

Table des matières

Dédicaces.....	i
Remerciements	ii
Résumé.....	iii
Abstract	iv
Liste des figures.....	vii
Liste d'Acronymes et Abréviations.....	viii
Introduction générale.....	1
Chapitre 1 : Le cadre général du projet	3
Introduction.....	3
1. Présentation du Groupe BMCI	3
1.1. Organigramme du Groupe BMCI.....	4
1.2. Fiche descriptive de la BMCI	4
1.3. Présentation de la DSI	5
2. Réseau de la BMCI.....	5
2.1. Architecture réseau de la BMCI.....	5
2.2. Architecture réseau du LAN	6
2.3. Architecture réseau téléphonique	7
2.4. Architecture réseau et téléphonique des sites liés au projet	8
2.4.1. L'architecture du Back Office (perna) et de la BMCI Crédit Conso	8
2.4.2. Immeuble Colline.....	9
2.4.3. Trade Centre.....	10
2.4.4. Inspection générale	12
2.5. Matériel utilisé au niveau de cette architecture	12
3. Limites de cette architecture	13
3.1. Limites au niveau du réseau informatique.....	13
3.2. Limites au niveau du réseau téléphonique	13
Conclusion	14
Chapitre 2 : La solution proposée.....	16
Introduction.....	16
1. La nouvelle architecture proposée.....	16
1.1. L'architecture réseau cible	16
1.1.1. Couche Access	17

1.1.2. Couche distribution	17
1.1.3. Couche core.....	17
1.2. Les protocoles liés à l'architecture cible	18
1.2.1. Principes et protocoles de Niveau 2.....	18
1.2.2. Principes et protocoles de Niveau 3.....	18
1.2.3. Principes et protocoles de Niveau sécurité.....	19
1.3. Amélioration de l'architecture cible.....	19
1.3.1. Introduction de la téléphonie sur IP (ToIP)	20
1.3.2. Introduction du wifi.....	23
1.3.3. Introduction de la visioconférence.....	25
2. Les avantages de l'architecture proposée.....	27
Conclusion	29
Chapitre 3 : La mise en place de la solution	31
Introduction.....	31
1. Site bénéficiaire du projet	31
2. Le matériel utilisé au niveau de l'architecture cible	32
3. L'installation du matériel.....	33
3.1. Câblage électrique et informatique	33
3.2. Equipements et configuration de l'architecture cible.....	33
3.3. Equipements de la TOIP	34
3.4. Equipements du wifi.....	35
3.5. Equipements de la visioconférence.....	35
4. La configuration de l'architecture cible.....	38
4.1. Description de la configuration cible.....	38
4.2. Fichiers de la configuration cible.....	38
4.2.1. Configuration d'un commutateur de distribution.....	38
4.2.2. Configuration d'un commutateur d'accès.....	46
Conclusion	52
Conclusion générale	53
Références.....	54

Liste des figures

Figure 1 : Réseau d'agences du groupe BMCI [3].....	3
Figure 2 : Organigramme du Groupe BMCI [4].....	4
Figure 3 : Fiche descriptive de la BMCI [5], [1].....	4
Figure 4 : Architecture réseau de la BMCI.....	5
Figure 5 : Architecture réseau LAN de la BMCI.	6
Figure 6 : Architecture téléphonique de la BMCI.	7
Figure 7 : Architecture informatique et téléphonique de la BMCI.....	7
Figure 8: Architecture informatique et téléphonique du site Back Office.	8
Figure 9: Architecture informatique et téléphonique du site BMCI Crédit Conso.....	9
Figure 10 : Architecture informatique et téléphonique du site Immeuble Colline.....	10
Figure 11 : Architecture informatique et téléphonique du site Trade Center.	11
Figure 12 : Architecture informatique et téléphonique d'une agence typique de la BMCI.....	11
Figure 13 : Architecture informatique et téléphonique du site Inspection générale.	12
Figure 14 : Répartition des coûts en %.....	14
Figure 15 : L'architecture cible proposée.....	16
Figure 16 : Exemple du Cluster Call Manager.	21
Figure 17 : Architecture globale de la solution TOIP [19].	22
Figure 18 : L'architecture cible proposée avec la TOIP.	22
Figure 19 : Architecture globale du WIFI.....	24
Figure 20 : L'architecture cible proposée avec le service WIFI.	24
Figure 21 : Usage de la visioconférence en entreprise [25].	25
Figure 22 : Architecture globale pour le service de la visioconférence.	26
Figure 23 : Architecture cible proposée avec le service de la visioconférence.....	27
Figure 24 : Changement de la répartition des coûts en %.	28
Figure 25 : Localisation du site sur Google map [27].	31
Figure 26 : Vue du site sur Google earth [28].....	32
Figure 27 : Etat des lieux.	33
Figure 28 : La mise en place des équipements.....	34
Figure 29 : La mise en place du cluster Call Manager et les téléphones IP.....	34
Figure 30 : La mise en place du contrôleur WIFI (WLC).	35
Figure 31 : La mise en place des points d'accès.	35
Figure 32 : Photo de la salle 1 avant l'introduction de la visioconférence.....	36
Figure 33 : Photo de la salle 1 après l'introduction de la visioconférence.....	36
Figure 34 : Photo de la salle 2 avant l'introduction de la visioconférence.....	37
Figure 35 : Photo de la salle 2 après l'introduction de la visioconférence.....	37

Liste d'Acronymes et Abréviations

ACL	: Access Control List.
AP	: Access Point.
AS	: Autonomous System.
BGP	: Border Gateway Protocol.
BMCI	: Banque marocaine pour le commerce et l'industrie.
BNP	: Banque Nationale de Paris.
BT	: British Telecom.
CUCM	: Cisco Unified Call Manager.
DMVPN	: Dynamic Multipoint Virtual Private Network.
DSI	: Direction des systèmes d'information.
DVR	: Digital Video Recorder.
EGP	: Exterior Gateway Protocol.
EIGRP	: Enhanced Interior Gateway Routing Protocol.
GRE	: Encapsulation Générique de Routage.
GSM	: Global System for Mobile Communications.
Hi-Fi	: high fidelity.
HSRP	: Hot Standby Router Protocol.
IAM	: Itissalat Al-Maghrib
IGP	: Interior gateway protocol.
IMEX	: Immobilier et Exploitation.
IPSEC	: Internet Protocol Security.
LAN	: Local Area Network.
MPLS	: Multi Protocol Label Switching.
NIC	: Network interface controller.

NVR	: Network video recorder.
OSI	: Open Systems Interconnection.
PABX	: Private Automatic Branch Exchange.
PoE	: Power over Ethernet.
PRI	: Primaire.
PVDM	: packet voice/data module.
QoS	: Quality of service.
RDC	: Rez-de-chaussée.
RF	: Radio Frequency.
RTC	: Réseau téléphonique commuté.
SA	: Société anonyme
SNMP	: Simple Network Management Protocol.
STP	: Spanning Tree Protocol.
TCP	: Transmission Control Protocol.
TOIP	: Telephony over Internet Protocol.
UTP	: Unshielded Twisted Pair.
VID	: VLAN Identifier.
VLAN	: Virtual Local Area Network.
VPN	: Virtual Private Network.
VTP	: VLAN Trunking Protocol.
WAN	: Wide area network.
Wi-Fi	: Wireless Fidelity.
WLAN	: Wireless Local Area Network.

Introduction générale

Un réseau informatique désigne un ensemble d'équipements reliés entre eux physiquement ou grâce à des ondes radio. Le but du réseau informatique est de centraliser les données, partager les ressources, communiquer entre collaborateurs et accéder à Internet. Les réseaux informatiques d'aujourd'hui sont de plus en plus répandus et complexes et permettent la mise à disposition de la data, de la voix et de la vidéo.

La documentation détaillée, la conception intelligente et l'implantation d'une architecture réseau optimale constituent un enjeu stratégique pour l'entreprise et garantissent l'amélioration de sa productivité sur le long terme.

L'architecture réseau existante au sein de la BMCI présente plusieurs limites. En effet, c'est une architecture classique, mal structurée et difficile à superviser. De plus, elle est sans redondance, intolérante aux pannes et ses équipements sont obsolètes.

Le projet de la refonte LAN va permettre de résoudre ces limites et de mettre en place un réseau uni-fonctionnel, performant, fiable et sécurisé. L'avantage de ce réseau est qu'il est évolutif, autrement dit, il permet l'intégration de plusieurs services tels que la téléphonie sur IP, le Wifi et la visioconférence. De ce fait, le design et l'installation d'une nouvelle architecture conforme aux normes de la BNP Paribas, dont la BMCI est une filiale, a été le plan optimal dans le cadre de cette société.

Les chapitres suivants constituent les trois principaux axes de ce rapport, organisés tel que suit :

Le 1^{er} chapitre présente l'organisme d'accueil, l'étude de l'architecture existante dans les différents sites de la société et les limites de cette architecture.

Le 2^{ème} chapitre donne un aperçu détaillé sur la nouvelle architecture proposée et ses nombreux avantages.

Le 3^{ème} chapitre décrit la mise en place de l'architecture cible, il détaille le matériel acquis, son installation et enfin la configuration de cette architecture.

Ce rapport sera clôturé par une conclusion générale qui va récapituler tout le travail mené dans ce projet.

Chapitre 1: Le cadre général du projet

Chapitre 1 : Le cadre général du projet

Introduction

Ce chapitre comporte la présentation de la BMCI, y compris son réseau d'agences, l'organigramme et la fiche descriptive de la société où se déroule ce projet de fin d'étude. Par la suite, nous allons expliquer en détail, pour la BMCI, l'architecture du réseau informatique, le réseau LAN, le réseau téléphonique, et nous allons décrire l'architecture de chacun des sites centraux de la BMCI qui sont liés au projet, et le recensement des ressources matérielles utilisées. Enfin, nous allons exposer les limites de cette architecture.

1. Présentation du Groupe BMCI

La Banque marocaine pour le commerce et l'industrie, acronymisé en BMCI a été créé en **1943** en tant que **société anonyme SA** à Directoire et Conseil de Surveillance au capital **1 327 928 600 de Dirhams**, et dont le siège social se situe à Casablanca, au Maroc [1].

La BMCI s'adresse à tout type de clientèle : les particuliers, y compris les marocains résidents à l'étranger, les professionnels, et les grandes entreprises et institutionnels. Elle a développé un réseau de près de **370 agences** dont plus de **40 villes** marocaines et une large gamme de produits et de services [2].

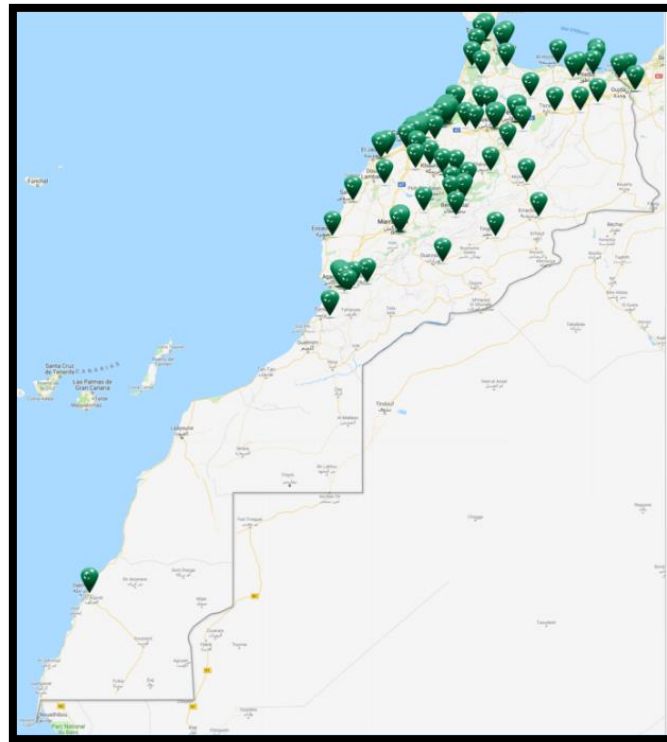


Figure 1 : Réseau d'agences du groupe BMCI [3].

1.1. Organigramme du Groupe BMCI

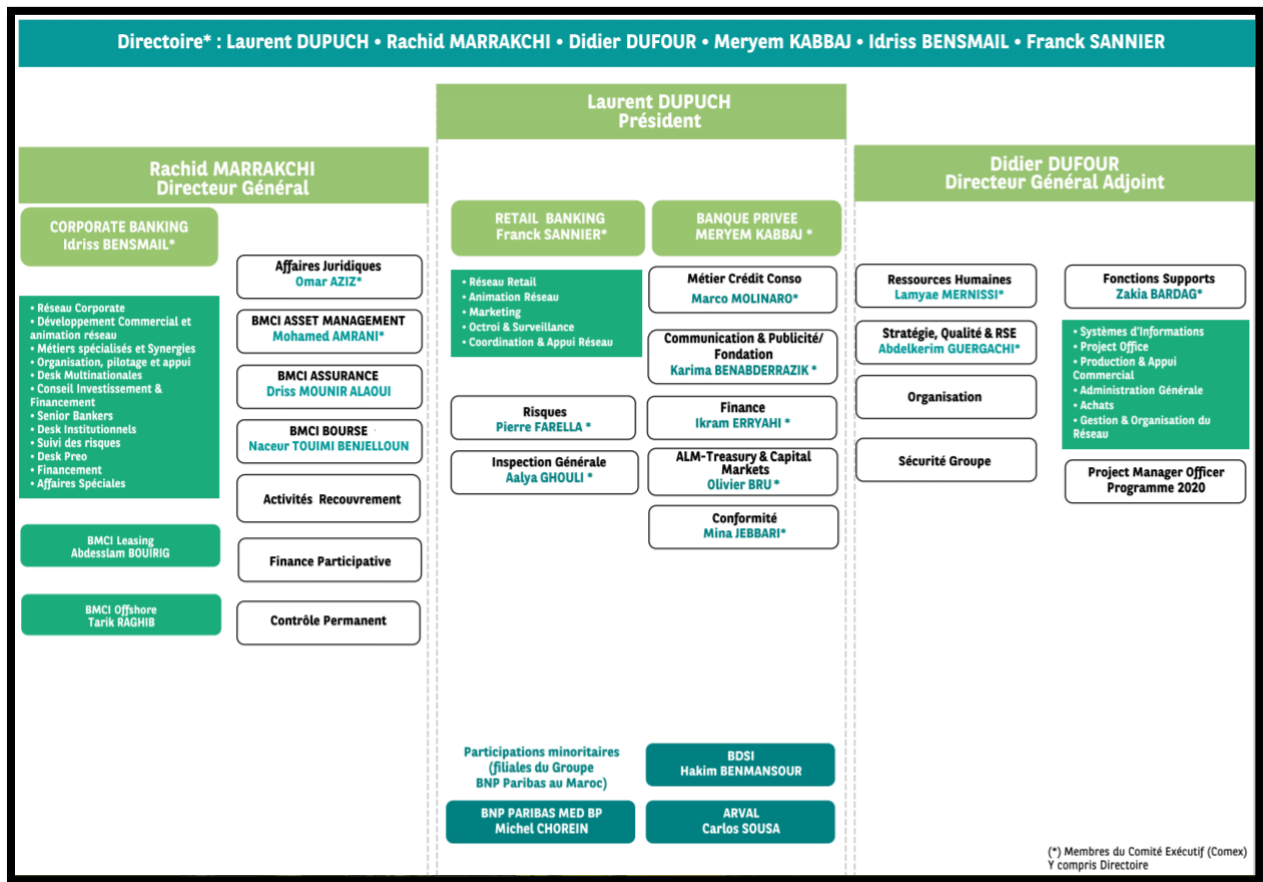


Figure 2 : Organigramme du Groupe BMCI [4].

1.2. Fiche descriptive de la BMCI

Dénomination sociale	Banque Marocaine du Commerce et de l'Industrie
Secteur d'activité	Bancaire
Forme juridique	Société Anonyme (S.A)
Capital de Casablanca	1 327 928 600 DH
Date de Constitution	1943
Président du directoire	Laurent DUPUCH
Directeur Général	Rachid MARRAKCHI
Nombre d'agence	370 agences
Siège social	26, Place des Nations Unies Casablanca
Site Internet	www.bmci.ma

Figure 3 : Fiche descriptive de la BMCI [5], [1].

1.3. Présentation de la DSI

Ce stage a eu lieu au sein de la Direction des Systèmes d'Information DSI qui aide les organismes bancaires à mettre en place leurs différentes unités en mettant à leur disposition les moyens informatiques et télécoms (matériels et progiciels) de contrôle, transport, traitement, conservation et restauration des informations nécessaires à leur fonctionnement. La direction DSI se trouve au siège de la BMCI qui a plusieurs sites centraux : Back office (Perna), BMCI Crédit Conso, Immeuble Colline, Trade center et l'inspection générale.

2. Réseau de la BMCI

2.1. Architecture réseau de la BMCI

L'opérateur IAM assure à la BMCI deux réseaux MPLS, dont un réseau MPLS au niveau national, permet l'interconnexion entre les sites centraux et les agences de la BMCI et offre des services télécom, et le deuxième réseau MPLS assure l'interconnexion entre la BMCI du Maroc et la BNP Paribas en France. L'objectif est de partager des ressources (données, applications, et équipements informatiques) et travailler de façon collaborative en tant qu'une entité unique.

