



**Institut Universitaire de Technologie,  
Aix-Marseille Université**

**RAPPORT DE STAGE  
Diplôme Universitaire de Technologie  
Spécialité Réseaux et Télécommunications**

**TÉLÉPHONIE D'ENTREPRISE  
IP-PBX avec MiVoice Border Gateway**

**Jules BRAYARD**

**CONVERGENCES TÉLÉCOM**

Responsable entreprise : Fabrice FAU

Responsable académique : Damien MANOUKIAN

**2021**

---



## Table des matières

1	Introduction et Présentation de l'entreprise .....	4
1.1	Introduction .....	4
1.2	Présentation de l'entreprise .....	4
1.3	Localisation .....	5
1.4	Effectif.....	6
2	Sujet du stage .....	7
2.1	Comment fournir un service de téléphonie d'entreprise dans un contexte de télétravail ? .....	7
2.2	SBC : Session Border Controller.....	7
2.2.1	Avantage du SBC.....	8
2.3	MBG : MiVoice Border Gateway .....	8
2.3.1	Fonctionnement.....	9
2.4	Installation de l'Hyperviseur .....	10
2.5	Déploiement de l'OVA .....	11
2.6	Ouverture des ports .....	12
2.7	Génération du HASH .....	13
2.7.1	Distribution .....	13
2.8	Configuration du serveur MBG.....	14
2.9	Lien entre le PBX et le MBG .....	16
2.10	Service poste TMA .....	18
2.11	Problèmes et Difficultés liés à l'installation du MBG .....	20
3	Conclusion .....	21
4	Remerciements .....	23
5	Glossaire.....	25
6	Bibliographie.....	27

# 1 Introduction et Présentation de l'entreprise

## 1.1 Introduction

Dans le cadre de ma formation au département Réseaux & Télécommunications de l'Institut Universitaire de Technologie d'Aix Marseille j'ai effectué un stage de fin d'étude. Ce stage de dix semaines avait pour but de me permettre de vivre une première expérience en entreprise et de me sensibiliser au monde professionnel, tout en mettant en pratique mes connaissances acquises pendant ces deux années d'études.

Dans cet objectif, j'ai intégré l'entreprise Convergence Télécom du 19 Avril 2021 au 26 Juin 2021. J'ai été chargé de missions techniques dans toute la région PACA en compagnie de Patrick Loques, technicien chez Convergence Télécom. Nous avons effectué un grand nombre de missions, de dépannage et de déploiement sur beaucoup d'installations différentes. J'ai également été amené à travailler sur des chantiers de câblage informatique et j'ai pu accompagner le service commercial dans une de ses démarches.

Bien que j'ai pu traiter un grand nombre de problématiques et de besoins durant ce stage, je me concentrerai sur un sujet précis dans ce rapport. En effet j'ai pu travailler de façon ponctuelle, entre deux missions, sur une maquette d'un MBG afin que Convergence Télécom puisse déployer cette technologie dans le futur. De plus j'ai également eu la chance de pouvoir déployer cette solution chez un des clients de l'entreprise à la fin de mon stage. Ce document portera donc sur ce point.

## 1.2 Présentation de l'entreprise

Convergence Télécom est une entreprise fondée en 1999 par Fabrice FAU et son associé Jean-Luc BAGNIS. C'est une entreprise SARL\* possédant un capital de 15 000€ dont le siège est basé à Aubagne. Convergence Télécom dispose d'une équipe de 5 personnes avec plus de 20 ans d'expérience dans le domaine de la téléphonie et des courants faibles. L'entreprise est capable de répondre à tous les besoins en matière de télécommunication.

Convergence Télécom propose des services dans quatre grands domaines différents :

- **TÉLÉPHONIE :**
  - Serveurs de télécom PABX\*, IPBX\* (Spécialistes Mitel)
  - Postes téléphoniques : Standards, Téléphones IP, Softphones
  - Opérateur téléphonie et accès internet
  
- **CÂBLAGE RÉSEAU / INFORMATIQUE & WIFI :**
  - Câblage de réseau LAN Ethernet
  - Installation et maintenance de réseaux informatiques
  - Déploiement de points d'accès WIFI

- VIDÉO SURVEILLANCE :
  - Packs de vidéo surveillance avec caméras, enregistreur et écrans
  - Enregistreur Numérique DVR / Enregistreur hybride IP
  - Caméra vidéo surveillance intérieur / extérieur / Mini dôme / IP
  
- COURANT FAIBLE :
  - Appel d'urgence, appel malade
  - Installation d'alarme anti-intrusion

### 1.3 Localisation

Durant la période du stage j'étais basé au siège d'Aubagne qui se trouve dans la zone industrielle les Paluds. Voici sa localisation (figure 1) et ses coordonnées :



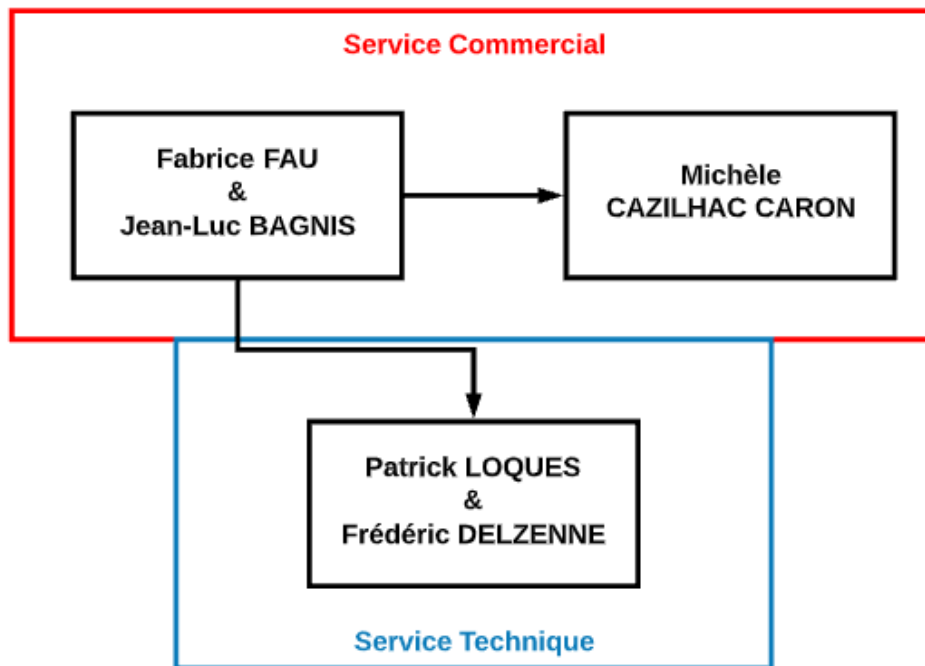
672, avenue de la Fleuride, ZI Les Paluds, 13400 AUBAGNE (Figure 1)

Téléphone : 04 42 82 99 99    Fax : 04 42 82 15 15    Courriel : [contact@convergences-telecom.fr](mailto:contact@convergences-telecom.fr)

La localisation du siège est un choix stratégique. En effet les fournisseurs ainsi que plusieurs clients de l'entreprise se trouvent également dans la zone industrielle Les Paluds. De plus le siège est directement situé à proximité de l'autoroute A50, cette implantation permet donc à Convergences Télécom d'être située à proximité de Marseille, Aubagne, Aix en Provence, mais également de pouvoir rayonner partout dans la région PACA.

