

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane MIRA- BEJAIA
Faculté des Sciences Exactes
Département d'Informatique



Mémoire de fin de cycle

En vue de l'obtention du diplôme Master professionnel

Spécialité :

Administration et sécurité des réseaux

Conception d'une architecture réseau hiérarchique à trois niveaux et mise en place des VLANs

Réalisé par :

Mr MEDJOU DJ Menad

Mr HADDAD Fouad

Soutenu le 29/09/2022, Devant le jury composé de :

M. TOUAZI Djoudi

Président

Mme. TASSOULT Nadia

Encadreur

Mr. IDRI Bachir

Responsable Entreprise

Année universitaire 2021/2022



DEDICATION

Nous dédions ce modeste travail

À nos très chers parents qui ont légué un sens à notre existence, pour leur confiance
et leur énorme soutien.

À nos merveilleux frères et soeurs pour leur présence et leur appui .

À nos familles .

À nos précieux amis qui ont toujours cru en nous.

À vous tous,

Nous dédions ce travail.



REMERCIEMENTS

En préambule à ce mémoire nous remercions **ALLAH** qui nous a aidé et nous a donné la patience et le courage durant ces longues années d'études.

Nous tenons d'abord à remercier très chaleureusement Mme **TASSOULT Nadia**, les conseils qu'elle nous a prodigués, la patience, la confiance qu'elle nous a témoigné ont été déterminant dans la réalisation de notre travail.

Nous remercions les plus vifs vont tout particulièrement à notre encadreur de stage Mr **IDRI Bachir** pour son encadrement et orientation avec toute rigueur tout le long de notre stage inspirant notre curiosité et passion pour promouvoir la réalisation de ce travail.

Nous remercions les membres du jury, Mr. **TOUAZI Djoudi** et Mme **HOUHA Amel**, pour l'honneur qu'ils nous ont fait d'avoir accepté d'examiner ce travail..

Un profond respect et un remerciement particulier pour le chef de département et tous les enseignants de l'Université Abderrahmane Mira de Bejaia pour la bonne contribution de ce travail.

Enfin, nous remercions tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Merci à vous tous.



TABLE DES MATIÈRES

LISTE DES FIGURES	vii
LISTE DES ABRÉVIATIONS	viii
INTRODUCTION GÉNÉRALE	x
1 Présentation de l'organisme d'accueil	2
1.1 INTRODUCTION	3
1.2 PRESENTATION GENERALE DE L'ORGANISME D'ACCUEIL	3
1.2.1 Présentation du groupe SONELGAZ	3
1.2.2 Historique	3
1.2.3 Missions du groupe SONELGAZ	6
1.2.4 Filiales de SONELGAZ	7
1.3 SONELGAZ SADEG CD BEJAIA	8
1.3.1 Présentation de la Concession de Distribution Bejaïa	8
1.3.2 Organigramme général de la Direction de Distribution de l'électricité et du gaz de Bejaïa	9
1.3.3 Présentation de l'infrastructure réseau de la concession de distribution Bejaïa	9
1.4 PROBLEMATIQUE	10
1.5 SOLUTION PROPOSEE	11
1.6 CONCLUSION	11
2 Généralités sur les réseaux informatiques	12
2.1 INTRODUCTION	13
2.2 DEFINITION D'UN RESEAU INFORMATIQUE	13
2.3 OBJECTIFS DES RESEAUX INFORMATIQUE	13
2.4 ARCHITECTURE DES RESEAUX	14
2.5 CLASSIFICATION DES RESEAUX INFORMATIQUES	14
2.6 LES PROTOCOLES RESEAUX	17

2.7	ARCHITECTURES PROTOCOLAIRES	18
2.7.1	Modèle OSI (Open System Interconnexion)	19
2.7.2	Modèle TCP/IP (Transmission Control Protocol/Internet Protocol)	20
2.7.2.1	Architecture en couche du modèle TCP/IP	21
2.8	LES PRINCIPAUX COMPOSANTS D'INTERCONNEXION	22
2.9	CONCLUSION	24
3	Les Réseaux Locaux Virtuels (VLANs)	25
3.1	INTRODUCTION	26
3.2	PROBLEMES LIES A L'ARCHITECTURE RESEAU	26
3.3	RESEAU LOCAL VIRTUEL (VLAN)	27
3.3.1	Définition	27
3.3.2	Avantage	28
3.3.3	Fonctionnement du VLAN	29
3.3.4	Agrégation des VLANs ou "Trunking"	30
3.3.4.1	Trunk ou Liaison d'agrégation :	30
3.3.4.2	Protocole "Trunk" :	30
3.3.4.3	Etiquette 802.1q	31
3.3.5	Implémentation de la technologie	32
3.3.6	Types de VLAN	33
3.3.7	Le protocole DTP (<i>Dynamic Trunking Protocol</i>)	35
3.3.8	Le protocole VTP (<i>VLAN Trunking Protocol</i>)	36
3.4	LE PROTOCOLE STP (<i>Spanning Tree Protocol Protocol</i>)	38
3.5	ARCHITECTURES HIERARCHIQUES	39
3.6	CONCLUSION	40
4	Conception et Simulation	41
4.1	INTRODUCTION	42
4.2	PRESENTATION DE L' ANCIENNE INFRASTRUCTURE RESEAU DE CONCESSION DE DISTRIBUTION BEJAIA	42
4.3	SOLUTION ADAPTEE	43
4.4	OUTIL DE SIMULATION	44
4.4.1	Cisco packet tracer	44
4.5	CREATION ET CONFIGURATION DES NOUVEAUX RESEAUX	46
4.5.1	Création	46
4.5.2	Configuration	46
4.5.2.1	Plan d'adressage	47

4.5.2.2	Configuration de basse du Router et du Switch	47
4.5.2.3	La configuration de protocole VTP sur les Switch	48
4.5.2.4	Création des VLANs	49
4.5.2.5	Configuration des ports (agrégation)	50
4.5.2.6	Configuration des sous interfaces	52
4.5.2.7	Configuration du DHCP	52
4.5.2.8	Configuration de protocole STP	53
4.5.2.9	Configuration de la voix IP	54
4.5.2.10	Configuration des caméras de surveillance	54
4.6	TEST ET VALIDATION DE LA CONFIGURATION	58
4.6.1	Contrôle de la bonne configuration du protocole VTP	58
4.6.1.1	Contrôle du VTP serveur	58
4.6.1.2	Contrôle du VTP client	58
4.6.2	Contrôle des réseaux locaux virtuels créés sur le switch serveur	59
4.6.3	Vérification du routage inter VLAN	60
4.6.4	Vérification de la distribution des adresses IP sur le serveur DHCP	60
4.6.5	Vérification des adresses IP des machines attribuées par le DHCP	61
4.6.6	Vérification de la communication entre les machines	61
4.6.6.1	Test des différents VLANs sur un même commutateur entre différents équipements	61
4.6.6.2	Test des différents VLANs sur différentes commutateur entre différents équipements	62
4.6.7	Test de la téléphonie IP	63
4.6.8	Test des cameras de surveillance	63
4.7	CONCLUSION	64
	CONCLUSION GÉNÉRALE	65
	BIBLIOGRAPHIE	66
	Résumé	69
	Abstract	70



LISTE DES FIGURES

1.1	Filiales de SONELGAZ	7
1.2	L'organigramme de la direction de la distribution de Bejaia	9
2.1	Les différents types de réseaux informatiques [2]	15
2.2	Les différents topologies de réseaux informatiques [3]	17
2.3	Modèle OSI [5]	20
2.4	Modèle TCP/IP	22
3.1	Virtual LAN	27
3.2	Trafic de broadcast [8]	29
3.3	Etiquette 802.1q	31
3.4	Etiquette 802.1q [10]	31
3.5	Le fonctionnement de DTP	36
3.6	Les modes de VTP	37
3.7	Le protocole VTP [13]	37
3.8	Le protocole STP [15]	38
3.9	Architecture hiérarchique 3-tiers [17]	39
4.1	l'ancienne infrastructure réseau de la CD de bejaia	43
4.2	Nouvelle architecture créée	44
4.3	Le CLI	45
4.4	Nouvelle infrastructure	46
4.5	Configuration de basse router	47
4.6	Configuration de basse Switch	48
4.7	Configuration du VTP en mode server sur Switch coeur	48
4.8	Configuration du VTP en mode client sur Switch Etage1	49
4.9	Création des VLANs au niveau du Switch cœur	50
4.10	Configuration des liens Trunk	51
4.11	Attribution des ports de commutateurs au VLANs	51
4.12	Configuration des sous interface	52

4.13	Configuration du DHCP	53
4.14	Configuration du STP	53
4.15	Configuration de la voie IP	54
4.16	Configuration de l'adresse IP	54
4.17	Étape 1 de création d'un compte de IOT	55
4.18	Étape 2 de création d'un compte de IOT	55
4.19	Étape 3 de création d'un compte de IOT	55
4.20	Étape 4 de création d'un compte de IOT	56
4.21	Étape 5 de création d'un compte de IOT	56
4.22	Étape (a) de la configuration des cameras	57
4.23	Étape (b) de la configuration des cameras	57
4.24	Contrôle du VTP serveur	58
4.25	Contrôle du VTP client	59
4.26	Contrôle des VLANs créé	59
4.27	Vérification du routage inter VLAN	60
4.28	Vérification de la distribution des adresses IP	60
4.29	Vérification de la distribution des adresses IP des PC	61
4.30	Ping entre deux machines	61
4.31	Ping entre deux machines	62
4.32	Test de la téléphonie IP	63
4.33	Test des cameras de surveillance	64



LISTE DES ABRÉVIATIONS

ARP Adress Resolution Protocol

BPDU Bridge Protocol Data Unit

BID Bridge identifier

CD Sonelgaz-Distribution

DTP Dynamic Trunking Protocol

DNS Domain Name Serveur

DHCP Dynamic Host Configuration Protocol

DP Designated Port

EGA Electricité et Gaz d'Algérie

EPIC Etablissement Public à caractère Industriel et Commercial

FTP File Transfer Protocol

IP Internet Protocol

IEEE Institute of Electrical and Electrons Engineers

LISTE DES ABRÉVIATIONS

LAN Local Area Network

MAN Métropolitain Area Network

MAC Média Access Control

OSI Open Système Interconnexion

OS Operating System

PAN Personal Area Network

RP ROOT Port

RB ROOT Bridge

SADEG Société Algérienne de Distribution de l'Electricité et de Gaz

SONELGAZ Société Nationale d'Electricité et de Gaz

STP Spanning Tree Protocol

SW Switch

TCP Transmission Control Protocol

TFTP Trivial File Transfer Protocol

UDP USER Datagram Protocol

VLAN Virtual Local area network

VTP VLAN Trunking Protocol



INTRODUCTION GÉNÉRALE

En ces temps modernes, nombreuses sont les entreprises qui se sont dotées d'un réseau informatique. Ce dernier se présente comme un ensemble de ressources mises en place pour offrir un nombre important de service. Ces dernières années, l'évolution des services et du trafic a suscité un développement technologique permettant d'augmenter la capacité et les fonctionnalités des ressources.

Au sein d'une organisation, un réseau informatique est peut être vu comme le cœur de la majeure partie de son activité. Il met en relation des équipements terminaux (ordinateurs, imprimantes, stations de travail, terminaux passifs), et des serveurs. Tous ces éléments sont entièrement sous la responsabilité de l'entreprise. En effet, l'utilisation d'un réseau local est primordiale au bon fonctionnement d'une entreprise car il facilite la transmission, la duplication, le partage des dossiers et des périphériques. Il permet aussi le traitement et la consultation des bases de données et une transmission rapide et fiable des données.

Parallèlement, le développement de l'entreprise entraîne de nombreuses contraintes pouvant réduire les performances de son réseau local : accroissement du nombre des utilisateurs, volume important du trafic sur le réseau, peu de sécurité et d'agilité dans l'administration du réseau.

Cependant, l'évolution des réseaux locaux a vu l'introduction d'un concept appelé VLAN, réseau local virtuel, afin de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, etc..) en définissant une segmentation logique basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc..).

A travers notre projet de fin de cycle, nous allons proposer une nouvelle architecture pour le réseau local du site principal de la CD de Bejaia tout en le segmentant grâce essentiellement à

l'implémentation des VLANs dans le but d'assurer le fonctionnement optimal de ses ressources réseaux et d'assurer à ses membres un accès rapide à l'information et un partage facile des données au quotidien, également une souplesse dans l'administration et la gestion du réseau.

Dans le présent mémoire, nous présenterons en détail les étapes que nous allons suivre afin de réaliser notre projet, structuré en quatre chapitres organisés comme suit :

- Le premier chapitre s'intitulant « **Présentation de l'organisme d'accueil** », consiste en la présentation de l'entreprise « SONELGAZ », nous présentons dans ce chapitre l'organigramme des directions, le matériel informatique existant ainsi que le réseau existant dans le but de détecter les problèmes qu'il rencontre, puis proposer une solution à adopter.
- Le second chapitre nommé « **Généralités sur les réseaux informatiques** », définit quelques notions théoriques de base, qui seront utiles pour la compréhension de la problématique posée, à savoir la définition d'un réseau, les topologies, les types, etc.
- Le troisième chapitre « **Les Réseaux locaux virtuels (VLANs)** », présente un état de l'art sur les réseaux informatiques virtuels. Dans ce chapitre nous mettons l'accent sur le concept des VLANs, la description de leurs types, leurs utilités et quelques protocoles permettant leurs gestion.
- Le dernier chapitre « **Conception et Simulation** », illustre la solution mise en place et la configuration des différents protocoles et les tests de validation de la solution proposée.

Nous terminons notre mémoire par une conclusion générale résumant les points forts accomplis dans ce travail effectué ainsi que l'expérience acquise durant ce projet.

Présentation de l'organisme d'accueil

Sommaire

1.1	INTRODUCTION	3
1.2	PRESENTATION GENERALE DE L'ORGANISME D'ACCUEIL	3
1.2.1	Présentation du groupe SONELGAZ	3
1.2.2	Historique	3
1.2.3	Missions du groupe SONELGAZ	6
1.2.4	Filiales de SONELGAZ	7
1.3	SONELGAZ SADEG CD BEJAIA	8
1.3.1	Présentation de la Concession de Distribution Bejaïa	8
1.3.2	Organigramme général de la Direction de Distribution de l'électricité et du gaz de Bejaïa	9
1.3.3	Présentation de l'infrastructure réseau de la concession de distribution Bejaïa	9
1.4	PROBLEMATIQUE	10
1.5	SOLUTION PROPOSEE	11
1.6	CONCLUSION	11

1.1 INTRODUCTION

Tout au long de ce chapitre, nous présenterons des données recueillies auprès de la Compagnie d'engineering d'électricité et du gaz.

Dans la première section, nous allons présenter la compagnie d'engineering d'électricité et du gaz en générale (*son histoire , ses activités ainsi que ses filière*).

Dans la deuxième section nous allons focaliser sur l'une des filières de sonelgaz et qui est la CD (*Sonelgaz-Distribution*) Bien précis **la CD de Bejaia**.

1.2 PRESENTATION GENERALE DE L'ORGANISME D'ACCUEIL

Dans ce qui suit nous allons présenter l'organisme d'accueil.

1.2.1 Présentation du groupe SONELGAZ

SONELGAZ [1] (*Société nationale de l'électricité et du gaz*), est un groupe industriel énergétique algérien, spécialisé dans la production, le transport, la distribution d'électricité, ainsi que de l'achat, le transport, la distribution de gaz naturel. Son siège social est situé à Alger.

1.2.2 Historique

L'entreprise Electricité et Gaz d'Algérie "EGA" a été créée en 1947 par décret n°62.1002 de juin 1947. Ce dernier a été modifié et reconduit en 1962 par la loi n° 62.157 du 31.12.1962. Par ordonnance N° 6959 du 26 juillet 1969 parue dans le journal officiel du 1er Août 1969, Société Nationale de l'Electricité et du Gaz (SONELGAZ) est créée en substitution à EGA (1947-1969) dissoute par ce même décret. L'ordonnance lui assigne pour mission générale de s'intégrer de façon harmonieuse dans la politique énergétique intérieure du pays.

Le monopole de la production, du transport, de la distribution, de l'importation et de l'exportation de l'énergie électrique attribué à SONELGAZ a été renforcé. De même, SONELGAZ s'est vue attribuer le monopole de la commercialisation du gaz naturel par canalisations à l'intérieur du pays, et ce pour tous les types de clients (industries, centrales de production de l'énergie électrique, clients domestiques). Pour ce faire, elle réalise et gère des canalisations de transport et un réseau de distribution.

A partir de 1971, SONELGAZ est devenue une société nationale régie par l'ordonnance n° 71.74 du 16 novembre 1971 portant gestion socialiste des Entreprises. Lors de la restructuration organique opérée par l'Etat en 1983, les unités de SONELGAZ ont été transformées en entreprises publiques autonomes.

Une opération qui a donné naissance à six entreprises, à savoir :

- **KAHRIF** : Entreprise de Travaux d'électrifications.
- **KAHRAKIB** : Entreprise de Montage des infrastructures et installations électriques.
- **KANAGAZ** : Entreprise de Réalisation des canalisations de transport et de distribution.
- **INERGA** : Entreprise de Travaux de génie civil.
- **ETTERKIB** : Entreprise de Montage industriel.
- **AMC** : Entreprise de Fabrication des compteurs et des appareils de mesure et de contrôle.

