الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
المركز الجامعي لعين تموشنت
Centre Universitaire Belhadj Bouchaib d'Ain-Temouchent
Institut de Technologie
Département de Génie Electrique

Projet de fin d'études
Pour l'obtention du diplôme de Master en :
Domaine : SCIENCE ET TECHNOLOGIE
Filière : TELECOMMUNICATION
Spécialité : Réseau et Télécommunication

Thème

Configuration d'un réseau LAN-WAN avec prise en charge de la QoS (VoIP) et la sécurité (Chap, ACL, VPN)

Présenté Par :
1) HASSANE Samia.
2) RAOUD Mama.

Devant les jurys composés de :

Mr. Mohammed Mourad BENOSMAN	MCB	C.U.B.B (Ain Temouchent)	Président
Mme. Zohra ABDLMALEK	MCA	C.U.B.B (Ain Temouchent)	Encadrant
Mr. Abdelfatih BENGANA	MCB	C.U.B.B (Ain Temouchent)	Examinateur

Année universitaire 2018/2019

Dédicace

A la raison de ma vie, mes chers parents,
Que je dédie ce modeste travail et à qui j'exprime mon ultime amour et ma profonde reconnaissance pour leurs patiences, leurs bénédictions, leurs sacrifices et leurs soutiens.
A ma chère sœurs Naouel, mes frères Sid Ahmed, Abdelaziz et Yoycef, à mon adorable bien aimée ma nièce Nihel
A mon binôme Mama RAOUD et sa tendre famille
J'exprime mes sincères remerciements, ma profonde gratitude.
A mes encadrant Dr. Zohra ABDELMALEK et Dr. Mohammed DEBBAL Pour les efforts déployés et le temps qu'ils m'ont consacré.
A Tous Ceux Qui m'ont aidé de près ou de loin par un mot, un geste, un soutien dont je leur suis reconnaissant.

HASSANE Samia

A la raison de ma vie, mes chers parents,
Que je dédie ce modeste travail et à qui j'exprime mon ultime amour et ma profonde reconnaissance pour leurs patiences, leurs bénédictions, leurs sacrifices et leurs soutiens.
A mes sœurs Asmaa et Hiba, à ma famille
A mon binôme Samia HASSANE et sa tendre famille
J'exprime mes sincères remerciements, ma profonde gratitude.
A mes encadrant Dr. Zohra ABDELMALEK et Dr. Mohammed DEBBAL Pour les efforts déployés et le temps qu'ils m'ont consacré.
A Tous Ceux Qui m'ont aidé de près ou de loin par un mot, un geste, un soutien dont je leur suis reconnaissant.

RAOUD Mama

Remerciements

Nous voudrons remercier ALLAH le tout puissant qui nous a donné le courage et la patience pour faire ce modeste travail.

Nous tenons à exprimer notre reconnaissance à monsieur ***BENOSMAN Mourad M.*** d'avoir accepté de présider ce jury. Egalement, nous somme très reconnaissantes à monsieur ***BENGANA Abdelfatih*** qui a bien voulu témoigner son intérêt pour ce travail en tant qu'examinateur.

Nous exprimons notre gratitude à notre encadreur, madame ***ABDELMALEK Zohra***, pour la confiance et la patience qu'elle nous a témoigné, et pour toutes les idées et les conseils qu'elle a partagé avec nous.

Nous tenons à remercier notre co-encadreur Monsieur ***DEBBAL.M*** pour son aide et sa patience.

Finalement, nos remerciements vont aussi à tous nos enseignants qui ont participé à notre formation, ainsi qu'à toutes les personnes qui nous ont aidés, de près ou de loin, pour faire ce modeste travail.

Résumé :

Dans les entreprises dont les services reposent en grande partie sur leur système informatique, la performance du réseau et la haute disponibilité des différents services applicatifs sont primordiaux.

L'objectif de ce travail est de réussir à mettre en œuvre une architecture réseau opérationnel pour une entreprise quelconque possédant plusieurs sites distants afin de gérer et sécuriser au mieux les communications entre ces derniers.