## 1.4 Effectif

En interne l'entreprise est divisée en deux services distincts (figure 2). Le service commercial qui se charge du SAV, de la planification des chantiers et de la partie vente. Et le service technique qui traite les demandes des clients en ce qui concerne la maintenance et le déploiement des installations.



Organigramme Convergences Télécom (Figure 2)

L'équipe de Convergence est constituée de 5 personnes :

- Fabrice FAU et Jean-Luc BAGNIS
  - Responsables et technico-commerciaux de l'entreprise, leur rôle est de gérer la partie commerciale, le suivi des clients, les démarches auprès des fournisseurs et la gestion du planning des techniciens.
- Patrick LOQUES et Frédéric DELZENNE
  - Techniciens spécialistes dans la téléphonie chargés de la mise en place d'autocommutateurs et de postes téléphoniques sur les chantiers et de leur configuration. Leur autre mission principale est d'assurer les dépannages clients sur les installations déjà existantes. Ils sont également amenés à effectuer du câblage réseau.
- Michèle CAZILHAC CARON
  - Secrétaire comptable, assistante commerciale chargée de la comptabilité, de la rédaction des devis et des commandes chez les fournisseurs.

## 2 Sujet du stage

### 2.1 Comment fournir un service de téléphonie d'entreprise dans un contexte de télétravail ?

De nos jours le bureau traditionnel est en pleine mutation. Les travailleurs sont plus mobiles que jamais et sont souvent amenés à travailler en dehors de leur lieu de travail, que ce soit à leur domicile ou en déplacement. Fournir un accès au réseau téléphonique de l'entreprise dans ce contexte impose certaines contraintes. De quelles solutions dispose-t-on dans ce cas ?

Dans ce rapport je présenterais une solution permettant d'accéder aux ressources téléphoniques d'une entreprise dans un contexte de télétravail, le MiVoice Border Gateway de Mitel.

Le déploiement présenté sera sur une VM hébergée, sur un serveur présent sur site chez le client. Cette présentation a pour but de revenir sur toutes les étapes de l'installation, mais également d'en expliquer son fonctionnement. Je reviendrais donc sur les notions de SBC et de MBG. Je détaillerais également l'installation du serveur et de l'hyperviseur utilisé lors de cette mise en place. J'expliquerais ensuite la configuration du MBG en lui-même, et pour finir je m'attarderais sur les difficultés que j'ai pu rencontrer et les problèmes auxquels il est possible d'être confronté lors la mise en place de cet équipement.

### 2.2 SBC : Session Border Controller

Il existe diverses solutions pour la téléphonie d'entreprise en distanciel. Toutefois elles sont toutes basées sur le principe du SBC\* ou Session Border Controller.

Les SBC sont des dispositifs déployés en périphéries entre les réseaux privés et publics, ou plus précisément dans une DMZ. Ces systèmes permettent de transférer de manière sûre et efficace des données entre un poste téléphonique IP et un PBX\* (Private Branch Exchange). Ils peuvent également transmettre des flux vidéo. Les SBC créent donc des sessions de communication entre deux ou plusieurs utilisateurs.

- Ici une session de communication est un échange de données en temps réel sous la forme d'un appel téléphonique. Une session de communication est basée sur le protocole SIP\* (Session Initiation Protocol).
- Le SIP est un protocole universel utilisé par les équipements téléphoniques pour établir, modifier et terminer des sessions de communication. Le SIP est également utilisé dans le cadre de la technologie SIP Trunking qui permet de connecter le SBC au réseau public.

Les SBC sont également capables de transcoder les signaux dans des bandes passantes de meilleures ou moins bonne qualité afin de s'adapter aux capacités actuelles du réseau. Cela permet de maintenir des sessions de communication fluides malgré des connexions entre plusieurs infrastructures et différents fournisseurs.

En résumé un SBC est un dispositif placé dans une DMZ. Cet équipement est chargé d'initier des appels entre les utilisateurs et le PBX de l'entreprise via internet. Le SBC achemine donc les données des sessions vers le réseau public en les convertissant au langage du protocole SIP afin de s'assurer que les différents systèmes puissent communiquer entre eux.

### 2.2.1 Avantage du SBC

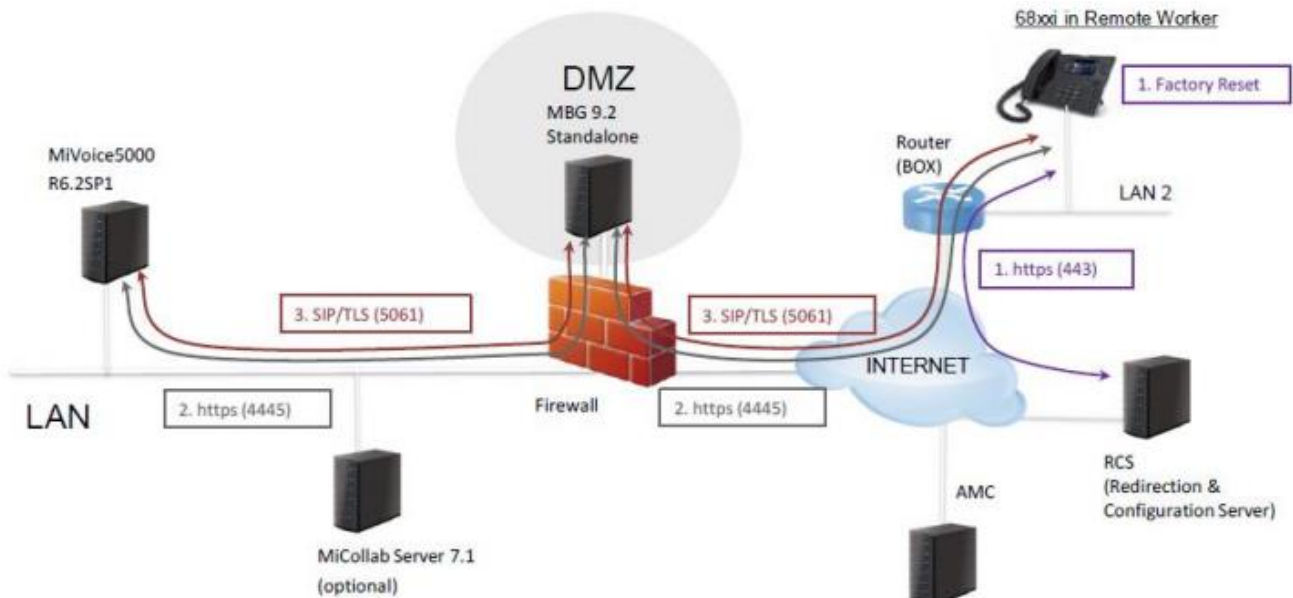
Les avantages que procure un SBC sont au nombre de trois :