En 1991, la Société Nationale d'Electricité et du Gaz s'est vue changer de nature juridique par le décret exécutif n° 91.475 du 14 Décembre 1991 et devenue un Etablissement Public à Caractère Industriel et Commercial « EPIC ».

Le décret exécutif n° 95-280 du 17 septembre 1995 confirme la nature juridique de SONELGAZ en tant qu'Etablissement Public à caractère Industriel et Commercial. Ainsi, la SONELGAZ est :

- Placée sous la tutelle du Ministre chargé de l'énergie ;
- Dotée de la personnalité morale et jouit de l'autonomie financière ;
- Régie par les règles de droit public dans ses relations avec l'état ;

— Réputée commerçant dans ses rapports avec les tiers.

Dans le cadre de sa stratégie de recentrage sur son métier de base et de promotion industrielle, en 1995 SONELGAZ a réorganisé un certain nombre d'activités périphériques sous forme de filiales, et constitué des joints - ventrues avec des partenaires algériens et étrangers.

Il s'agit notamment de :

- **TRANSMEX** : Société de Transport et de Manutention Exceptionnels des Equipements Industriels
- **SPAS** : Société de Surveillance et de Sécurité
- **MEI** : Maintenance des Equipements Industriel
- **SAT-INFOS** : Imprimerie
- **MPVA** : Maintenance et Prestation Véhicules Alger.
- **MPVO** : Maintenance et prestation véhicules ouest.
- **MPVE** : Maintenance et Prestation Véhicules Est.
- **MPVS** : Maintenance et Prestation Véhicules Sud.
- **SAFIR** : Société Algéro-Française d'ingénierie et de réalisation.
- **SIMAS** : Société de mécanique Lourde et Chaudronner sous Pression
- **INMA** : Société d'ingénierie de Maintenance
- **ABBESCO** : ABB Electric Services Company
- **ALGESCO** : Société Mixte Algéro-Américaine de réparation de turbine à Gaz
- **TRANSFOS Centre** : Réparation des transformateurs MT/BT
- **TRANSFOS Est** : Réparation des transformateurs MT/BT
- **TRANSFOS Ouest** : Réparation des transformateurs MT/BT

Le décret présidentiel n° 02/195 du 01.06.2002, s'inspirant de la loi n° 02/01 du 05.02.2002 relative à l'électricité et la distribution du gaz par canalisation, a attribué à SONELGAZ un nouveau statut de Société Par Actions sous forme de Groupe industriel et commercial constitué de plusieurs entreprises spécialisées et une nouvelle dénomination en devenant Société Algérienne de l'Electricité et du Gaz.

1.2.3 Missions du groupe SONELGAZ

Les différentes missions de SONELGAZ se résument en :

- La production, le transport, la distribution et la commercialisation de l'électricité, tant en Algérie qu'à l'étranger
- Le transport du gaz pour les besoins du marché national.
- La distribution et la commercialisation du gaz par canalisations tant en Algérie qu'à l'étranger.
- Le développement et la fourniture de toutes prestations en matière de service énergétiques
- L'étude, la promotion et la valorisation de toutes formes et sources d'énergie.
- Le développement par tout moyen de toute activité ayant un lien direct ou indirect avec les industries électriques et gazières et de toute activité pouvant engendrer un intérêt pour SONELGAZ et généralement toute opération de quelque nature qu'elle soit pouvant se rattacher directement ou indirectement à son objet social, notamment la recherche, l'exploration, la production et la distribution d'hydrocarbures.
- Le développement de toute forme d'activités conjointes en Algérie et hors d'Algérie avec des sociétés algériennes ou étrangères.

1.2.4 Filiales de SONELGAZ

Le groupe SONELGAZ est divisé en 4 catégories de filiales comme le montre le tableau 1.1 et la figure 1.1 ci dessous [1] :

Métier	Travaux	SéVICES	Participation
CEEG	INERKIB	FOSC	SEDIVER
Sonelgaz-Production de l'électricité	KAHRAGHAZ	Sonelgaz-Services	GEAT
Sonelgaz-Tranport de l'électricité	SAIEG	SWAT	BHI
OS			VIJAI
Sonelgaz-Transport Gaz			BAOSEM
Sonelgaz- Distribution			COMINTAL
Sonelgaz-Énergies Renouvelables			ALGESCO
SKE			NEAL
			HYNECO

TABLE 1.1 – Catégories des filiales

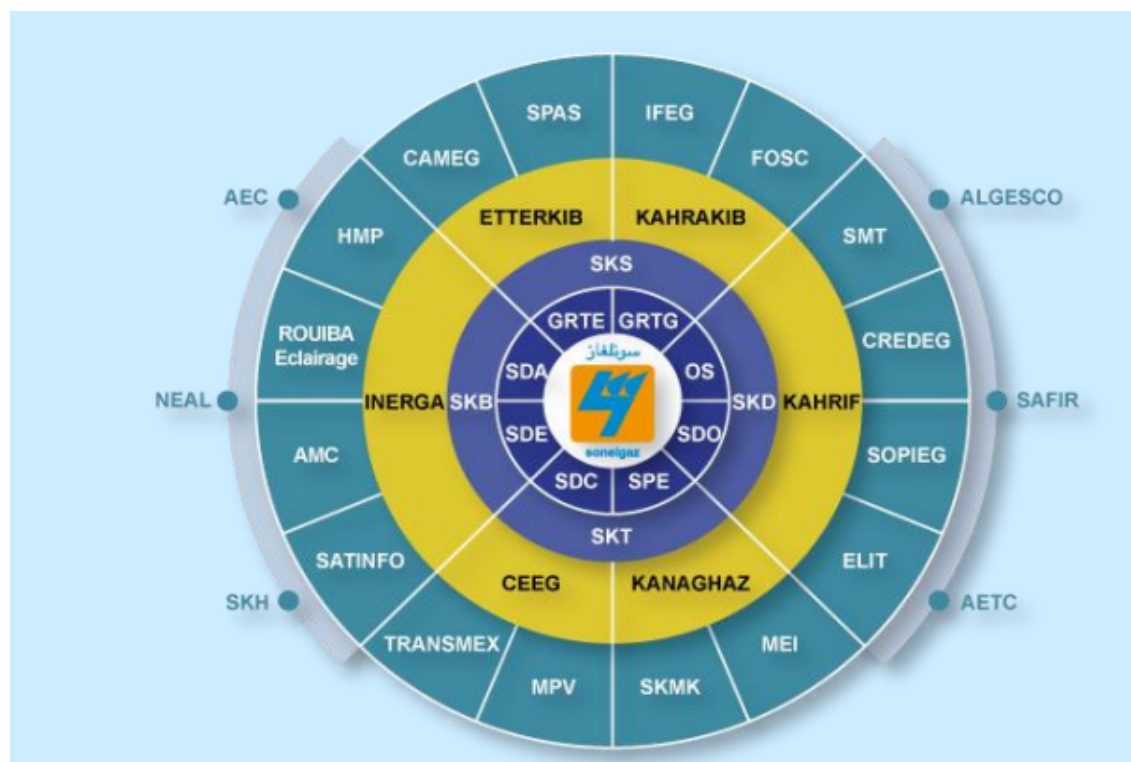


FIGURE 1.1 – Filiales de SONELGAZ

1.3 SONELGAZ SADEG CD BEJAIA

1.3.1 Présentation de la Concession de Distribution Bejaïa

La Direction de Distribution de Bejaïa alimente en énergie électrique et gazière les clients résidant sur le territoire de la Wilaya, son siège social se situe a cité Tobal – Bejaïa.

Son Nombre de clients d'Electricité dépasse 310000 clients, et le nombre de clients Gaz dépasse 110000 clients.

La concession de distribution de Bejaia contient :

Dix agences commerciales chargées de la prise en charge de la clientèle d'où cinq agences sont chargées de développement et de la maintenance du réseau électrique. Les cinq autres agences sont chargées de développement et de la maintenance du réseau gaz.

1.3.2 Organigramme général de la Direction de Distribution de l'électricité et du gaz de Bejaia

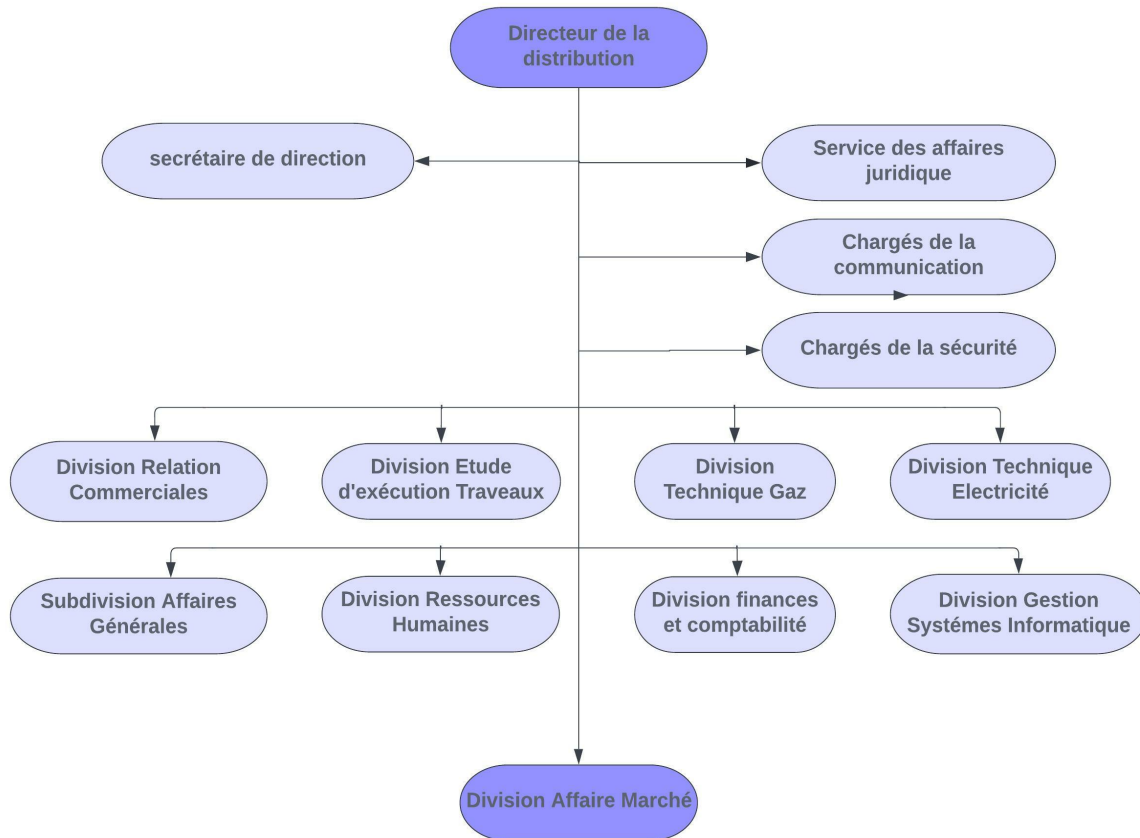


FIGURE 1.2 – L'organigramme de la direction de la distribution de Bejaia

1.3.3 Présentation de l'infrastructure réseau de la concession de distribution Bejaia

Une infrastructure réseau a pour objectif de centraliser les données d'une entreprise afin de simplifier leur échange sécurisé et la communication entre les agents. Elle instaure une plateforme de travail collaboratif. Elle contribue à une amélioration des procédures décisionnelles. Elle booste sensiblement la performance et la productivité de la société concernée. La mise en place d'une infrastructure favorise une réduction importante des impressions sur papier. Cet outil joue également d'autres rôles déterminants.

Dans la CD de Bejaia on a deux ingénieurs et trois techniciens supérieurs qui travaillent dans le service informatique. Ce dernier se situe au rez-de-chaussée du bâtiment de l'entreprise qui contient :

- Une Salle de machine .
- Une Salle de serveur .
- Un Serveur téléphonie .
- Une Station télé- relève .
- Une Station ZDFA .

Pour assurer un bon service pour les clients, une gestion de l'entreprise .

Et pour éviter le maximum possible les coupures de réseaux, la CD de Bejaia utilise trois types de connexion qui sont :

- Fibre optique .
- Réseaux ADSL .
- Réseaux 3G .

1.4 PROBLEMATIQUE

Après avoir étudié le réseau mis en place depuis des années, nous relevons quelques critiques qui sont :

- Le câblage réseau est réalisé d'une façon non étudiée, ce qui peut poser un problème de lourdeur, de boucles, de congestion et de maintenance.
- Les Switchs sont placés en cascades, ce qui génère une latence au niveau de chaque switch concernant la recherche dans les tables MAC.
- L'absence de segmentation du trafic réseau, ce qui implique l'arrivée d'un trafic non souhaité sur les périphériques des utilisateurs.
- Des difficultés d'intervenir dans le cadre de la maintenance.
- Des difficultés de mettre en place des procédures de sécurité.

- Des difficultés de faire évoluer le réseau par la mise en place de la redondance, de la tolérance aux pannes et de la haute disponibilité.

1.5 SOLUTION PROPOSEE

Nous allons mettre en place une autre architecture réseau avec un concept hiérarchique à trois niveaux. De plus nous allons segmenter le trafic réseau de la couche 2 en mettant en place le concept des VLANS et le routage inter VLANS.

1.6 CONCLUSION

A travers ce chapitre nous avons pris conscience de l'importance des investissements que SONALGAZ a fait en matière de nouvelles technologies de l'information et de communication.

Nous avons présenté la concession de distribution de Bejaia, accompagné de l'organigramme général de la direction et son réseau informatique existant. Nous avons aussi rénuméré ces faiblesses, et exposé la problématique.

Généralités sur les réseaux informatiques

Sommaire

2.1	INTRODUCTION	13
2.2	DEFINITION D'UN RESEAU INFORMATIQUE	13
2.3	OBJECTIFS DES RESEAUX INFORMATIQUE	13
2.4	ARCHITECTURE DES RESEAUX	14
2.5	CLASSIFICATION DES RESEAUX INFORMATIQUES . .	14
2.6	LES PROTOCOLES RESEAUX	17
2.7	ARCHITECTURES PROTOCOLAIRES	18
2.7.1	Modèle OSI (Open System Interconnexion)	19
2.7.2	Modèle TCP/IP (Transmission Control Protocol/Internet Protocol)	20
2.8	LES PRINCIPAUX COMPOSANTS D'INTERCONNEXION	22
2.9	CONCLUSION	24

2.1 INTRODUCTION

A l'origine, un réseau était un rassemblement de personnes ou d'objets. De nos jours on entend par réseau, les réseaux d'entreprises, qui connectent différentes machines afin de pouvoir les faire communiquer entre elles. Que ce soit pour le partage de fichiers ou l'envoi de messages, la plupart des entreprises sont aujourd'hui dotées d'un réseau afin d'être plus efficaces .

Au cours de ce chapitre, nous verrons d'abord ce qu'est généralement un réseau informatique, ce qui le constitue, ainsi que les techniques et moyens utiles pour l'interconnexion.

2.2 DEFINITION D'UN RESEAU INFORMATIQUE

Un réseau informatique est un ensemble d'équipement informatiques (*ordinateur et périphériques*) reliés entre eux grâce à des supports de communication (*câble : réseau câblé, ou onde : réseau sans fil..*) permettant la communication (*transfert des informations électroniques*) et le partage de ressources (*matérielles et logicielles*) [2].

2.3 OBJECTIFS DES RESEAUX INFORMATIQUE

Nous appelons réseau un ensemble d'ordinateurs interconnectés entre eux et réalisant des tâches différentes.

Les objectifs d'un réseau sont classiquement les suivants [2] :

- **Partage des ressources** : Rendre accessible à chacun les données, les programmes et les équipements indépendamment de leur situation physique par rapport à l'utilisateur.
- **Augmenter la fiabilité** : Permettre des copies d'un même fichier sur plusieurs machines ce qui augmente la fiabilité face aux pannes d'une machine.
- **Réduction des coûts** : Plusieurs petits ordinateurs revient moins cher que de gros serveurs à performance égale.

- **Médium de communications** : Des personnes éloignées géographiquement peuvent travailler ensemble plus facilement.

2.4 ARCHITECTURE DES RESEAUX

Les réseaux sont structurés du point de vue fonctionnel en deux catégories [2] :

- **Réseaux poste a poste (peer to peer)** : Les réseaux postes à postes ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs.
- **Réseaux à serveur dédié (client/serveur)** : Comportent en général plus de dix postes. La plupart des stations sont des « postes clients », c'est à dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs.

2.5 CLASSIFICATION DES RESEAUX INFORMATIQUES

On peut classer les réseaux selon plusieurs critères, par exemple la distance entre entité communicantes, la topologie, et le types d'accès. La figure 2.1 illustre les différents types de réseaux informatiques.

- **Classification selon Leur étendu**

1. **Les réseaux personnel PAN (Personal Area Network)**

La plus petite étendue de réseau. Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique.

2. **Les réseaux locaux LAN (Local Area Network)**

De taille supérieure de pan, en français Réseau Local d'Entreprise (RLE), relie entre eux des ordinateurs, des serveurs.