Ce projet s'intéresse à une étude de cas d'un réseau LAN-WAN avec prise en charge de la QoS (VoIP) et la sécurité (PPP CHAP, PPPoE, SSH, VPN).

Les configurations et les tests de validation sont conduits sous l'environnement de simulation Cisco Packet Tracer.

Mots clés **:** VLAN, VTP, Spaning Tree, VPN, IPsec, SSH, PPPoE.

Abstract :

In companies whose services rely largely on their computer system, the performance of the network and the high availability of the various application services are paramount.

The goal of this work is to successfully implement operational network architecture for any company with several remote sites to manage and secure the communications between them.

This project focuses on a case study of a LAN-WAN network with support for QoS (VoIP) and security (Chap, ACL, VPN).

Configuration and validation tests are conducted under the Cisco Packet Tracer simulation environment.

Key words: VLAN, VTP, Spaning Tree, VPN, IPsec, SSH, PPPoE.

ملخص:

في الشركات التي تعتمد خدماتها بشكل كبير على نظام الإعلام الآلي الخاص بهم، يعتبر أداء الشبكة والتوفير العالي لمختلف الخدمات التطبيقية أمر بالغ الأهمية.

الهدف من هذا العمل هو التنفيذ النجاح لبنية شبكة ذات فعالية لأي شركة كانت لها عدة مواقع بعيدة من أجل إدارة الاتصالات وتأمينها بشكل أفضل.

جاء هدا المشروع لدراسة حالة لشبكةLAN-WAN مع دعم جودة الخدمة (VoIP) والأمن (PPP CHAP, PPPoE, SSH et VPN).

من أجل تنفيذ هذا المشروع والتحقق من فعاليته قمنا باستعمال برنامج Cisco Packet Tracer.

الكلمات الرئيسية: PPPoE, SSH, ipSEC, VPN, Spaning Tree, VTP, VLAN .

Table des matières

CHAPITRE II

Configuration de la QoS pour un déploiement de VOIP

CHAPITRE III

Technologie WAN et Sécurité

CHAPITRE IV

Configuration

Liste des figures

Figure **page**

Figure **page**

Figure **page**

Liste des tableaux

Acronymes

AH	Authentication Header
ACL	Access Control List
AP	Access Point
AR	Access router
CFI	Canonical Format Indicator
CPE	Customer Premise Equipment
CoS	Class of Service
DHCP	Dynamic Host Configuration Protocol
DCE	DCE
DLCI	Data Link Connection Identifiers
DiffServ	Differentiated Services
DSCP	Differentiated Service Code Point
DTE	Data Terminal Equipment
CRC	Cyclic Redundancy check
CHAP	Challenge Handshake Authentication Protocol
ESP	Encapsulation Security Payload
FIFO	First In First Out
FTP	File Transfer protocol
FR	Frame Relay
FSI	Le Fonds Spécial Invalidité
FCS	Frame Check Sequence
IEEE	Institute of Electrical and Electronics Enginneers
IETF	Internet Enginering Task Force
IPBX	Private Branche Xchange
IOS	Organisation internationale de normalisation
IP	Internet Protocol
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS	Information Server
ISL	Inter Switch Link
L2	Layer 2

L3	Layer 3
LAN	Local Area Network
LCP	Link Control Protocol
MAC	Media Access Control
MLS	Multilayer Switching
MAP	Mobility Anchor Point
MLSP	MultiLayer Switching Protocol
MTU	Maximum Transmission Unit
NCP	Network Control Protocol
NSP	Name Server Protocol
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PPP	Protocole point-à-point
PPPoE	point-to-point protocol over Ethernet
PQ	Priority Queuing
PVC	Circuit virtuel permanent
QoS	Quality of Service
RSTP	Rapid SpanningTree Protocol
RTPC	Real time Transport Control Protocol
RFC	request for comment
RSH	Remote Shell
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree
ToS	Type of Service
TCP	Transport Control Protocol
TCI	Tag Control Information
TPID	Tag Protocol Identifier
TLS	Transport Layer Security
UDP	User Data Protocol
VLAN	Virtual Local Area Network
VTP	VLAN Trunking Protocol
VPN	Virtual Private Network
VPID	Vlan Protocol Identification
WFQ	Weighted Fair Queuing
WAN	Wide Area Network

Introduction générale

Introduction Générale

Depuis des années, la majorité des entreprises ont mis leurs ressources informatiques en réseau.