- **Communications depuis n'importe quelle localisation** : Un SBC permet aux salariés distants d'une entreprise de travailler et de collaborer en proposant une expérience de communications professionnelles, sans obligation de présence physique dans les locaux.
- **Sécurité** : Les SBC sont amenés à surveiller le trafic qu'ils initient, ils sont donc autonomes dans le maintien du niveau de sécurité et ne nécessitent pas l'installation de services pare-feu tiers, cela simplifie également leur configuration et leur déploiement. Généralement les SBC utilisent des ACLs\* (Liste de contrôle d'accès) spécifiant le trafic autorisé à transiter dans le réseau privé de l'entreprise. En fonction des SBC on peut aussi trouver des limites de vitesse mais aussi du cryptage de données. De plus les SBC se trouvent les DMZ en périphérie des réseaux privés, de ce fait ils masquent une partie de l'architecture du réseau interne ou se trouve le PBX, le rendant ainsi plus difficile d'accès.
- **Fiabilité** : Outre la sécurité, les SBC rendent les communications plus fiables et plus constantes. Les SBC peuvent détecter et normaliser les différents langages du protocole SIP afin de fournir des appels fluides sans interruption. Ils transcodent également les signaux audios en temps réel pour prendre en charge des sessions entre des dispositifs et des réseaux différents. De plus le SBC peut également gérer le RTP\* (Real-Time Protocol) qui permet de délivrer les flux audio et vidéo en temps réel.

### 2.3 MBG : MiVoice Border Gateway

L'entreprise Mitel, leader dans les équipements VoIP\*, propose des solutions de communication professionnelle et dans notre cas un service pour répondre à notre problématique. Le MiVoice Border Gateway (MBG) est un SBC constructeur fonctionnant sur les principes précédemment évoqués et disposant d'un flux SIP crypté, mais destiné à être utilisé dans un environnement Mitel aujourd'hui largement répandu. Cela comprend toutes les solutions MiCollab Client qui vont des postes SIP classiques, aux softphones, en passant par l'application téléphone ou le client web. Pour rappel le but du MBG est donc de permettre à des collaborateurs d'utiliser les ressources téléphoniques de leur entreprise, en utilisant un point d'accès internet privé par exemple. Ainsi les utilisateurs peuvent téléphoner en "interne" (avec des numéros courts) depuis chez eux, que ce soit en France ou à l'étranger.

Le MBG sera situé en périphérie du réseau, c'est à dire à la frontière ou plus généralement dans une DMZ, de plus il servira de serveur proxy pour les flux HTTPS, SIP/TLS\* (Transport Layer Security, ici c'est le protocole SIP qui est crypté) et RTP. (figure 3). Le MBG sera le pont entre notre autocommutateur (ou IPBX\* : Internet Protocol Private Branch eXchange) et les différents périphériques qui viendront se connecter depuis l'extérieur.



Plan de la configuration réseau et des flux (Figure 3)

Les postes SIP compatible pour le MBG chez mitel sont les postes de de la série 6800i. Pour ce rapport je me concentrerais sur ces postes puisque je n'ai pas eu l'occasion de travailler avec le reste de l'environnement MiCollab. Avant de commencer à présenter l'installation et la configuration je vais revenir rapidement sur les différentes étapes du processus.

### 2.3.1 Fonctionnement

La mise en place de la connexion MBG s'effectue en trois grandes étapes. Il est à noter qu'à chaque redémarrage des postes 6800i ces trois étapes sont reprises depuis le début.

- **Étape 1 :** Le poste 6800i effectue une demande de connexion au serveur MBG grâce à ce qu'on nomme le HASH\*. Le HASH est une clé que l'on couple avec l'adresse IP publique du MBG (ou le FDQN c'est à dire un nom de domaine pointant sur le serveur) et le port via lequel le contacter (ici 4445 qui est le port HTTPS\*) pour former un lien direct vers le PBX de l'entreprise (Figure 4).

Lorsque le MBG reçoit la demande du poste il contrôle la clé HASH. Si elle correspond il initie la connexion entre le PBX et le poste 6800i. La clé HASH permet ainsi au poste de récupérer une URI\* (adresse HTTPS). C'est au moyen de cette adresse que les postes SIP récupérerons leurs fichiers de configuration.

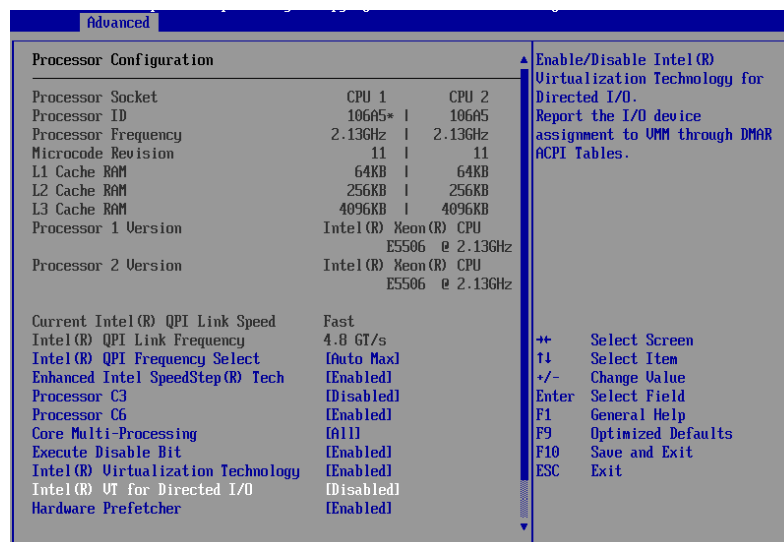


HASH (Figure 4)

- **Étape 2 :** Grâce à l'adresse précédemment récupérée sur l'autocom de l'entreprise le poste télécharge les fichiers de configuration et redémarre pour se mettre à jour. Il effectue enfin deuxième redémarrage avant d'être opérationnel.
- **Étape 3 :** Arrivé ici le poste 6800i est reconnu par le système et possède le firmware de l'entreprise. Le MBG met donc en place le protocole SIP/TLS, qui est un protocole SIP chiffré au moyen de la clé HASH (clé présente sur tous les éléments du système, autocom MBG et poste.).

## 2.4 Installation de l'Hyperviseur

Mitel met à disposition de ses partenaires des ISO\* et des OVA\* pour MBG, cette technologie peut donc être installée directement sur un équipement physique ou virtualisée sur un serveur ou dans un cloud. Ici nous parlons de la solution virtualisée. Avant tout chose il faudra donc vérifier que la machine utilisée supporte la virtualisation. Dans mon cas il s'agissait d'un processeur Intel, je suis donc aller activer le paramètre Intel VT (Virtual Technologie) (figure 5).