3. Les réseaux MAN (Métropolitain Area Network)

Le réseau métropolitain ou Metropolitan Area Network (MAN) est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN.

4. Les réseaux étendus WAN (Wide Area Network)

Les étendues de réseaux les plus conséquentes sont classées en Wide Area Network (WAN). Constitués de réseaux de type LAN. Les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux.



FIGURE 2.1 – Les différents types de réseaux informatiques [2]

— Classification selon la topologie (mode de diffusion des informations)

Parmi les topologie de réseau, nous citons :

1. Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantages d'être facile à mettre en oeuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

Cette topologie est obsolète dans les réseaux de données mais couramment utilisée dans les réseaux de terrain.

2. Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé switch (commutateur). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du commutateur sans pour autant paralyser le reste du réseau.

3. Topologie en anneau

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour. On a donc une boucle d'ordinateurs sur laquelle chacun d'entre-eux va "avoir la parole" successivement.

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.

Sur les réseaux de données, c'est la topologie en étoile qui est la plus répandue.

La figure 2.2 ci-dessous illustre les différentes topologies de réseau :

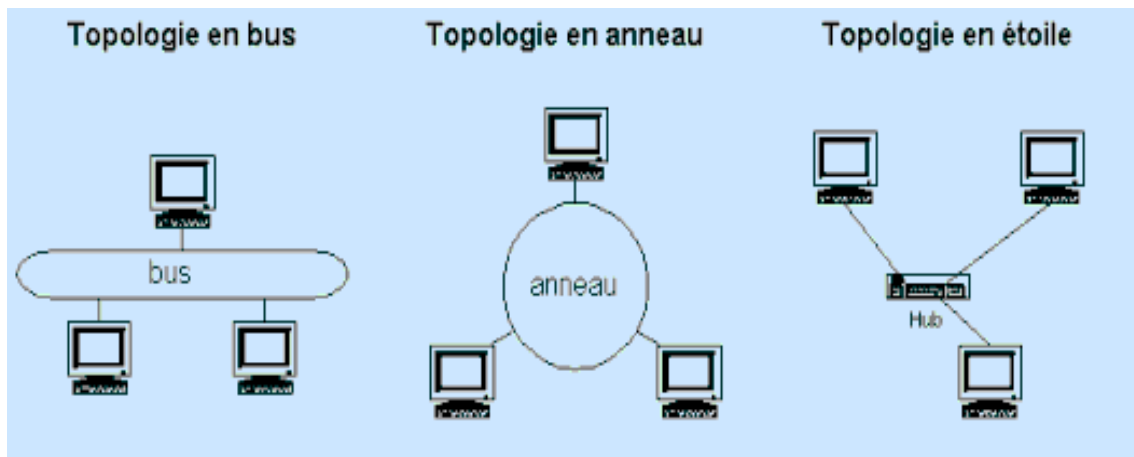


FIGURE 2.2 – Les différents topologies de réseaux informatiques [3]

— **Classification selon la méthode d'accès**

1. Méthode d'accès CSMA/CD
2. Méthode d'accès par Token ring
3. Méthode d'accès par Standard FDDI

— **Classification selon le mode de connexion**

1. Modes avec connexion
2. Modes sans connexion

2.6 LES PROTOCOLES RESEAUX

Il existe de nombreux protocoles réseaux, mais ils n'ont pas tous, ni le même rôle, ni la même façon de procéder. Certains protocoles réseaux fonctionnent au niveau de plusieurs couches du modèle OSI, d'autres peuvent être spécialisés dans la réalisation d'une tâche correspondant à une seule couche du modèle OSI, parmi ces protocoles on cite [3] :

- **Protocole DNS (Domaine Name Service)** : est une base de données utilisée sur les réseaux IP pour transposer les noms d'ordinateurs en adresse IP.
- **Protocole TCP (Transmission Control Protocol)** : est un protocole fiable, orienté connexion qui permet l'acheminement sans erreur de paquets issues d'une station à une autre.

- **Protocole ICMP (Internet Control Message Protocol)** : est un protocole qui permet le contrôle des erreurs de transmission. En effet, comme le protocole IP ne gère que le transport des paquets et ne permet pas l'envoi de message d'erreur, c'est grâce à ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau.
- **Protocole DHCP (Dynamic Host Configuration Protocol)** : est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut.
- **FTP (File Transfert Protocol)** : permet de transférer des fichiers d'une machine à une autre. L'utilisation de FTP depuis un poste client pour aller chercher ou déposer un fichier sur un serveur nécessite de la part de l'utilisateur de se connecter avec un nom et un mot de passe, donc si l'utilisateur n'est pas reconnu la connexion ne sera pas établie.
- **HTTP (Hyper Text Transfer Protocol)** : est le protocole de communication du web permettant d'échanger des documents hyper textes contenant des données sous la forme de texte, d'image fixes ou animées et de sons. Tout client web communique avec le port **80** d'un serveur HTTP.
- **TFTP (Trivial File Transfer Protocol ou Protocole simplifié de transfert de fichiers)** : est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port **69**, au contraire du FTP qui utilise TCP. TFTP reste très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feu, etc.) ou pour démarrer un PC à partir d'une carte réseau.

2.7 ARCHITECTURES PROTOCOLAIRES

Ces protocoles nous aident à comprendre comment les informations circulent dans un réseau, il explique comment les paquets transitent à travers les différentes couches vers un autre équipement du réseau[4].

2.7.1 Modèle OSI (Open System Interconnexion)

Est une norme établie par l'international Standard Organisation, afin de permettre aux systèmes ouverts (ordinateur, terminal, réseau, ...) d'échanger des informations avec d'autres équipements hétérogènes. Cette norme est constituée de sept couches, dont les quatre premières sont dites basses et les trois supérieures dites hautes. Le principe est simple, la couche la plus basse (directement au-dessus du support physique) ne peut communiquer directement avec une couche $n+1$: chacune des couches est composée d'éléments matériels et/ou logiciels chargés de « transporter » le message à la couche immédiatement supérieure.

— La Couche physique

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédurales nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entre deux entités de liaisons de données.

— La Couche de liaisons de données

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de données entre les entités du réseau. Cette couche détecte et corrige, quand cela est possible, les erreurs de la couche physique et signale à la couche réseau les erreurs irrécupérables.

— La Couche Réseau

Cette couche assure toutes les fonctionnalités de relais et d'amélioration de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche 2 (liaison) pour préparer le travail de la couche .

— La Couche Transport

Cette couche définit un transfert de données transparent entre les entités en les déchargeant des détails d'exécution (*contrôle entre l'OS et le support de transmission*). Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requises par la couche 5 (*session*).

— **La Couche Session**

Cette couche fournit aux entités de la couche présentation les moyens d’organiser et de synchroniser les dialogues et les échanges de données. Il s’agit de la gestion d’accès, de la sécurité et de l’identification des services.

— **La Couche présentation**

Cette couche assure la transparence du format des données à la couche 7 (application).

— **La Couche Application**

Cette couche assure aux processus d’application le moyen d’accès à l’environnement OSI et fournit tous les services directement utilisables par l’application (transfert de données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications).

La figure 2.3 ci-dessous représente les différentes couches du modèle OSI.

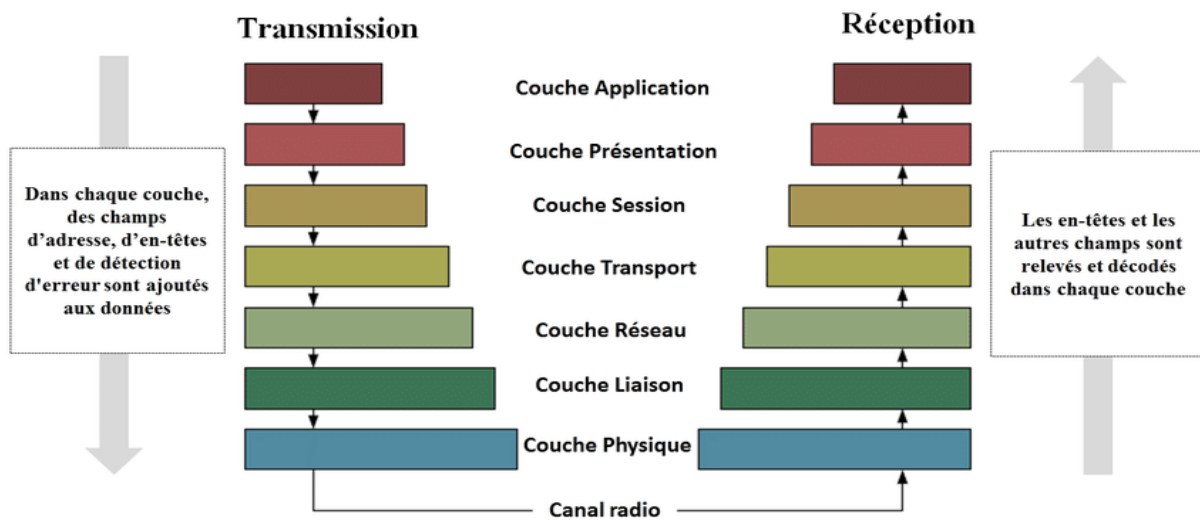


FIGURE 2.3 – Modèle OSI [5]

2.7.2 Modèle TCP/IP (Transmission Control Protocol/Internet Protocol)

Le modèle OSI plutôt théorique a été remplacé par un modèle plus pratique, le modèle TCP/IP. A la différence du modèle OSI, qui a d’abord été normalisé avant d’être appliqué, le modèle TCP/IP, a tout d’abord été déployé avec succès avant d’être normalisé. TCP/IP ou la « pile TCP/IP » est une suite de protocoles. Le sigle TCP/IP signifie « Transmission Control

Protocol/Internet Protocol ». Il provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire les protocoles TCP et IP[4].

2.7.2.1 Architecture en couche du modèle TCP/IP

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches

— Couche Accès réseau

Cette couche est regroupe les couches physique et liaison de données du modèle OSI. Il assure la bonne gestion du médium (détection de collisions) et permet l'acheminement des informations entre émetteur et destinataire au niveau des adresses MAC.

— Couche Internet

Ce sont des protocoles de haut niveau de la couche réseau. IP permet le routage des informations entre réseaux, c'est ici que l'adresse IP est utilisée. ICMP est un protocole de contrôle il met à disposition des outils de dépistage d'erreur et de signalisation. C'est un protocole important qui mérite que l'on s'y arrête. Nous en reparlerons plus en détail. Ne pas oublier le protocole ARP.

— Couche Transport

La couche transport permet d'identifier les applications qui communiquent. Pour faciliter la communication on a défini non pas des noms d'applications, mais des ports de communication spécifiques à chaque application. La couche transport gère deux protocoles de livraison des informations : UDP est dit "sans connexion" et TCP est dit "avec connexion".

— Couche application

C'est la couche de haut niveau, c'est celle que voient la plupart des utilisateurs, elle englobe les couches OSI d'application, de présentation et de session. Elle s'assure que les données soient correctement "empaquetées" pour qu'elles soient lisibles par la couche suivante.

La figure 2.4 ci-dessous représente le modèle TCP/IP.

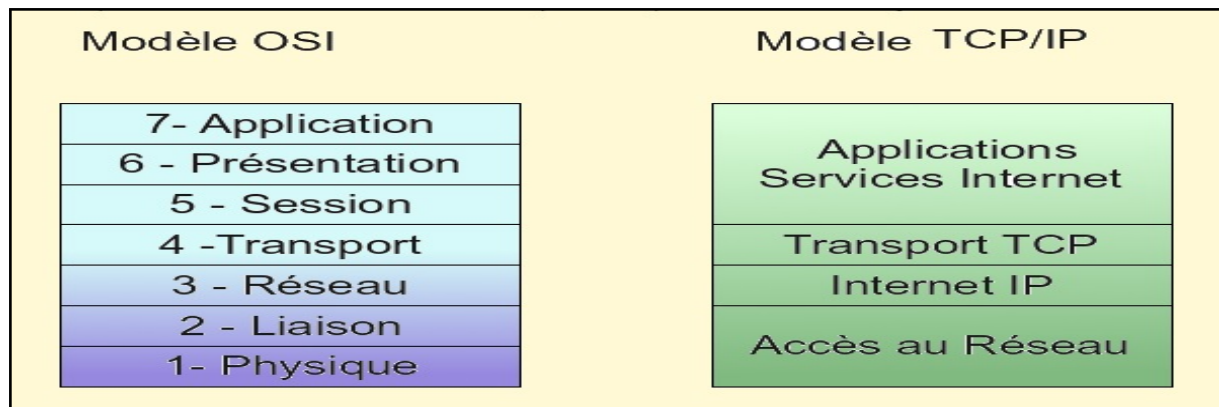


FIGURE 2.4 – Modèle TCP/IP

2.8 LES PRINCIPAUX COMPOSANTS D'INTERCONNEXION

Pour mettre en place un réseau informatique, plusieurs équipements informatiques sont mis en jeu. La plupart de ces équipements sont des équipements d'interconnexion. Chacun de ces équipements joue un rôle spécifique. [6]

— La carte réseau

La carte réseau constitue l'interface physique entre l'ordinateur et le support de communication.

Pour qu'un ordinateur soit mis en réseau, il doit être muni d'une carte réseau.

— Le concentrateur

Le concentrateur est un équipement physique à plusieurs ports. Il sert à relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données reçues sur un port et les diffuser bêtement sur l'ensemble des ports.

— Le répéteur

Le répéteur, est un équipement qui sert à régénérer le signal entre deux nœuds pour le but d'étendre la distance du réseau. Il est à noter qu'on peut utiliser un répéteur pour relier deux supports de transmission de type différents.

— Le pont

Le pont appelé bridge en anglais est un équipement qui sert à relier deux réseaux utilisant le même protocole. Quand il reçoit la trame, il est en mesure d'identifier l'émetteur et le récepteur, comme ça il dirige la trame directement vers la machine destinataire.

— **Le commutateur**

Le commutateur, est un équipement multiport comme le concentrateur. .

— **La passerelle**

La passerelle est un système matériel et logiciel qui sert à relier deux réseaux utilisant deux protocoles et/ou architectures différents.

— **Le routeur**

Le routeur est un matériel de communication de réseau informatique qui a pour rôle d'assurer l'acheminement des paquets, le filtrage et le control du trafic. Le terme router signifie emprunter une route. Le routage est la fonction qui consiste à trouver le chemin optimal que va emprunter le message depuis l'émetteur vers le récepteur.

— **Pont routeur**

Le Pont routeur se comporte à la fois comme un pont et un routeur. Si le protocole n'est pas routable, le B-routeur est capable de se replier vers un niveau inferieur et se comporter comme un pont. Dans le cas contraire, le B-routeur joue le rôle d'un routeur.

— **Proxy**

En réseau informatique, un proxy appelé serveur proxy ou serveur mandataire est souvent une machine et/ou logiciel servant de liaison entre une machine cliente et le serveur. La plupart des cas, le serveur proxy est utilisé entre un réseau local et internet. Le rôle principal d'un proxy est d'assurer l'accélération de la navigation, la journalisation des requêtes, la sécurité du réseau local, le filtrage et l'anonymat.

— **Le modem**

Le modem (modulateur-démodulateur) est un équipement qui sert à lier le réseau téléphonique au réseau informatique.

— **Le MAU**

C'est l'équivalent de Hub utilisé en token ring. Sa seule différence avec le Hub, c'est sa capacité d'isoler le circuit non utilisé. Il travail au niveau physique du model OSI.

2.9 CONCLUSION

Dans ce chapitre nous avons présenté les réseaux informatiques d'une façon générale, en citant les critères basiques qui montrent le rôle d'un réseau informatique dans le but de définir bien définir le concept d'administration d'un réseau au sein d'une entreprise.

Dans le prochain chapitre nous allons définir les VLANs et quelques protocoles d'administration et de gestion des VLANs.

Les Réseaux Locaux Virtuels (VLANs)

Sommaire

3.1	INTRODUCTION	26
3.2	PROBLEMES LIES A L'ARCHITECTURE RESEAU	26
3.3	RESEAU LOCAL VIRTUEL (VLAN)	27
3.3.1	Définition	27
3.3.2	Avantage	28
3.3.3	Fonctionnement du VLAN	29
3.3.4	Agrégation des VLANs ou "Trunking"	30
3.3.5	Implémentation de la technologie	32
3.3.6	Types de VLAN	33
3.3.7	Le protocole DTP (<i>Dynamic Trunking Protocol</i>)	35
3.3.8	Le protocole VTP (<i>VLAN Trunking Protocol</i>)	36
3.4	LE PROTOCOLE STP (<i>Spanning Tree Protocol Protocol</i>) . .	38
3.5	ARCHITECTURES HIERARCHIQUES	39
3.6	CONCLUSION	40

3.1 INTRODUCTION

Auparavant, pour constituer des domaines de diffusion, il était nécessaire de créer des réseaux physiques, reliés entre eux par deux routeurs, cette obligation liée à la localisation géographique des stations étaient contraignante pour l'administrateur réseau.

Dans ce chapitre, nous allons présenté les principales notions d'un réseau local virtuel, les méthodes d'implémentation des VLANs, ces protocoles de transport, ces avantages et enfin ces protocoles d'administration et de gestion.