Un réseau est un ensemble d'éléments reliés entre eux et réglés de manière qu'ils puissent communiquer. C'est aussi simple que ça. Et les réseaux informatiques n'échappent pas à cette règle [1].

Un réseau informatique est un ensemble d'équipements informatiques reliés – disons plutôt interconnectés – entre eux et paramétrés de manière qu'ils puissent communiquer. L'intégration de la parole téléphonique et de la vidéo sur ces réseaux informatiques devient naturelle même si cela ne va pas sans difficulté [2].

Afin qu'on puisse éviter les risques des attaques, il faut impérativement garantir une sécurité du réseau informatique de l'entreprise et le rendre moins vulnérable [3].

Il existe différentes sortes de réseaux, en fonction de la taille, du débit des informations, des types de protocoles de communication, etc.

Les différents types de réseaux sont : les réseaux locaux (LAN), les réseaux locaux virtuels (VLAN), les réseaux métropolitains (MAN), les réseaux étendus (WAN), les réseaux privés (VPN) et les réseaux sans fil (wireless) [1].

Nous serons ainsi en mesure de réaliser un projet de conception d'un réseau d'entreprise avec une vision globale de la mise en réseau.

Pour bien mener ce travail, nous avons organisé notre mémoire en quatre chapitres structurés comme suit :

Nous aborderons dans le premier chapitre quelque notion théorique utile dans notre travail. D'abord, nous parlerons sur les Switch MLS et leurs fonctionnements. Ensuite nous évoquerons la technologie VLAN et en fin nous parlerons du protocole spaning tree.

Dans le deuxième chapitre, nous parlerons de la qualité service de la VOIP, son fonctionnement général ainsi sa configuration dans un réseau d'entreprise.

Nous donnerons en premier lieu, dans le troisième chapitre, une vue générale sur la technologie WAN, ensuite nous entamerons l'implémentation de la sécurité au niveau du réseau informatique d'une entreprise.

Dans le quatrième et dernier chapitre, nous allons enfin passer à la «Configuration», on premier lieu nous introduirons les outils et logiciels ayant servi à l'élaboration du projet, tout en expliquant les configurations, nous passerons ensuite au deuxième lieu qui sera consacrée à l'implémentation de la VOIP et la solution VPN grâce au protocole IPSec.

Enfin, dans la conclusion générale, nous ferons une récapitulation du travail effectué ainsi que l'expérience acquise.

CHAPITRE

Switch « MLS », technologie « VLAN » et protocole « STP »

Chapitre I : Switch « MLS », technologie « VLAN » et protocole « STP »

I.1/ Introduction :

Dans ce premier chapitre nous allons aborder brièvement quelques notions théoriques sur les réseaux locaux. D'abord, on commence par définir le réseau local virtuel. Ensuite on présente les équipements tels que le Switch MLS et les protocoles réseaux utilisaient (VTP, SpaningTree, RSTP..) dans un réseau d'entreprise.

I-2/ Définition d'un réseau Local :

Un réseau local est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux grâce à des lignes de communication et pouvant échanger des informations et partager des ressources dans une petite aire géographique par un réseau. [4]

I-3/ Model OSI :

La première évolution des réseaux informatiques a été des plus anarchiques, chaque constructeur développant presque sa propre technologie. Pour palier à cela, l'ISO (Institut de normalisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseau. Le modèle de référence OSI (Figure I-1) comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. Cette répartition des fonctions réseau est appelée organisation en couches [5].