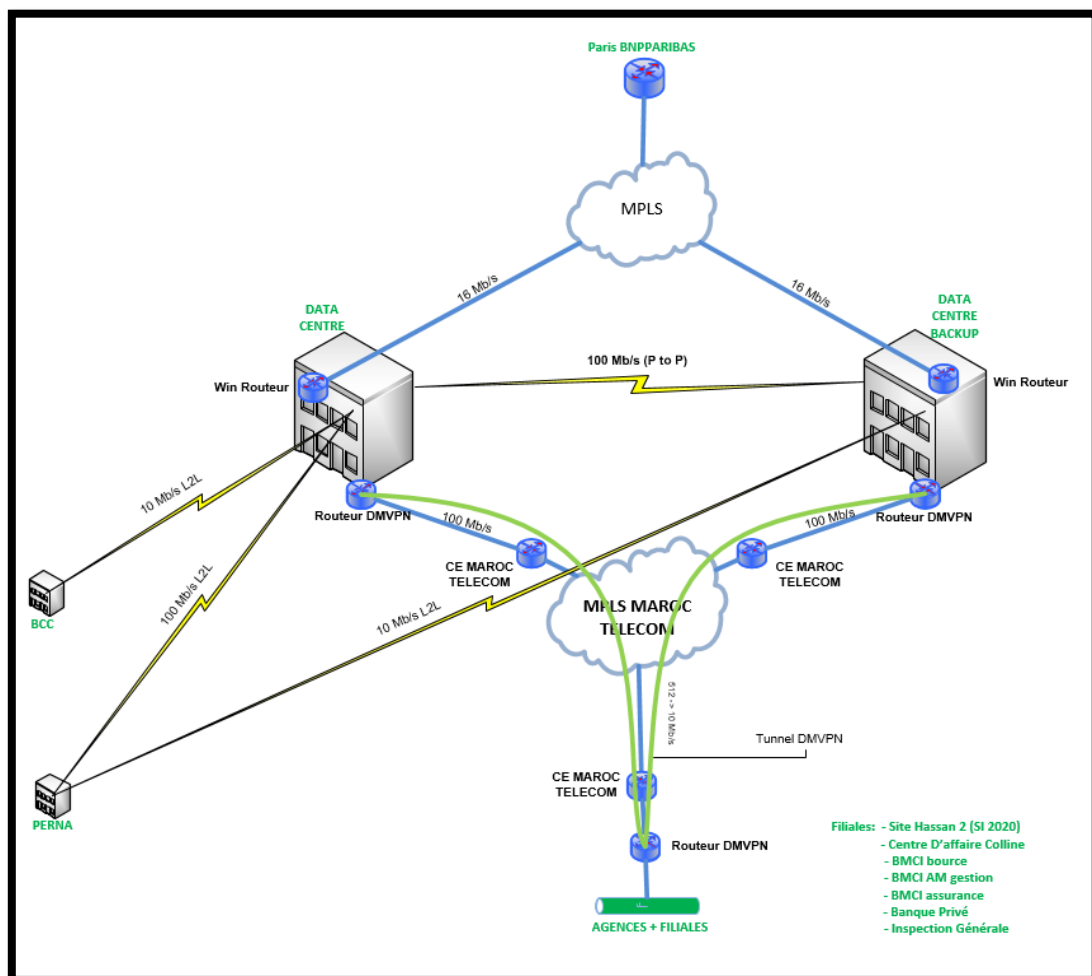


Figure 4 : Architecture réseau de la BMCI.

2.2. Architecture réseau du LAN

L'architecture LAN de la BMCI se présente comme suit :

Au niveau des sites, il existe un local technique qui contient une armoire de brassage dans chaque étage, et chaque armoire regroupe les équipements terminaux informatiques et téléphoniques. Les commutateurs de chaque armoire sont reliés par des câbles RJ45 aux équipements informatiques de cet étage (postes, imprimantes, serveurs, etc.). Ensuite, un commutateur fédérateur, auquel sont connectés les commutateurs de tous les étages, est lié à un routeur. Enfin, ce routeur est lui-même lié à un routeur opérateur par un tunnel VPN (Virtual Private Network).

Au niveau des agences, le commutateur de l'armoire de brassage qui relie les équipements informatiques est lié directement au routeur de la BMCI qui est lié à un routeur opérateur par un tunnel VPN.

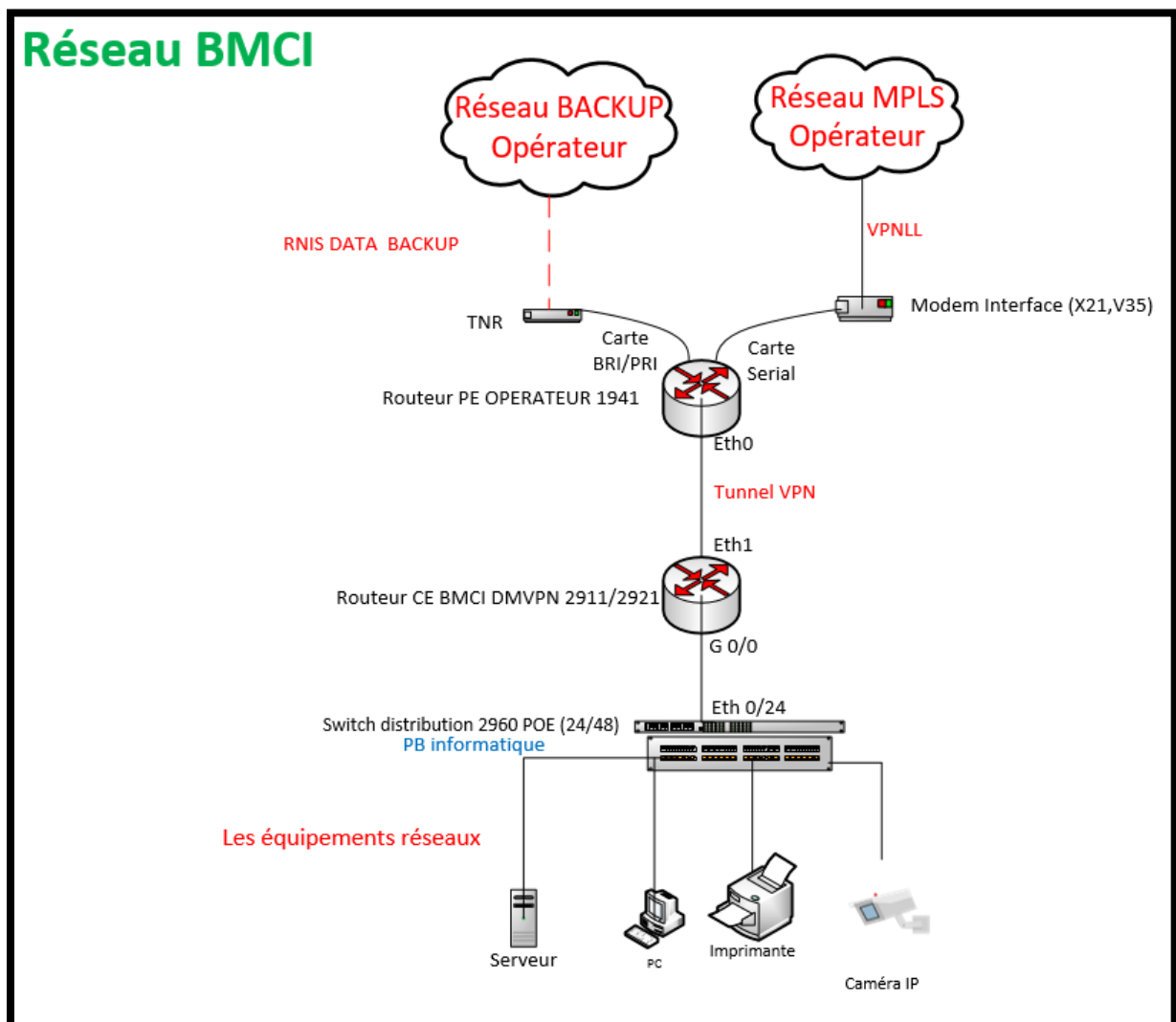


Figure 5 : Architecture réseau LAN de la BMCI.

2.3. Architecture réseau téléphonique

Les appareils téléphoniques sont liés par des câbles à un switch téléphonique lié à un PABX (Private Automatic Branch Exchange). Ce PABX est lié au réseau de l'opérateur, pour les appels fixes entrants et sortants, on passe par l'opérateur IAM ; et pour les appels sortants GSM, on passe par l'opérateur INWI car le coût d'appel est moins cher.

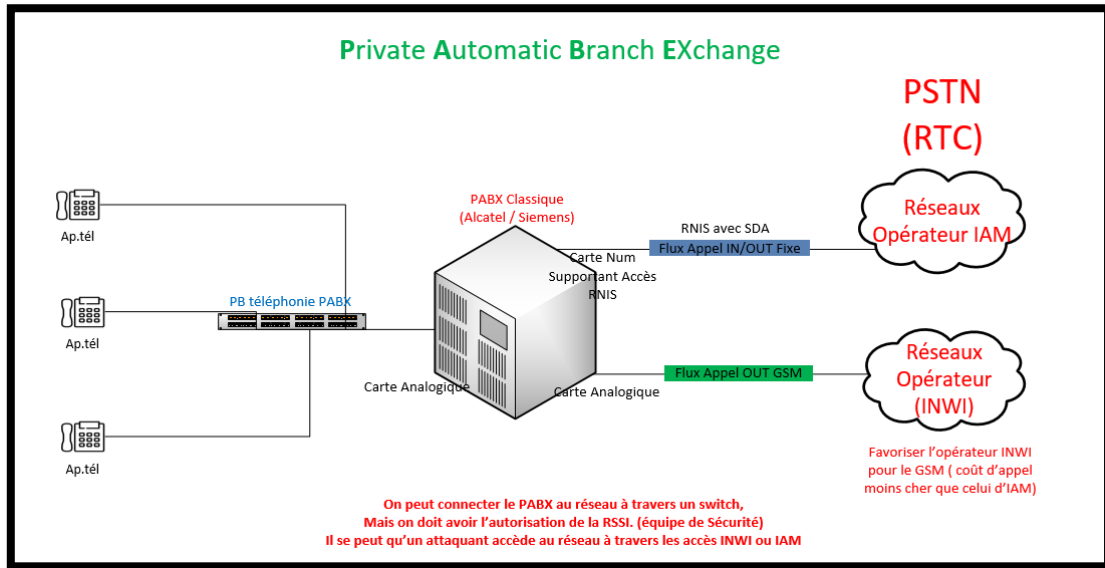


Figure 6 : Architecture téléphonique de la BMCI.

Le schéma ci-dessous représente en détail l'architecture informatique et téléphonique de la BMCI :

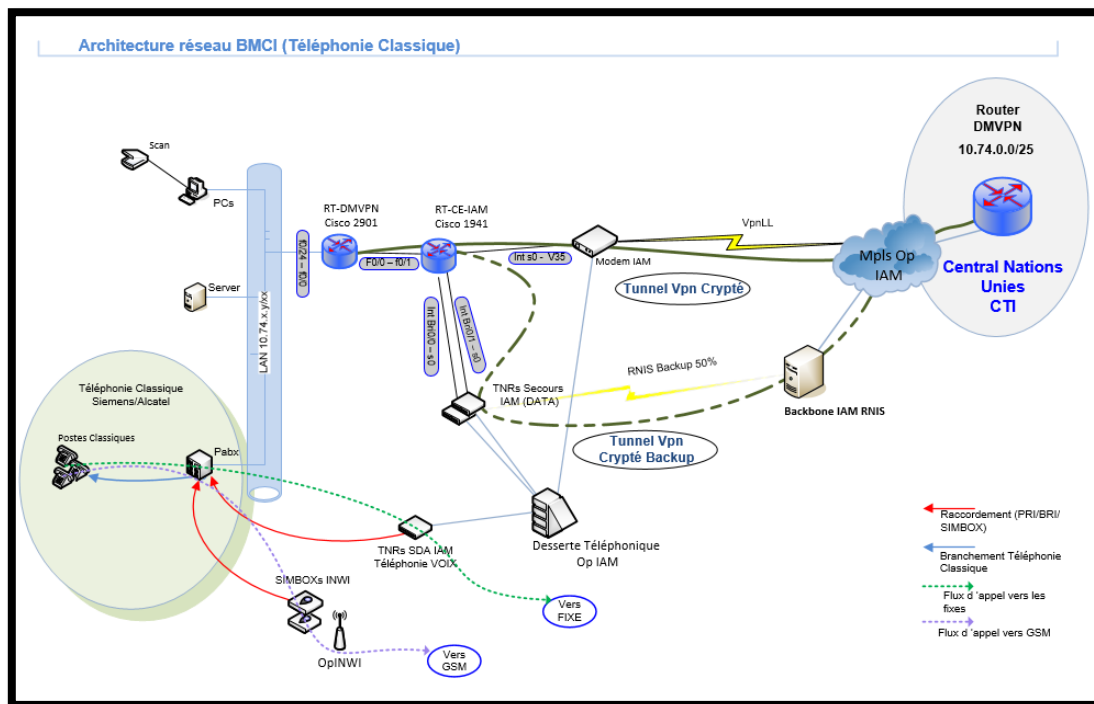


Figure 7 : Architecture informatique et téléphonique de la BMCI.

2.4. Architecture réseau et téléphonique des sites liés au projet

Dans cette partie, nous allons détailler l'architecture de chacun des sites suivants :

- **Back office (Perna).**
- **BMCI Crédit Conso.**
- **Immeuble Colline.**
- **Trade center.**
- **Inspection générale.**

2.4.1. L'architecture du Back Office (perna) et de la BMCI Crédit Conso

Ces deux grands sites ont presque la même architecture, la différence est minime :

Back Office (Perna)

Cet immeuble est constitué de 5 étages, le local technique de chaque étage (service) contient une armoire de brassage qui contient des commutateurs informatiques et des commutateurs téléphoniques, où les équipements terminaux informatiques et téléphoniques sont connectés. Le PABX et le commutateur fédérateur de cet immeuble se trouve au premier étage. Le commutateur fédérateur est lié au data centre par une liaison de 100 méga et au data centre backup par une liaison de 10 méga.

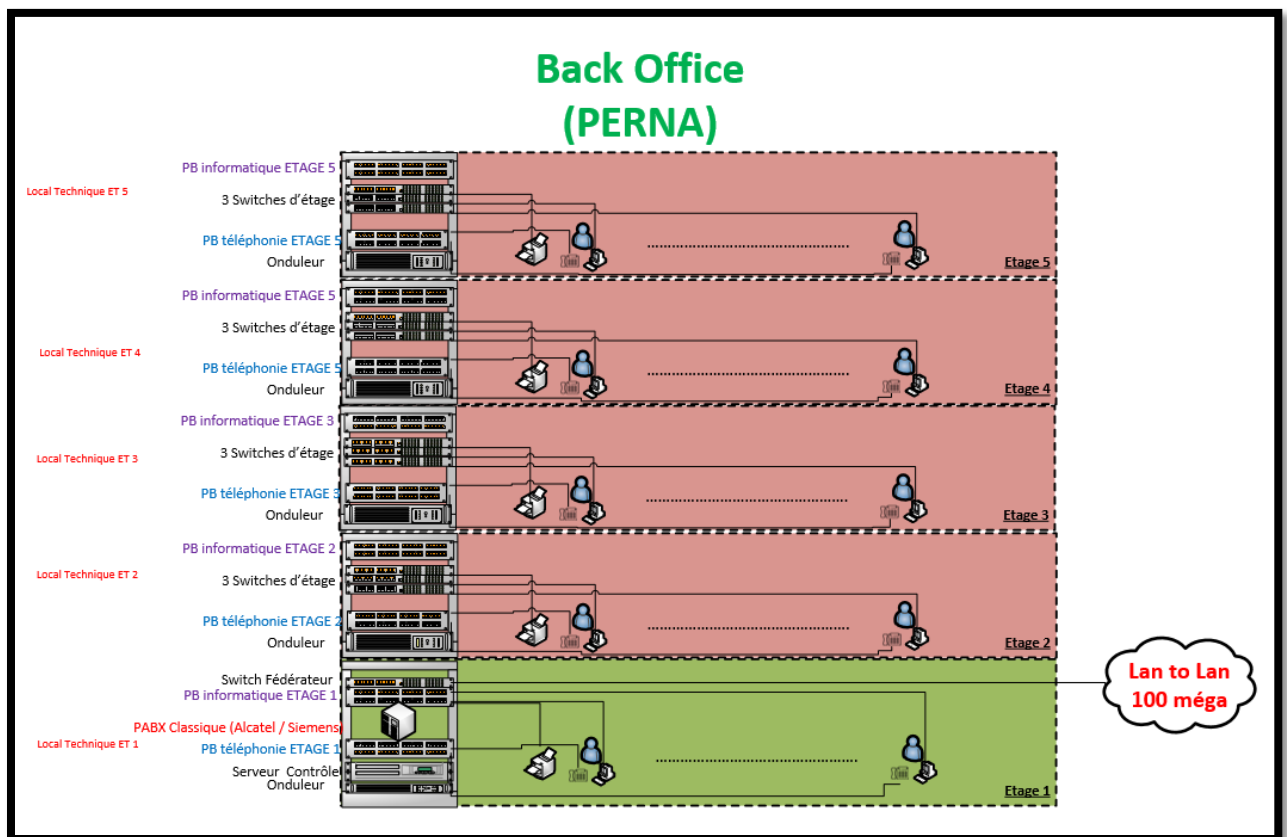


Figure 8: Architecture informatique et téléphonique du site Back Office.

BMCI Crédit Conso

Cet immeuble est constitué de 8 étages, les 6 premiers étages (services) contiennent un local technique où se trouve l'armoire de brassage qui contient des commutateurs informatiques et des commutateurs téléphoniques où les équipements terminaux informatiques et téléphoniques sont connectés. Les 2 derniers étages disposent d'un seul local technique contenant l'armoire de brassage et le PABX de cet immeuble. Le commutateur fédérateur est lié au data centre par une liaison de 100 méga.