3.2 PROBLEMES LIES A L'ARCHITECTURE RESEAU

Un réseau mal conçu peut faire augmenter fortement les couts de support, provoquer une disponibilité réduite des services et également un soutien limité pour les nouvelles applications et solutions. Une performance moins optimale affecte directement les utilisateurs finaux et leur accès aux ressources.

Voyons plusieurs types de problèmes qu'on peut retrouver sur des réseaux mal conçus :

- **Les Domaines de Broadcast étendus** : Des broadcasts existent dans tous les réseaux. De nombreuses applications et opérations réseau utilisent les broadcasts pour fonctionner correctement. Par conséquent, on ne pourra pas les éliminer complètement. De la même manière, pour éviter une propagation des problèmes il faut définir clairement les limites.
- **Les Difficultés de gestion** : Un réseau mal conçu peut être désorganisé, mal documenté et les flux de trafic devenir difficilement identifiable. Ces problèmes peuvent rendre le support, la maintenance et la résolution des problèmes très difficiles.
- **Les Faiblesses de sécurité** : Un réseau commuté qui a été conçu avec peu d'attention aux exigences de sécurité sur la couche d'accès peut compromettre l'intégralité de l'ensemble du réseau.
- **Les Problèmes étendus** : L'une des raisons d'implémenter une architecture de réseau efficace est de minimiser l'étendue des problèmes lorsqu'ils se produisent. Lorsque l'on

ne définit pas clairement les limites de la couche 2 et 3, une défaillance dans une zone de réseau peut avoir un effet de grande portée.

Un réseau mal conçu a toujours un effet négatif. Il devient un fardeau pour le support et un fardeau financier pour n'importe quelle entreprise.

3.3 RESEAU LOCAL VIRTUEL (VLAN)

Dans l'intention d'améliorer la gestion du réseau, d'optimiser la bande passante et d'améliorer la sécurité dans une entreprise, il est recommandé d'avoir des VLANs.

3.3.1 Définition

La virtualisation d'un LAN consiste en la séparation de l'infrastructure physique et des services de transfert rapide fournis par les commutateurs. L'objectif fondamental d'un VLAN est de rendre la fonction d'un LAN indépendante de l'infrastructure physique.

L'idée de base des VLANs est de découper un seul réseau local en des réseaux logiques totalement disjoints : c'est comme si on avait plusieurs réseaux physiques totalement disjoints, un par VLAN, comme le montre la figure 3.1 ci-dessous [7].

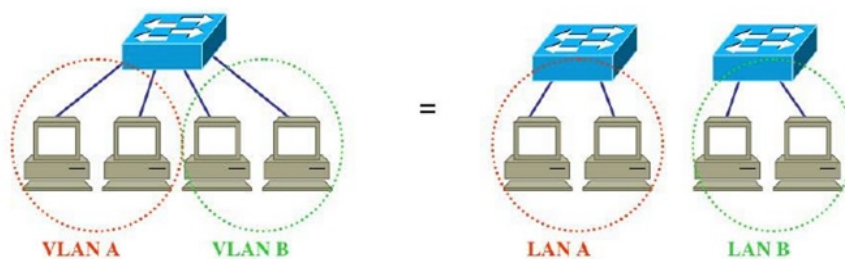


FIGURE 3.1 – Virtual LAN

3.3.2 Avantage

Ce nouveau mode de segmentation des réseaux locaux modifie radicalement la manière dont les réseaux sont conçus, administrés et maintenus. La technologie de VLAN comporte ainsi de nombreux avantages et permet de nombreuses applications intéressantes.

— **La flexibilité de segmentation du réseau**

Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés en des groupes de travail indépendants de l'infrastructure physique. Il est aussi envisageable qu'une station appartienne à plusieurs VLAN en même temps.

— **La simplification de la gestion**

L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

— **L'augmentation considérable des performances du réseau**

Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, la bande passante est libérée, ce qui augmente les performances du réseau.

— **Une meilleure utilisation des serveurs réseaux**

Lorsqu'un serveur possède une interface réseau compatible avec le VLAN, l'administrateur a l'opportunité de faire appartenir ce serveur à plusieurs VLAN en même temps. Cette appartenance à de multiples VLAN permet de réduire le trafic qui doit être routé (*traité au niveau du protocole de niveau supérieur, par exemple IP*) "de" et "vers" ce serveur, et donc d'optimiser ce trafic. Tout comme le découpage d'un disque dur en plusieurs partitions permet d'augmenter les performances (*la fragmentation peut être diminuée*) de son ordinateur, le VLAN améliore considérablement l'utilisation du réseau.

— **Le renforcement de la sécurité du réseau**

Les frontières virtuelles créées par les VLAN ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).

— **La régulation de la bande passante**

il est important de pouvoir contrôler ce gaspillage de capacité de trafic (bande passante). Ici encore, le VLAN offre à l'administrateur les moyens de réguler l'utilisation de la capacité de trafic disponible au sein de l'infrastructure.

3.3.3 Fonctionnement du VLAN

Un VLAN et un LAN logique fonctionnant sur une infrastructure physique commuté. Une infrastructure physique commune peut supporter plusieurs VLANs.

Chaque LAN virtuel fonctionnera comme n'importe quel LAN distinct. Concrètement, les ports du commutateur prennent un identifiant VLAN. Cet identifiant logique définit l'étendue du domaine de diffusion : le trafic de diffusion ne sera transféré que sur les ports ayant le même identifiant. Autrement dit, par exemple, le trafic de diffusion venant d'un port appartenant au VLAN 66 ne sera transféré que sur les ports ayant pour attribution le VLAN 66. La séparation fonctionnelle entre deux ports ayant des identifiants VLAN différents correspond à une séparation physique. En quelque sorte, la technologie VLAN permet de diviser logiquement les ports du commutateur, soit l'infrastructure physique elle-même.

La figure 3.2 ci-après illustre le trafic de broadcast émanant respectivement des hôtes A et H.

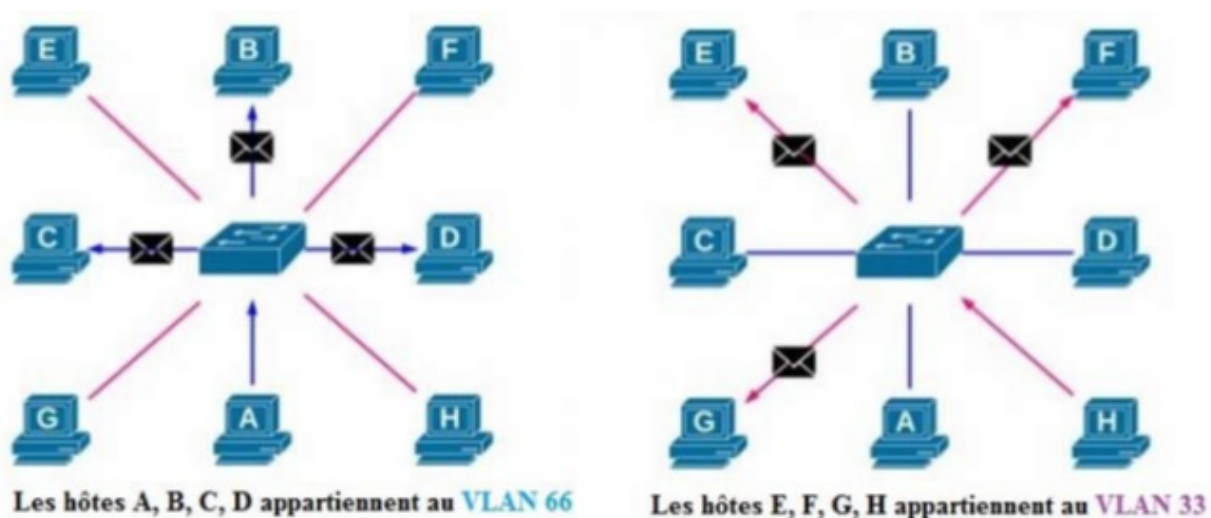


FIGURE 3.2 – Trafic de broadcast [8]

Cette fonctionnalité peut être étendue sur des ports de commutateurs distants à travers toute l'infrastructure. Dans ce cas, les commutateurs devront transporter entre eux du trafic appartenant à plusieurs VLAN sur une ou plusieurs liaisons spécifiques. Ce qui nous mène à l'agrégation des VLANs.

3.3.4 Agrégation des VLANs ou "Trunking"

3.3.4.1 Trunk ou Liaison d'agrégation :

Les ports d'une liaison qui agrègent le trafic de plusieurs VLAN s'appellent un « *Trunk* » chez le constructeur Cisco Systems et « *liaison d'agrégation* » chez d'autres. Sur ce type de liaison, le commutateur ajoute des champs supplémentaires dans ou autour de la trame Ethernet. Ils servent notamment à distinguer le trafic de différents VLANs car ils contiennent entre autres le numéro d'identification du VLAN.

Les commutateurs isolent le trafic entre les VLANs distincts mais transfèrent le trafic d'un même VLAN sur une liaison Trunk en ajoutant une étiquette dans chaque trame.

3.3.4.2 Protocole "Trunk" :

Deux protocoles de « *Trunk* » peuvent être rencontrés. Ils agissent au niveau de la couche 2 (*liaison de données*). Ils opèrent sous les couches TCP/IP[9].

— **Inter-Switch Link (ISL)**

C'est un protocole propriétaire Cisco qui encapsule la trame d'origine avec un en-tête spécifique qui contient entre autres le numéro de VLAN et un nouveau champ FCS. Il est indépendant de la technologie sous-jacente. Il est de moins en moins rencontré au profit de IEEE 802.1q.

— **IEEE 802.1q**

La norme 802.1q date de décembre 1998. C'est un protocole Standardisé et interopérable. Le standard supporte les technologies IEEE 802.3 (*Ethernet*), IEEE 802.11 (*WIFI*), IEEE 802.5 (*Token-Ring*), etc., en tant que protocole de « pontage » (*bridging, IEEE 802.1*).

3.3.4.3 Etiquette 802.1q

IEEE 802.1q ajoute une étiquette dans l'en-tête de la trame (*un ensemble de champs juste après le champ d'adresse MAC d'origine*). Cette étiquette a une taille de 4 octets ou 32 bits dont 12 bits sont consacrés au numéro de VLAN. Vu que la trame sera modifiée, le commutateur recalculera la valeur du champ CRC/FCS, (voir la figure 3.3).

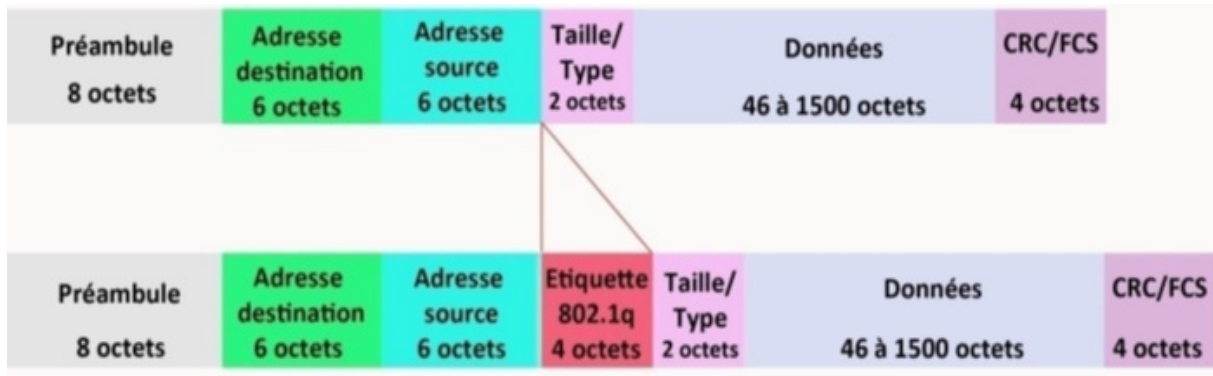


FIGURE 3.3 – Etiquette 802.1q

La norme définit trois types de trames :

- les trames non étiquetées (*untagged frame*) : une trame non étiquetées est une trame qui ne contient aucune information sur son appartenance à un Vlan.
- Les trames étiquetées (*tagged frame*) : une trame étiquetée est une trame qui contient un entête supplémentaire. Cet entête modifie le format standard d'une trame, notamment de la trame 802.3.
- Les trames étiquetées par une priorité (*priority-tagged frame*)

Le format de cette étiquette est illustré dans la figure 3.4.

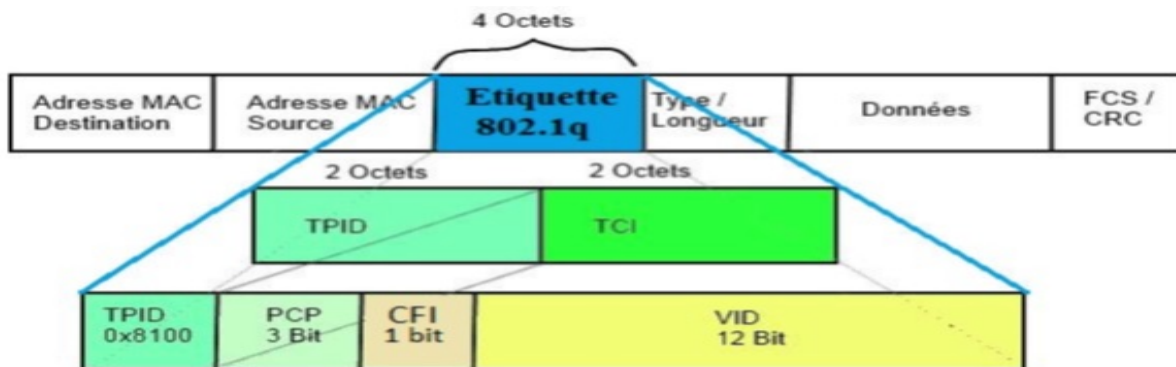


FIGURE 3.4 – Etiquette 802.1q [10]

Le champ Ethertype ou Tag Protocol Identifier (*TPID*), sur 16 bits, est utilisé pour identifier le type de la balise insérée. Pour le 802.1q la valeur est fixée à 0x8100.

Le champ TCI (*Tag Control Identifier*) de 16 bits est utilisé pour l'identification d'un control de l'étiquette. Il est comporte :

- Un champ priorité ou PCP (*Priority Code Point*) de 3 bits, qui est utilisé pour coder 8 niveaux de priorités d'un VLAN par rapport à l'autre.
- Un champ CFI (*Canonical Format Indicator*) sur 1 bit pour la compatibilité entre les adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe ce champ à 0 (*si la trame n'est pas propagée*).
- Un champ VID (*VLAN Identifier*) sur 12 bits. Ce champ permet de définir l'appartenance d'un trame à un VLAN, la valeur maximale est de 4095 (*Vlan 0 signifie que la trame n'appartient à aucun vlan*).

3.3.5 Implémentation de la technologie

Il existe trois différents types de réseau local virtuel : de niveau 1 (aussi appelé VLAN par port), de niveau 2 (VLAN par adresse MAC) et de niveau 3 (VLAN par adresse IP).

— Niveau 1

C'est le mode d'association par défaut. L'association des trames à un VLAN se fait en fonction du PVID¹ du port Access des matériels sur lesquels sont branchées les stations. Cette solution permet d'affecter précisément un VLAN en fonction du port sur lequel est branché une station.

Un pirate ne pourra donc avoir accès à un VLAN spécifique au niveau 2 du modèle OSI seulement si il se branche sur un port ayant le PVID correspondant au VLAN visé.

Le problème de ce mode d'affectation est principalement sa lourdeur d'administration. En effet si l'on déplace un matériel et que l'on désire qu'il soit toujours dans le même VLAN il faudra alors configurer le nouveau port. Cependant il est possible de simplifier

1. l'acronyme de Port VLAN identifier.

l'administration des ports en couplant cette solution avec une solution d'authentification 802.1X afin de configurer dynamiquement le port en fonction de la personne authentifiée. Cette méthode est fréquemment utilisée dans les entreprises.

— Niveau 2

Ce mode d'association est situé au niveau de la couche 2 du modèle OSI (couche liaison). L'association à un VLAN s'effectue en fonction de tables d'adresse MAC configurées sur les commutateurs ou routeurs pour chaque VLAN. Ainsi, la trame sera marquée en fonction de l'adresse MAC source de la trame. Si une adresse MAC n'est pas déclarée elle est selon les matériels et leur configuration soit associée au VLAN correspondant au PVID du port d'entrée, soit associée à un VLAN par défaut, soit refusée. Ce mode d'affectation permet d'avoir une gestion plus modulable et centralisée de l'affectation des VLAN. Cependant l'architecture est sensible au spoofing MAC.

— Niveau 3

Les trames sont associées aux différents VLANs en fonction du protocole de niveau 3 utilisé pour les transmettre. Cette fonctionnalité peut être utile si l'on désire effectuer une différenciation de service 802.1p en fonction du protocole de niveau 3. Cependant elle est très peu utilisée dans des contextes d'entreprise. De plus la désencapsulation des paquets entraîne une lourdeur de traitement.