Emplacement du paramètre VT dans le boot (Figure 5)

Pour déployer l'OVA fourni par Mitel j'ai utilisé un hyperviseur de VMware. Aussi appelé moniteur de VM\* (machines virtuelles), un hyperviseur\* est un processus permettant de créer et d'exécuter des VM sur une même machine (généralement un serveur dédié à cette tâche, c'est notre cas ici). L'hyperviseur VMware est basé sur l'OS ESXi\* (une distribution de linux), il est disponible gratuitement sur le site de VMware à condition d'avoir créé un compte (cf bibliographie).

Après avoir récupérer l'ISO de l'hyperviseur, j'ai monté une clé bootable en utilisant le logiciel Rufus\*. Cependant je n'ai pas effectué une installation simple. En effet la machine sur laquelle j'ai installé l'hyperviseur possède un stockage limité. Or l'hyperviseur VMware s'attribue un large espace de stockage afin de pouvoir accueillir des fichiers partagés dans le cas d'une architecture en cluster. C'est à dire un cas où plusieurs hyperviseurs différents gèrent le même parc de VM.

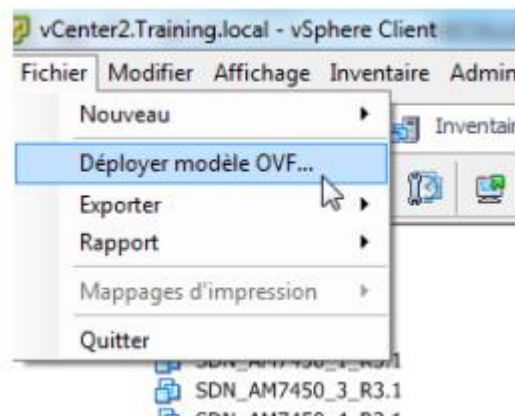
Comme ce n'est pas notre cas ici il nous faut lancer l'installateur ESXi en avancé, pour ce faire on appuie sur shift + O lors du démarrage. Cela permet d'accéder à un Shell depuis lequel on peut exécuter des commandes. Pour cette configuration j'ai alloué l'espace minimal à notre Hyperviseur, de façon à laisser le plus d'espace à nos futures VM. La commande pour modifier l'espace d'installation est la suivante : `runweasel cd-romBoot autoPartitionOSDataSize=16384`

Lorsqu'on exécute cette commande, l'installation se lance mais l'hyperviseur ne prendra que 16Go d'espace. Pour le reste de l'installation on il suffit de suivre les instructions et de choisir la bonne langue.

L'accès à l'hyperviseur se fait ensuite en local sur une interface web à l'adresse de notre machine.

## 2.5 Déploiement de l'OVA

Un fois sur l'interface web de l'hyperviseur (on utilisera le mot de passe et l'utilisateur précédemment créés lors de l'installation du système pour entrer dans l'interface.) il faut désormais déployer la VM MBG. Le fichier utilisé est un .OVA, ou .OVF\* (les deux formats sont similaires), nous allons donc utiliser l'assistant de VMware pour déployer la VM (figure 6).



Menu de déploiement OVF (Figure 6)

L'assistant demande ensuite un nom pour la machine et des paramètres de configuration : la langue, le clavier (attention à bien mettre fr-latin1). Une fois ces réglages terminés il reste à gérer la configuration réseau. Si le réseau ne dispose pas de DHCP (Dynamic Host Configuration Protocol) il faudra donner manuellement une IP, en ce qui concerne notre configuration nous aurons simplement besoin d'une IP pour le MBG et de l'IP de la passerelle WAN (Wide Area Network).

Après quoi il nous suffira de démarrer la VM.

## 2.6 Ouverture des ports

Afin que le système puisse fonctionner il faudra apporter des modifications sur le pare-feu s'il y en a un ou sur le routeur. Les modifications porteront principalement sur l'ouverture de certains ports, entre le réseau WAN et la DMZ et entre la DMZ et le réseau LAN (Local Area Network).

En premier lieu il faudra s'assurer que le MBG puisse utiliser le port 4445 (Port HTTPS) en sortie comme en entrée, afin que les postes 6800i puissent récupérer leur configuration. Après quoi il faudra certainement ouvrir le port 5061 (Port SIP/TLS) afin que les liaisons avec l'IPBX soient possibles. Enfin il ne nous restera plus qu'à autoriser les ports 20000 à 31000 pour les flux voix puissent entrer et sortir du réseau. Voici une table récapitulative des ports à ouvrir : (figure 7)

Port Range	Direction	Description
TCP 4445 (HTTPS)	Internet -> DMZ (MBG)	https connection between 68xxi and MBG (download configuration files, XML features)
TCP 4445 (HTTPS)	DMZ (MBG) -> LAN	https connection between MBG and MiV5000 (download configuration files, XML features)
TCP 5061 (SIP/TLS)	Internet -> DMZ (MBG)	SIP connection between 68xxi and MBG
TCP 5061 (SIP/TLS)	DMZ (MBG) -> LAN	SIP connection between MBG and MiV5000
UDP 20000 to 31000	Internet -> DMZ (MBG) DMZ (MBG) -> LAN	Range of SRTP ports configured in MBG settings

Listes des ports à configurer (Figure 7)

## 2.7 Génération du HASH

Comme expliqué précédemment (cf Fonctionnement du MBG), nous aurons besoin d'une clé de chiffrement nommée HASH. Cette clé permettra non seulement de sécuriser les échanges, mais également de permettre aux postes 6800i d'aller récupérer leurs fichiers de configuration sur le serveur XML du PBX de notre réseau. Il faudra donc se rendre dans l'interface web de celui-ci, dans le menu Réseau et liaisons > Qualité de service > Chiffrement et paramètres IP. Dans ce menu tout en bas on trouvera un champ "génération du hash" qu'il faudra passer en oui. Après quoi nous pourrons récupérer la clé dans le champ juste en dessous (figure 8).

Chiffrement et paramètres IP  
Service téléphonique>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP (4,4,5)

paramètres IP et Chiffrement    Certificats

octet TOS voix (hexa)    B8  
octet TOS signalisation (hexa)    A0  
priorité VLAN voix    6  
priorité VLAN signalisation    6

Chiffrement signalisation et voix  
état fonction    INTERDIT

dates de validité certificat actif :  
début 05/07/16 11:41  
fin 05/07/17 11:41  
nom de l'autorité de certification :  
100.100.100.71  
chiffrement voix postes      
chiffrement inter-IPBX      
certificat auto signé   

Régénération du certificat

Chiffrement voix (i7xx)  
état fonction    CLEF INEXISTANTE

mise à jour le ..... éd .....  
mode de fonctionnement    ESCLAVE ▾  
chiffrement    AUTORISE ▾

**Génération du hash    NON ▾**  
- Chemin pour le téléchargement des fichiers    /16a78df75f29020a19fb5fd14bfac940/ftp\_67xxi

Génération du HASH (Figure 8)

### 2.7.1 Distribution

Nous sommes désormais en possession de la clé HASH, mais il faut maintenant la transmettre aux postes 6800i. Deux options sont possibles.