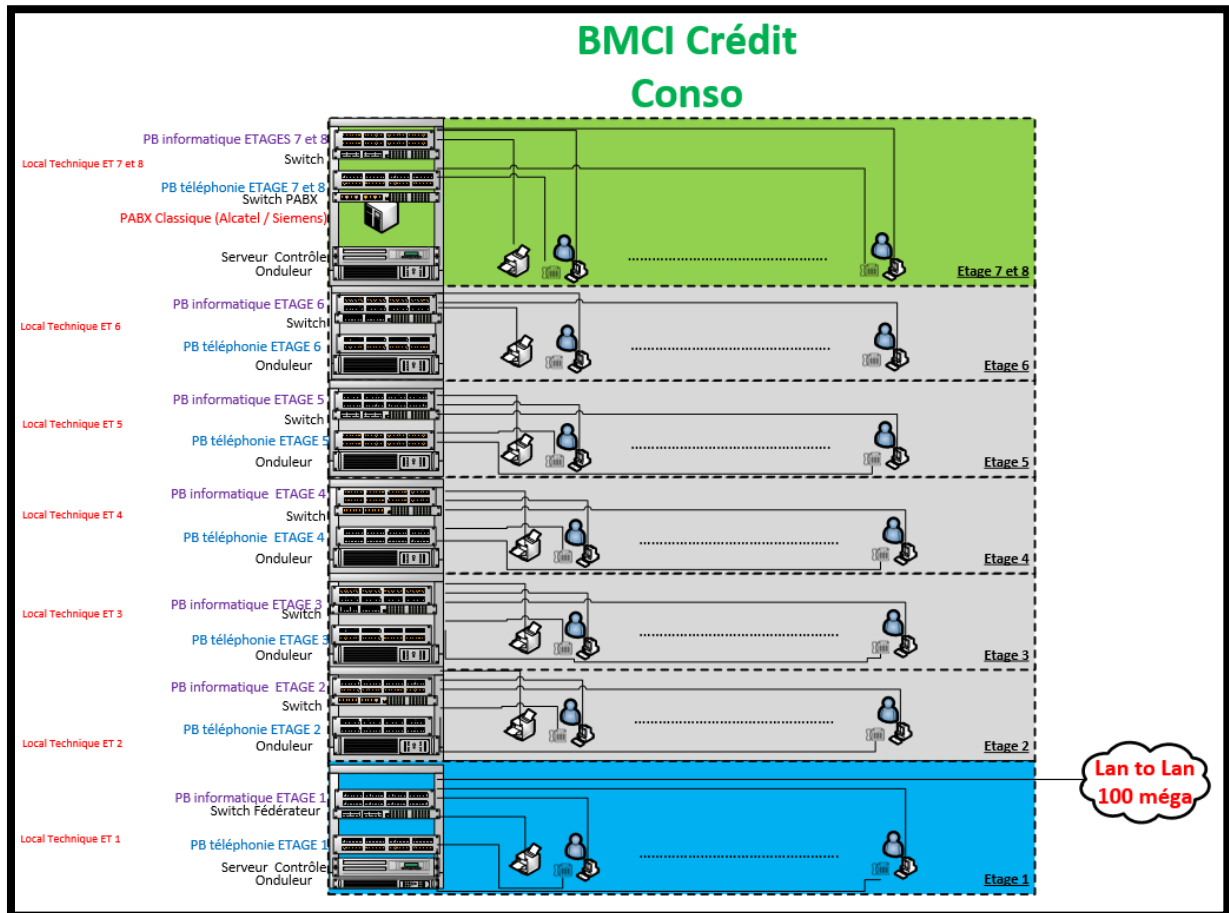


Figure 9: Architecture informatique et téléphonique du site BMCI Crédit Conso.

2.4.2. Immeuble Colline

Ce site contient 1 RDC et 3 étages dont le 2^{ème} est vide, les commutateurs de chaque étage sont connectés à un commutateur fédérateur au RDC. Le PABX du réseau téléphonique se trouve au RDC. Le 1^{er} étage contient 2 services séparés, chacun avec ses propres équipements. Le commutateur fédérateur est lié au routeur BMCI qui est aussi lié au routeur de l'opérateur par un tunnel VPN.

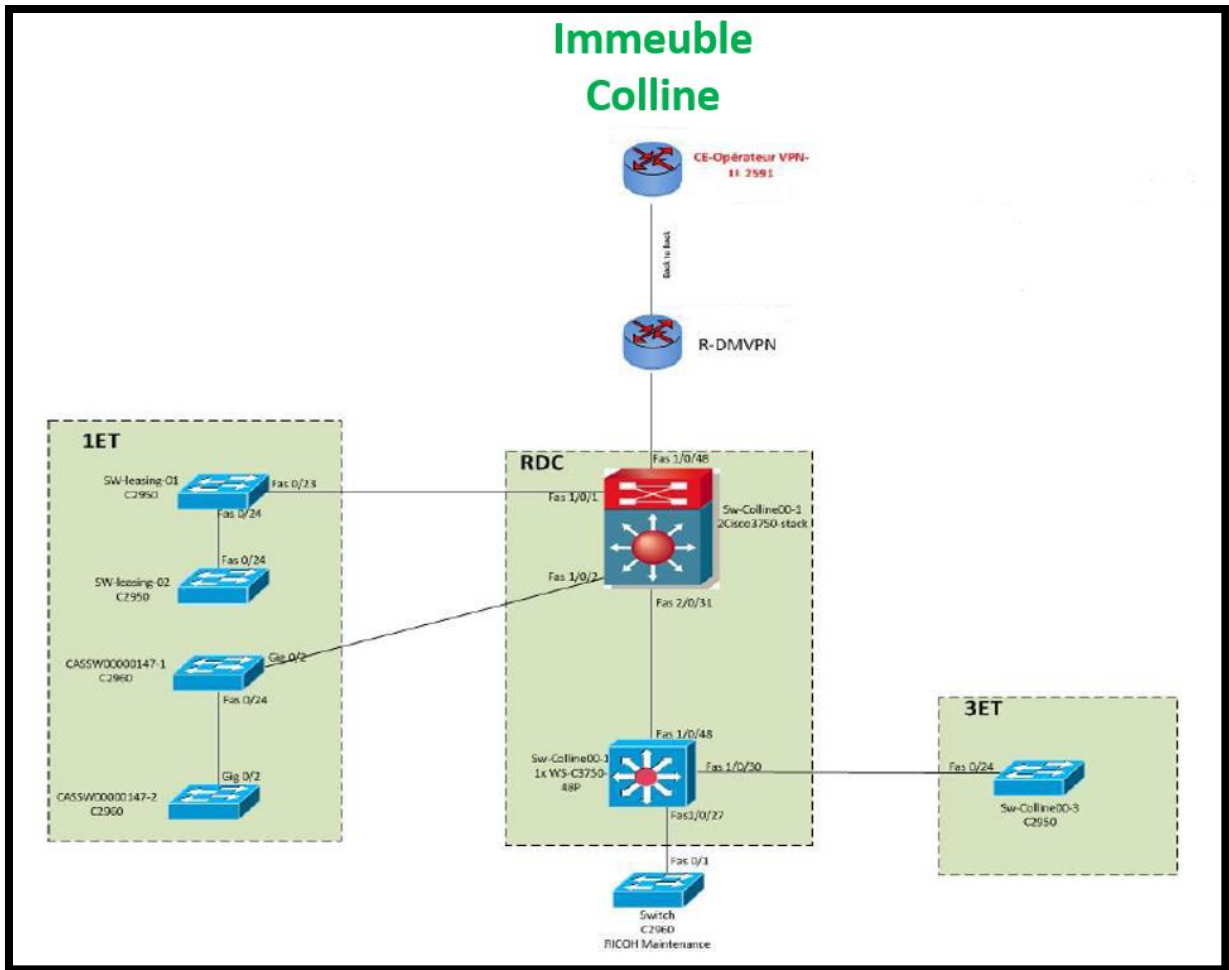


Figure 10 : Architecture informatique et téléphonique du site Immeuble Colline.

2.4.3. Trade Centre

Ce site est constitué de plusieurs services : Le service IMEX Immobilier et Exploitation, le service Centre de formation et l'agence 16 Novembre contiennent un local technique où se trouve l'armoire de brassage qui contient les commutateurs informatiques et téléphoniques où les équipements terminaux informatiques et téléphoniques sont connectés. Par contre, les équipements du service Restaurant sont connectés au commutateur du service IMEX.

Les commutateurs de chaque service sont liés à un commutateur fédérateur qui est lié à un routeur BMCI qui est aussi lié au routeur de l'opérateur par un tunnel VPN.

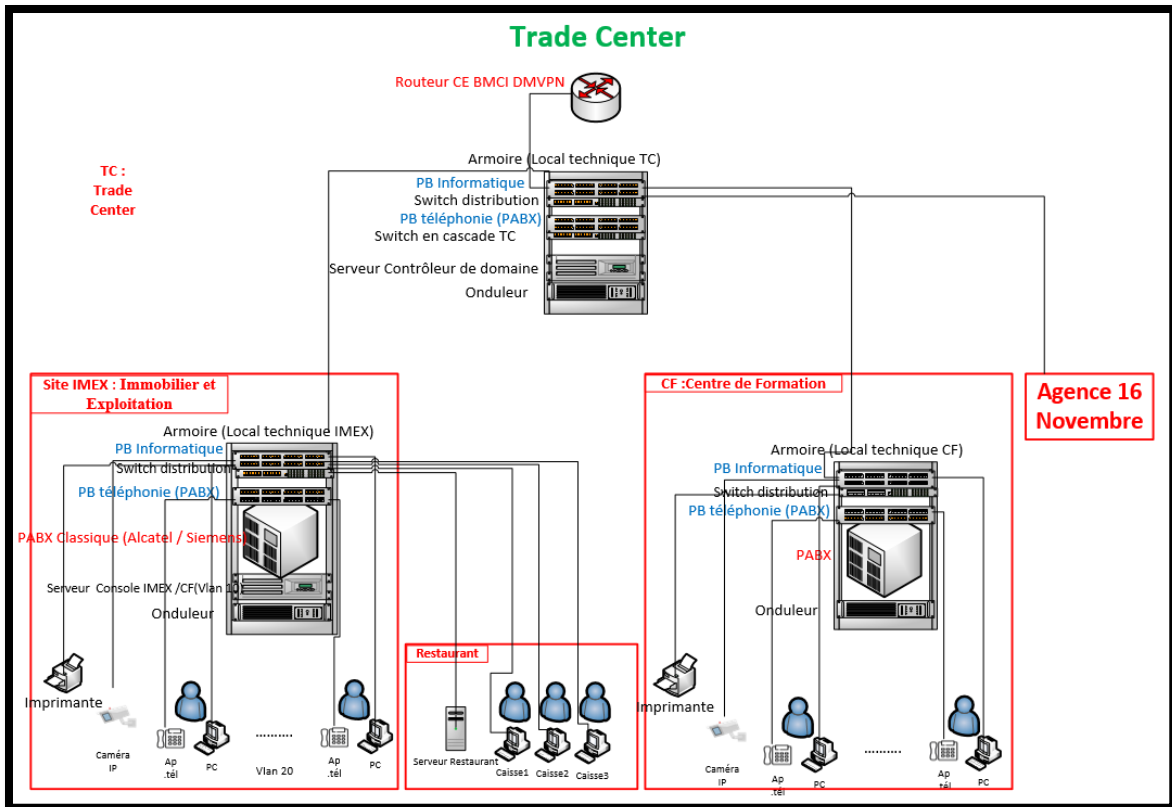


Figure 11 : Architecture informatique et téléphonique du site Trade Center.

L'architecture d'une agence typique de la BMCI se présente comme suit :

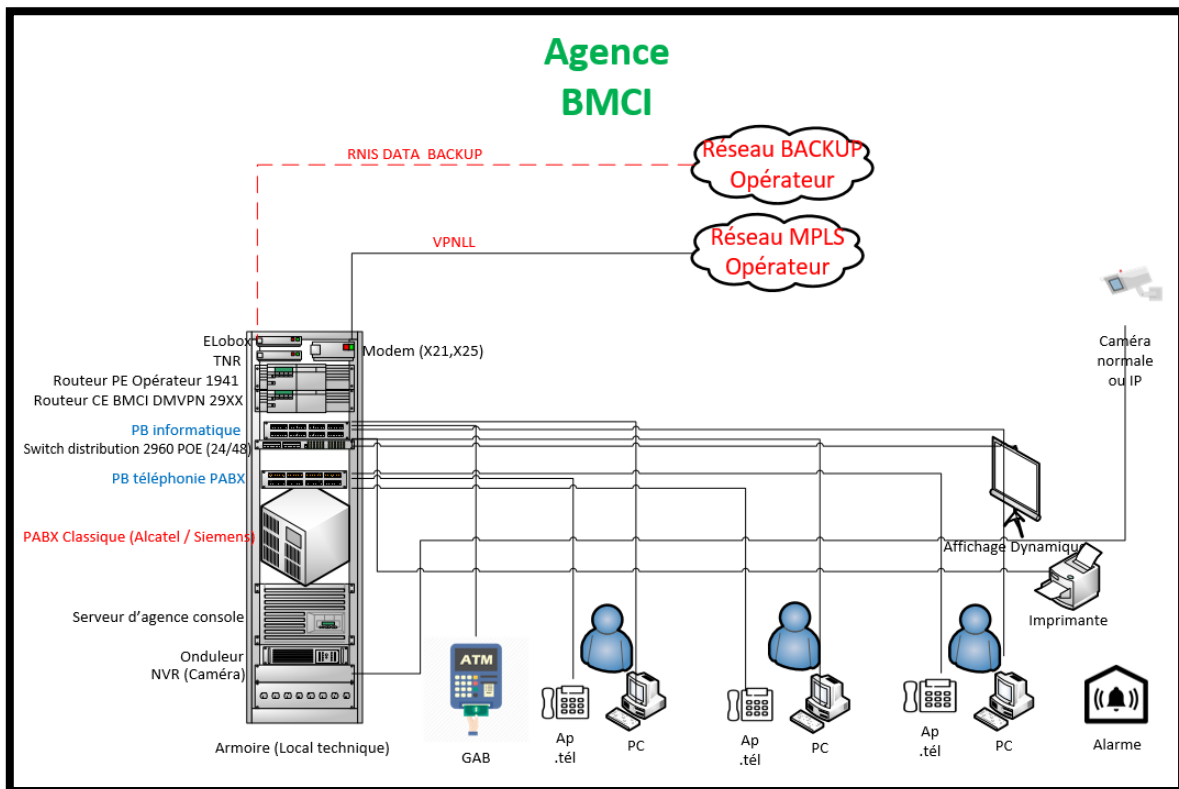


Figure 12 : Architecture informatique et téléphonique d'une agence typique de la BMCI.

2.4.4. Inspection générale

Ce site contient un local technique où se trouve l'armoire de brassage qui contient les commutateurs informatiques et téléphoniques où les équipements terminaux informatiques et téléphoniques sont connectés. Le commutateur informatique est lié à un routeur BMCI qui est aussi lié au routeur de l'opérateur par un tunnel VPN. Le commutateur téléphonique est lié au PABX de ce site.

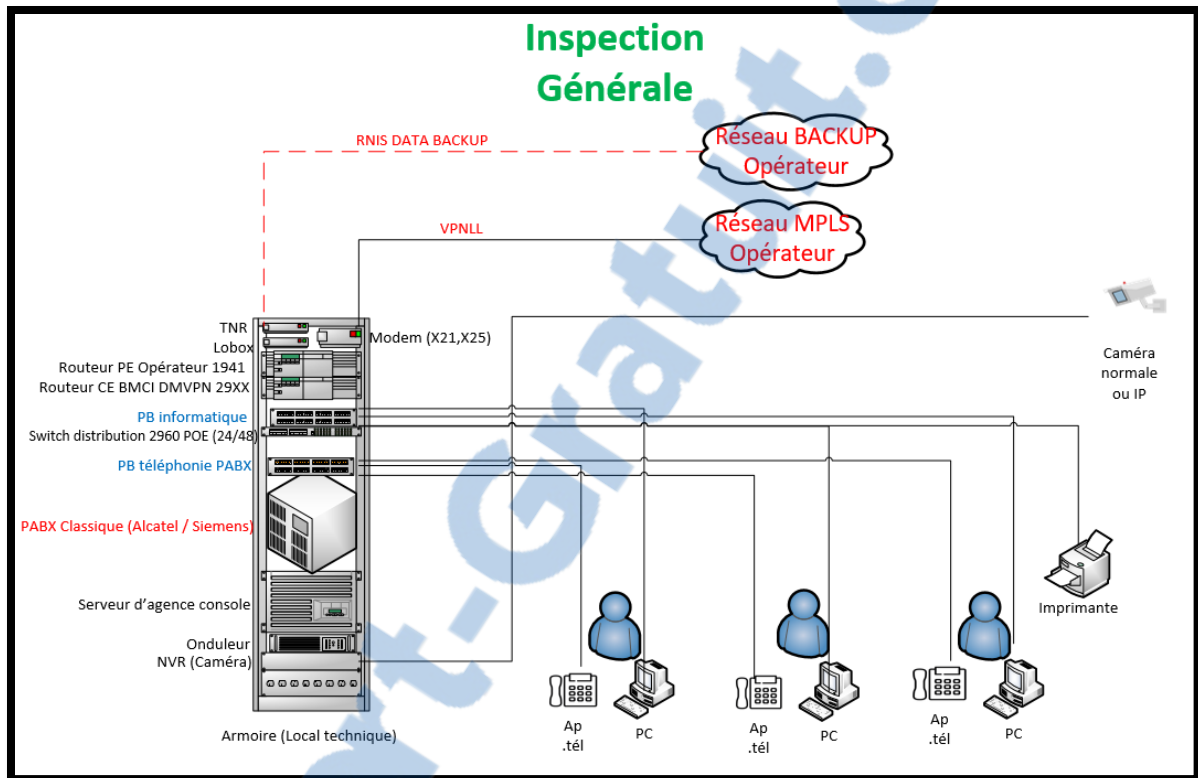


Figure 13 : Architecture informatique et téléphonique du site Inspection générale.