3.3.6 Types de VLAN

Il existe 5 principaux types de VLAN selon le type de réseau qu'ils véhiculent[11] :

— VLAN par défaut

Lorsque le commutateur démarre pour la première fois, tous les ports du commutateur deviennent membres du VLAN par défaut (généralement tous les commutateurs ont un VLAN par défaut nommé VLAN 1), ce qui les place tous dans le même domaine de diffusion. L'utilisation du VLAN par défaut permet à tout périphérique réseau connecté à

l'un des ports du commutateur de se connecter à d'autres périphériques sur d'autres ports du commutateur. Une caractéristique unique du VLAN par défaut est qu'il ne peut pas être renommé ou supprimé.

— VLAN de données

Le VLAN de données est utilisé pour diviser l'ensemble du réseau en 2 groupes. Un groupe d'utilisateurs et un autre groupe d'appareils. Ce VLAN également connu sous le nom de VLAN utilisateur, le VLAN de données est utilisé uniquement pour les données générées par l'utilisateur. Ce VLAN ne transporte que des données. Il n'est pas utilisé pour transporter le trafic de gestion ou la voix.

— VLAN voix

Le VLAN voix est configuré pour transporter le trafic voix. Les VLANs voix se voient généralement accorder une priorité de transmission élevée par rapport aux autres types de trafic réseau. Pour garantir la qualité de la voix sur IP (VoIP) (délai inférieur à 150 millisecondes (ms) sur le réseau), nous devons disposer d'un VLAN voix distinct, car cela préservera la bande passante pour les autres applications.

— VLAN de gestion

Un VLAN de gestion est configuré pour accéder aux capacités de gestion d'un commutateur (trafic comme la journalisation du système, la surveillance). VLAN 1 est le VLAN de gestion par défaut (VLAN 1 serait un mauvais choix pour le VLAN de gestion). N'importe quel VLAN de commutateur peut être défini comme VLAN de gestion si l'administrateur n'a pas configuré un VLAN unique pour servir de VLAN de gestion. Ce VLAN garantit que la bande passante pour la gestion sera disponible même lorsque le trafic utilisateur est élevé.

— VLAN natif

Ce VLAN identifie le trafic provenant de chaque extrémité d'une liaison trunk. Un VLAN natif est alloué uniquement à un port de jonction 802.1Q. Le port de jonction 802.1Q place le trafic non balisé (*trafic qui ne provient d'aucun VLAN*) sur le VLAN natif. Il est préférable de configurer le VLAN natif en tant que VLAN inutilisé.

3.3.7 Le protocole DTP (*Dynamic Trunking Protocol*)

DTP est un protocole réseau propriétaire de Cisco Systems il permet de gérer dynamiquement l'activation/désactivation du mode trunk d'un port sur un commutateur. Il gère la négociation trunk seulement si le port de l'autre commutateur est configuré dans un mode trunk supporté par DTP.

Une interface peut être configurée de 4 façons différentes :

- *Switch(config-if) #switchport mode access :*

Cette commande force le switch à être un port d'accès, et désactive l'envoi de requête DTP sur le réseau.

- *Switch(config-if)#switchport mode trunk :*

Cette commande force le port à être un port trunk, et envoie des requêtes DTP au switch d'en face.

-*Switch(config-if)#switchport mode dynamic auto :*

Le mode dynamique est en quelque sorte un mode passif. Il attend patiemment un message du switch en face pour s'autoconfigurer. Un port en mode auto deviendra uniquement un lien trunk si le port du switch en face est configuré soit en mode trunk ou en mode desirable, sinon il sera un port en mode access. Ce mode envoie également des requêtes DTP sur le réseau.

- *Switch(config-if)#switchport mode dynamic desirable :*

Le mode desirable, est un mode actif. C'est-à-dire qu'il envoie des requêtes DTP au switch en face pour lui faire une proposition de trunk.

La Figure 3.5 ci-après nous récapitule le fonctionnement de DTP :

	Dynamic auto	Dynamic desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	-
Access	Access	Access	-	Access

FIGURE 3.5 – Le fonctionnement de DTP

3.3.8 Le protocole VTP (*VLAN Trunking Protocol*)

Pour minimiser les erreurs de configuration des VLAN dans son réseau, il faut utiliser le protocole VTP (*VLAN Trunking Protocol*).

VTP est un protocole propriétaire Cisco servant à maintenir la base de données de Vlan sur plusieurs commutateurs. Il permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (*le serveur*) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (*clients*). VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local.

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants[12], comme illustré dans la figure 3.6 :

1. Le mode serveur

- L'information est stockée dans la NVRAM.
- Il définit le nom de domaine VTP.
- Il peut ajouter, modifier ou supprimer un VLAN.
- Il stocke la liste des VLANs du domaine VTP.

2. Le mode client

- Il possède un nom de domaine.
- Il stocke une liste de VLANs non modifiable.

3. Le mode transparent

- Il ne participe pas aux domaines VTP du réseau.
- Il transmet les paquets VTP via ses liens trunk.
- Il possède sa propre liste de VLANs qu'il est possible de modifier.

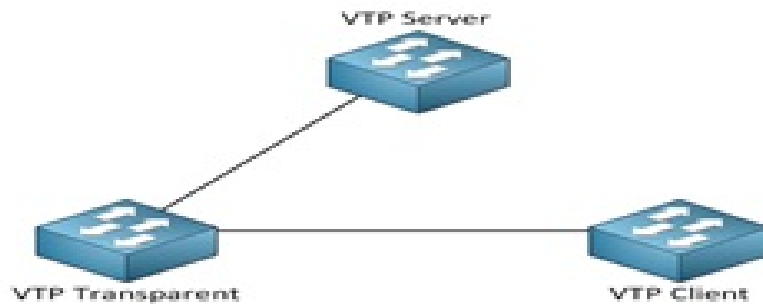


FIGURE 3.6 – Les modes de VTP

Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas :

- Il faut assigner le même nom de domaine de VTP à chaque commutateur.
- L'option trunk pour l'interconnexion des commutateurs doit être activée.

(voir la figure 3.7).

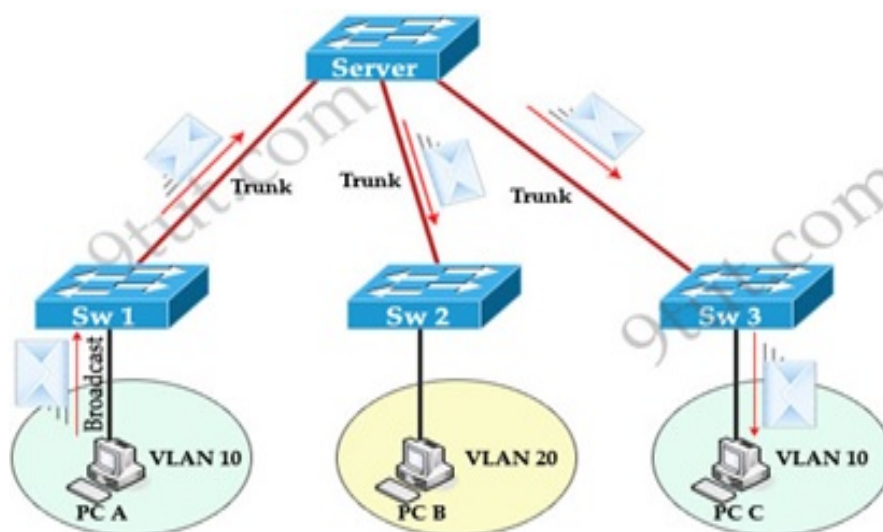


FIGURE 3.7 – Le protocole VTP [13]

3.4 LE PROTOCOLE STP (*Spanning Tree Protocol Protocol*)

Afin d'éviter les tempêtes de diffusion au sein du réseau qui peuvent entraîner l'arrêt complet du trafic réseau, il est recommandé d'utiliser le protocole STP.

STP est un protocole de gestion de la couche 2 (*liaison des données*), qui fournit un chemin redondant tout en prévenant le boucles dans un réseau. Ce protocole permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde, la figure 3.8 représente le protocole STP.

Son fonctionnement est tel que dans un réseau local commuté en redondance, toutes les trames doivent toujours passer par un Switch « Root » pour être acheminées à sa destination. Pour cela, une fois tous les switch up, chacun annoncera par des messages BPDU (Bridge Protocol Data Unit) ses informations ou ses identités à ses voisins. L'identité dont il est question est la combinaison de la priorité (32768 priorité par défaut) plus l'adresse MAC[14].

Le protocole STP procède en quatre phases :

- Election du commutateur racine (Root Bridge ou RB)
- Détermination du port racine (Root Port ou RP) sur chaque commutateur
- Détermination du port désigné (Designated Port ou DP) sur chaque segment
- Blocage des autres ports

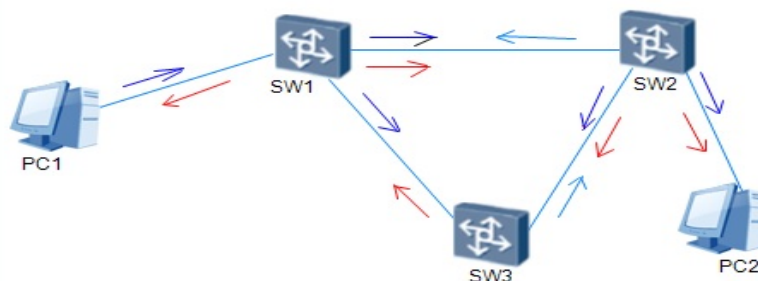


FIGURE 3.8 – Le protocole STP [15]

3.5 ARCHITECTURES HIERARCHIQUES

Dans le domaine des réseaux, la conception hiérarchique divise le réseau en couches distinctes. Chaque couche de la hiérarchie offre des fonctions spécifiques qui définissent son rôle dans le réseau. Ceci permet au concepteur et à l'architecte du réseau de sélectionner le matériel et les logiciels réseau adaptés, ainsi que les fonctionnalités nécessaires aux rôles de cette couche réseau.

Les modèles hiérarchiques appliquent à la fois les conceptions LAN et WAN.

Une conception de réseau typique de LAN hiérarchique comprend les 3 couches suivantes[16],

- Couche cœur de réseau
- Couche de distribution
- Couche d'accès

Comme illustre la figure 3.9 :

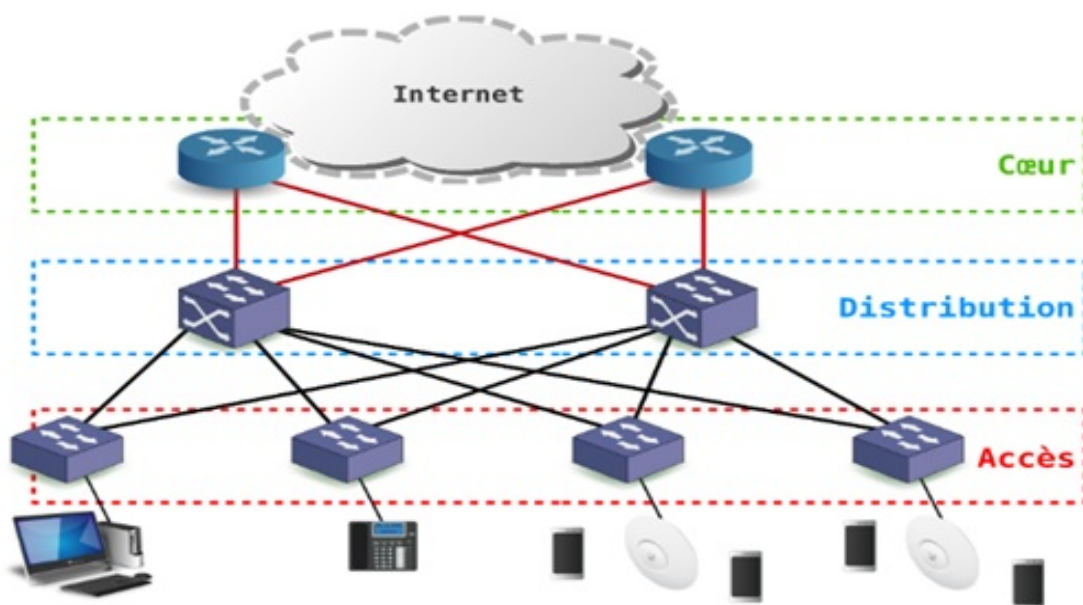


FIGURE 3.9 – Architecture hiérarchique 3-tiers [17]

— **Cœur**

Cette couche correspond à la dorsale du réseau de l'entreprise qui relie entre eux les blocs fonctionnels d'équipements. Les objectifs à ce niveau sont les performances, la stabilité et

le moins de complexité possible. C'est la raison pour laquelle on ne trouve généralement que deux routeurs redondants à ce niveau.

Le débit binaire utile est le critère de dimensionnement d'un routeur qui conditionne les performances. Par débit binaire utile, on entend la transmission de flux réseau classifiés, routés et filtrés.

— **Distribution**

Cette couche repose sur la convergence, l'équilibrage de charge, la qualité de service et la haute disponibilité. On y trouve l'isolation vis-à-vis de la couche accès avec le moins de commutation de circuits (*ou d'adresses MAC*) possible. Vue de la couche accès, c'est à ce niveau que l'on offre la redondance des passerelles réseau par défaut des hôtes.

— **Accès**

Plus les usages réseau évoluent, plus cette couche doit être riche en fonctionnalités diverses. Elle ne se limite plus à fournir des ports de commutateur en vis-à-vis de postes de travail fixes qui utilisent tous le même système. On y trouve maintenant des fonctions de gestion de l'alimentation des équipements raccordés au commutateur (*téléphones, points d'accès Wifi, etc.*) via la technologie PoE (*Power over Ethernet*). On y trouve aussi les fonctions d'authentification de ces mêmes hôtes ou équipements raccordés à l'aide du protocole IEEE 802.1X. Pour optimiser l'utilisation de la bande passante radio, les commutateurs intègrent de plus en plus des logiciels de contrôle radio qui permettent par exemple de réguler les puissances rayonnées par les antennes des points d'accès Wifi.

3.6 CONCLUSION

Dans ce chapitre, nous avons présenté les réseaux local virtuel. Puis, nous avons cité les différents avantages des VLANs et leurs différents types. Ensuite, nous avons passé en revue les différentes méthodes d'implémentation des VLANs et quelques protocoles d'administration et de gestion de ce type de réseau.

Conception et Simulation

Sommaire

4.1	INTRODUCTION	42
4.2	PRESENTATION DE L'ANCIENNE INFRASTRUCTURE RESEAU DE CONCESSION DE DISTRIBUTION BEJAIA	42
4.3	SOLUTION ADAPTEE	43
4.4	OUTIL DE SIMULATION	44
4.4.1	Cisco packet tracer	44
4.5	CREATION ET CONFIGURATION DES NOUVEAUX RESEAUX	46
4.5.1	Création	46
4.5.2	Configuration	46
4.6	TEST ET VALIDATION DE LA CONFIGURATION	58
4.6.1	Contrôle de la bonne configuration du protocole VTP	58
4.6.2	Contrôle des réseaux locaux virtuels créés sur le switch serveur	59
4.6.3	Vérification du routage inter VLAN	60
4.6.4	Vérification de la distribution des adresses IP sur le serveur DHCP	60
4.6.5	Vérification des adresses IP des machines attribuées par le DHCP	61
4.6.6	Vérification de la communication entre les machines	61
4.6.7	Test de la téléphonie IP	63
4.6.8	Test des cameras de surveillance	63
4.7	CONCLUSION	64

4.1 INTRODUCTION

Ce présent chapitre consistera à mettre en oeuvre les solutions proposées pour la réalisation de notre projet, en exposant les différentes configurations nécessaires à implémenter sur le LAN. Ces configurations entourent entre la configuration des VLANs, VTP et STP en utilisant sur le simulateur Cisco packet tracer.

Pour présenter les configuration que nous avons réaliées, nous allons utiliser un outil de capture sur notre logiciel de simulation, a fin d'illustré les différents étapes de nos configuration et d'éclaircir chaque composant de cette dernière et son fonctionnement.

Enfin, des tests de validation pour confirmer le bon fonctionnement du réseau seront réalisés.

4.2 PRESENTATION DE L'ANCIENNE INFRASTRUCTURE RESEAU DE CONCESSION DE DISTRIBUTION BEJAIA

Le réseau informatique de SONELGAZ de Bejaia est composé d'une armoire informatique au premier étage qui contient :

- Deux Switch Cisco catalyste 2900 connectés en cascades.
- Un routeur Cisco 2600.
- Chaque bureau contient une seule prise.

La figure 4.1 présente l'ancienne infrastructure de la CD de Bejaia.

