se pose la question : « Le SBC doit-il être placé à la périphérie du réseau ou dans le DMZ, derrière un pare-feu ? » Vous pourriez croire que la réponse est simple, mais les « experts » sont divisés en deux groupes.

- **Groupe un : à la périphérie du réseau**
  L'argument qui prévaut dans ce groupe repose sur le principe selon lequel un SBC est un appareil de sécurité autonome. Il a été conçu pour garder les «méchants» à l'extérieur et laisser entrer les «gentils». C'est en fait un pare-feu en temps réel.

  Un SBC effectue une inspection approfondie de chaque paquet SIP entrant dans le réseau ou sortant. Il peut détecter les paquets SIP malformés ou suspects et les bloquer. Il peut arrêter les attaques par déni de service (DoS) et déni de service distribué (DDoS). Il peut détecter les tentatives d'intrusion par des pirates informatiques. Un SBC détient une liste noire à jour des adresses IP malveillantes et empêche les utilisateurs hostiles d'accéder à votre système de communication.

  En d'autres mots, un SBC est un pare-feu SIP. Il n'est donc pas nécessaire de placer derrière ce système un pare-feu traditionnel pour les données.

  La façon dont les messages SIP accèdent au SBC dépend de la topologie du réseau. Si les paquets SIP arrivent sur une connexion WAN dédiée, vous devez tout simplement les envoyer vers le SBC. Toutefois si les paquets SIP partagent la même connexion WAN que d'autres paquets de données (par exemple HTTP), il est dès lors nécessaire d'effectuer une séparation sous forme de VLAN. Un VLAN sera dédié au SIP et au SBC, tandis que l'autre VLAN sera utilisé pour le pare-feu.

- **Groupe deux : derrière un pare-feu**
  Dans ce cas-ci, le flux SIP transite via le pare-feu des données avant d'être transmis au SBC. De ce fait, il est extrêmement important que le traitement du trafic SIP soit désactivé à l'intérieur du pare-feu. Ce qui signifie que tous les systèmes doivent être désactivés à savoir «SIP-detection», «SIP-inspection» et «SIP ALG». Tout ce qui entre sur les ports 5060 (SIP) ou 5061(TLS) doit être directement renvoyé pour traitement vers le SBC. Le SBC donne au pare-feu des instructions pour expédier le trafic ultérieur RTP et SRTP vers le SBC.

  Une fois que le trafic SIP est transmis au SBC, tous les avantages des partisans du «Groupe un» se concrétisent. Un pare-feu pour les données n'empêchera pas le SBC d'appliquer son rôle d'agent de sécurité. Les partisans du «Groupe deux» font valoir plusieurs arguments.

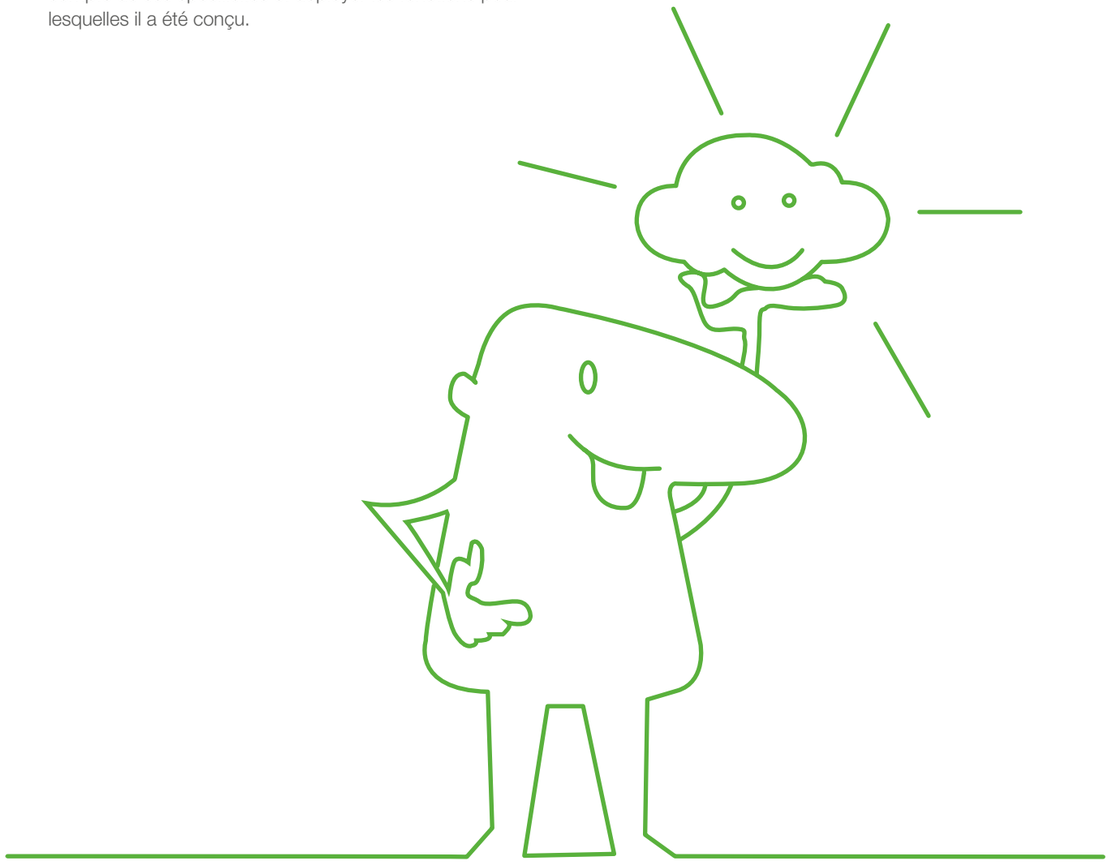
  Premièrement, les entreprises les plus modernes font usage d'un DMZ. Le DMZ est généralement protégé par des pare-feu interne et externe. Un Session Border Controller doit s'inscrire dans une architecture de sécurité standard et à ce titre, ne peut être traité comme une anomalie.