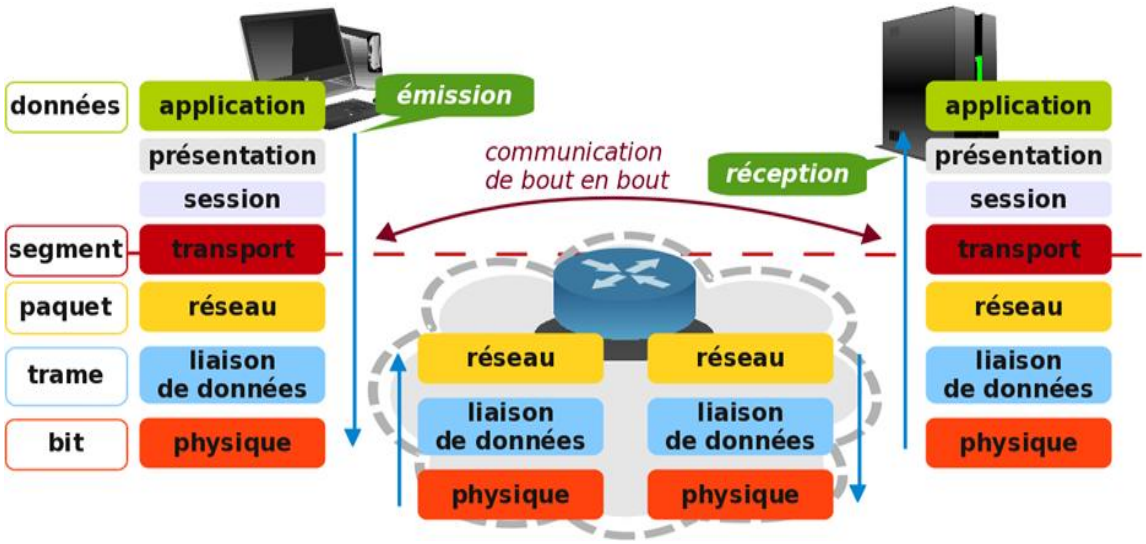


Figure I-1 : Modèle OSI

I-4/ Multilayer Switching (MLS):

La commutation multicouche (MLS) est une technologie de commutation de routeur basée sur Ethernet qui offre la commutation de couche 3 (L3) conjointement aux routeurs existants.

La technique MLS est utilisée pour accroître les performances du routage IP au moyen de commutation de paquets et des fonctions de réécriture basées sur le "Hardware".

La technique MLS peut être implémentée en utilisant un commutateur de couche 3 ou une topologie avec routeur externe [6].

I-4-1/ Fonctionnement MLS:

❖MLS utilise trois composants:

- MLS Route Processor (MLS-RP)
- MLS Switching Engine (MLS-SE)
- MultiLayer Switching Protocol (MLSP)

❖Processus en quatre étapes :

- Le MLS-RP transmets des paquets MLSP Hello.
- Le MLS-SE identifie les paquets candidats.
- Le MLS-SE identifie les paquets validés.
- Le MLS-SE établit un chemin direct pour les paquets suivants [6].

I-5/ Les Réseaux Locaux virtuels(VLAN) :

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique. Il est distribué sur des équipements fonctionnant au niveau 2 du modèle OSI : la couche liaison.

Les principales différences entre la commutation traditionnelle et les LAN virtuels sont :

- ❖ Les LAN virtuels fonctionnent au niveau des couches 2et3 du modèle OSI.
- ❖ La commutation inter LAN virtuels est assurée par le routage de couche 3.
- ❖ Les LAN virtuels fournissent une méthode de contrôle des broadcasts.
- ❖ Les LAN virtuels permettent d'effectuer une segmentation selon certains critères :
  - Des collègues travaillant dans le même service.
  - Une équipe partageant le même applicatif.
- ❖ Les LAN virtuels peuvent assurer la sécurité des réseaux en définissant quels nœuds réseaux peuvent communiquer entre eux [7].

I-5-1/ Principe de fonctionnement des VLAN :

On distingue 2 méthodes pour regrouper les utilisateurs en VLAN :

- Le filtrage de trames
  - Un examen de chaque trame permet d'élaborer pour chaque commutateur une table de filtrage afin de permettre de prendre les décisions appropriées.
  - Cela suppose une table de filtrage par commutateurs, donc des temps de mise à jour lents ainsi que des problèmes d'évolutivité [7].
- L'identification des trames
  - Chaque trame dispose d'un code d'identification Vlan (TCI=Tag Control Information) définit par la norme IEEE802.1q
  - L'identificateur est utilisé lors du transfert des paquets sur le réseau.
  - Il est enlevé lorsque le paquet quitte le réseau pour atteindre les hôtes ou les routeurs [7].