- Premièrement rentrer manuellement la clé HASH dans le poste téléphonique. Pour rappel il faut que le lien contienne l'IP publique du MBG le port 4445 et la clé HASH (cf la partie fonctionnement du MBG) (figure 9). Cette manipulation requiert d'avoir le poste physiquement avec soit, elle peut s'avérer plus si l'administrateur à les postes avec lui, mais difficiles à mettre en place si ce n'est pas le cas.

[https://micollab1.training.frvoip.mitel.com:4445/16a78df75f29020a19fb5fd14bfac940/ftp\\_67xxi](https://micollab1.training.frvoip.mitel.com:4445/16a78df75f29020a19fb5fd14bfac940/ftp_67xxi)

Exemple en vert d'une clé HASH (Figure 9)

- Deuxièmement utiliser le RCS\* (Remote Configuration Server) de Mitel. Ce serveur mis en place par Mitel permet aux postes 6800i de récupérer eux même l'adresse rentrée manuellement dans la première option. Pour ce faire il faudra se rendre à cette adresse <https://rcs.aastra.com/rcs/login.php>, il faudra cependant disposer d'un compte Mitel. Rendez-vous ensuite dans le menu Servers où il faudra enseigner l'adresse que nous aurions normalement rentrée manuellement dans les postes, puis dans Phones où on rentrera cette fois-ci l'adresse mac de tous nos postes 6800i. Lors du premier démarrage des postes il suffira de choisir le mode MBG pour que les téléphones se rendent sur le RCS et récupèrent le lien vers notre PBX.

## 2.8 Configuration du serveur MBG

Pour commencer il faut renseigner le port XML et l'adresse IP du PBX de notre réseau dans la configuration du MBG. Pour ce faire il faudra se rendre sur son interface web puis dans le menu Service configuration > ICPs (figure 10).

Manage ICP	
Name	mv5000
Hostname or IP address	100.100.100.71
Type	MiVoice 5000
MiNet installer password	
SIP capabilities	UDP, TCP, TLS
Indirect call recording capable	<input type="checkbox"/>

MiVoice 5000 support	
Link to this ICP?	<input checked="" type="checkbox"/>
XML listen port	4445
XML destination port	4445
Enable	<input checked="" type="checkbox"/>
TLS?	<input checked="" type="checkbox"/>
TLS?	<input checked="" type="checkbox"/>

Services XML du PBX

Configuration du menu Service configuration > ICPs (Figure 10)

Après quoi il serait nécessaire de configurer les paramètres des flux SIP, afin que la liaison entre le PBX et les postes distant puisse s'effectuer correctement. Cela se passe dans le menu System configuration > Settings (figure 11). Attention en fonction de la configuration, si les postes 6800i ne passent pas par un RCS, il faudra renseigner l'adresse IP du PBX (FDQN).

SIP support	
UDP	<input type="checkbox"/>
TCP	<input checked="" type="checkbox"/>
TCP/TLS	<input checked="" type="checkbox"/>

Registration Mode	
Registration Mode	Max Set-Side
Set-side registration expiry time	900
ICP-side registration expiry time	
Allowed URI names	Add another

Local streaming	
Codec support	Unrestricted
RTP framesize	Dynamic
Set-side RTP security	Require
Icp-side RTP security	Prefer

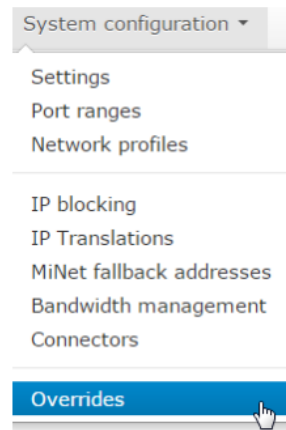
  

PRACK support	
PRACK support	<input checked="" type="checkbox"/>
Send options keepalives	Only behind NAT
Options interval	20
Challenge methods	Invite, Subscribe

Rentrer le FQDN publique  
Si pas de RCS (6800 SIP)

Configuration du menu System configuration > Settings (Figure 11)

Enfin il ne reste plus qu'à configurer les redirections, en effet le MBG sert de serveur proxy pour les SIP et HTTPS il doit donc pouvoir rediriger correctement ces flux. Ce fois cela se passera dans le menu System configuration > Overrides (figure 12). Il faudra créer les règles en remplaçant les paramètres présents dans l'encadré ci-dessous (figure 13). Si la configuration ne comprend pas de lien direct vers le PBX (FDQN), il faudra mettre deux fois l'IP publique.



Menu System configuration > Overrides (Figure 12)

Filename	Sort order	Section	Parameter	Content
tug.ini	50	proxy::aastra_xml_a5000	secure_in::ssl::use_cert	0
tug.ini	50	proxy::aastra_xml_a5000	secure_in::ssl::resign_add_subjectaltname	DNS=FQDN,DNS=Public IP address,IP=Public IP address
tug.ini	50	proxy::sip_tls	secure_in::ssl::resign_add_subjectaltname	DNS=FQDN,DNS=Public IP address,IP=Public IP address

Configuration des Overrides (Figure 13)

## 2.9 Lien entre le PBX et le MBG

Plusieurs prérequis seront nécessaires afin d'appairer le MBG et le PBX entre eux. En premier lieu les deux équipements doivent être à la même heure. Il faudra donc s'en assurer avant de commencer la configuration côté PBX. Après quoi si le PBX est un MiVoice 5000 Server il faudra impérativement que celui-ci soit dans la version 6.7 de son OS (ou une version plus récente).

Si ces deux conditions sont remplies la configuration pour lier le MBG et le PBX peut être entreprise. Pour commencer il faudra se rendre dans l'interface web du PBX et aller dans le menu Administration > Web service et ajouter un nouvel utilisateur (figure 14). Ensuite il faudra régler les paramètres de la façon suivante (figure 15).

The screenshot shows the 'Configure MSL Web Services' page. On the left is a navigation menu with 'Administration' > 'Web services' selected. The main content area has a title 'Configure MSL Web Services' and a subtitle '» Location: MSL web services'. Below this is a status bar showing 'Manage web service availability' with 'Start' and 'Stop' buttons, and 'Web service status Enabled' with 'Access URL https://<hostname or ip add'. A text block says 'Below you will find the registered consumers of this web service. These are vendors of web service clients,' followed by a link 'Add a new consumer' and 'Consumer information'. Below is a table of consumers:

Active	Name	Consumer ID	Share
<input checked="" type="checkbox"/>	Oria	oria	497
<input checked="" type="checkbox"/>	MiCollab Client Deployment	MiCollabClientDeployment	ad3

Ajout d'un nouvel utilisateur MSL (Figure 14)

The screenshot shows the 'Add new consumer' form in the 'Configure MSL Web Services' interface. The form has the following fields and options:

- Active:**
- Name:** mv5000
- Consumer ID:** mv5000
- Shared secret:** 9a9f9e0570fc8aeb98efcf8290bb
- RSA certificate:** Choisissez un fichier (Aucun fichier choisi)
- Permissions:** A list of paths with checkboxes for Read and Write permissions. The following paths have both Read and Write permissions checked: Base/managetoken/, /msl/v1/netbackup/, /msl/v1/netrestore/, /msl/v1/events/, /msl/v1/configuration/, /msl/v1/blades/, /msl/v1/installed\_blades/, /msl/v1/metrics/, /msl/v1/amc/, /msl/v1/sysuser/, MBG/mbg/v1/globaloptions/, /mbg/v1/metrics/, /mbg/v1/icps/, and /mbg/v1/devices/.