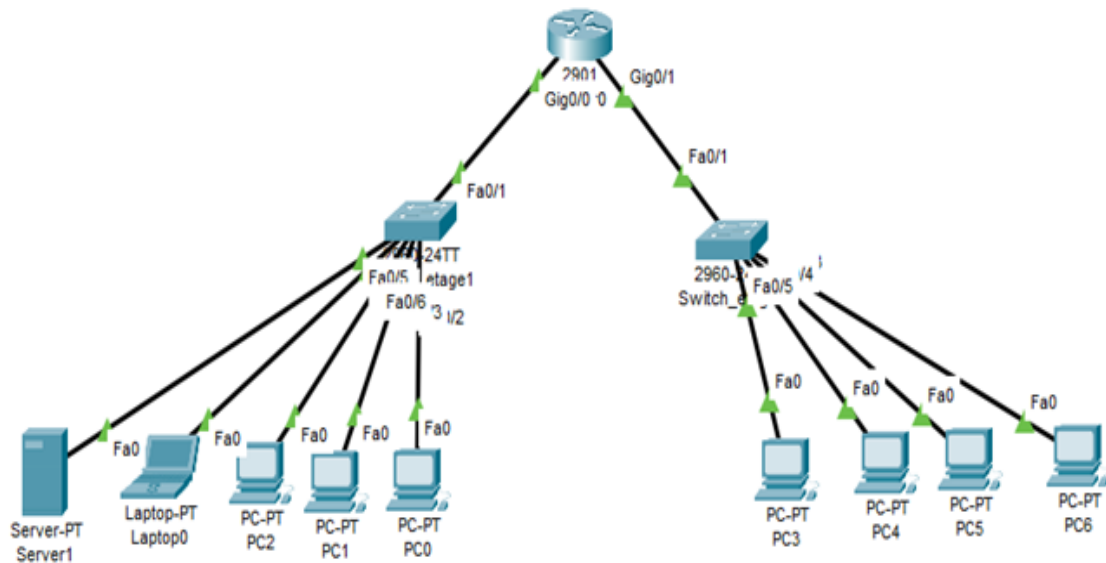


FIGURE 4.1 – l’ancienne infrastructure réseau de la CD de bejaia

4.3 SOLUTION ADAPTEE

De nombreuses insuffisances ont été découvertes lors de l’étude du réseau de la CD de Bejaia, ce qui nous a permis également de définir un nombre important de contraintes pouvant réduire ses performances voir le dégrader.

Nous avons remarqué :

- Une surcharge très grande au niveau des commutateurs.
- Une forte utilisation de la bande passante .
- Mal organisation des équipements de l’entreprise.
- Le manque de sécurité dans le réseau.

Pour remédier à ces problèmes, nous allons reconfigurer le réseau informatique (*câblage, switch, prise*), à fin qu’il répond aux exigences des utilisateurs en matière de :

- Eliminer la lenteur due à l’architecture adoptée (un seul domaine de diffusion, les boucles).
- Diviser les domaines de diffusion.
- Rendre le réseau évolutif.

— Sécuriser le réseau, les équipements et les données sensibles.

Afin de réaliser ces objectifs nous allons implémenter un réseau local hiérarchique à trois niveaux précédemment présenté, (voir section 3.5).

La figure 4.2 ci-dessous, nous montre la nouvelle architecture a 3 niveau que nous voulons créer pour mettre fin aux problèmes qui ont été découverts.

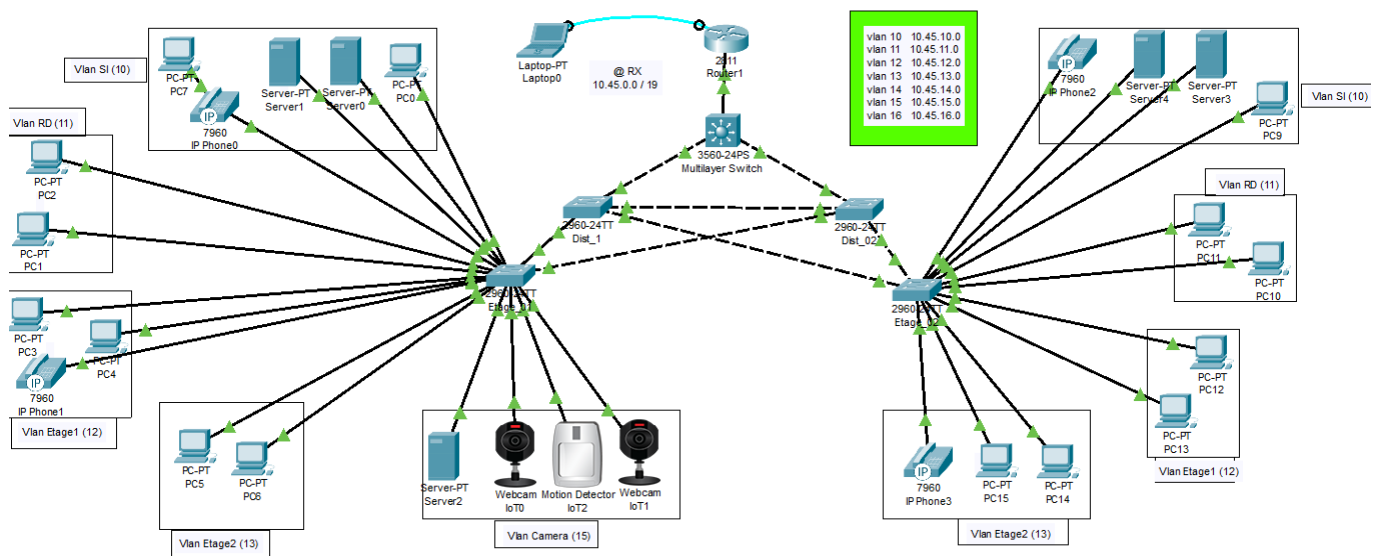


FIGURE 4.2 – Nouvelle architecture créé

4.4 OUTIL DE SIMULATION

Pour la simulations de notre réseau, nous avons utiliser le simulateur Cisco packet tracer.

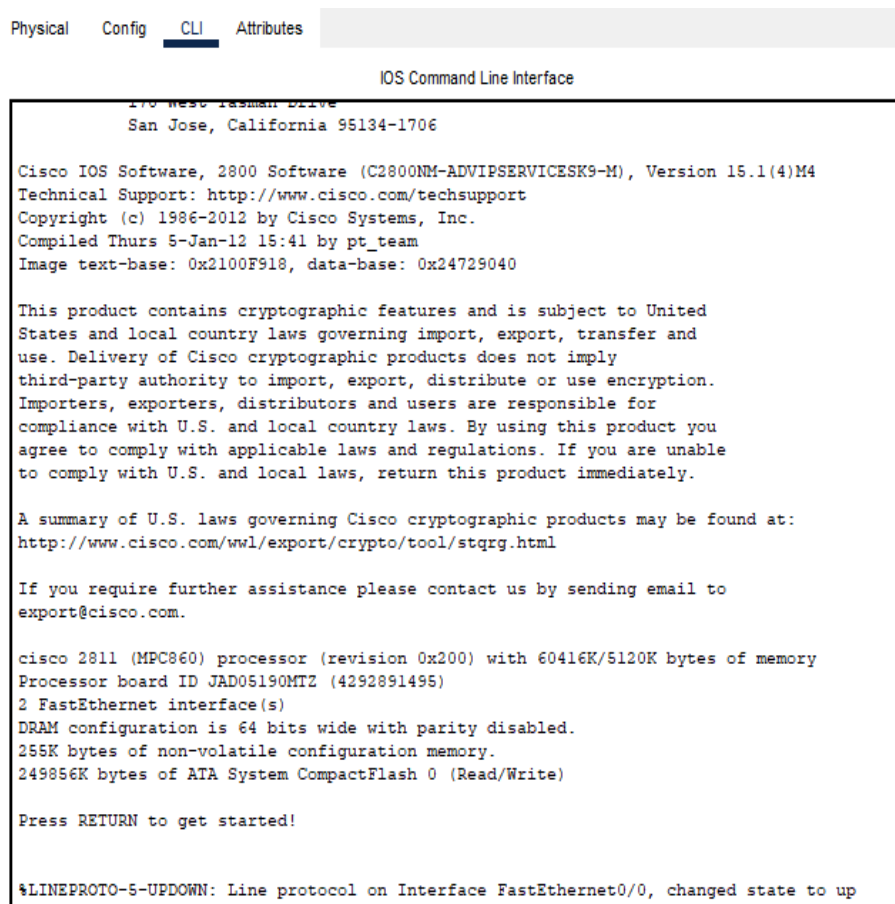
4.4.1 Cisco packet tracer

Cisco packet tracer est un logiciel développé par CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs.

Ces équipements doivent ensuite être reliés via des connexions (câbles divers ou fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP et les services disponibles.

Toutes les configurations des équipements du réseau sont réalisées au niveau de CLI (*Command Langage Interface*). CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes. C'est-à-dire qu'à partir des commandes introduites par l'utilisateur du logiciel que la configuration est faite.

La figure 4.3 suivante représente l'interface CLI du Packet Tracer :



```
Physical  Config  CLI  Attributes
IOS Command Line Interface
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 15.1(4)M4
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stgrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
2 FastEthernet interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

FIGURE 4.3 – Le CLI

4.5 CREATION ET CONFIGURATION DES NOUVEAUX RESEAUX

4.5.1 Création

Cette phase consiste à la création de notre infrastructure (Routeur, Switch, PC, Serveur, téléphone et Camera) comme la montre la figure 4.4 ci-dessous :

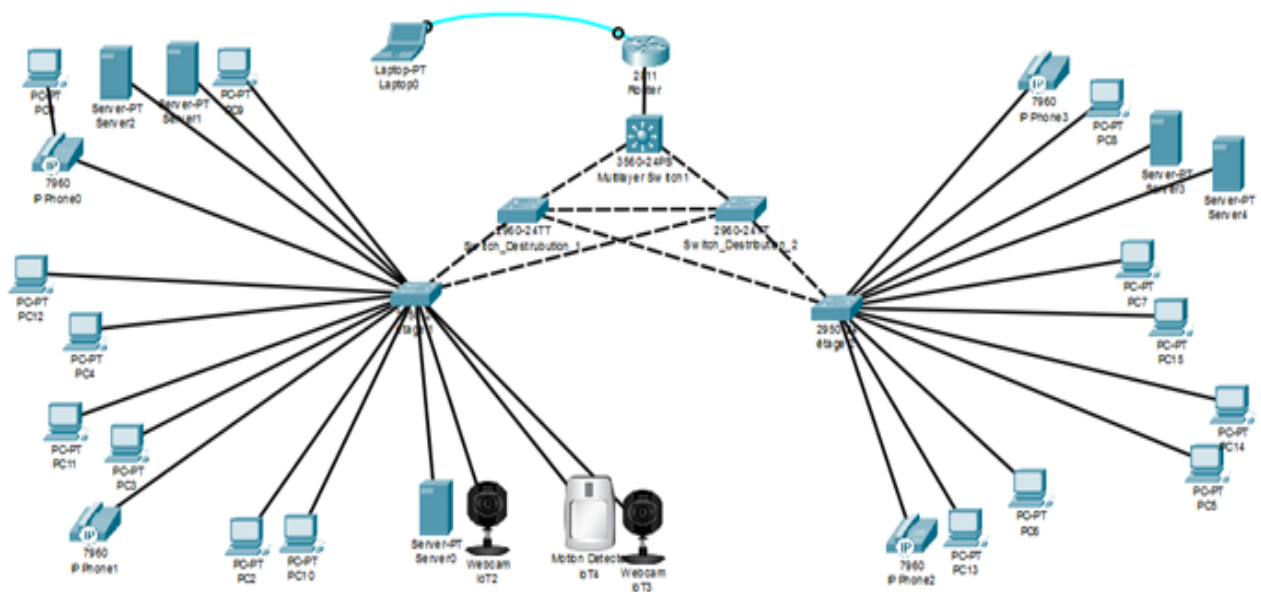


FIGURE 4.4 – Nouveau infrastructure

4.5.2 Configuration

Dans cette étape, nous allons configurer le nouveau réseau que nous avons crée pour qu'il fonctionne.

Avant de procéder à la configuration du réseau précédemment crée nous présentons tout d'abord notre plan d'adressage :

4.5.2.1 Plan d'adressage

La concession de distribution de Bejaia possède une adresse réseau de classe A qui est 10.45.0.0/19 (*masque réseau est 255.255.224.0*).

Pour des raisons de segmentation en VLANs, on a opté à diviser l'adresse réseau en 32 sous réseaux distincts du 10.45.0.x à 10.65.31.x, ce qui signifie que le nouvel adressage devient 10.45.0.0/24 (*masque réseau est 255.255.255.0*).

4.5.2.2 Configuration de base du Router et du Switch

— Configuration de base router

La configuration de base router est illustré dans la figure 4.5

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router
Router(config)#enable secret SONELGAZ
Router(config)#line console 0
Router(config-line)#password SONELGAZ
Router(config-line)#login
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#password SONELGAZ
Router(config-line)#login
Router(config-line)#exit
Router(config)#no ip domain-lookup
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

FIGURE 4.5 – Configuration de base router

— Configuration de base Switch

La configuration de base switch est illustré dans la figure 4.6

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch_Coeur
Switch_Coeur(config)#enable secret SONELGAZ
Switch_Coeur(config)#no ip domain-lookup
Switch_Coeur(config)#exit
Switch_Coeur#
%SYS-5-CONFIG_I: Configured from console by console

Switch_Coeur#
```

FIGURE 4.6 – Configuration de basse Switch

De la même façon le reste des Switch ont été configurés.

4.5.2.3 La configuration de protocole VTP sur les Switch

Pour le VTP On utilisera deux modes, « server et client ».

Nous allons configurer le Switch coeur en mode server le reste des Switch en mode client.

— Configuration du VTP en mode server sur Switch coeur

La configuration du VTP en mode server sur Switch coeur est illustré dans la figure 4.7

```
Switch_Coeur>en
Password:
Switch_Coeur#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Coeur(config)#vtp mode server
Device mode already VTP SERVER.
Switch_Coeur(config)#vtp version 2
Switch_Coeur(config)#vtp domain SONELGAZ
Changing VTP domain name from NULL to SONELGAZ
Switch_Coeur(config)#vtp password bejaia06
Setting device VLAN database password to bejaia06
Switch_Coeur(config)#exit
Switch_Coeur#
%SYS-5-CONFIG_I: Configured from console by console

Switch_Coeur#
```

FIGURE 4.7 – Configuration du VTP en mode server sur Switch coeur

— Configuration du VTP en mode client sur Switch Etage1

La configuration du VTP en mode client sur Switch coeur est illustré dans la figure 4.8

```
Switch_distribution_1>en
Password:
Switch_distribution_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch_distribution_1(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_distribution_1(config)#vtp domain SONELGAZ
Domain name already set to SONELGAZ.
Switch_distribution_1(config)#vtp password bejaia06
Setting device VLAN database password to bejaia06
Switch_distribution_1(config)#exit
Switch_distribution_1#
%SYS-5-CONFIG_I: Configured from console by console

Switch_distribution_1#
```

FIGURE 4.8 – Configuration du VTP en mode client sur Switch Etage1

De la même façon le reste des Switch ont été configurés.

4.5.2.4 Création des VLANs

Le tableau 4.1 suivant présente les différents VLANs créés :

VLAN	Nom	Adresse
vlan10	Service informatique	10.45.10.1
vlan11	Rez-de-chaussée	10.45.11.1
vlan12	Etage 01	10.45.12.1
vlan13	Etage 02	10.45.13.1
vlan14	Téléphony IP	10.45.14.1
vlan15	Caméra de surveillance	10.45.15.1

TABLE 4.1 – Les VLANs

La création des VLANs est faite au niveau des commutateurs multifonctions (*serveur VTP*) comme le montre la figure 4.9 :

— Création des VLANs au niveau du Switch cœur

```
Switch_Coeur>en
Password:
Switch_Coeur#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Coeur(config)#vlan 10
Switch_Coeur(config-vlan)#name Service_Informatique
Switch_Coeur(config-vlan)#exit
Switch_Coeur(config)#vlan 11
Switch_Coeur(config-vlan)#name Rez_De_Chausee
Switch_Coeur(config-vlan)#exit
Switch_Coeur(config)#vlan 12
Switch_Coeur(config-vlan)#name Etage_01
Switch_Coeur(config-vlan)#exit
Switch_Coeur(config)#vlan 13
Switch_Coeur(config-vlan)#name Etage_02
Switch_Coeur(config-vlan)#exit
Switch_Coeur(config)#vlan 14
Switch_Coeur(config-vlan)#name Telephony_Ip
Switch_Coeur(config-vlan)#exit
Switch_Coeur(config)#vlan 15
Switch_Coeur(config-vlan)#name Camera_De_Surveillance
Switch_Coeur(config-vlan)#exit
Switch_Coeur(config)#exit
Switch_Coeur#
%SYS-5-CONFIG_I: Configured from console by console
Switch_Coeur#
```

FIGURE 4.9 – Création des VLANs au niveau du Switch cœur

Automatiquement les vlan seront crier dans les autres Switch grâce au protocole VTP.

4.5.2.5 Configuration des ports (agrégation)

— Configuration des liens Trunk

Les interfaces des équipements d'interconnexion à configurer en mode trunk, toutes situées entre l'ensemble des switchs d'accès et le switch Coeur.

Les commandes suivantes nous permettent d'associer un port à un VLAN en mode trunk.

La commande "range" permet de réunir toutes les interfaces en une seule fois comme illustré la figure 4.10 :

```
Switch_Coeur>en
Password:
Switch_Coeur#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Coeur(config)#interface range fastethernet 0/1-3
Switch_Coeur(config-if-range)#switchport mode trunk
```

FIGURE 4.10 – Configuration des liens Trunk

— **Attribution des ports de commutateurs au VLANs**

C'est au niveau de chaque switch d'accès que les ports vont être assignés aux différents VLANs existants, chaque port d'un switch appartiendra à un VLAN donné.