I-6/ Le Protocole VTP (VLAN Trunking Protocol)

Le rôle du protocole VTP est de faire en sorte que la cohérence de la configuration des VLAN sur un réseau commun soit maintenue. Le VTP est un protocole de messagerie utilisant les trames d'agrégation pour gérer l'ajout, la suppression et l'attribution de noms aux VLAN.

Le VTP autorise les changements qui sont communiqués aux autres commutateurs du réseau. Les messages VTP sont encapsulés dans des trames ISL ou IEEE 802.1Q, puis transmis sur des liens multi-VLAN aux autres éléments du réseau.

Normalement, les ports des commutateurs sont affectés à un seul VLAN, mais les ports multi-VLAN transportent les trames de tous les VLANs du réseau. Ce port dit "port trunking", dans lequel passeront plusieurs VLANs, est un lien "trunk" [8].

I-7/ Déploiements de VLAN 802.1Q :

La norme 802.1q est née en 1998 pour répondre à un besoin de normalisation sur le transport des VLANs afin que certains ports du Switch puissent être assignés à plusieurs VLANs, ce qui fera économiser du câble et aussi des ports sur le Switch. Son principe consiste à ajouter dans l'entête de la trame Ethernet un marqueur qui va identifier le VLAN. [9] [10]

1-7-1/ Description de la norme 802.1q :

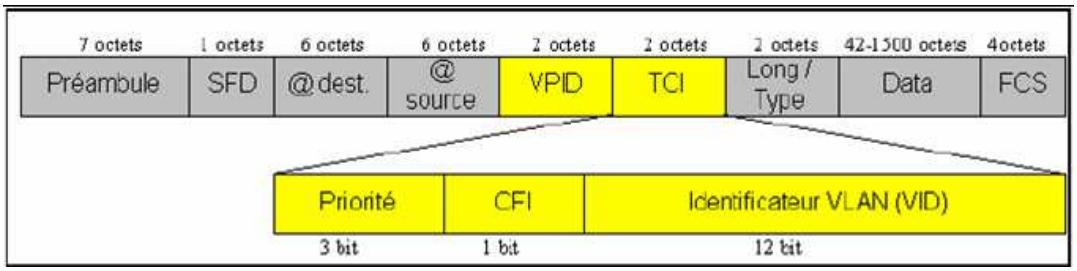


Figure I-2 : Extension de la trame Ethernet modifiée par la norme 802.1q.

La Figure I-2 illustre la modification de la trame Ethernet et l'ajout d'un champ sur 4 octets par la norme 802.1Q. [10]

La norme définit sur la trame Ethernet le champ VPID à 0x8100 pour désigner la trame 802.1q.

La norme 802.1q prévoit également un mécanisme de priorisation de flux. Cette priorisation est définie par la norme 802.1p.

Un champ protocole définit sur 1 bit est prévu pour pouvoir utiliser le 802.1q aussi bien sur Ethernet que sur TokenRing.

Enfin, le champ Vlan ID permet de fixer un identifiant sur 12 bits d'un Vlan [7].

I-8/ Le protocol spaningtree (STP) et (RSTP):

I-8-1/ Le protocole (STP) :

Ce protocole standard appelé « SpanningTree » Protocol normalisé IEEE 802.1d a pour rôle principal d'éviter les boucles de transmission. Après une phase de découverte de la topologie physique du réseau, l'algorithme de «SpanningTree » Protocol établit une arborescence logique sans boucle [11].