Configuration MSL pour le MBG (Figure 15)

Une fois ces paramètres validés on obtient un code de vérification pour pouvoir enregistrer un équipement sur ce nouvel utilisateur. Il faudra donc retourner sur le MBG dans le menu Abonnés > Terminaux et Applications > Connexion et fournir le code obtenu précédemment sur le PBX (figure 16).

The screenshot displays a web administration interface. On the left, there are navigation menus for 'Applications', 'ServiceLink', and 'Administration'. The main content area is titled 'Temporary tokens' and contains a table with the following data:

Approved	Consumer	Token ID	Expiry	Verifier
	mv5000	euy5xsg2sco0t3wjvawooq==	Tue, Aug 30, 2016 @ 14:58:37 UTC	<a href="#">Approve</a> <a href="#">Reject</a>
	mv5000	fq7daftdrx2teacsbn2fa==	Tue, Aug 30, 2016 @ 15:01:45 UTC	<b>708433</b> <a href="#">Reject</a>

Below the table, there is a form for 'MBG' (Service téléphonique) with the following fields:

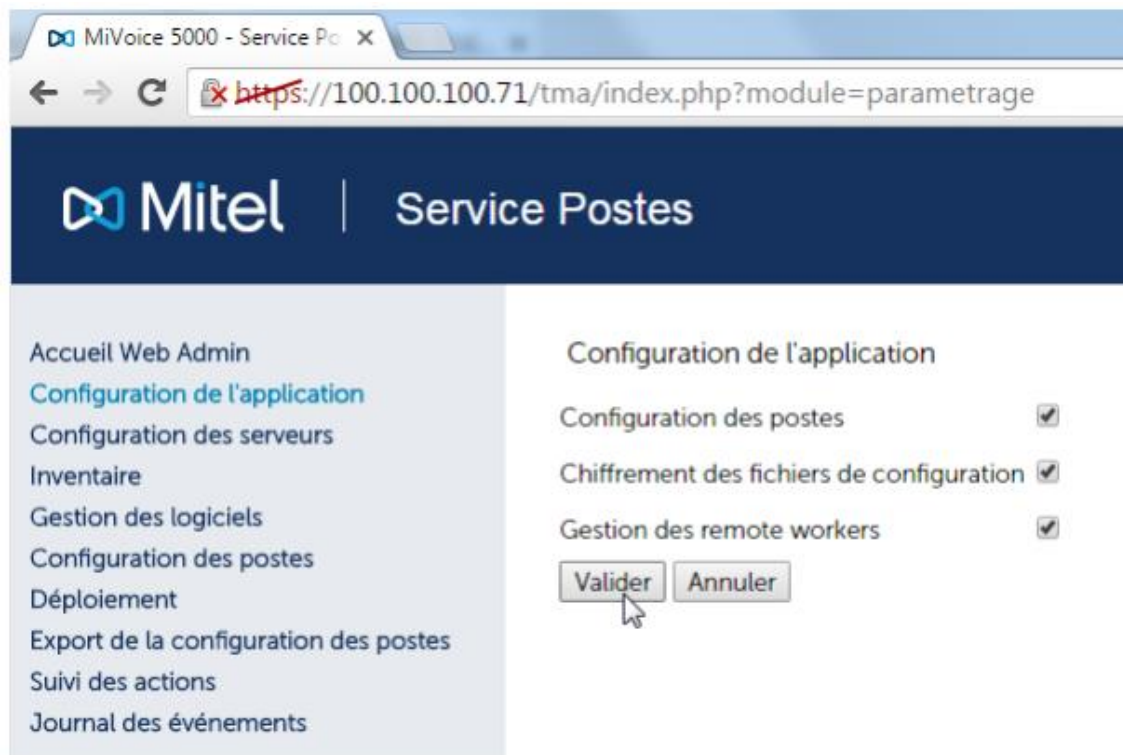
- Adresse IP du MBG: 100.70.10.20
- Compte utilisateur (défini sur le MBG): mv5000
- Secret partagé (défini sur le MBG): 9a9f9e0570fc8aeb98efcf8290bb8e862ce82df5
- Code de vérification: [Empty field]

A red box highlights the 'Code de vérification' field, and a red arrow points from the '708433' value in the 'Verifier' column of the table above to this field.

Emplacement du code de vérification sur le MBG (Figure 16)

## 2.10 Service poste TMA

La dernière étape du déploiement MBG est l'activation du service TMA sur le PBX de notre réseau. Il faudra donc retourner sur l'interface web de celui-ci dans le menu Configuration de l'application (figure 17). Le service TMA est l'application qui prendra en charge les demande des postes 6800i lorsqu'ils viendront récupérer leurs fichiers de configuration.



Menu Configuration de l'application et les réglages du service (Figure 17)

Une fois ce service activé, il faudra remplir le fichier de déploiement pour qu'il puisse répondre aux demandes extérieures. Pour ce faire il faudra utiliser le Template de fichier xls TMA\_provisioning\_6xxxi@version.xls (figure 18) fournit par Mitel qu'il faudra ensuite téléverser dans le PBX, au menu Déploiement dans "Fichier (csv) spécifique" (figure 19).

Le fichier xls renseigne pour chaque poste 6800i :

- MAC\_ADDRESS : Adresse MAC des postes 6800 SIP phone Remote Worker
- sip line1 user name : Login de l'abonné (issu du MBG fichier devices\_mbg.csv)
- sip line1 auth name : Login abonné (issu du MBG fichier devices\_mbg.csv)
- En mode SSO : Login abonné
- Sans mode SSO : Numéro de l'abonné
- sip line1 password : Mot de passe Set-side (issu du MBG fichier devices\_mbg.csv)

Ainsi que ces valeurs (identique pour chaque poste) :

- sip proxy ip : Adresse publique ou nom du MBG
- sip registrar ip : Adresse publique ou nom du MBG
- Serveur HTTPS : Adresse publique ou nom du MBG
- HTTPS Path : Valeur du hash du MiVoice 5000
- keyboard script : URI d'accès à l'iPBX

**Fonction / Function:**  
 Cet onglet est utilisé pour générer un fichier ".csv", pour TMA, contenant les paramètres requis pour la fonctionnalité Téléworker par terminal 68xx SIP RemoteWorker pour les postes 68xxi via MBG. TMA permet ensuite de charger ce fichier ".csv", créant les fichiers MAC mis dans le répertoire FTP embarqué défini. Se référer à la documentation MIV5000 "XXX".  
 / This sheet is used to generate a ".csv" file, for TMA, including the parameters required for the feature Teleworker by terminal 68xx SIP. After TMA allows to load this file ".csv" file, creating MAC files put into the defined embedded FTP server. Please refer to the MIV5000 documentation "XXX".