  Deuxièmement, la sécurité doit s'appliquer en couches, et les fonctions du SBC ne doivent venir se superposer que comme une couche supplémentaire dans un processus de sécurité global et cohérent.

  Troisièmement, si les entreprises évoluent de connexions aux SIP trunks de base vers des utilisateurs SIP à distance, d'autres protocoles, en plus de SIP, sont nécessaires. Dans ce cas, le pare-feu se chargera des protocoles non SIP et le SBC, quant à lui, s'occupera des aspects SIP. L'utilisateur externe envoie ses paquets à une seule adresse IP et le pare-feu fonctionne comme un agent de la circulation.

- **Décision**
  Si la politique d'une entreprise est de tout faire transiter via le DMZ et les pare-feu, c'est son droit le plus strict. Pare-feu et SBC peuvent être configurés pour collaborer très étroitement.

  Si vous avez des utilisateurs à distance qui ont besoin de plus que SIP pour pouvoir fonctionner correctement, il est dès lors recommandé de placer le SBC derrière le pare-feu. Laissez chacun des éléments de sécurité tenir compte de ses spécificités et déployer les fonctions pour lesquelles il a été conçu.



PRÉSENTATION DES PARTENAIRES

4. PRÉSENTATION DES PARTENAIRES

Quant ICT, expert en communication

www.quant.be

Quant ICT est spécialisée dans le déploiement des réseaux filaires et sans fil ainsi que de leur sécurisation. Elle est expérimentée dans l'installation de centraux téléphoniques, hybrides et IP, et plus largement dans les Communications Unifiées. Elle a développé la marque Telic qui regroupe ses activités Cloud. Quant ICT se distingue par le niveau d'expertise de son personnel qui détient les plus hautes certifications dans les produits qu'elle déploie.

BeIP, premier partenaire de téléphonie SIP

www.beip.be

BeIP est la filiale de recherche et développement de Quant ICT. Elle concentre son activité dans la création de solutions de Communications Unifiées basées sur le protocole SIP. BeIP fait également partie du réseau européen TELKEA Group dont Quant ICT est un des membres clés.

Telic, des Communications Unifiées en Private Cloud

www.telic.eu

Telic est la version hébergée des solutions proposées par Quant ICT. Installée dans un data center situé au centre de la Belgique parmi les plus fiables du marché, elle peut communiquer avec plus d'une septantaine d'opérateurs nationaux et internationaux.

Téléphonie SA

www.telephonie.lu

Fondée en 1929, cette entreprise a une présence continue sur le marché luxembourgeois et la Grande Région, mais aussi bien au-delà à travers TELKEA Group. La réputation de qualité, de proximité et d'expertise de Téléphonie S.A. est reconnue de tous, de même que son rôle de leader sur le marché.

ICT Control SA

www.ictcontrol.eu

ICT Control SA est un cabinet de conseil créé en 1999 regroupant des experts dans le domaine de la gouvernance informatique, sous la direction de Georges Ataya.

L'activité d'ICT Control SA se focalise dans les différents aspects de gestion et d'architecture de l'informatique, du contrôle des fournisseurs externes et des coûts, de la gestion de la sécurité et de mise en place de méthodes de gouvernance de l'informatique selon les méthodes les plus optimales.

Alcatel-Lucent Entreprise sa

enterprise.alcatel-lucent.com

Alcatel-Lucent Entreprise propose un ensemble complet de solutions de communication et de réseau pour répondre aux besoins en constante évolution des petites et moyennes entreprises, ainsi que des multinationales.

Fujitsu

www.fujitsu.com/be

La gestion actualisée des données critiques de l'entreprise constitue le pilier de toute activité professionnelle. Les solutions de stockage en ligne de Fujitsu protègent ces données contre les risques de perte et les conservent de la manière la plus efficace possible.

Oracle

www.oracle.com

Etabli sur un portefeuille exhaustif de produits et de services intégrés de pointe, le Cloud privé d'Oracle prend en charge les Clouds au niveau des applications, des plates-formes et des infrastructures, offrant une excellente visibilité en matière de sécurité, de conformité aux réglementations et de niveaux de service.