- Pourquoi le « SpanningTree » est-il nécessaire?
  - ❖ Il permet d'autoriser la présence de boucles sur le réseau.
  - ❖ Il permet de faire une redondance alternative de liens en cas de panne.
- Les versions :
  - IEEE 802.1d Spanning Tree Protocol, STP
  - IEEE 802.1w Rapid Spanning Tree Protocol, RSTP
  - IEEE 802.1s Multiple Spanning Tree Protocol, MSTP

En effet, dans les réseaux Ethernet, un seul chemin actif peut exister entre deux stations. L'existence de plusieurs chemins actifs entre des stations cause inévitablement des boucles dans le réseau. Lorsque les boucles surviennent, certains commutateurs reconnaissent une

même station sur plusieurs ports. Cette situation entraîne des erreurs au niveau de l'algorithme d'expédition et autorise la duplication de trames qui seront expédiées.

L'algorithme « spanningtree » fournit des chemins redondants en définissant un arbre qui recense tous les commutateurs dans un réseau étendu et force ensuite certains chemins de données à être à l'état bloqué.

À intervalles réguliers, les commutateurs dans le réseau émettent et reçoivent des paquets « spanningtree » qu'ils emploient pour identifier le chemin.

Si un segment de réseau devient inaccessible, l'algorithme « spanningtree » reconfigure la topologie et rétablit la liaison en activant le chemin de réserve.

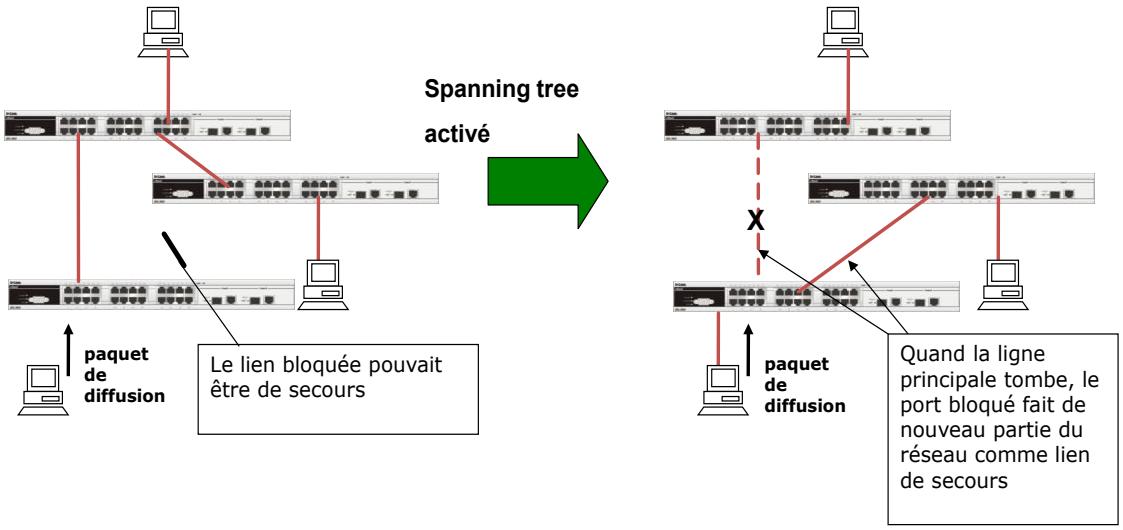


Figure I-3 : Le principe de fonctionnement du STP

I-8-2/ Le protocole (RSTP) :

C'est un protocole qui a fourni des améliorations significatives de la vitesse de convergence pour le réseau maillé en permutant immédiatement les ports racines et désignés à l'état de transmission. Il est standardisé par la norme IEEE 802.1W [11].

➢ Points communs entre RSTP et STP :

En général, RSTP fonctionne de la même manière que STP :

- Mêmes règles d'élection du commutateur Root
- Mêmes règles de sélection d'un port Root sur un commutateur non-Root
- Mêmes règles d'un unique port Designated sur un segment physique et les autres en état "Blocking".