2.5. Matériel utilisé au niveau de cette architecture

Dans l'architecture existante, nous avons constaté l'utilisation de plusieurs matériaux.

Les équipements au niveau du réseau informatique sont les suivants :

- Les panneaux de brassage 24/48 ports
- Les commutateurs Cisco Catalyst 2960 (24/48 ports) et 3750 (24/48 ports)
- Les routeurs Cisco 1900, 2900 et 3800
- Les modems
- Les onduleurs

Les équipements au niveau du réseau téléphonique sont les suivants :

- Les PABX Alcatel et Siemens
- Les panneaux de brassage PABX
- Les commutateurs PABX
- Les téléphones Alcatel et Siemens

D'autres types d'équipements tel que :

- Les baies de brassage
- Les câbles UTP CAT 5
- Les Caméras analogiques
- Les DVR Digital Vidéo Recorder
- Les alarmes RTC
- Les PC, les imprimantes, le TNR, etc.

3. Limites de cette architecture

3.1. Limites au niveau du réseau informatique

- La qualité de service est moyenne à cause de la dégradation du réseau, du temps de latence élevé (ralentissement), et des pannes fréquentes.
- L'architecture réseau est mal structurée ce qui rend difficile la détection des problèmes et augmente le temps de leur résolution.
- L'architecture est une architecture en étoile sans redondance des liens, d'équipements réseau et de passerelles, ce qui implique que si un équipement tombe en panne, tous les équipements terminaux connectés à cet équipement n'auront pas de réseau.
- Une partie du matériel du réseau informatique est obsolète.

3.2. Limites au niveau du réseau téléphonique

- Le coût des équipements au niveau de la téléphonie classique est très élevé, par exemple : le prix d'un PABX varie entre 20000 et 30000 DH.
- Les postes téléphoniques sont reliés physiquement à des lignes, ce qui empêche leur mobilité tout en conservant le même numéro de téléphone.
- La facturation est par appel (appel externe).
- Le coût de maintenance est très élevé, et recours à des prestataires externes ce qui empêche d'avoir une visibilité sur le réseau téléphonique.
- La difficulté de management et de supervision du réseau téléphonique.
- Le débit est limité (<120 kbits/seconde).
- Le recours à des prestataires pour d'autres services tels que l'enregistrement des appels.
- Une partie du matériel du réseau téléphonique est obsolète.

La séparation entre les réseaux téléphoniques et informatiques implique des coûts ajoutés de câblage, d'équipements téléphoniques et de contrat de maintenance, etc.

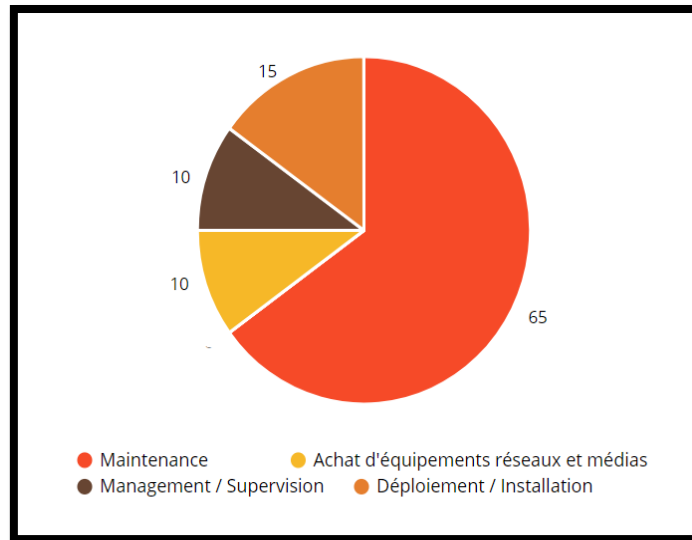


Figure 14 : Répartition des coûts en %.

Actuellement, 65% de la totalité des coûts sont des coûts de maintenance assignée à des prestataires externes, 10% pour les coûts de management et de supervision du matériel par ces prestataires, et 10% aussi pour les coûts d'achat d'équipements réseaux et médias, et enfin 15% pour les coûts de déploiement et d'installation.

Conclusion

Ce chapitre introductif sert globalement à présenter le cadre général du projet. Nous avons donc présenté la société dans laquelle s'est déroulé le projet, ainsi que l'architecture informatique et téléphonique de la société, et l'architecture de chaque site lié au projet. De plus, nous avons présenté les ressources matérielles utilisées. Enfin, nous avons exposé les limites de cette architecture. Dans le chapitre suivant, nous allons nous focaliser sur l'architecture proposée et ses avantages.

Chapitre 2 : La solution proposée

Chapitre 2 : La solution proposée

Introduction

Dans ce chapitre, nous allons proposer une nouvelle architecture que nous allons décrire en détail, ainsi que les principes et protocoles que nous allons utiliser dans cette architecture. Nous avons constaté que celle-ci peut être améliorée ; par conséquent, nous allons intégrer dans l'architecture proposée le service de la ToIP, puis le service du wifi, et enfin le service de la visioconférence. Nous allons expliquer chaque service introduit et l'amélioration qu'il apportera à notre architecture proposée que nous allons réexpliquer en détail. En dernier lieu, nous allons exposer les différents avantages que peut apporter notre architecture cible améliorée vis-à-vis des limites de l'architecture existante.

1. La nouvelle architecture proposée

Afin de remédier aux problèmes de l'architecture existante que nous avons constaté auparavant, nous avons décidé de conduire plusieurs réunions en interne avec les principaux responsables concernés par le projet de la refonte. Nous avons aussi eu recours à des consultants externes dans le domaine réseau et télécoms. Ces réunions et ces consultations nous ont mené à définir une nouvelle architecture réseau qui respecte les normes de BNP Paribas.

1.1. L'architecture réseau cible

Le schéma suivant représente l'architecture réseau proposée :

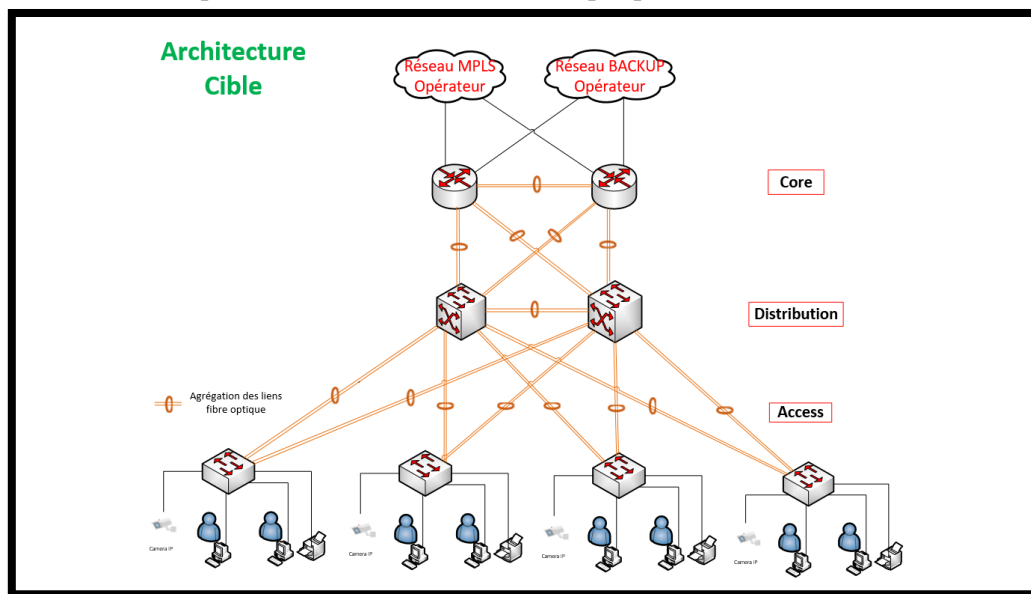


Figure 15 : L'architecture cible proposée.

L'architecture proposée est composée de trois niveaux : access, distribution, core.

1.1.1. Couche Access

Dans l'architecture cible, les commutateurs d'étages sont des commutateurs d'accès connectés à des PC d'utilisateurs, à des caméras et à des imprimantes multifonctionnelles via des câbles UTP catégorie 6 avec un débit de 100 Mbps.

Dans chaque étage, il se peut que le nombre d'équipements dépasse le nombre de ports dans un commutateur d'accès, dans ce cas, on ajoute des commutateurs pour faire ce qu'on appelle le stack. Le principe du stack est de fusionner deux ou plusieurs commutateurs physiques pour constituer un seul commutateur logique avec un nombre élevé de ports, afin de pouvoir connecter plus d'équipements et faciliter la configuration qui sera appliqué sur l'ensemble des commutateurs physiques.

Ces commutateurs d'accès sont interconnectés avec des commutateurs de distribution via deux liaisons fibre optique agrégées, avec un débit de 1 Gbps pour chacune. Le but de cette agrégation est d'avoir une redondance des liens en utilisant l'EtherChannel, assurer une haute disponibilité de réseau lorsqu'un des câbles fibres tombe en panne, augmenter le débit, permettre la communication et l'envoi des données et accéder aux serveurs situé au niveau du data center.

1.1.2. Couche distribution

Chaque commutateur de distribution est connecté avec des routeurs core pour accéder au WAN via deux liaisons fibre optique agrégées, avec un débit de 1 Gbps pour chacune. De plus, les commutateurs de distribution et les routeurs sont aussi connectés entre eux avec deux liaisons fibre optique. Le but de la redondance des équipements réseau au niveau de la couche distribution et la couche core est d'assurer une grande disponibilité au réseau, autrement dit, lorsqu'un commutateur de distribution ou un routeur de la couche core tombe en panne, l'autre commutateur de distribution ou l'autre routeur de core prend le relais.

1.1.3. Couche core

Chaque routeur de la couche core est connecté à deux réseaux MPLS, l'un d'eux est le principal et l'autre est le backup. Le but de la redondance du réseau MPLS est d'assurer la disponibilité au réseau au cas où il y'aurait un problème au niveau du réseau MPLS principal. Les liaisons qui relient le réseau backup aux routeurs sont secondaires par rapport aux liaisons qui lient le réseau MPLS principal aux routeurs. Il y'a une répartition de la charge entre chaque deux commutateurs ou deux routeurs (load balancing) afin de ne pas surcharger l'un ou l'autre.

L'architecture réseau proposée décrite ci-dessus est une architecture flexible du moment qu'elle permet l'introduction de plusieurs services sans aucun problème. De ce fait, elle peut

être améliorée de façon incrémentale. Le premier service que nous avons décidé d'intégrer est le service de la téléphonie sur IP.

1.2. Les protocoles liés à l'architecture cible

L'architecture que nous avons proposé utilise plusieurs principes et protocoles de niveau 2 et 3 du modèle OSI et une technologie de niveau sécurité.

1.2.1. Principes et protocoles de Niveau 2

Réseau local virtuel (Virtual Local Area Network)

Un réseau local virtuel, est un réseau logique indépendant. L'objectif d'une configuration de vlan (Virtual LAN) est de permettre la configuration de réseaux différents sur un même commutateur. Les VLANs sont utilisés pour réduire la taille d'un domaine de diffusion, optimiser la bande passante, améliorer la gestion du réseau et permettre de créer un ensemble logique isolé pour améliorer la sécurité (séparation entre les services) [6].

Le protocole spanning tree (STP norme IEEE 802.1D)

Spanning-Tree est un protocole L2 formalisé IEEE 802.1D qui crée un chemin sans boucle basé sur le chemin le plus court, afin de profiter de la redondance des liens et d'équipements tout en évitant la problématique des boucles [7].

Les protocoles d'agrégation des liens

EtherChannel est une technologie d'agrégation de liens utilisée principalement sur les commutateurs de Cisco ou non Cisco. Elle permet d'assembler plusieurs liens physiques Ethernet (8 liens au maximum) en un lien logique. Le but est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs [8].

1.2.2. Principes et protocoles de Niveau 3

Routage Inter-VLAN

Les VLANs étant au niveau 2 du modèle OSI, l'interconnexion entre deux VLAN ne peut s'effectuer que par l'intermédiaire d'une passerelle de niveau trois. Il est donc nécessaire de réaliser du routage entre deux VLAN au même titre qu'entre deux réseaux Ethernet. Ce routage est réalisé entre des interfaces virtuelles (une par VLAN) de la même manière qu'il serait réalisé entre des interfaces physiques. Pour router les trames entre deux VLANs, les routeurs doivent pouvoir les détaguer puis les tagguer à nouveau avec le bon VID. Il est conseillé de filtrer les réseaux en utilisant des ACLs (Access Control List) [9].

Protocole de redondance de la passerelle.

HSRP ou « Hot Standby Routing Protocol » est un protocole propriétaire Cisco qui a pour fonction d'accroître la haute disponibilité dans un réseau par une tolérance aux pannes. Cela se fait par la mise en commun du fonctionnement de plusieurs routeurs physiques ou switches niveau 3 (au minimum deux) qui, de manière automatique, assureront la relève entre eux d'un routeur à un autre. Plus précisément, la technologie HSRP permettra aux routeurs situés dans un même groupe (que l'on nomme « standby group ») de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local. En se « cachant » derrière ce routeur virtuel aux yeux des hôtes. Les routeurs garantissent en fait qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe [10].

Le protocole EIGRP

L'EIGRP était un protocole propriétaire Cisco (il est ouvert depuis 2013). Il s'agit d'un protocole de routage interne IGP (Interior Gateway Protocol). Il est capable de réaliser du routage au sein d'un Autonomous System, qui est un ensemble de réseaux sous une même autorité et il permet de déterminer les meilleures routes en fonction de l'encombrement du réseau [11].

Le protocole BGP

BGP (Border Gateway Protocol) est le seul type de protocole de routage du EGP (Exterior Gateway Protocol) qui assure le routage entre les AS. Il est aussi prévu pour fonctionner sur de très grands réseaux [12].

Le Protocole MPLS

MPLS (Multi-Protocol Label Switching) est une technique réseau utilisée pour combiner les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2. Il doit permettre d'améliorer le rapport performance/prix des équipements de routage, d'améliorer l'efficacité du routage (en particulier pour les grands réseaux) et d'enrichir les services de routage (les nouveaux services étant transparents pour les mécanismes de commutation de label, ils peuvent être déployés sans modification sur le cœur du réseau) [13].

1.2.3. Principes et protocoles de Niveau sécurité

La technologie DMVPN

Le DMVPN désigne un « Point to Multipoint overlay VPN Tunneling » où Overlay veut dire que le DMVPN fonctionne au-dessus d'autres protocoles (GRE/IPsec) [14]. Il s'agit d'un mécanisme qui vous permet d'établir les tunnels IPsec+GRE directement entre les routeurs qui veulent dialoguer ensemble avec une simplicité et une scalabilité déconcertante et surtout de façon totalement dynamique [15].

1.3. Amélioration de l'architecture cible

1.3.1. Introduction de la téléphonie sur IP (ToIP)

Définition de la ToIP

La téléphonie sur IP ou ToIP est un service de téléphonie fourni sur un réseau de télécommunications ouvert au public ou privé utilisant le protocole internet. Cette technologie permet d'utiliser des infrastructures déjà existantes s'appuyant sur le protocole TCP/IP pour y raccorder de nouveaux terminaux IP [16].

Avantages de la ToIP

- Coûts amoindris en comparaison des coûts télécoms de l'opérateur historique,
- Simplification de la gestion administrative et technique,
- Meilleur suivi et maîtrise de la consommation,
- La qualité et la disponibilité garantis grâce à l'amélioration constante des réseaux [16].

Les règles à respecter pour la migration en ToIP

- Dimensionner notre réseau local (s'assurer que l'on dispose d'une bande passante suffisante et surtout de sa disponibilité).
- Autoalimenter les postes téléphoniques (POE : Power over ethernet norme 802.3af).
- Assurer la sécurité.
- Optimiser le Délai de transmission : Il s'agit du temps de transfert de paquets qui doit être compris en 150 et 400 ms.
- Limiter le phénomène d'écho (réverbération du signal) [16].

Le transport de la téléphonie sur IP ne doit souffrir d'aucun retard de transmission, ni d'altérations, ni de perte de paquets. Dans le cas contraire, les échanges deviennent rapidement impossibles.

Le matériel nécessaire à la téléphonie sur IP

Pour installer la solution de la téléphonie sur IP, on doit disposer de trois éléments essentiels suivants :

- Les téléphones IP

Dans notre cas, les téléphones IP doivent être reliés à nos commutateurs d'accès qui sont des commutateurs POE (Power Over Ethernet), autrement dit, ils peuvent alimenter les téléphones IP sans utiliser de câbles électriques avec une tension de 48 V.

- Le Call Manager

Le Call Manager est une solution de traitement d'appel pour les entreprises. Plusieurs serveurs Call Manager peuvent être formés en cluster et administrés comme une seule entité. Le modèle en cluster permet une évolution de 1 à 30.000 téléphones IP pour un cluster, et permet le

partage de charge entre serveurs et la redondance du service de traitement d'appel. Notre cluster sera situé au data center [17].

Voici un exemple du Cluster Call Manager :

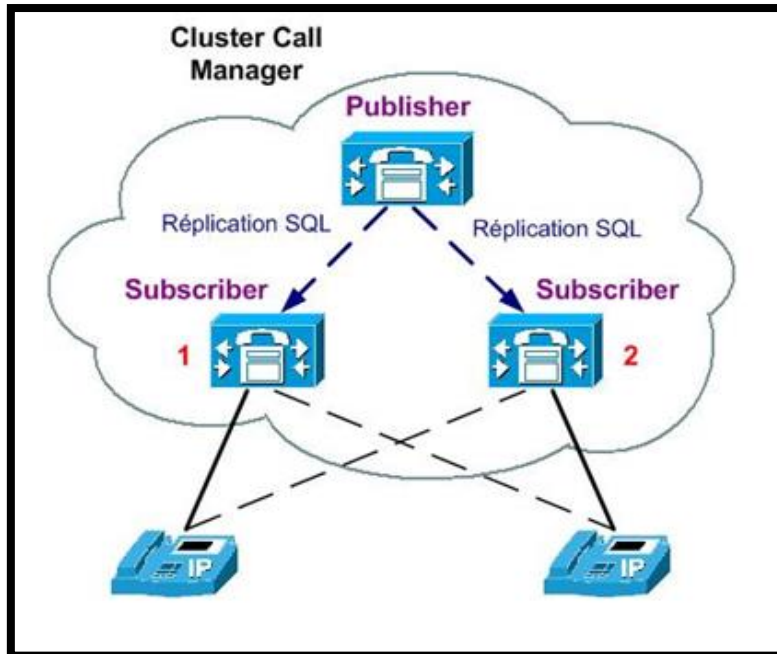


Figure 16 : Exemple du Cluster Call Manager.