Aruba

www.arubanetworks.com

Aruba conçoit et fournit des réseaux Mobility-Defined NetworksTM destinés à développer tout le potentiel technologique de la nouvelle génération.

Polycom

www.polycom.fr

Les téléphones d'entreprise Polycom sont faciles à utiliser et s'adaptent intégralement à votre environnement existant en matière de communication. Grâce à leur haute qualité vocale, vous avez l'impression de vous trouver dans la même pièce que votre interlocuteur.

Fortinet

www.fortinet.com

Fortinet est le leader mondial d'une sécurité réseau novatrice et performante. Notre mission consiste à offrir la plate-forme de sécurité réseau la plus innovante et la plus fiable afin de sécuriser et simplifier votre infrastructure IT.

Lifesize

www.lifesize.com

Aucune autre solution de visioconférence HD n'est aussi simple que Lifesize. Désormais, chacun peut participer en personne à n'importe quelle réunion, que ce soit dans la salle de conférence, derrière son ordinateur ou un appareil mobile.

REMERCIEMENTS

Chris Herdt	Quant ICT	Team Leader Cloud & Infrastructure
Steven Demets	Quant ICT	Solutions Designer
Nathalie Van Ingelgem	Quant ICT	Sales & Marketing Assistant
Damien Sandras	BeIP	Chief Operating Officer
Marc Vrambout	Telic	Cloud Solution Expert
Walter De Neve	Fujitsu	Datacenter Business Development Manager
Ann Van Cauter	Fujitsu	Account Manager
Diego Coene	Fujitsu	Business Development Manager
Régis Kampangala	Image & Communication	Strategic & Business Development Manager
Brigitte Ledune	Edito3	Managing Partner
Alain Odeurs	Imprimerie Agora Media	Administrateur

LA TÉLÉPHONIE : COMPRENDRE LES NOUVEAUX ENJEUX

Qui aurait cru, en 2010, que la naissance d'une célèbre tablette et la montée en puissance des smartphones allaient à ce point modifier en profondeur notre vision des télécommunications ? Il est loin le temps où l'on investissait pour une dizaine d'années dans un solide central téléphonique avec quelques mises à jours ponctuelles.

La téléphonie a bien changé. Le monde des PABX a rejoint aujourd'hui celui des systèmes informatiques et des réseaux de données. Avec la convergence des technologies apparaissent de nouveaux outils.

PRA, SBC, B2BUA, Rapid Session Shift… Qu'est-ce que ces notions évoquent pour vous ? À quoi servent ces technologies et où les trouve-t-on dans une configuration ? Ou encore, pourquoi migrer sa téléphonie dans le Private Cloud ?

Voici autant de questions et bien d'autres auxquelles nous tentons de répondre dans ce «livre blanc». Son objectif : permettre à tout un chacun d'y trouver ce qu'il cherche dans le domaine de la téléphonie, quelles que soient ses compétences.

Les Communications Unifiées dans le Private Cloud intriguent ou inquiètent. Pourtant, face à la multiplication des outils de communications, cette solution s'avère l'une des plus efficaces pour maintenir à jour une infrastructure capable de faire face aux évolutions.

Que nous réservent les années à venir, et à quoi ressembleront les outils que nous emploierons ?

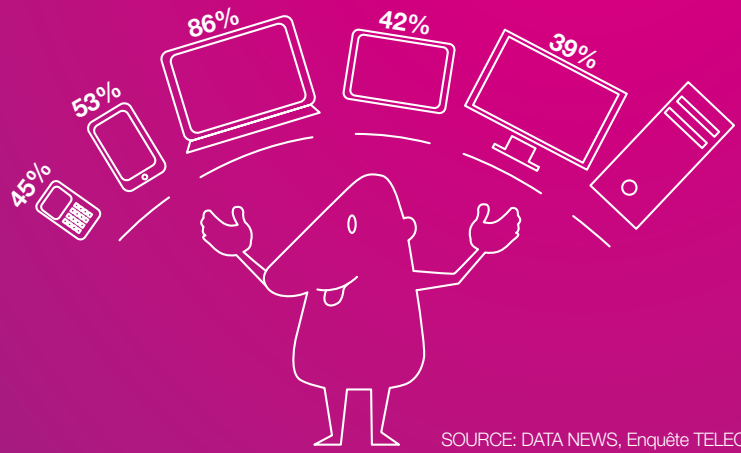
Les dispositifs qu'utilisent à l'heure actuelle vos collaborateurs montrent clairement à quel point notre manière de travailler est en train d'évoluer.

La génération montante nous impose des outils dynamiques et adaptatifs qui se défient des investissements à long terme. Dompter le Cloud pour l'adopter, c'est ce que nous proposons de découvrir au fil de ces pages.

Cet ouvrage peut être lu de A à Z, pour celui qui veut appréhender progressivement toutes les notions utiles dans le secteur. Il peut également être conservé à portée de main afin d'y trouver, au moment voulu, l'une ou l'autre information sur un point précis.

Pierre-André Guillaume
CEO Quant ICT

Quels outils votre entreprise propose-t-elle au personnel ?



SOURCE: DATA NEWS, Enquête TELECOM 2014

Telic
Infinite Connections

QUANT ICT