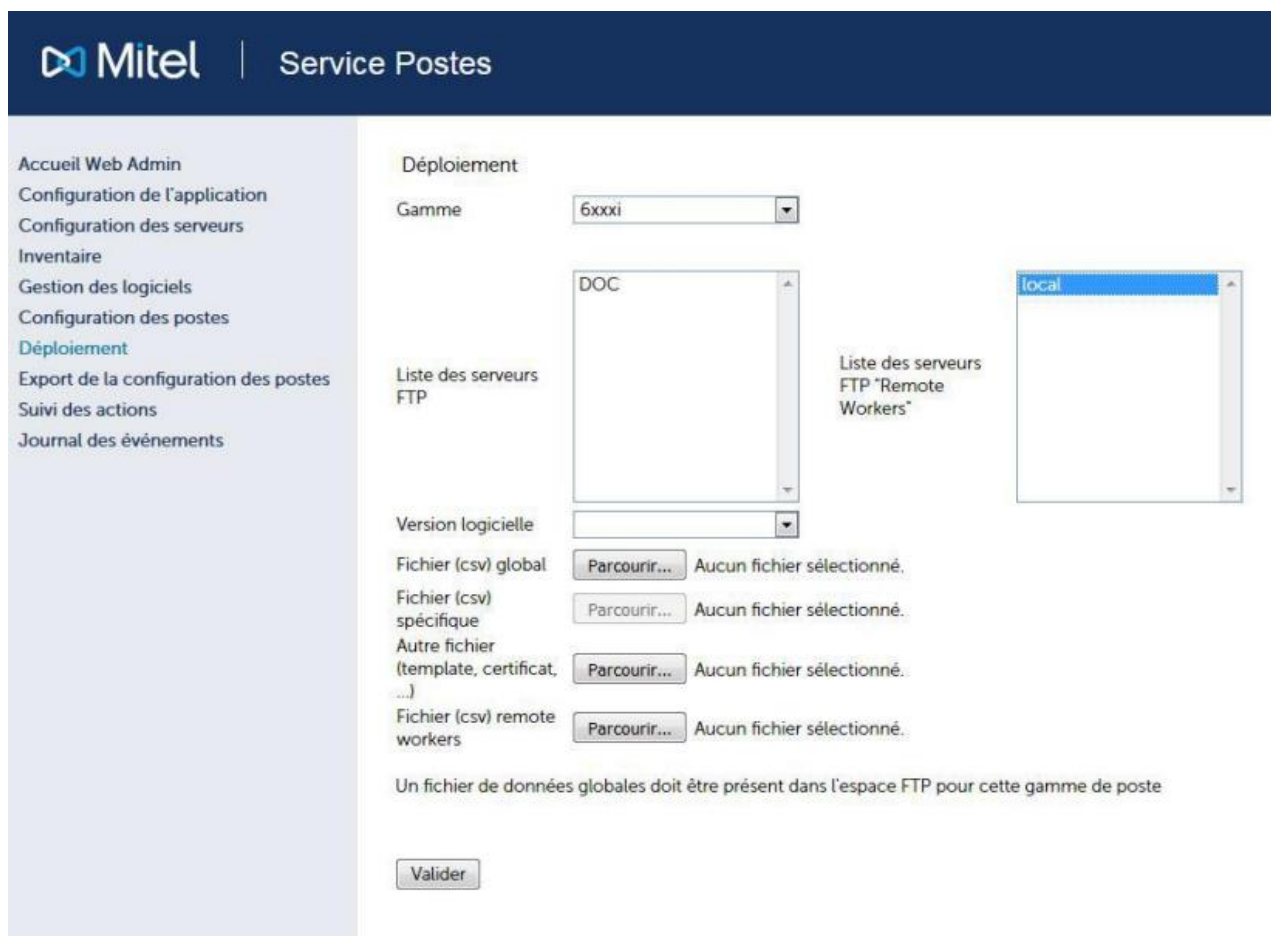
**Rules:**  
 3 types de données différenciés par la couleur de la police / 3 kind of data differentiated by the font color:  
 - Noir / Black: donnée par terminal-abonné / data by terminal-subscriber  
 - Marron / Brown: Donnée système - même valeur pour toutes les adresses MAC / system data - same value for all MAC\_ADDRESS  
 - Rouge / Red: données obligatoires - éviter de les modifier / compulsory data - avoid to modify them

**Attention / Caution:**  
 - Merci de ne pas modifier le nom de cette onglet / Please do not modify the name of this sheet.  
 - Merci de ne pas créer de ligne avant 'MAC\_ADDRESS' / Please do not create any line before 'MAC\_ADDRESS'

Generation.csv      D:\templexport\_global.csv

TERMINAL - SUBSCRIBER				SYSTEM			
MAC_ADDRESS	!sip line1 user name	!sip line1 auth name	!sip line1 password	!sip proxy ip	!sip registrar ip	!https server	!https path
00085D4330B8	7000	7000	password1	64.101.10.1	64.101.10.1	64.101.10.1	9a48085c1b816fd1b512e8b186686a6
08000F9F7305	7001	7001	password2	public.test.com	public.test.com	public.test.com	9a48085c1b816fd1b512e8b186686a6

Exemple d'un fichier xls de Mitel (Figure 18)



Emplacement du lien de téléversement du menu Déploiement (Figure 19)

## 2.11 Problèmes et Difficultés liés à l'installation du MBG

Cette partie est un inventaire des potentielles difficultés que l'on peut rencontrer et dont j'ai pu faire l'expérience.