Le cluster est constitué d'un publisher qui est un serveur Call Manager "maître" chargé de définir les fonctions de chaque subscriber, et de partager les charges, c'est aussi le serveur principal, donc l'ensemble du cluster ne fonctionnera plus s'il est hors service, et d'un ou plusieurs subscriber qui est un serveur Call Manager "esclave" chargé d'assurer les fonctions que le publisher lui demande, celui-ci effectue une réplication de la base de données du publisher (avec synchronisation), afin de ne se servir que de la sienne pour effectuer ses actions. De manière générale, les subscribers sont mis en place par pair, afin de se partager les charges, et assurer un système de secours en cas de hors service d'un subscriber [17].

- La passerelle de la téléphonie (gateway)

Une passerelle est un périphérique réseau qui est spécifiquement conçue pour permettre aux messages vocaux provenant d'un réseau téléphonique traditionnel d'être transmis sur un réseau utilisant le protocole IP, tout en leur offrant la possibilité d'effectuer le chemin inverse [18].

L'architecture globale de la téléphonie sur IP est la suivante :

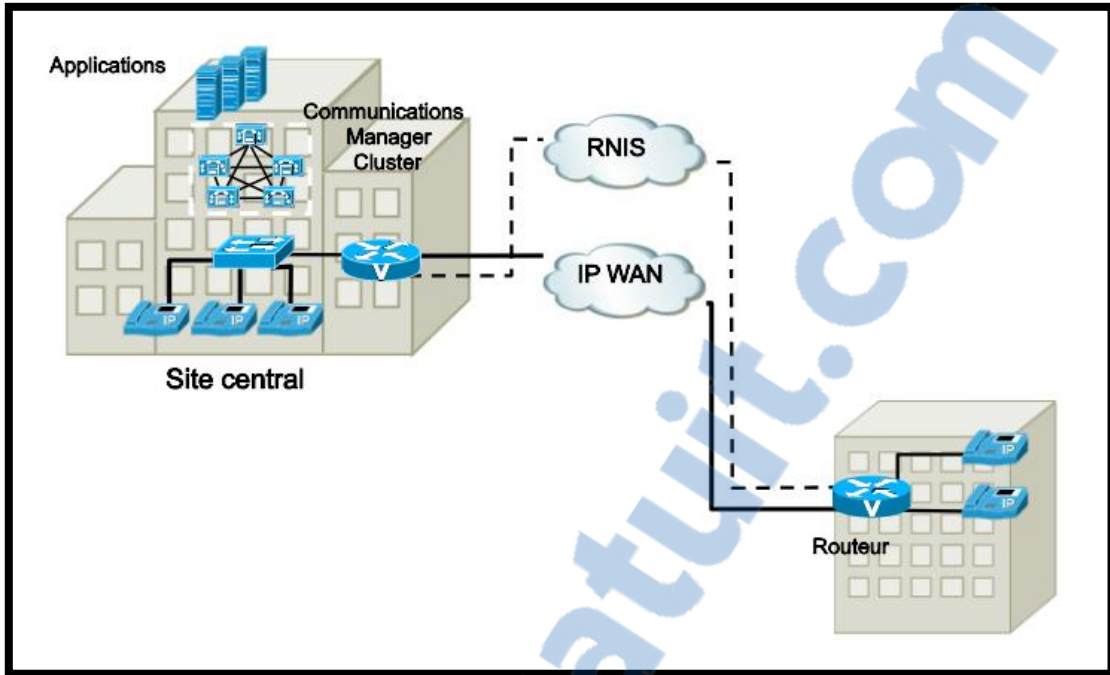


Figure 17 : Architecture globale de la solution TOIP [19].

Le schéma de l'architecture cible avec la téléphonie sur IP est le suivant :

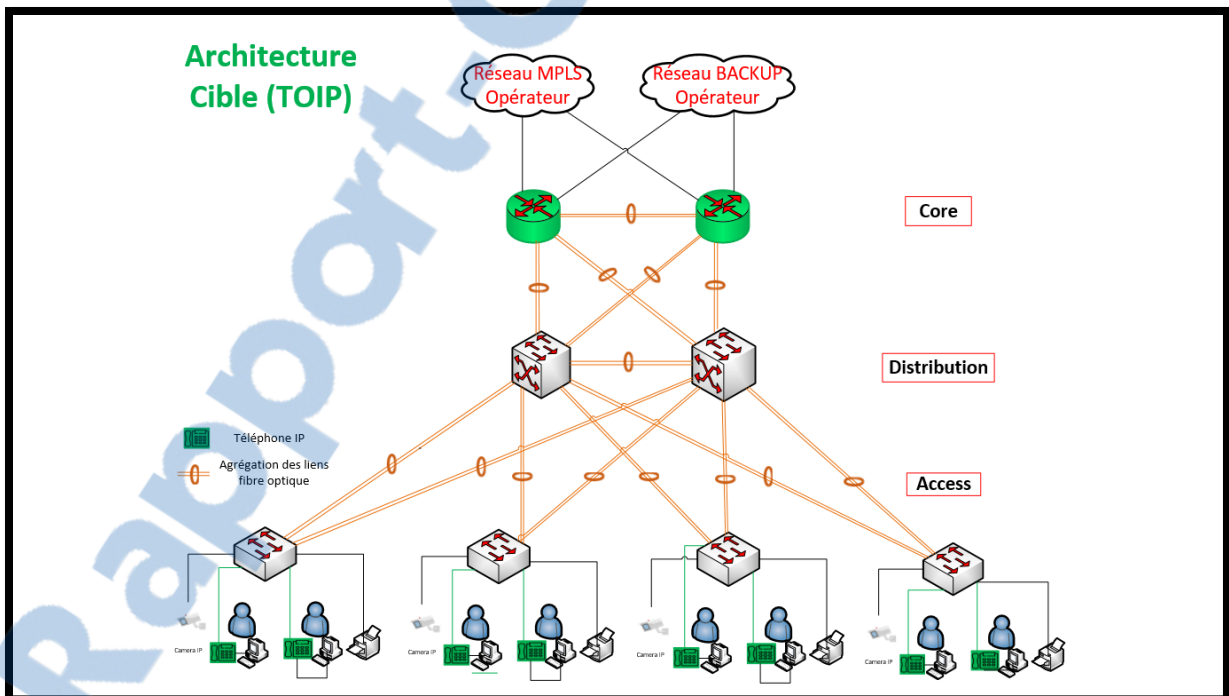


Figure 18 : L'architecture cible proposée avec la TOIP.

Afin d'améliorer notre architecture proposée, nous allons introduire des téléphones IP qui seront liés aux commutateurs de la couche access. Pour acheminer les appels, notre passerelle VoIP est représentée par nos deux routeurs de la couche core. Enfin, pour

gérer les appels, nous allons construire le Cluster Call Manager au niveau du Data center.

1.3.2. Introduction du wifi

Définition du Wi-Fi

Le Wi-Fi (Wireless Fidelity) est une technologie de transmission Haut-Débit sans fil qui utilise les ondes radio. Il s'agit de la dénomination de la norme IEEE 802.11 qui est le standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN) [20].

Le Wi-Fi offre une connectivité sans fil, il facilite grandement la création des réseaux locaux entre plusieurs ordinateurs reliés sans fil à un seul et même modem-routeur. Il permet de relier des ordinateurs portables, des PC de bureau, des assistants personnels (PDA) ainsi que des périphériques mobiles à une liaison haut débit ou à des appareils électroniques communiquant dans un rayon de plusieurs dizaines de mètres en intérieur à plusieurs centaines de mètres à l'extérieur [20].

Parmi les avantages du Wi-Fi c'est qu'il permet la mobilité car les câbles ne sont plus nécessaires dans un réseau sans fil, il peut aussi couvrir des zones difficiles d'accès aux câbles et le coût est rentabilisé sur le moyen terme car les réseaux sans fil ont des coûts de maintenance très réduits [21].

Les équipements du Wifi

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wifi :

- Les adaptateurs sans fils ou cartes d'accès (en anglais wireless adapters ou network interface controller, noté NIC) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil [22].
- Les points d'accès (notés AP pour Access point, parfois appelés bornes sans fils) permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes wifi [22].
- Les contrôleurs WLAN (Wireless LAN) sont particulièrement adaptés aux déploiements des réseaux locaux sans fil d'entreprise et fournissent à l'ensemble du système des fonctions WLAN comme les politiques de sécurité, la prévention d'intrusions, la gestion RF, la qualité de service (QoS) et la mobilité [23].

Architecture wifi proposée

Dans le cadre de l'amélioration de l'utilisation de son Système d'Information et de l'efficacité du travail, BMCI souhaite installer un WLAN sécurisé pour une meilleure collaboration. L'objectif du projet est de mettre en place une solution WIFI Entreprise hautement sécurisée au niveau du siège BMCI, avec toute l'infrastructure câblage qui va avec. L'architecture globale pour intégrer le service wifi est la suivante :

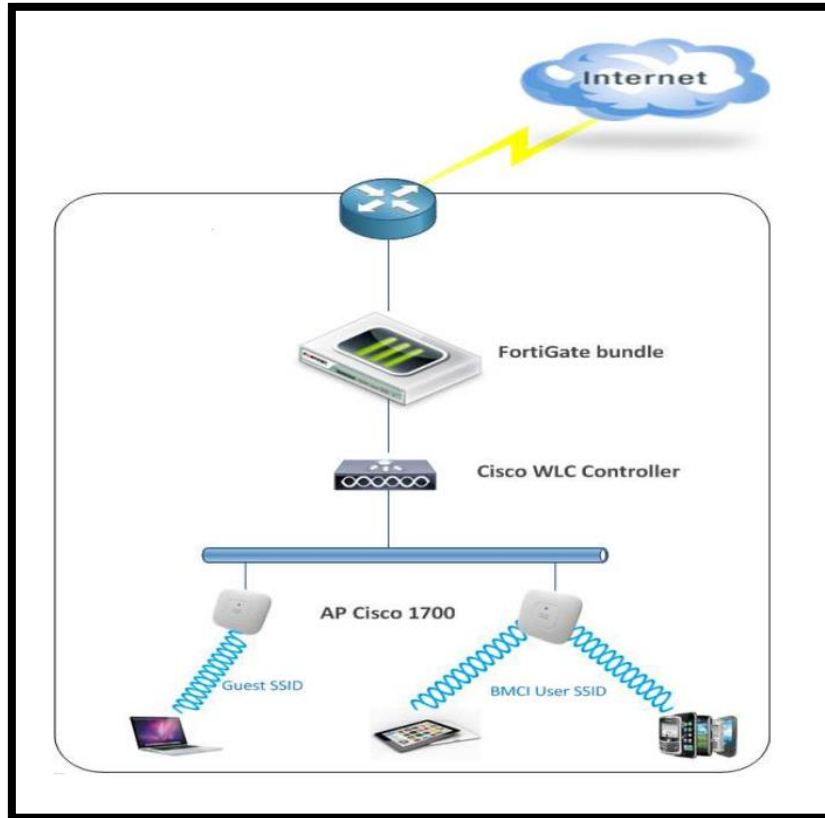


Figure 19 : Architecture globale du WIFI.

Notre architecture proposée peut être améliorée d'avantage grâce à l'introduction du service wifi. Le schéma suivant récapitule la nouvelle architecture avec wifi :

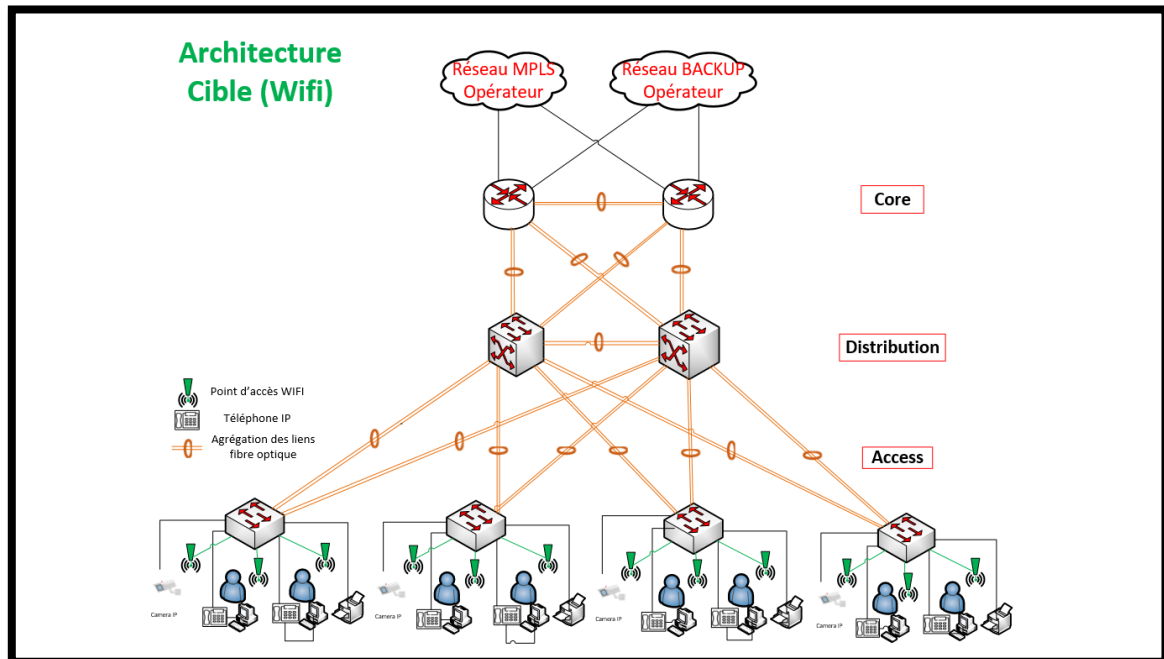


Figure 20 : L'architecture cible proposée avec le service WIFI.

Avec l'intégration du service wifi, nous allons installer des points d'accès qui vont être connectés aux commutateurs de la couche access et gérés par le contrôleur WIFI qui se trouve au data center.

1.3.3. Introduction de la visioconférence

Définition

La visioconférence peut être définie comme un système visuel et auditif permettant de communiquer oralement en temps réel et de façon interactive. La visiophonie, technologie permettant de voir et dialoguer avec son interlocuteur, offre différentes possibilités [24] :

- Le « point à point » est sans doute ce qui se rapproche le plus d'une conversation téléphonique : deux sites sont mis en relation via la vidéo.
- Le « multipoint » autorise quant à lui deux personnes ou plus à prendre part à une visioconférence via une salle de réunion, un ordinateur (au bureau ou à domicile), un smartphone ou une tablette.
- La diffusion, offrant à d'autres personnes la possibilité d'accéder à une réunion à l'aide d'un logiciel et non de matériel.



Figure 21 : Usage de la visioconférence en entreprise [25].

Les avantages de la visioconférence

Les entreprises bancaires réparties sur des sites distants utilisent la visioconférence pour réduire les coûts de déplacement, tout en ayant des réunions fréquentes. Elles se servent d'Internet pour communiquer par téléphone et par visioconférence à l'étranger. Elles peuvent donc établir des salons de visioconférence entre pays grâce à des logiciels de routage des appels sur Internet tel que Asterisk, avec un prix d'un abonnement Internet seulement.

Matériels de la visioconférence

- **Un écran**, c'est l'interface nécessaire afin de voir les interlocuteurs avec lesquels communiquer. Voir l'image de son interlocuteur rendra la communication des plus réelles.
- **Une caméra**, la caméra permettra d'être vu par vos interlocuteurs.
- **Un système audio doté d'un micro**, nécessaire pour pouvoir recevoir le son et communiquer en direct avec ses interlocuteurs.
- **Une interface ou un système de pilotage** permettant de lier les différents appareils entre eux et de pouvoir établir la visioconférence. Le PC fixe ou portable, le smartphone, la tablette peuvent être des interfaces de visioconférence. Sachez qu'il existe également des systèmes de visioconférences reliant les appareils indépendants entre eux [26].

Architecture visioconférence proposée

Parmi les problèmes rencontrés par la BMCI, la difficulté d'organisation des réunions, surtout avec les responsables qui se trouvent dans d'autres sites ou d'autres pays. C'est pour cela que la société a décidé d'introduire le système de la visioconférence pour limiter ces problèmes. La BMCI a choisi le système de salle haut de gamme qui est relativement coûteux et offre généralement une vidéo de qualité (écrans avec projecteurs ou écrans plasma de grande taille), un son Hi-Fi, et un environnement bien étudié : éclairage, aspects acoustiques, etc.