Les commandes suivantes nous permettent d'associer un port à un VLAN en mode Accès comme illustré la figure 4.11 :

```
Switch_Etage_01>en
Password:
Switch_Etage_01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Etage_01(config)#interface range fastethernet 0/3-6
Switch_Etage_01(config-if-range)#switchport acces vlan 10
Switch_Etage_01(config-if-range)#exit
Switch_Etage_01(config)#interface range fastethernet 0/7-8
Switch_Etage_01(config-if-range)#switchport acces vlan 11
Switch_Etage_01(config-if-range)#exit
Switch_Etage_01(config)#interface range fastethernet 0/9-11
Switch_Etage_01(config-if-range)#switchport acces vlan 12
Switch_Etage_01(config-if-range)#exit
Switch_Etage_01(config)#interface range fastethernet 0/12-13
Switch_Etage_01(config-if-range)#switchport acces vlan 13
Switch_Etage_01(config-if-range)#exit
Switch_Etage_01(config)#interface range fastethernet 0/14-17
Switch_Etage_01(config-if-range)#switchport acces vlan 15
Switch_Etage_01(config-if-range)#exit
Switch_Etage_01(config)#end
Switch_Etage_01#
%SYS-5-CONFIG_I: Configured from console by console
Switch_Etage_01#
```

FIGURE 4.11 – Attribution des ports de commutateurs au VLANs

4.5.2.6 Configuration des sous interfaces

Dans cette partie on va permettre aux VLANs créés de communiquer entre eux en appliquant sur le routeur la méthode «router-on-a-stick »(*création d'une sous interface pour chaque VLAN*) en suivant les commandes illustrées dans la figure 4.12 suivante :

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.45.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, ch

Router(config-if)#exit
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10,

Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.45.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.11
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.11,

Router(config-subif)#encapsulation dot1Q 11
Router(config-subif)#ip address 10.45.11.1 255.255.255.0
Router(config-subif)#exit
Router(config)#.....|
    
```

FIGURE 4.12 – Configuration des sous interface

4.5.2.7 Configuration du DHCP

Afin de simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise le protocole DHCP qui permet de configurer les paramètres de réseaux clients, au lieu de les configurer sur chaque ordinateur client. La figure 4.13 illustre les commandes qui nous permettent de configurer ce protocole au niveau du serveur.

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool vlan10
Router(dhcp-config)#network 10.45.10.0 255.255.255.0
Router(dhcp-config)#default-router 10.45.10.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan11
Router(dhcp-config)#network 10.45.11.0 255.255.255.0
Router(dhcp-config)#default-router 10.45.11.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan12
Router(dhcp-config)#network 10.45.12.0 255.255.255.0
Router(dhcp-config)#default-router 10.45.12.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan13
Router(dhcp-config)#network 10.45.13.0 255.255.255.0
Router(dhcp-config)#default-router 10.45.13.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan14
Router(dhcp-config)#network 10.45.14.0 255.255.255.0
Router(dhcp-config)#default-router 10.45.14.1
Router(dhcp-config)#option 150 ip 10.45.14.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan15
Router(dhcp-config)#network 10.45.15.0 255.255.255.0
Router(dhcp-config)#default-router 10.45.15.1
Router(dhcp-config)#exit
Router(config)#

```

FIGURE 4.13 – Configuration du DHCP

4.5.2.8 Configuration de protocole STP

La figure 4.14 illustre les différentes commandes utilisées pour configurer le protocole STP

```

Switch_Coeur>en
Password:
Switch_Coeur#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Coeur(config)#spanning-tree mode rapid-pvst
Switch_Coeur(config)#spanning-tree vlan 10 root primary
Switch_Coeur(config)#spanning-tree vlan 11-15 root secondary
Switch_Coeur(config)#exit
Switch_Coeur#
%SYS-S-CONFIG_I: Configured from console by console
Switch_Coeur#

```

FIGURE 4.14 – Configuration du STP

4.5.2.9 Configuration de la voix IP

Nous avons configuré la voie IP au niveau du routeur comme le montre la figure 4.15 :

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#telephony-service
Router(config-telephony)#max-ephone 40
Router(config-telephony)#max-dn 40
Router(config-telephony)#ip source-address 10.45.14.1 port 2000
Router(config-telephony)#auto assign 1 to 40
Router(config-telephony)#ephone-dn 1
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 1.1,
Router(config-ephone-dn)#number 1001
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 2.1,

Router(config-ephone-dn)#number 1002
Router(config-ephone-dn)#ephone-dn 3
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 3.1,

Router(config-ephone-dn)#number 1003
Router(config-ephone-dn)#ephone-dn 4
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 4.1,

Router(config-ephone-dn)#number 1004
Router(config-ephone-dn)#ephone-dn 5
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 5.1,

Router(config-ephone-dn)#number 1005
Router(config-ephone-dn)#.....
    
```

FIGURE 4.15 – Configuration du la voie IP

4.5.2.10 Configuration des caméras de surveillance

Pour la configuration des caméras de surveillance, nous avons crée et configuré un serveur comme le montre les figures 4.16, 4.17, 4.18, 4.19, 4.20, 4.21 ci-dessous :

— Configuration du serveur

1. Configurer l'adresse IP (voir figure 4.16)

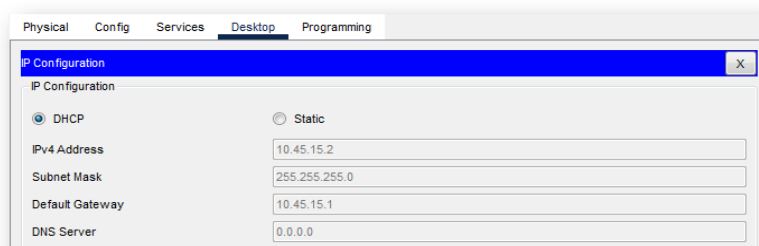


FIGURE 4.16 – Configuration de l'adresse IP

2. Création d'un compte IOT² (voir figures ci-dessous)

Les figures 4.17, 4.18, 4.19, 4.20, 4.21 ci-dessous illustre les différentes étapes de la création d'un compte «Iot».

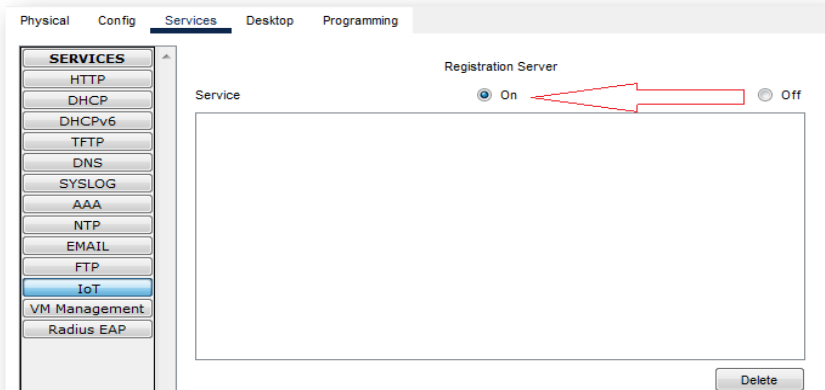


FIGURE 4.17 – Étape 1 de création d'un compte de IOT

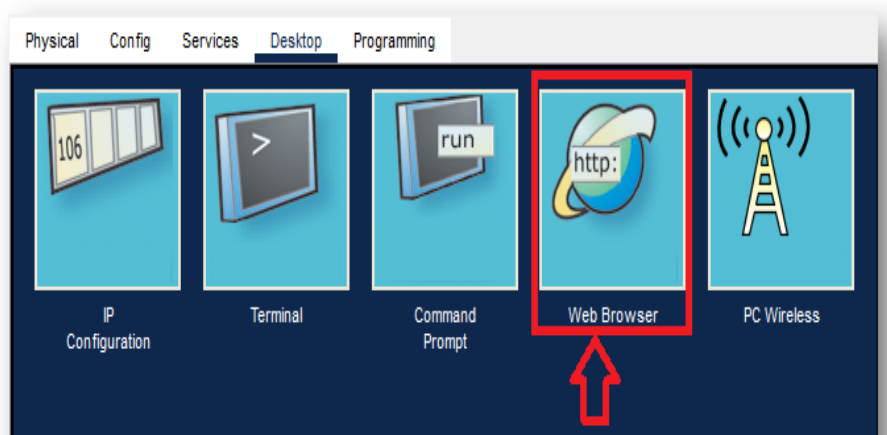


FIGURE 4.18 – Étape 2 de création d'un compte de IOT

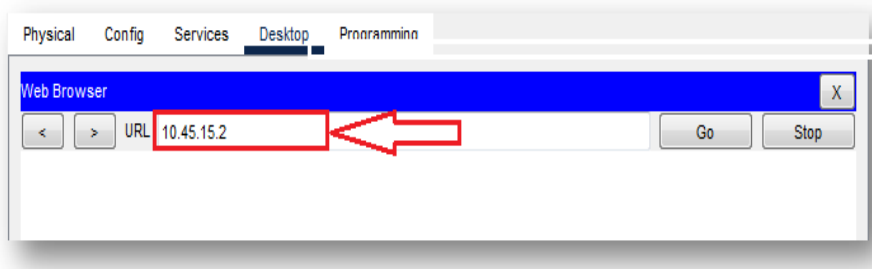


FIGURE 4.19 – Étape 3 de création d'un compte de IOT

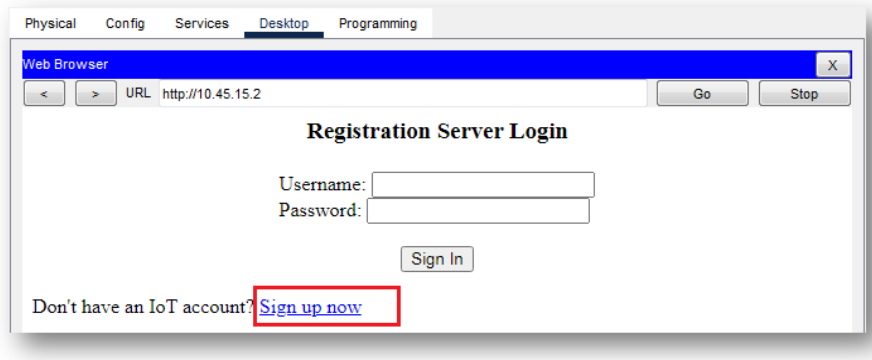


FIGURE 4.20 – Étape 4 de création d’un compte de IOT

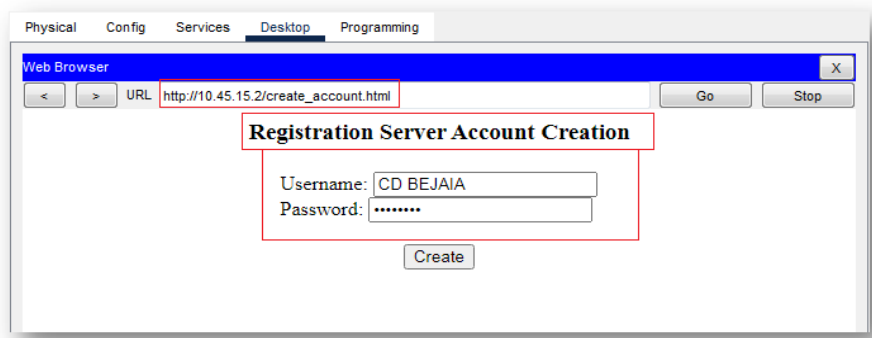


FIGURE 4.21 – Étape 5 de création d’un compte de IOT

— **Configuration des caméras**

Après avoir terminer la configuration de notre serveur nous passons à la configuration de nous cameras en suivant les étapes illustrés sur les figures 4.22, 4.23 ci-dessous :

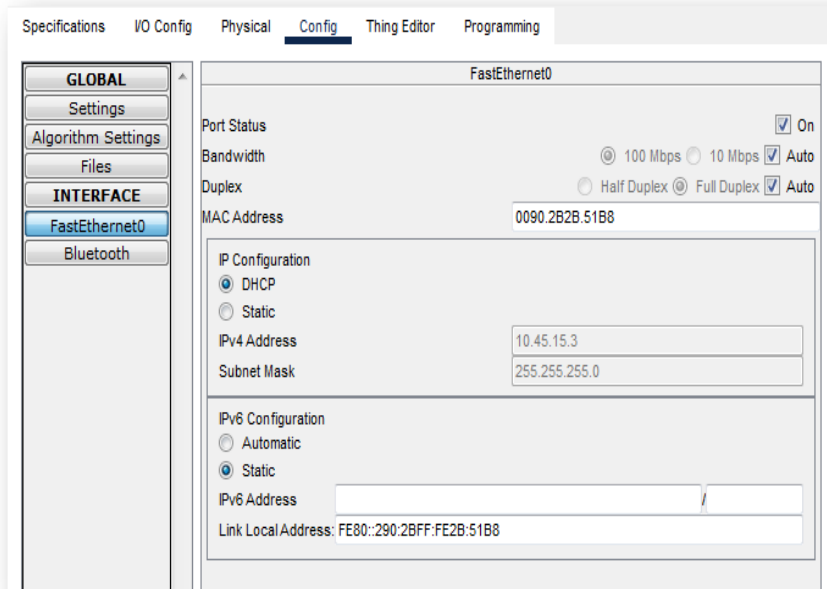


FIGURE 4.22 – Étape (a) de la configuration des cameras

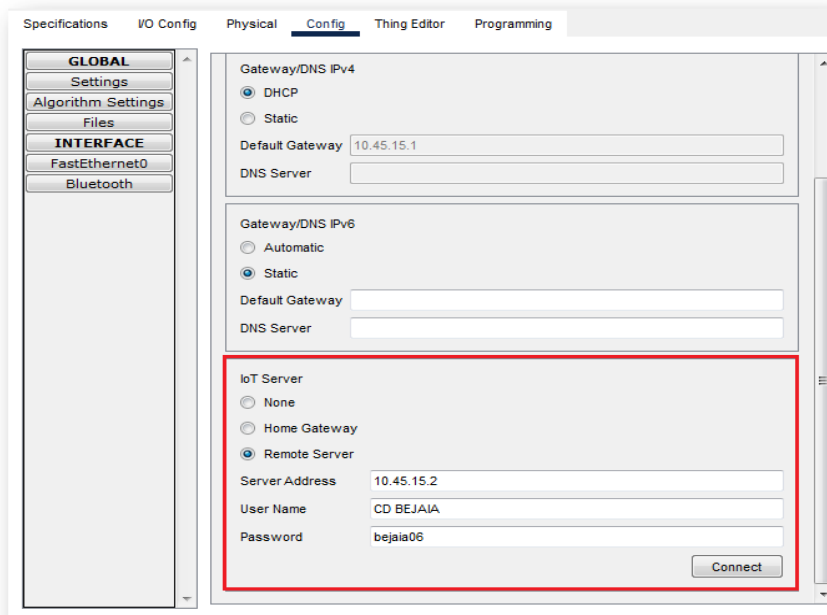


FIGURE 4.23 – Étape (b) de la configuration des cameras

4.6 TEST ET VALIDATION DE LA CONFIGURATION

Dans cette partie nous avons vérifié la configuration de tous les équipements à l'aide des commandes de vérification.

4.6.1 Contrôle de la bonne configuration du protocole VTP

4.6.1.1 Contrôle du VTP serveur

Pour contrôler la configuration du protocole VTP, nous utilisons la commande *"show VTP status"* sur le Switch Multilayer, (voir la figure 4.24) ci-dessous :

```
Switch_Coeur#show vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : SONELGAZ
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0050.0F47.8B00
Configuration last modified by 0.0.0.0 at 3-1-93 00:34:58
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 11
Configuration Revision  : 0
MD5 digest              : 0xF6 0x2F 0x44 0x03 0x66 0x98 0xB9 0x42
                       : 0xCE 0xFC 0x13 0x12 0x2C 0x10 0x44 0xD1
Switch_Coeur#
```

FIGURE 4.24 – Contrôle du VTP serveur

4.6.1.2 Contrôle du VTP client

A fin de contrôler la configuration du protocole VTP, nous utilisons la commande *"show VTP statu"* sur le Switch distribution, (voir figure 4.25) .

```

Switch_distribution_1#show vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : SONELGAZ
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 0001.6431.4800
Configuration last modified by 0.0.0.0 at 3-1-93 00:34:58

Feature VLAN :
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 11
Configuration Revision  : 0
MD5 digest              : 0xF6 0x2F 0x44 0x03 0x66 0x98 0xB9 0x42
                        : 0xCE 0xFC 0x13 0x12 0x2C 0x10 0x44 0xD1
Switch_distribution_1#
    
```

FIGURE 4.25 – Contrôle du VTP client

4.6.2 Contrôle des réseaux locaux virtuels créés sur le switch serveur

Après avoir créé les VTP nous allons passer à la vérification de la distribution des VLANs dans les switches clients, nous nous sommes servis de la commande "*show vlan brief*" , (voir la figure 4.26).