- Configuration des Vlan : Même si le MBG peut être déployé de façon indépendante dans un réseau, il est possible qu'ils doivent passer par le même lien WLAN que le reste du réseau. Dans ce cas il faudra prendre en compte que l'infrastructure réseau existante ne comporte pas forcément de switch configurable et que la mise de place de Vlan sera impossible
- Le service poste TMA : S'il s'avère que le MBG est déployé dans un réseau avec un PBX MiVoice 5000 et qu'il a été nécessaire de le mettre à jour celui-ci pour que son OS soit dans une version supérieure à la 6.7. Il faudra être particulièrement attentif aux paramètres TMA du PBX qui ont tendance à se désactiver lors de la mise à jour.
- La présence de plusieurs DHCP : Les PBX Mitel peuvent fournir un DHCP exclusif aux matériels Mitel, cependant ces mêmes matériels peuvent aussi recevoir une réponse d'un autre DHCP du réseau. Cela engendrera des difficultés si les postes 6800i sont déployés sur le réseau de l'entreprise avant d'être distribués ailleurs. En effet cela implique qu'ils n'auront pas forcément récupéré tous les paramètres nécessaires qui sont délivrés par le DHCP Mitel.
- MSL Mitel Software Linux : Le MSL est l'OS de Mitel qui peut servir au déploiement du MBG. J'ai rencontré beaucoup de difficultés sur un serveur avec une configuration RAID et j'ai même échoué à l'installer sur cette machine. Je suppose donc que le MSL ne supporte pas le RAID. D'une façon générale je conseillerais de choisir la solution virtualisée pour le déploiement d'un MBG.
- La RAM serveur : Bien que la VM du MBG ne demande pas énormément de ressources il faudra être attentif à la quantité de RAM de la machine hôte. En effet il est conseillé de lui allouer 2Go de mémoire, cependant il s'avère qu'au démarrage elle semble avoir besoin de beaucoup plus (Je ne sais pas si cela est lié au format OVA). Dans mon cas la machine que nous avons utilisée possédait 4Go de RAM et n'était destinée qu'à héberger seulement le MBG, cependant il a tout de même fallu rajouter 4Go de RAM pour la VM puisse démarrer correctement. Il est à noter que plus le parc de téléphone sera important plus le MBG pourra avoir besoin de ressources, ce paramètre est donc également à prendre en compte dans la configuration de la machine hôte.

### 3 Conclusion

Bien que je n'aie pas pu en présenter la globalité dans ce rapport, ce stage fut riche en expériences. J'ai parcouru toute la région PACA afin d'assurer des dépannages et des installations. Chacune de ses missions fut une expérience différente, d'abord d'un point de vue technique, puisque chaque installation est différente et possède ses propres particularités et contraintes. D'autant que les conditions furent totalement différentes de ma propre expérience scolaire. En effet il a fallu collaborer plus d'une fois avec d'autres parties tierces car nous n'avions pas la main sur le reste du réseau et parfois même faire sans intervention extérieure avec nos propres moyens.

Mais aussi d'un point de vue humain, j'ai pu rencontrer et interagir avec toutes sorte de personnes, que ce soient des clients ou des techniciens tous on apporter quelque chose d'unique que ce soit dans leurs attentes ou leur aide. J'ai aussi fait l'expérience d'une vie d'entreprise, avec ses routines, ses habitudes et les liens entre collègues de travail.

Ce stage bien que très lié aux réseaux informatiques fut principalement centré sur la téléphonie, un domaine où j'étais totalement novice. C'est pourquoi ce stage fut d'autant plus enrichissant, j'ai découvert et appris énormément durant ces dix semaines. Pas seulement en téléphonie, mais aussi dans la démarche professionnelle, l'anticipation des problèmes et des besoins, la formation des clients, le travail méthodique et organisé, la conscience professionnelle.

En ce qui concerne le MBG, ce fut un sujet d'étude entre deux missions, avec pour objectif d'effectuer un déploiement en fin de stage. J'ai pu rencontrer un certain nombre de difficultés dans sa mise en place, des difficultés matérielles et logicielles. Ce fut parfois rébarbatif, mais la satisfaction fut d'autant plus grande lorsque le système a fini par fonctionner. Au-delà de l'expérience acquise sur ce sujet, cela m'a permis de me confronter à toute sorte de difficultés. Aujourd'hui si je devais faire un retour, j'aimerais pouvoir continuer à déployer des solutions MBG. En effet je n'en maîtrise pas encore toutes les subtilités et refaire l'expérience de quelques installations me permettrait de solidifier mes acquis et d'être parfaitement à l'aise sur le sujet.



## 4 Remerciements

J'aimerais remercier ici mon tuteur de stage monsieur Fabrice FAU, sans qui cette expérience n'aurait jamais été possible. Je le remercie pour m'avoir accueilli au sein de Convergences Télécom alors que la situation sanitaire était incertaine, mais aussi pour la confiance qu'il m'a accordée.

Je voudrais remercier aussi tout particulièrement Patrick LOQUES avec qui j'ai travaillé tout au long de ces dix semaines. Il a su transmettre son savoir et son expérience dans la téléphonie d'entreprise, mais aussi sur le monde professionnel et ceci toujours avec bienveillance et dans la bonne humeur. Ce fut un véritable plaisir de l'épauler dans toutes ses missions. Je remercie aussi Frédéric DELZENNE que nous avons pu croiser et qui m'a lui aussi fait profiter de ses connaissances sur les PBX.

Je remercie tout le reste de l'équipe de Convergences Télécom pour leur gentillesse et leur accueil, c'est grâce à eux tous que j'ai pu passer un stage agréable et m'intégrer dans l'équipe. Merci à Michèle CAZILHAC CARON et Jean-Luc BAGNIS pour leur soutien concernant ce rapport, merci également à Didier DAO avec qui j'ai pu mettre à profit et approfondir mes cours sur le câblage réseau, mais aussi et surtout connaître la réalité du chantier.

Enfin je remercie Christopher CAUVIN et Sébastien PISTOL dont l'expertise fut précieuse pour la rédaction de ce rapport.



## 5 Glossaire

**ACL** : Access Control List

**Autocommutateur ou Autocom** : PBX, PABX, IPBX

**DHCP** : Dynamic Host Configuration Protocol

**DMZ** : DeMilitarized Zone, zone du réseau séparée du reste de l'architecture pour plus de sécurité

**ESXi** : OS linux

**FDQN** : Fully Qualified Domain Name, un nom de domaine pointant directement sur une machine

**HASH** : Fonction de hachage, qui permet de créer une empreinte numérique

**HTTPS** : HyperText Transfer Protocol Secure

**Hyperviseur** : Gestionnaire de machines virtuelles

**IP** : Internet Protocol

**IPBX** : Internet Protocol Private Branch eXchange

**ISO** : Image de disque

**LAN** : Local Area Network

**MBG** : Mitel Border Gateway

**OVA ou OVF** : Open Virtual Machine Format

**PABX** : Private Automatic Branch EXchange

**PBX** : Private Branch Exchange

**RCS** : Remote Configuration Server

**RTP** : Real-Time Protocol

**SARL** : Société commerciale où la responsabilité des associés est limitée au montant de leurs apports.

**SBC** : Session Border Controller

**SIP** : Session Initiation Protocol

**TLS** : Transport Layer Security

**URI** : Adresse HTTPS

**VM** : Machine virtuelle

**WAN** : Wide Area Network

**WIFI** : Wireless Fidelity

**XML** : Extensible Markup Language, langage utilisé pour la mise en page web



## 6 Bibliographie

- Documentation Mitel : <https://www.mitel.com/document-center/applications>
- Principes du SBC : <https://loopup.com/fr/resource-center/blog/what-is-a-session-border-controller-sbc-how-does-it-work/>
- Les termes et questions d'ordre général : <https://www.wikipedia.org/>