L'architecture globale pour intégrer le service de la visioconférence est la suivante :

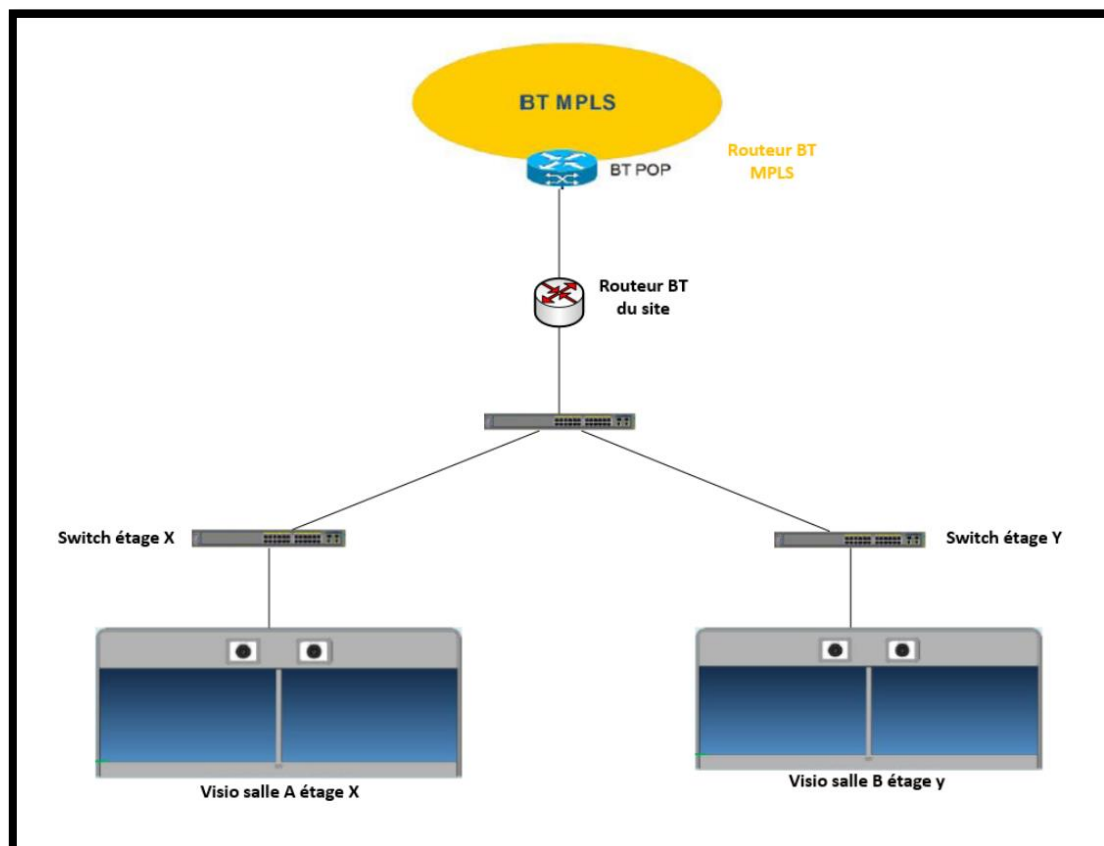


Figure 22 : Architecture globale pour le service de la visioconférence.

Avec l'intégration du service de la visioconférence, le schéma de l'architecture que nous avons proposé sera comme suit :

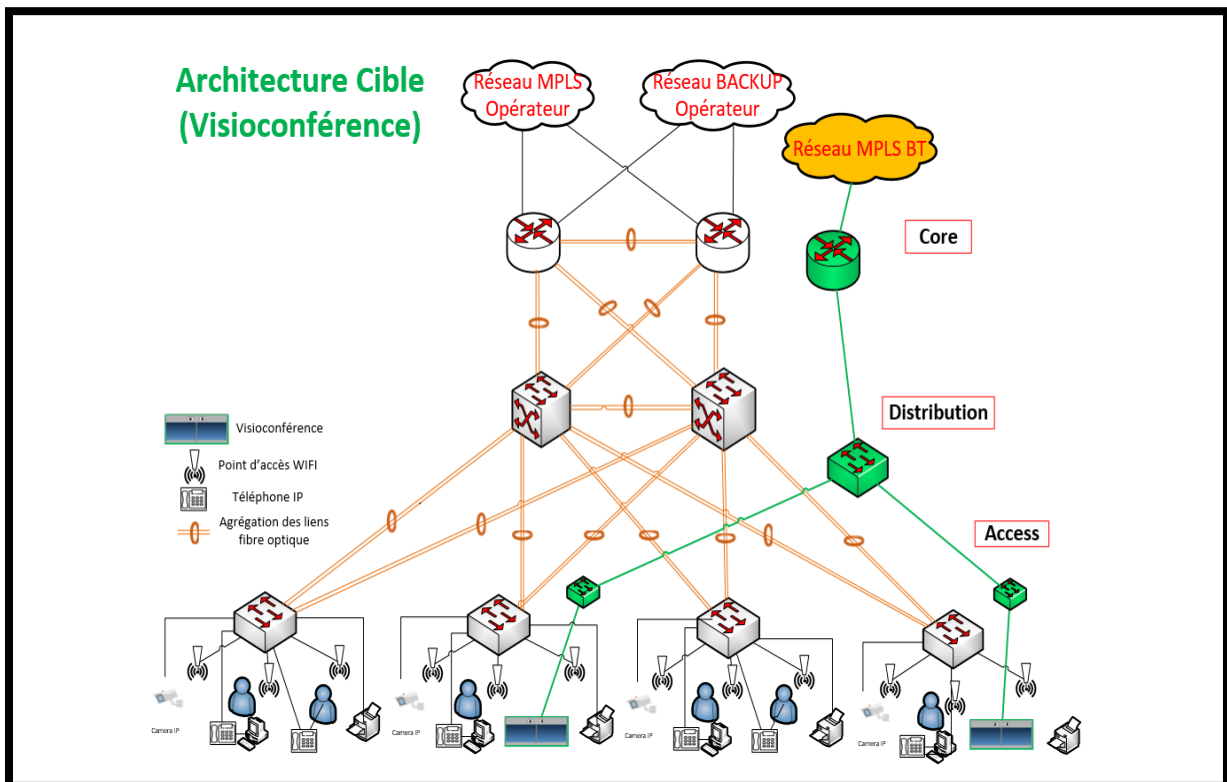


Figure 23 : Architecture cible proposée avec le service de la visioconférence.

Concernant le réseau de la visioconférence, c'est un réseau indépendant où chaque équipement de la visioconférence qui se trouve dans une salle de réunion est connecté à un commutateur. Ce commutateur est lié à un routeur BT installé au niveau du site de ce dernier, et ce routeur est connecté par le routeur d'entrée au réseau MPLS BT.

2. Les avantages de l'architecture proposée

Les avantages de l'architecture proposée sont nombreux, on cite :

- Refonte et amélioration de l'architecture existante
 - o Avoir un réseau uni-fonctionnel qui regroupe le réseau téléphonique et le réseau informatique, et par conséquent la réduction des coûts (de câblage, d'équipements téléphoniques, et de leur maintenance).
 - o Remplacer certains matériaux obsolètes (câbles, switches, routeurs, etc.) par les dernières nouveautés pour avoir plus de sécurité, et dans le cas où on n'arrive pas à résoudre une panne d'un matériel réseau en interne, on pourrait renvoyer la demande de réparation au fournisseur.
 - o Obtenir une architecture réseau simple et bien structurée, afin de faciliter la détection des pannes, diminuer le temps de leur résolution et avoir une visibilité globale sur notre réseau.

- Les numéros des postes téléphoniques au niveau de la TOIP ne dépendent pas de l'endroit mais de la personne, ce qui facilite la mobilité tout en conservant le même numéro de téléphone.
- La facturation n'est plus par appel mais gratuite et illimitée vers les téléphones internes.
- Le nombre de prestataires est très faible, ce qui implique un coût de maintenance réduit par rapport à l'architecture existante.
- Possibilité de transmission audio et vidéo.
- La bonne QoS
 - Assurer une bonne qualité de service en favorisant le trafic téléphonique sur le trafic des données, un temps de latence faible et des pannes rares.
- La gestion de la redondance
 - Implémenter une architecture en étoile avec redondance des liens, d'équipements réseau et de passerelles, et de ce fait si un équipement tombe en panne, notre réseau reste fonctionnel.
- L'augmentation du débit
 - Le débit est très élevé par rapport à la téléphonie classique qui va jusqu'à 25 Mbits/seconde.
- L'intégration d'autres services
 - Plusieurs services seront intégrés tel que le Wifi, la téléphonie sur IP (CISCO) et la Visio-conférence.
- La sécurité
 - Sécurisation des ports
 - ACL (Access List).
 - Utilisation de la technologie DMVPN.
 - Plus de contrôle sur le réseau.
- Une meilleure répartition des coûts

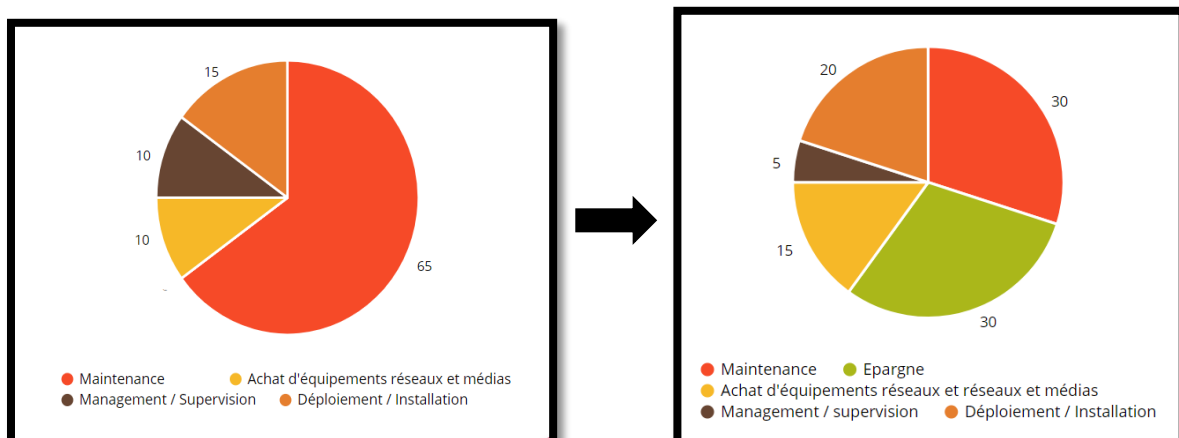


Figure 24 : Changement de la répartition des coûts en %.

La nouvelle architecture va nous permettre d'avoir une meilleure répartition des coûts. Tout d'abord, dans la totalité des coûts (100%), nous allons passer de 65% de coûts de maintenance

dans l'architecture existante à 30% de ces coûts dans l'architecture proposée. Cette réduction sera due à moins de recours aux prestataires externes. Ensuite, les coûts de management et de supervision vont aussi diminuer de 10% dans l'architecture existante à 5% dans l'architecture proposée car la supervision sera faite en interne. En plus, les coûts d'achat d'équipements réseaux et médias vont augmenter de 15% dans l'architecture existante à 20% dans l'architecture proposée et les coûts de déploiement et d'installation vont aussi augmenter de 10% dans l'architecture existante à 15% dans l'architecture proposée. Ces faibles augmentations seront dues à l'achat de nouveaux équipements nécessaires au projet et à leur installation. Ce projet va nous permettre alors d'épargner 30% des coûts sur le long terme.

Conclusion

Ce chapitre nous a permis non seulement de présenter une nouvelle architecture et les principes et protocoles utilisés dans cette architecture, mais aussi de voir comment nous avons pu l'améliorer en intégrant à chaque fois un service innovant tel que la ToIP, le wifi, et la visioconférence. Enfin, nous avons expliqué les nombreux avantages de cette architecture qui nous a permis de dépasser les limites de l'architecture existante. Le chapitre suivant sera consacré à la mise en place de la solution.

Chapitre 3 : La mise en place de la solution

Chapitre 3 : La mise en place de la solution

Introduction

Dans ce chapitre, nous allons déterminer la localisation du premier site où l'architecture cible sera implémentée, après avoir reçu la confirmation des responsables. Nous allons présenter le matériel livré nécessaire à la mise en place de cette architecture. Puis, nous allons exposer les travaux de câblage électrique et informatique et les travaux d'installation des équipements de l'architecture cible avec les services de ToIP, wifi et visioconférence. Enfin, nous allons aborder la configuration de l'architecture cible, sa description et ses fichiers.

1. Site bénéficiaire du projet

L'immeuble colline a été choisi comme le premier site qui va bénéficier du projet de la refonte LAN, cet immeuble est situé au Lot N°3 Route de Nouasser, Sidi Maarouf 20000 Casablanca. Il contient environ 200 personnes, il est composé d'un rez-de-chaussée et de trois étages.

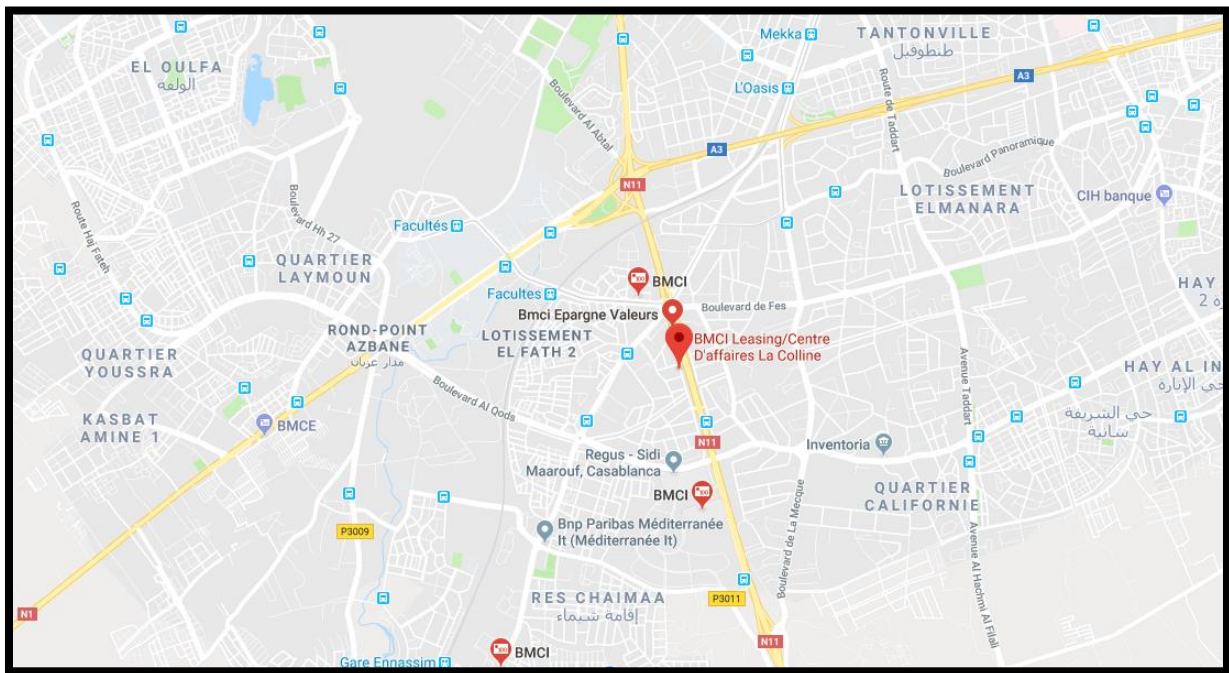


Figure 25 : Localisation du site sur Google map [27].



Figure 26 : Vue du site sur Google earth [28].

2. Le matériel utilisé au niveau de l'architecture cible

Après l'envoi de plusieurs bons de commande aux fournisseurs, nous avons reçu le matériel livré nécessaire à la mise en place de l'architecture cible.

Les équipements de l'architecture réseau cible sont les suivants :

- Les baies de brassage
- Les câbles Fibre Optique
- Les câbles UTP CAT 6
- Les panneaux de brassage 24/48 ports
- Les commutateurs Cisco Catalyst 2960 PEO (Power over Ethernet) 24/48 ports
- Les commutateurs Cisco Catalyst 3750 (Niveau 3) 24/48 ports
- Les routeurs Cisco 2900
- Les licences sécurité
- Les onduleurs
- Les modems

Les équipements nécessaires à l'introduction de la ToIP sont les suivants :

- Les cartes PRI [78] et PVDM (Packet Voice DSP Module)
- Les licences voix
- Les licences Cisco Unified Call Manager (CUCM) et enregistreurs d'appel Carine
- Les téléphones IP
- Les pieuvres pour conférence call

Les équipements nécessaires à l'introduction du Wi-Fi sont les suivants :

- Un Controlleur WIFI (WLC)
- Les Points d'accès

Les équipements nécessaires à l'introduction de la Visioconférence sont les suivants :

- Les écrans (MX800 G2)

- Les tablettes
- Les micros

D'autres types d'équipements tel que :

- Les caméras IP
- Les NVR Caméras

3. L'installation du matériel

3.1. Câblage électrique et informatique

Après la réception des équipements du site bénéficiaire, l'étape prochaine a été de refaire le câblage électrique et informatique. L'infrastructure réseau repose sur un bon système de câblage, il est alors primordial de bien le concevoir.



Figure 27 : Etat des lieux.