```

Switch_Etage_01#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                Gig0/2
10   Service_Informatique    active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
11   Rez_De_Chausee         active    Fa0/7, Fa0/8
12   Etage_01               active    Fa0/9, Fa0/10, Fa0/11
13   Etage_02               active    Fa0/12, Fa0/13
14   Telephony_Ip           active
15   Camera_De_Surveillance active    Fa0/14, Fa0/15, Fa0/16, Fa0/17
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
    
```

FIGURE 4.26 – Contrôle des VLANs créé

4.6.3 Vérification du routage inter VLAN

A l'aide de la commande *"show IP interface brief"*, nous pouvons vérifier l'attribution des adresses IP sur les VLANs, (voir la figure 4.27).

```
Router#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    10.45.0.1       YES manual up          up
FastEthernet0/0.10 10.45.10.1      YES manual up          up
FastEthernet0/0.11 10.45.11.1      YES manual up          up
FastEthernet0/0.12 10.45.12.1      YES manual up          up
FastEthernet0/0.13 10.45.13.1      YES manual up          up
FastEthernet0/0.14 10.45.14.1      YES manual up          up
FastEthernet0/0.15 10.45.15.1      YES manual up          up
```

FIGURE 4.27 – Vérification du routage inter VLAN

4.6.4 Vérification de la distribution des adresses IP sur le serveur DHCP

Il est possible de vérifier que chaque poste a bien récupéré une adresse DHCP à l'aide de la command *"show ip DHCP binding"*, (voir la figure 4.28).

```
Router>en
Password:
Router#show ip dhcp binding
IP address          Client-ID/
                   Hardware address
10.45.10.6           00D0.BCA0.8D33
10.45.10.9           0060.5C43.10CE
10.45.10.2           0060.47BC.A837
10.45.10.5           000C.8589.DA6C
10.45.10.7           00E0.A31D.4E86
10.45.10.8           00E0.F91D.B80D
10.45.10.10          0010.1150.4B28
10.45.11.5           00D0.FFA7.CB4B
10.45.11.6           0000.0CE2.2EDD
10.45.11.7           00E0.8F74.0934
10.45.11.2           000C.85ED.98C0
10.45.12.5           0060.2F8A.30D0
10.45.12.6           0009.7C45.2C73
10.45.12.7           0002.1716.A04C
10.45.12.8           0001.97D8.9608
10.45.13.3           0006.2AAD.2297
10.45.13.5           00D0.FFCD.032E
10.45.13.6           0003.E499.7BC1
10.45.13.7           0010.1112.BCE2
10.45.15.4           000A.41B7.980E
--More--
```

FIGURE 4.28 – Vérification de la distribution des adresses IP

4.6.5 Vérification des adresses IP des machines attribuées par le DHCP

La figure 4.29 montre l'attribution des adresses IP par le DHCP.

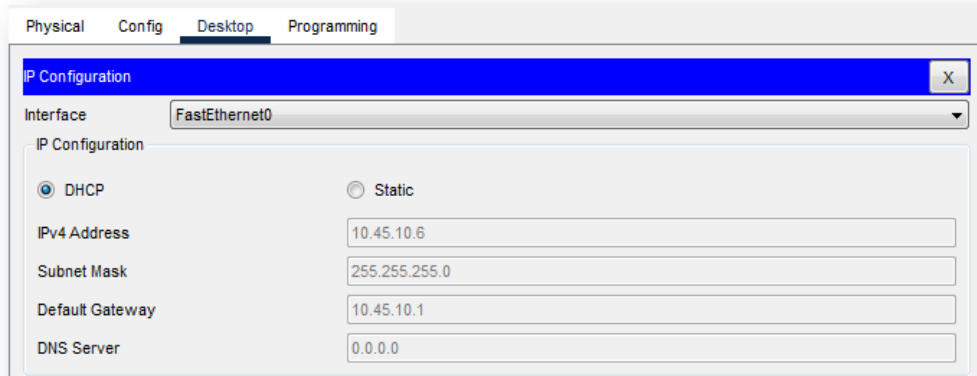


FIGURE 4.29 – Vérification de la distribution des adresses IP des PC

4.6.6 Vérification de la communication entre les machines

4.6.6.1 Test des différents VLANs sur un même commutateur entre différents équipements

A ce stade, vérifiant l'accessibilité des différents équipements dans un même réseau mais dans deux VLANs distincts.

La figure 4.30 illustre le succès du test effectué entre les différents VLANs sur un même commutateur.

```

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.45.11.5

Pinging 10.45.11.5 with 32 bytes of data:

Reply from 10.45.11.5: bytes=32 time=10ms TTL=127
Reply from 10.45.11.5: bytes=32 time=10ms TTL=127
Reply from 10.45.11.5: bytes=32 time=10ms TTL=127
Reply from 10.45.11.5: bytes=32 time=10ms TTL=127

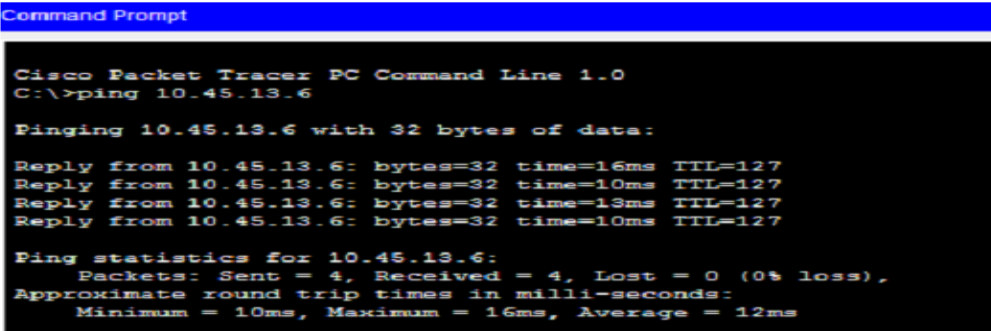
Ping statistics for 10.45.11.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms
    
```

FIGURE 4.30 – Ping entre deux machines

4.6.6.2 Test des différents VLANs sur différents commutateur entre différents équipements

Nous allons maintenant vérifier l'accessibilité des équipements qui sont pas du même VLAN et qui sont situés dans un réseau local distinct.

La figure 4.31 illustre le succès du test effectué entre deux machines qui se trouvent dans des VLANs et des commutateurs d'accès différents.



```
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.45.13.6

Pinging 10.45.13.6 with 32 bytes of data:

Reply from 10.45.13.6: bytes=32 time=16ms TTL=127
Reply from 10.45.13.6: bytes=32 time=10ms TTL=127
Reply from 10.45.13.6: bytes=32 time=13ms TTL=127
Reply from 10.45.13.6: bytes=32 time=10ms TTL=127

Ping statistics for 10.45.13.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 16ms, Average = 12ms
```

FIGURE 4.31 – Ping entre deux machines

4.6.7 Test de la téléphonie IP

Nous allons dans ce qui suit tester la téléphonie en appelant du téléphone (1001) qui se situe au niveau du VLAN10 vers le téléphone (1003) du VLAN13.

La figure 4.32 illustre le succès du test.



FIGURE 4.32 – Test de la téléphonie IP

4.6.8 Test des cameras de surveillance

En allant sur le compte déjà créé sur le serveur nous remarquons bien que les cameras vérifiez affichent comme le montre la figure 4.33 ci-dessous :

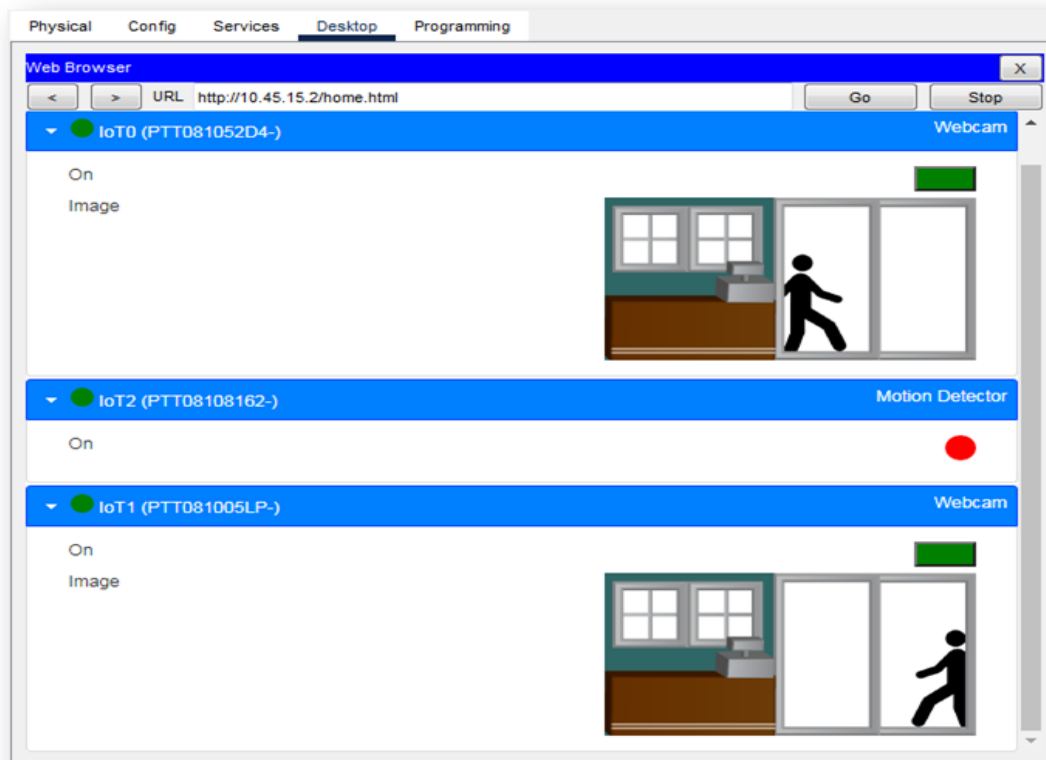


FIGURE 4.33 – Test des cameras de surveillance

4.7 CONCLUSION

Dans ce chapitre, nous avons présenté l'architecture du réseau existant et nous avons exposé les différents problèmes et insuffisances au niveau de ce réseau. De plus, nous avons proposé une nouvelle architecture pour remédier à ces insuffisances et ces problèmes.

Pour la réalisation de la solution proposée, nous avons commencé par la présentation du simulateur « Cisco Packet Tracer ». Ainsi que l'ensemble des configurations réalisées au niveau de notre architecture à savoir les routeurs et les commutateurs.

De plus, nous avons créé les différents VLANs nécessaires pour la mise en marche de notre architecture. Pour valider notre solution nous avons effectué un ensemble de tests et de vérification afin de prouver l'efficacité du réseau proposé.



CONCLUSION GÉNÉRALE

Ce mémoire s'inscrit dans le cadre d'un projet de fin d'étude. Il aboutit à l'implémentation d'une solution réseau LAN hiérarchique à trois niveaux au profit de la C.D Bejaia.

Dans ce présent travail, nous avons présenté premièrement l'organisme d'accueil de l'entreprise, puis quelques concepts sur les généralités des réseaux informatiques. Pour apporter une solution au différents problèmes du réseau existant du CD Bejaia, une étude de l'existant réseau informatique de l'entreprise S.A.D.E.G/CD. Bejaia a été faite pour recenser toutes ses insuffisances et ces problèmes. Finalement, nous avons présenté toutes les phases nécessaires à la réalisation de l'architecture réseau proposée au sein de l'entreprise en illustrant les configurations nécessaires au niveau des VLANs et les différents équipements du réseau.

Le réseau LAN hiérarchique à trois niveaux présente de nombreux avantages, mais il doit néanmoins relever de nombreux défis et pallier certaines difficultés techniques notamment la qualité de service. Malgré ses inconvénients, le réseau hiérarchique à trois niveaux reste une bonne solution qui nous permet de :

- Supprimer les contraintes physiques relatives aux communications d'un groupe de travail.
- Coût réduit.
- Modifier facilement la configuration LAN.
- Contrôler facilement le trafic réseau.
- Domaines de diffusion plus petits.
- Efficacité de gestion.
- Création de groupes de travail indépendamment de l'infrastructure physique.
- Une meilleure utilisation des serveurs réseaux.

CONCLUSION GÉNÉRALE

- L'augmentation considérable des performances du réseau.
- Le renforcement de la sécurité du réseau.

Ce projet a été une expérience fructueuse qui nous a permis de mieux s'approcher du milieu professionnel. Ça nous a permis de savoir comment gérer et optimiser le temps dans le but d'en profiter au maximum.

En guise de perspectives, nous envisageons d'implémenter d'autres protocoles afin de renforcer la sécurité de réseau de l'entreprise.



BIBLIOGRAPHIE

- [1] <https://www.sonelgaz.dz/fr>, consulté le 20 Août 2022.
- [2] A.PHILIPPE. "Réseaux informatiques", notions fondamentales, 2eme Edition, ENI Editions, 2006.
- [3] P.JAQUET. "Les réseaux et l'informatique de l'entreprise", Edition Lavoisier, 2003.
- [4] <https://cisco.goffinet.org/ccna/fondamentaux/modeles-tcp-ip-osi/>, consulté le 25 Aout 2022.
- [5] O.Salma. "Analyse de la robustesse et des améliorations potentielles du protocole Radio Fréquences Sub-GHz KNX utilisé pour l'IoT domotique", Université de Limoges, France, thèse doctorat, 2016.
- [6] <https://www.samomoi.com/reseauxinformatiques/lesprincipauxcomposantdinterconnexion.php>, consulté, le 28 Aout 2022.
- [7] H.GILBERT. "Les réseaux locaux virtuels", Edition InterEditions, 1998.
- [8] <https://www.cisco.goffinet.org/ccna/vlans/concepts-vlan-cisco/>, consulté le 01 Septembre 2022.
- [9] https://www.cisco.com/c/fr_ca/support/docs/lan-switching/8021q/8758-43.html, consulté le 02 Septembre 2022.
- [10] J-F.PILLOU. "Tous sur les réseaux et Internet", Edition Dunod, Paris, 2006.
- [11] www.cisco.ofppt.info/ccna2/course/module3/3.1.1.3/3.1.1.3.html, consulté le 03 Septembre 2022.
- [12] <http://www-igm.univ-mlv.fr/dr/XPOSE2006/SURZUR-DEFRANCE/vlan.html>
- [13] <https://www.formip.com/dtp/>, consulté le 03 Septembre 2022.

[14] A.VAUCAMPS. "Cisco CCNA", ENI édition, 2010.

[15] <https://www.openspacecourse.com/le-protocole-stp/>, consulté le 04 Septembre 2022.

[16] J-L.MONTAGIER. "Réseau d'entreprise par la pratique", EYROLLES Edition, 2007.

[17] <https://www.inetdoc.net/articles/lan-segmentation/lan-segmentation.modele-hierarchique.html>, consulté le 04 Septembre 2022.



Résumé

La flexibilité d'un réseau local est un paramètre très important auquel toute organisation doit faire face compte tenu de son évolution. A cet effet, afin de gérer au mieux l'extensibilité de son réseau et apporter plus d'agilité dans sa gestion, plusieurs techniques et concepts sont apparus tel que les VLANs.

Dans notre projet, nous nous sommes intéressés à l'amélioration de l'architecture du réseau de l'entreprise « SONELGAZ BEJAIA », en proposant une autre architecture du réseau à trois niveaux qui répond à la mise en place des VLANs.

Les Switch placés en cascades et le câblage réseau qui est réalisé d'une façon non étudiée à l'intérieur de la CD de Bejaia peuvent entraîner des problèmes de lourdeur, de boucles, de congestion et de maintenance. Et, peuvent générer une latence au niveau de chaque switch concernant la recherche dans les tables MAC.

Ainsi, ces switch placé en cascades peuvent entraîner des difficultés de mettre en place des procédures de sécurité. Pour palier à tous ces problèmes nous avons proposé une solution permettant de créer des groupes de travail indépendants de l'infrastructure physique et d'avoir des domaines de diffusions plus petits, ce qui nous aide à modifier facilement la configuration LAN et contrôler facilement le trafic réseau. Ainsi, cette solution conduit à une augmentation significative des performances du réseau et à une sécurité améliorée.

La mise en oeuvre de la solution et les simulations en utilisant le simulateur Cisco ont prouvé que la solution a bien répondu aux insuffisances du réseau existant.

Mot clés : Réseau local, VLAN, Simulation, Packet Tracer, MAC, LAN.



Abstract

The flexibility of a local network is a very important parameter that any organisation must face in view of its evolution. To this end, in order to better manage the scalability of its network and bring more agility in its management, several techniques and concepts have emerged such as VLANs.

In our project, we focused on improving the network architecture of the company SONELGAZ BEJAIA, by proposing another Three-tier architecture that meets the implementation of VLANs.

Switches placed in cascades and network cabling that is carried out in a way not studied inside the Bejaia CD can cause problems of heaviness, loops, congestion and maintenance. And, can generate latency at the level of each switch regarding the search in the MAC tables. Thus, these switches placed in cascades can cause difficulties to set up security procedures. To overcome all these problems we proposed a solution that would allow for independent working groups of the physical infrastructure and to have smaller areas of dissemination, This helps us to easily change the LAN configuration and control network traffic. Thus, this solution leads to a significant increase in network performance and improved security.

The implementation of the solution and the simulations using the Cisco simulator have proven that the solution has successfully addressed the deficiencies of the existing network.

Keywords : LAN, VLAN, Simulation, Packet Tracer, MAC, LAN.