➢ Différences entre RSTP et STP :

Les différences par rapport à STP :

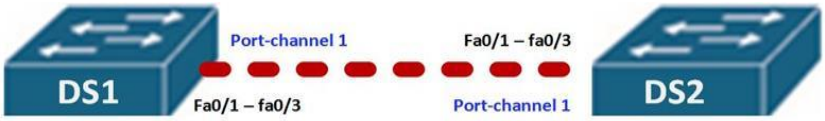
- Il n'y a plus que trois états pour les ports RSTP :
  - Discarding (au lieu de Disabled, Blocking et Listening)
  - Learning et Forwarding (gardant la même fonction)
- Les rôles port Root et port Designated subsitent. Les meilleurs ports alternatifs prennent le nom de lien de sauvegarde de ces derniers : port Alternate et port Backup. Ils prennent le rôle port Root et port Designated en cas de défaillance.
- Types. Les ports connectant des périphériques terminaux s'appellent des ports Edge. Les ports Point-to-Point connectent des commutateurs entre eux. Alors que STP attend passivement des BPDUs pour agir, RSTP négocie le statut des liens rapidement (3 X le Hello Time = 6 secondes).

I-9/ Ethernet channel :

Quel est le canal Ether ?

Comme nous l'avons vu dans ce chapitre, STP bloque les liens qui ne sont pas nécessaires pour éviter les boucles de la couche 2, mais illustre le scénario présenté ci-dessous [12].

Dans ce scénario, les deux commutateurs; DS1 et DS2 sont interconnectés par trois liaisons Ethernet rapides pour la redondance, ce qui peut constituer un problème majeur pour la boucle. Ainsi, lorsque le protocole STP est actif sur les commutateurs, 2 liaisons sont bloquées et une seule liaison est utilisée.



Cela signifie que seuls 100 Mbits seront utilisés alors que si toutes les liaisons étaient actives, nous aurions 300 Mbits utilisés, ce qui constituerait une utilisation plus efficace de la bande passante entre les commutateurs.

Ether channel permet d'utiliser plus efficacement la bande passante sur les liens redondants, en agrégeant les liens et en les transformant en une seule connexion logique, comme illustré ci-dessous.

Comme vous pouvez le constater dans notre topologie modifiée, les trois liaisons FastEthernet ont été regroupées dans une seule connexion logique, le canal de port 1.

➢ Avantage des canaux Ether

L'utilisation d'un canal Ether dans nos réseaux commutés présente plusieurs avantages.

- En utilisant le canal Ether, nous autorisons l'équilibrage de charge car le trafic sera dirigé sur trois liens au lieu d'un.
- En cas de défaillance de l'une des liaisons physiques sur le canal Ether, celui-ci fonctionnera toujours avec les liens restants - basculement automatique, c'est-à-dire que si fa0 / 1 dans notre scénario était en panne, le canal Ether continuerait à utiliser fa0 / 2 et fa0 / 3.
- Le troisième avantage de l'utilisation de canaux Ethernet est qu'ils simplifient la configuration des interfaces. Cela signifie que lorsqu'un canal Ethernet est implémenté, nous pouvons le configurer comme n'importe quelle autre interface, ce serait plus simple que de configurer les trois interfaces de manière répétitive.

I-10/ Conclusion :

Les Vlans sont aujourd'hui en pleine expansion dans le monde de l'entreprise pour répondre à des LANs de plus en plus grand et des services de plus en plus diversifiés. De nouvelles idées ont récemment vu le jour dans une utilisation plus complexe des Vlans et les constructeurs continuent à travailler sur des implémentations de la norme .

CHAPITRE II

Configuration de la QoS pour un déploiement de VOIP

Chapitre II : Configuration de la QoS pour un déploiement de VOIP

II.1/ Introduction:

La qualité de service varie d'un commutateur à l'autre, plus le commutateur de niveau est élevé, plus la couche d'application réseau avec laquelle il fonctionne est élevée.

Dans ce chapitre nous allons parler de la qualité de service et sa configuration dans un réseau d'entreprise hétérogène. Comme nous allons voir comment donnée des priorités au flux VOIP au détriment d'autre flux (données) dans la même architecture.