3.2. Equipements et configuration de l'architecture cible

Après les travaux de câblage du site bénéficiaire, l'étape prochaine a été de mettre en place les équipements de l'architecture cible. Les images suivantes nous donnent une idée sur l'avancement des travaux d'installation des équipements :

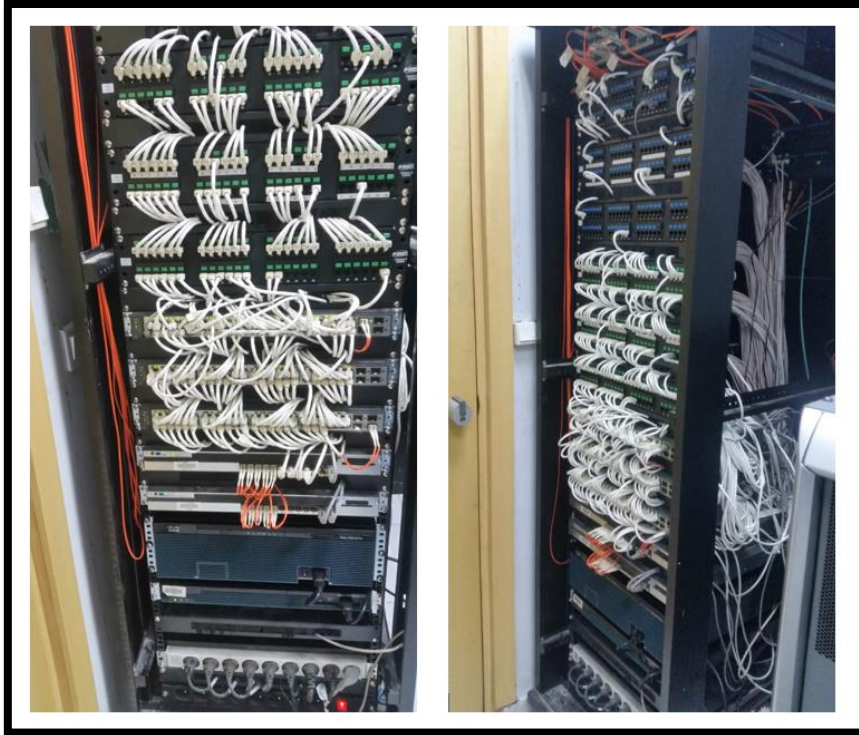


Figure 28 : La mise en place des équipements.

Pour l'architecture cible avec les services ToIP, wifi, et visioconférence, les équipements suivants ont aussi été mis en place :

3.3. Equipements de la TOIP

Les images suivantes montrent les équipements utilisés pour l'intégration de la ToIP dans notre architecture cible :



Figure 29 : La mise en place du cluster Call Manager et les téléphones IP.

3.4. Equipements du wifi

Les images ci-dessous reflètent les équipements utilisés pour l'intégration du wifi dans notre architecture cible :

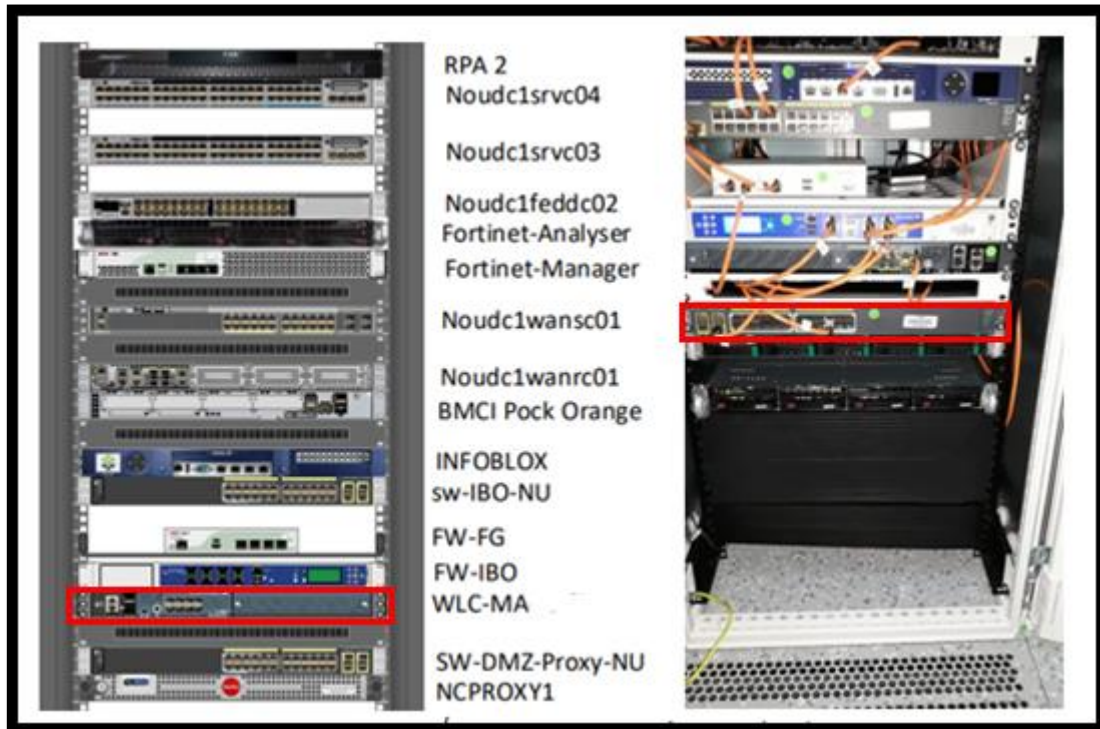


Figure 30 : La mise en place du contrôleur WIFI (WLC).



Figure 31 : La mise en place des points d'accès.

3.5. Equipements de la visioconférence

L'introduction du service de la visioconférence a eu lieu dans 2 salles au niveau de ce site.

Salle 1 :



Figure 32 : Photo de la salle 1 avant l'introduction de la visioconférence.



Figure 33 : Photo de la salle 1 après l'introduction de la visioconférence.

Salle 2 :



Figure 34 : Photo de la salle 2 avant l'introduction de la visioconférence.



Figure 35 : Photo de la salle 2 après l'introduction de la visioconférence.

4. La configuration de l'architecture cible

4.1. Description de la configuration cible

- Commutateurs d'accès :

La configuration de ces commutateurs se résume en deux étapes :

- Configuration standard d'administration (accès TACACS, SNMP, accès console, Telnet, etc.).
- Configuration L2, à savoir, la configuration du VTP, VLANS, STP, Etherchannel, etc.

- Commutateurs de distribution :

La configuration de ces commutateurs se résume comme suit :

- Configuration de l'interconnexion avec les commutateurs d'accès.
- Configuration de l'agrégation de liens avec les routeurs core et les commutateurs d'accès.
- Configuration du HSRP.
- Configuration du routage EIGRP.

- Routeurs core :

La configuration de ces routeurs se résume comme suit :

- Configuration de l'interconnexion avec les commutateurs de distribution.
- Configuration de l'agrégation de liens avec les commutateurs de distribution
- Configuration du routage EIGRP et BGP.
- Configuration MPLS
- Configuration DMVPN.

4.2. Fichiers de la configuration cible

4.2.1. Configuration d'un commutateur de distribution

```
CasaColdswc01#sh running-config //pour afficher la configuration
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption //Cryptage des MDP en MD5
service compress-config
!
hostname CasaColdswc01 // Le nom du switch
!
boot-start-marker
boot-end-marker
!
logging console emergencies
```

```
enable secret 5 password //Sécurité de l'accès au mode privilégié
!
username bmci password 7 password //sécuriser l'accès au mode console
username console secret 5 password
!
!
!
!
aaa new-model
!
    // Configuration du protocole Tacacs+ et AAA
    // pour contrôler l'accès aux réseaux
aaa group server tacacs+ WIN-TACACS
  server-private 159.XXX.XXX.XXX key 7 *****
  server-private 159.XXX.XXX.XXX key 7 *****
  ip tacacs source-interface Loopback0
!
aaa authentication login use-tacacs group WIN-TACACS local-case
aaa authentication login console group WIN-TACACS local-case
aaa authentication enable default group WIN-TACACS enable
aaa authorization console
aaa authorization exec use-tacacs group WIN-TACACS local
aaa authorization exec console group WIN-TACACS none
aaa accounting exec use-tacacs
  action-type start-stop
  group WIN-TACACS
!
aaa accounting commands 5 use-tacacs
  action-type start-stop
  group WIN-TACACS
!
aaa accounting commands 7 use-tacacs
  action-type start-stop
  group WIN-TACACS
!
aaa accounting commands 15 use-tacacs
  action-type start-stop
  group WIN-TACACS
aaa session-id common
switch 1 provision ws-c3650-12s
switch 2 provision ws-c3650-12s
ip routing
!
no ip domain-lookup // Résolution DNS
ip domain-name ma.net.intra // Nom serveur DNS
ip device tracking
!
!
vtp domain CasaColdswc01 //Configuration du protocole VTP
vtp mode transparent
!
!
spanning-tree mode rapid-pvst //Configuration du protocole STP
spanning-tree extend system-id
spanning-tree vlan 1700 priority 8192
spanning-tree vlan 1600 priority 8192
spanning-tree vlan 1800 priority 16384
spanning-tree vlan 1800 priority 16384
!
```

```
redundancy
 mode sso
!
 //Configuration des ports (adresse IP, mode, Etherchannel
 // Speed ,Duplex ,etc.)
interface Loopback0
 ip address 10.77.240.200 255.255.255.255
 ip mtu 1500
!
 //Configuration du protocole Etherchannel
interface Port-channel1
 description ###Connected_swc01###
 switchport mode trunk
!
interface Port-channel2
 description ###Connected_swc02###
 switchport mode trunk
!
interface Port-channel3
 description ###Connected_swc03###
 switchport mode trunk
!
interface Port-channel4
 description ###Connected_swc04###
 switchport mode trunk
!
interface Port-channel5
 description ###Connected_CasaColdswc02###
 switchport mode trunk
!
interface Port-channel6
 description ###Connected_RTR1###
 no switchport
 ip address 10.77.252.153 255.255.255.252
!
interface Port-channel7
 description ###Connected_RTR2###
 no switchport
 ip address 10.77.252.157 255.255.255.252
!
interface GigabitEthernet1/0/1
 description ###Connected_swc01###
 switchport mode trunk
 no ip address
 ip directed-broadcast
 channel-group 1 mode on
!
interface GigabitEthernet1/0/2
 description ###Connected_Casswc02###
 switchport mode trunk
 no ip address
 ip directed-broadcast
 channel-group 2 mode on
!
interface GigabitEthernet1/0/3
 description ###Connected_Casswc03###
 switchport mode trunk
 no ip address
 ip directed-broadcast
 channel-group 4 mode on
```

```
!  
interface GigabitEthernet1/0/4  
  description ###Connected_Casswc04###  
  switchport mode trunk  
  no ip address  
  ip directed-broadcast  
  channel-group 3 mode on  
!  
interface GigabitEthernet1/0/5  
description ###Connected_ CasaColdswc02###  
  switchport mode trunk  
  no ip address  
  ip directed-broadcast  
  channel-group 5 mode on  
!  
interface GigabitEthernet1/0/6  
!  
interface GigabitEthernet1/0/7  
!  
interface GigabitEthernet1/0/8  
!  
interface GigabitEthernet1/0/9  
!  
interface GigabitEthernet1/0/10  
!  
interface GigabitEthernet1/0/11  
description ###Connected_RTR1###  
  no switchport  
  no ip address  
  speed 100  
  duplex full  
  channel-group 6 mode on  
!  
interface GigabitEthernet1/0/12  
description ###Connected_RTR2###  
  no switchport  
  no ip address  
  speed 100  
  duplex full  
  channel-group 7 mode on  
!  
interface GigabitEthernet1/1/1  
!  
interface GigabitEthernet1/1/2  
!  
interface GigabitEthernet1/1/3  
!  
interface GigabitEthernet1/1/4  
!  
interface TenGigabitEthernet1/1/1  
!  
interface TenGigabitEthernet1/1/2  
!  
interface TenGigabitEthernet1/1/3  
!  
interface TenGigabitEthernet1/1/4  
!  
interface GigabitEthernet2/0/1  
  description ###Connected_sw01###
```

```
switchport mode trunk
no ip address
ip directed-broadcast
channel-group 1 mode on
!
interface GigabitEthernet2/0/2
description ###Connected_Casswc02###
switchport mode trunk
no ip address
ip directed-broadcast
channel-group 2 mode on
!
interface GigabitEthernet2/0/3
description ###Connected_Casswc03###
switchport mode trunk
no ip address
ip directed-broadcast
channel-group 4 mode on
!
interface GigabitEthernet2/0/4
description ###Connected_Casswc04###
switchport mode trunk
no ip address
ip directed-broadcast
channel-group 3 mode on
!
interface GigabitEthernet2/0/5
description ###Connected_CasaColdswc02###
switchport mode trunk
no ip address
ip directed-broadcast
channel-group 5 mode on
!
interface GigabitEthernet2/0/6
!
interface GigabitEthernet2/0/7
!
interface GigabitEthernet2/0/8
!
interface GigabitEthernet2/0/9
!
interface GigabitEthernet2/0/10
!
interface GigabitEthernet2/0/11
description ###Connected_RTR1###
no switchport
no ip address
speed 100
duplex full
channel-group 6 mode on
!
interface GigabitEthernet2/0/12
description ###Connected_RTR2###
no switchport
no ip address
speed 100
duplex full
channel-group 7 mode on
!
```

```
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface TenGigabitEthernet2/1/3
!
interface TenGigabitEthernet2/1/4
!
interface Vlan1
no ip address
//Configuration des interfaces virtuelles et du HSRP
interface Vlan1200
ip address 10.77.12.254 255.255.255.0
standby 1200 ip 10.77.12.252
standby 1200 priority 150
standby 1200 preempt
!
interface Vlan1600
ip address 10.77.16.254 255.255.255.0
standby 1600 ip 10.77.16.252
standby 1600 priority 150
standby 1600 preempt
!
interface Vlan1700
ip address 10.77.17.254 255.255.255.0
standby 1700 ip 10.77.17.252
standby 1700 priority 50
standby 1700 preempt
!
interface Vlan1800
ip address 10.77.18.254 255.255.255.0
standby 1800 ip 10.77.18.252
standby 1800 priority 150
standby 1800 preempt
!
//Configuration du protocole EIGRP
router eigrp 4
network 10.77.0.0 0.0.255.255
network 22.77.0.0 0.0.255.255
redistribute static
passive-interface default
no passive-interface Port-channel1
no passive-interface Port-channel2
no passive-interface Port-channel3
no passive-interface Port-channel4
no passive-interface Port-channel5
no passive-interface Port-channel6
no passive-interface Port-channel7
eigrp router-id 10.77.240.200
!
!
```



```

ip tacacs source-interface Loopback0
!
!
!
logging source-interface Loopback0
access-list 10 permit 10.77.42.8 //Configuration des ACLs
access-list 10 permit 10.77.53.194
access-list 101 permit udp 10.77.0.0 0.0.255.255 any eq discard
access-list 101 deny ip any any
// Configuration du protocole SNMP (Management/Supervision)
snmp-server community ***** RO 10
snmp-server community ***** RW 10
snmp-server community ***** RW
snmp-server community ***** RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
snmp-server *****
snmp-server ip precedence 7
snmp-server contact ## Morocco WhatsUpGold ## + 212 5 22 46 10 00
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps flowmon
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps rf
snmp-server enable traps memory
snmp-server enable traps cpu threshold
snmp-server enable traps wireless bsnMobileStation bsnAccessPoint
bsnRogue bsn80211Security bsnAutoRF bsnGeneral client mobility RRM mfp
AP rogue
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-
change
snmp-server enable traps ospf cisco-specific state-change shamlink
interface
snmp-server enable traps ospf cisco-specific state-change shamlink
neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps license
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps stackwise
snmp-server enable traps port-security
snmp-server enable traps fru-ctrl
snmp-server enable traps entity

```



```

snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err
conn-config-err binding-err conn-up conn-down binding-expn-fail oper-
nodeid-change binding-conflict
snmp-server enable traps trustsec-server radius-server provision-secret
snmp-server enable traps trustsec authz-file-error cache-file-error
keystore-file-error keystore-sync-fail random-number-fail src-entropy-
fail
snmp-server enable traps trustsec-interface unauthorized sap-fail
authc-fail supplicant-fail authz-fail
snmp-server enable traps bgp
snmp-server enable traps cef resource-failure peer-state-change peer-
fib-state-change inconsistency
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps local-auth
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-
pim-message
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-
inconsistency
snmp-server enable traps syslog
snmp-server enable traps ipsla
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-
trunk-down
snmp-server host 159.xxx.xxx.xxx *****
snmp-server host 10.xxx.xxx.xxx version 2c *****
snmp-server host 10.xxx.xxx.xxx version 2c *****
snmp ifmib ifindex persist
    // Les Serveurs Tacacs
tacacs-server host 159.XXX.XXX.XXX key 7 *****
tacacs-server host 159.XXX.XXX.XXX key 7 *****
!
line con 0          // Sécurité de l'accès par console
 session-timeout 5
 exec-timeout 30 0
 password 7 password
 authorization exec console
 accounting commands 5 use-tacacs
 accounting commands 7 use-tacacs
 accounting commands 15 use-tacacs
 accounting exec use-tacacs
 logging synchronous
 login authentication console
 stopbits 1
!
line vty 0 4        // Sécurité de l'accès par Telnet
 session-timeout 5
 exec-timeout 30 0

```

```

password 7 password
authorization exec use-tacacs
accounting commands 5 use-tacacs
accounting commands 7 use-tacacs
accounting commands 15 use-tacacs
accounting exec use-tacacs
logging synchronous
login authentication use-tacacs
transport input ssh
line vty 5 15      // Sécurité de l'accès par Telnet
 session-timeout 5
 exec-timeout 30 0
 password 7 password
 authorization exec use-tacacs
 accounting commands 5 use-tacacs
 accounting commands 7 use-tacacs
 accounting commands 15 use-tacacs
 accounting exec use-tacacs
 logging synchronous
 login authentication use-tacacs
 transport input ssh

```

4.2.2. Configuration d'un commutateur d'accès

```

Casswc02#sh running-config      //pour afficher la configuration
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption    //Cryptage des MDP en MD5
service compress-config
!
hostname Casswc02              // Le nom du switch
!
boot-start-marker
boot-end-marker
!
!
!
!
enable secret 5 password       //Sécurité de l'accès au mode privilégié
!
username bmci password 7 password //Sécurité de l'accès au mode console
username console secret 5 password
aaa new-model
!
      // Configuration du protocole Tacacs+ et AAA
      // pour contrôler l'accès aux réseaux
aaa group server tacacs+ WIN-TACACS
 server-private 159.XXX.XXX.XXX key 7 *****
 server-private 159.XXX.XXX.XXX key 7 *****
 ip tacacs source-interface Loopback0
!
aaa authentication login use-tacacs group WIN-TACACS local-case
aaa authentication login console group WIN-TACACS local-case
aaa authentication enable default group WIN-TACACS enable

```

```
aaa authorization console
aaa authorization exec use-tacacs group WIN-TACACS local
aaa authorization exec console group WIN-TACACS none
aaa accounting exec use-tacacs
  action-type start-stop
  group WIN-TACACS
!
aaa accounting commands 5 use-tacacs
  action-type start-stop
  group WIN-TACACS
!
aaa accounting commands 7 use-tacacs
  action-type start-stop
  group WIN-TACACS
!
aaa accounting commands 15 use-tacacs
  action-type start-stop
  group WIN-TACACS
!
aaa session-id common
switch 1 provision ws-c3650-48ps
switch 2 provision ws-c3650-48ps
switch 3 provision ws-c3650-48ps
ip routing
!
no ip domain-lookup // Résolution DNS
ip domain-name ma.net.intra // Le nom du serveur DNS
ip device tracking
vtp domain Casswc02 //Configuration du protocole VTP
vtp mode transparent
!
!
spanning-tree mode rapid-pvst //Configuration du protocole STP
spanning-tree extend system-id
spanning-tree vlan 1700 priority 32768
spanning-tree vlan 1600 priority 32768
spanning-tree vlan 1800 priority 32768
spanning-tree vlan 1800 priority 32768
!
!
!
//Création des vlans
vlan 1200
  name VIDEO
!
vlan 1600
  name VOIX
!
vlan 1700
  name DATA
!
vlan 1800
  name WIFI
!
//Configuration des ports (adresse IP, mode, Etherchannel
// Speed ,Duplex, affectation des port aux vlans, etc.)
interface Loopback0
  ip address 10.77.247.23 255.255.255.255
  ip mtu 1500
```

```
!  
interface Port-channel2  
  description ###Connected_ CasaColdswc01###  
  switchport mode trunk  
!  
  interface Port-channel3  
  description ###Connected_ CasaColdswc02###  
  switchport mode trunk  
!  
  interface range GigabitEthernet1/0/1-45  
  description ### PC/Phone ###  
  switchport access vlan 1700  
  switchport mode access  
  switchport nonegotiate  
  switchport voice vlan 1600  
  switchport port-security maximum 5 //sécuriser les ports.  
  switchport port-security  
  switchport port-security aging time 14  
  switchport port-security violation restrict  
  switchport port-security aging type inactivity  
  spanning-tree portfast  
!  
  interface range GigabitEthernet1/0/46-48  
  description ### WIFI ###  
  switchport access vlan 1800  
  switchport mode access  
  switchport nonegotiate  
  switchport port-security maximum 5  
  switchport port-security  
  switchport port-security aging time 14  
  switchport port-security violation restrict  
  switchport port-security aging type inactivity  
  spanning-tree portfast  
!  
interface GigabitEthernet1/1/1  
  description ###Connected_ CasaColdswc01###  
  switchport mode trunk  
  no ip address  
  channel-group 2 mode on  
!  
interface GigabitEthernet1/1/2  
description ###Connected_ CasaColdswc02###  
  switchport mode trunk  
  no ip address  
  channel-group 3 mode on  
!  
interface GigabitEthernet1/1/3  
!  
interface GigabitEthernet1/1/4  
!  
interface range GigabitEthernet2/0/1-45  
  description ### PC/Phone ###  
  switchport access vlan 1700  
  switchport mode access  
  switchport nonegotiate  
  switchport voice vlan 1600  
  switchport port-security maximum 5  
  switchport port-security  
  switchport port-security aging time 14
```

```
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
!
interface range GigabitEthernet2/0/46-48
description ### WIFI###
switchport access vlan 1800
switchport mode access
switchport nonegotiate
switchport port-security maximum 5
switchport port-security
switchport port-security aging time 14
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
!
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface range GigabitEthernet3/0/1-45
description ### PC/Phone ###
switchport access vlan 1700
switchport mode access
switchport nonegotiate
switchport voice vlan 1600
switchport port-security maximum 5
switchport port-security
switchport port-security aging time 14
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
!
interface range GigabitEthernet3/0/46-48
description ### PC/Phone ###
switchport access vlan 1800
switchport mode access
switchport nonegotiate
switchport port-security maximum 5
switchport port-security
switchport port-security aging time 14
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
!
!
!
interface GigabitEthernet3/1/1
description ###Connected_CasaColdswc01###
switchport mode trunk
no ip address
channel-group 2 mode on
!
interface GigabitEthernet3/1/2
```

```

description ###Connected_CasaColdswc02###
switchport mode trunk
no ip address
channel-group 3 mode on
!
interface GigabitEthernet3/1/3
!
interface GigabitEthernet3/1/4
!
interface Vlan1
no ip address
shutdown
!
        //Configuration d'une interface virtuelle (accès au switch
        // à distance)
interface Vlan1200
ip address 10.77.177.110 255.255.255.240
!
        // Configuration du protocole SNMP (Management/Supervision)
snmp-server enable traps rf
snmp-server enable traps memory
snmp-server enable traps cpu threshold
snmp-server enable traps wireless bsnMobileStation bsnAccessPoint
bsnRogue bsn80211Security bsnAutoRF bsnGeneral client mobility RRM mfp
AP rogue
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-
change
snmp-server enable traps ospf cisco-specific state-change shamlink
interface
snmp-server enable traps ospf cisco-specific state-change shamlink
neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps license
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps stackwise
snmp-server enable traps port-security
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err
conn-config-err binding-err conn-up conn-down binding-expn-fail oper-
nodeid-change binding-conflict
snmp-server enable traps trustsec-server radius-server provision-secret
snmp-server enable traps trustsec authz-file-error cache-file-error
keystore-file-error keystore-sync-fail random-number-fail src-entropy-
fail

```

```

snmp-server enable traps trustsec-interface unauthorized sap-fail
authc-fail supplicant-fail authz-fail
snmp-server enable traps bgp
snmp-server enable traps cef resource-failure peer-state-change peer-
fib-state-change inconsistency
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps local-auth
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-
pim-message

snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-
inconsistency
snmp-server enable traps syslog
snmp-server enable traps ipsla
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-
trunk-down
snmp-server host 159.xxx.xxx.xxx *****
snmp-server host 10.xxx.xxx.xxx version 2c *****
snmp-server host 10.xxx.xxx.xxx version 2c *****
snmp ifmib ifindex persist
    //Les serveurs Tacacs+
tacacs-server host 159.XXX.XXX.XXX key 7 *****
tacacs-server host 159.XXX.XXX.XXX key 7 *****
!
!
line con 0      // Sécurité de l'accès par console
session-timeout 5
exec-timeout 30 0
password 7 password
authorization exec console
accounting commands 5 use-tacacs
accounting commands 7 use-tacacs
accounting commands 15 use-tacacs
accounting exec use-tacacs
logging synchronous
login authentication console
stopbits 1

line vty 0 4      // Sécurité de l'accès par telnet
session-timeout 5
exec-timeout 30 0
password 7 password
authorization exec use-tacacs
accounting commands 5 use-tacacs
accounting commands 7 use-tacacs
accounting commands 15 use-tacacs

```



```
accounting exec use-tacacs
logging synchronous
login authentication use-tacacs
transport input ssh
line vty 5 15          // Sécurité de l'accès par telnet
session-timeout 5
exec-timeout 30 0
password 7 password
authorization exec use-tacacs
accounting commands 5 use-tacacs
accounting commands 7 use-tacacs
accounting commands 15 use-tacacs
accounting exec use-tacacs
logging synchronous
login authentication use-tacacs
transport input ssh
```

Conclusion

Dans ce chapitre, nous avons choisi le premier site bénéficiaire du projet de la refonte LAN où l'architecture cible validée sera mise en place. Nous avons passé la commande aux fournisseurs et nous avons reçu le matériel acheté pour cette fin. Puis, nous avons lancé les travaux de re-câblage du site et nous avons installé les équipements de l'architecture cible. Ensuite, nous avons réalisé la configuration des équipements réseau de l'architecture cible, c'est-à-dire la configuration des commutateurs accès, des commutateurs de distribution, et des routeurs core. Nous avons introduit dans l'architecture cible et de façon incrémentale le service ToIP et nous avons configuré ses équipements, puis le service Wi-Fi dont nous avons configuré les équipements aussi, et enfin le service de la visio-conférence de même avec la configuration de ses équipements. A la fin de ce chapitre, nous avons présenté les étapes de cette configuration et nous avons dévoilé les fichiers de cette dernière.

Conclusion générale

La réalisation du projet de la refonte LAN a été le moyen de traiter la problématique à laquelle nous avons été confrontés. En effet, nous avons constaté l'existence d'une architecture classique, mal structurée et difficile à superviser. De plus, elle était sans redondance, intolérante aux pannes et ses équipements étaient obsolètes. Tous ces éléments constituaient une réelle menace pour l'efficacité et la productivité de l'entreprise.

En se basant sur la constatation de la séparation entre le réseau informatique et le réseau téléphonique, nous avons eu l'idée de les regrouper et par conséquent, nous avons proposé à la direction DSI de mettre en place une nouvelle architecture qui va remédier à toutes les limites de l'architecture existante et qui se déploie sur trois niveaux. De plus, c'est une architecture conçue afin de pouvoir supporter l'introduction de plusieurs services tels que la téléphonie sur IP, le wifi et la visioconférence qui ne feront que l'améliorer.

La mise en place de cette architecture a nécessité un travail de re-câblage, l'achat de nouveaux équipements, et une configuration adéquate. Cette architecture est en effet bien structurée et avec redondance. Une fois installée, elle est entrée dans la phase des tests afin de s'assurer de la bonne marche de cette dernière comme prévu et de vérifier ses différents avantages précités.

En ce qui concerne les voies d'améliorations futures, on propose l'intégration de la nouvelle architecture dans les autres sites centraux de la BMCI, ainsi que dans les différentes agences et succursales. La migration vers cette solution sera incrémentale dans le temps.

Références

- [1] <http://www.bmci.ma/nous-connaitre/le-groupe-bmci/gouvernance/> Site officiel de la BMCI, onglet gouvernance, consulté en Mars 2018
- [2] <http://www.bmci.ma/nous-connaitre/activite-et-filiales/> Site officiel de la BMCI, onglet activités et filiales, consulté en Mars 2018
- [3] <http://www.bmci.ma/trouver-une-agence/> Site officiel de la BMCI, onglet trouver une agence, consulté en Mars 2018
- [4] <http://www.bmci.ma/wp-content/blogs.dir/sites/2/2017/10/organigramme-2017-version-16-10-2017.pdf> Site officiel de la BMCI, organigramme 2017, consulté en Mars 2018
- [5] <http://www.bmci.ma/> Site officiel présentant des informations sur la BMCI, consulté en Mars 2018
- [6] <http://tvaira.free.fr/reseaux/vlan.pdf> Site présentant des informations sur le réseau local virtuel VLAN, consulté en Avril 2018
- [7] <https://cisco.goffinet.org/protocole-spanning-tree/> Site présentant des informations sur le protocole spanning tree, consulté en Avril 2018
- [8] <http://superwebcrawler.fr/dokuwiki/doku.php?id=reseau:etherchannel> Site présentant des informations sur EtherChannel, consulté en Avril 2018
- [9] <http://www-igm.univ-mlv.fr/~dr/XPOSE2007/vlanparlegrandquinapascomprislesconsignes/interconnection.html> Site présentant des informations sur le routage inter-vlan, consulté en Avril 2018
- [10] <https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/> Site présentant des informations sur HSRP, consulté en Avril 2018
- [11] <https://www.networklab.fr/introduction-a-leigrp/> Site présentant des informations sur EIGRP, consulté en Avril 2018
- [12] <https://www.networklab.fr/introduction-a-bgp/> Site présentant des informations sur BGP, consulté en Avril 2018
- [13] <http://www.frameip.com/mps/#13-8211-applications> Site présentant des informations sur MPLS, consulté en Avril 2018
- [14] <http://www.networklife.net/2014/10/introduction-au-dmvpn/> Site présentant des informations sur le DMVPN, consulté en Avril 2018

- [15] <http://ccie.julienberton.fr/2012/10/17/dmvpn-les-tunnels-a-la-demande/> Site présentant des informations sur le DMVPN, consulté en Avril 2018
- [16] <http://www.resadia-telecom-securite.com/nos-prestations-telecom-et-securite/infrastructures-et-reseaux-telecoms/la-telephonie-sur-ip-toip-c391.html> Site présentant des informations sur la Téléphonie sur IP, consulté en Avril 2018
- [17] <http://igm.univ-mlv.fr/~dr/XPOSE2009/Introduction%20au%20Cisco%20Call%20Manager%204.2/cluster.html> Site présentant des informations sur le Call manager, consulté en Avril 2018
- [18] <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/Internet/fiches/8375807.html> Site présentant des informations sur la passerelle VoIP, consulté en Avril 2018
- [19] <http://slideplayer.fr/slide/519427/> Présentation en ligne, présentant des informations sur les communications sur IP, consulté en Avril 2018
- [20] <http://www.ariase.com/fr/guides/wifi.html> Site présentant des informations sur le Wi-Fi, consulté en Avril 2018
- [21] <https://www.commentcamarche.com/faq/3020-wifi-cours-d-introduction> Site présentant des informations d'introduction sur le Wi-Fi, consulté en Avril 2018
- [22] <https://www.commentcamarche.com/contents/1282-les-modes-de-fonctionnement-du-wifi-802-11-ou-wi-fi> Site présentant des informations sur les modes de fonctionnement du Wi-Fi, consulté en Avril 2018
- [23] https://www.cisco.com/c/dam/global/fr_ch/assets/docs/CONTROLEUR_WLAN.pdf Site présentant des informations sur les contrôleurs WLAN, consulté en Avril 2018
- [24] <http://www.elit-technologies.fr/quest-ce-que-la-visioconference-de-nos-jours/> Site présentant des informations sur la redéfinition de la visioconférence, consulté en Avril 2018
- [25] https://www.google.com/search?q=la+visioconf%C3%A9rence&rlz=1C1GGRV_enMA752MA752&source=lnms&tbn=isch&sa=X&ved=0ahUKEwjssGOgvLaAhXCvBOKHXO9CBOQ_AUICigB&biw=1280&bih=617#imgdii=jUySFUue8g2nyM:&imgcr=136tpLdxcKH8CM: Site de Google, image d'une visioconférence, consulté en Avril 2018
- [26] <https://www.rdview.live/blog/materiel-necessaire-a-la-visioconference> Site présentant des informations sur le matériel de la visioconférence, consulté en Avril 2018
- [27] <https://www.google.com/maps/place/BMCI+Leasing%2FCentre+D'affaires+La+Colline/@33.5369592,-7.6433945,14z/data=!4m8!1m2!2m1!1sbmci+la+colline!3m4!1s0x0:0x168bee453282f5a7!8m2!3d33.5363153!4d-7.6400471> Site de Google maps, image de la BMCI Leasing centre d'affaire la colline, consulté en Mai 2018

[28] <https://www.google.com/maps/place/BMCI+Leasing%2FCentre+D'affaires+La+Colline/@33.5359063,-7.6398925,3a,90y,350.1h,115.09t/data=!3m8!1e1!3m6!1sAF1QipNRM5RLcvueXQWR5urCOL1abUveRxjprJDHOMEX!2e10!3e11!6shttps:%2F%2Flh5.googleusercontent.com%2Fp%2FAF1QipNRM5RLcvueXQWR5urCOL1abUveRxjprJDHOMEX%3Dw203-h100-k-no-pi-0-ya177.47653-ro-0-fo100!7i10240!8i5120!4m8!1m2!2m1!1sbmci+la+colline!3m4!1s0x0:0x168bee453282f5a7!8m2!3d33.5363153!4d-7.6400471> Site de Google earth, image de l'immeuble colline de la BMCI , consulté en Mai 2018

LA REFONTE LAN DES SITES CENTRAUX DE LA BMCI

Résumé

Ce mémoire intitulé la refonte LAN des sites centraux de la BMCI récapitule mon projet de fin d'études. Nous avons d'abord présenté le groupe BMCI et plus spécifiquement la Direction des Systèmes d'Information DSI où s'est déroulé le stage. L'étude de l'existant a révélé une architecture réseau classique, mal structurée, sans redondances, difficile à superviser et avec des équipements obsolètes. De ce fait, nous avons proposé une nouvelle architecture qui résout toutes ces limites et qui facilite l'intégration incrémentale d'autres services tel que la téléphonie sur IP, le Wi-Fi et la visioconférence. De plus, cette architecture est uni-fonctionnelle, autrement dit, elle permet le fonctionnement simultané de tous ces services en tant qu'une seule entité. Après sa confirmation, nous avons choisi le premier site bénéficiaire de ce projet. Cette nouvelle architecture a été mise en place dans ce site après l'achat du matériel, son installation et sa configuration.

Mots clés : Refonte, LAN, ToIP, Wi-Fi, Visioconférence.

THE LAN REDESIGN OF THE CENTRAL SITES OF BMCI

Abstract

This study entitled the LAN redesign of the central sites of BMCI synthesizes my graduation project. We first introduced the BMCI group and more specifically the Directory of information systems DSI where the internship has taken place. An analysis of the existing situation has revealed a classic network architecture, poorly structured, free of redundancies, difficult to supervise and with obsolete equipment. Consequently, we have suggested a new architecture that addresses all these shortcomings and that facilitates the incremental integration of other services such as the IP Telephony, the Wi-Fi and the videoconferencing. Moreover, this network architecture is single-function, meaning that it allows the simultaneous functioning of all the above services as a single entity. After getting its confirmation, we have chosen the first site to benefit from this project. This new network architecture was set up in this site after receiving the equipment, installing it and configuring it.

Keywords : Redesign, LAN, ToIP, Wi-Fi, videoconferencing.