II.2/ Définition

Dans un réseau d'entreprise plusieurs types de flux peuvent coexister (flux vidéo, audio ou données). La voix sur réseau IP, ou « VoIP », est une technique qui permet de communiquer par la voix via Internet ou tout autre réseau acceptant le protocole TCP/IP. [13]

La VoIP est devenue une technologie accessible. Aujourd'hui, son déploiement au sein des entreprises devient une évidence. Pour que la VoIP puisse remplacer de manière réaliste les services de téléphonie sur réseau téléphonique public commuté (RTPC) standard, les clients doivent recevoir la même qualité de transmission vocale qu'ils reçoivent avec les services téléphoniques de base, ce qui signifie des transmissions vocales toujours de haute qualité. Comme d'autres applications en temps réel, la VoIP est extrêmement sensible à la bande passante et aux délais. Pour que les transmissions VoIP soient intelligibles pour le récepteur, les paquets vocaux ne doivent pas être abandonnés, retardés de manière excessive ou subir des retards variables (autrement appelés gigue).

Le facteur le plus important pour migrer vers la VoIP est la qualité de service (QoS). A ses débuts, la VoIP bénéficiait d'une mauvaise qualité de service et l'impact sur les communications des entreprises était mauvais. Aujourd'hui, la VoIP peut atteindre une excellente qualité de service mais ce n'est pas toujours garanti. Elle dépend des switcher qui contrôlent le trafic VoIP et aussi de la qualité de l'infrastructure réseau sur lesquels le trafic est transmis. Il est facile de comprendre que les clés d'une migration réussie vers la VoIP est le choix du fournisseur, le modèle fourni et les téléphones. [14]

La qualité de service est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau en management du système d'information ou d'un processus en logistique et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet de véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets…[15] [16]

Les facteurs clés nécessaires pour assurer une bonne QoS sur le réseau pour la VoIP sont les suivants : Priorité des paquets voix, une bande passante adaptée, résilience, et sécurité.

II.3/ Fonctionnement générale de la QoS :

En mode QoS , une série de bits inclus dans la trame ou le paquet IP qui circule indique que cette trame ou ce paquet a une priorité définie entre 0 à 7, selon son degré d'urgence d'acheminement (7 étant le plus urgent). Les valeurs 0 à 7 proviennent du standard 802.1p prévoyant un champ de priorité sur un octet. [17]

La priorisation ne peut se gérer qu'à l'intérieur de l'équipement : on ne peut pas organiser de file d'attente en entrée, bien évidemment ! Elle va permettre de traiter et de réémettre les trames non pas en fonction de leur ordre d'arrivée, mais en fonction de leur priorité.

Concrètement, la priorisation consiste à associer non pas une mais plusieurs files d'attente de traitement des trames à chacun des ports du commutateur, et à affecter une priorité différente à chacune de ces files d'attente. Les trames de priorité haute, seront placées dans une file d'attente de priorité haute. Les techniques de priorisation peuvent varier d'un constructeur à l'autre.

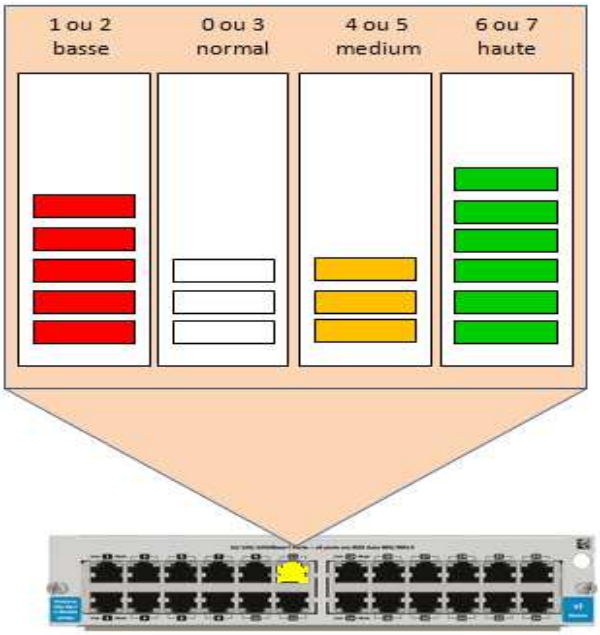


Figure II-1 : Exemple sur la technique de priorisation

Dans la figure II-1 nous avons 4 files d'attente de sortie associées au port 10 du commutateur. Toutes les trames destinées à sortir par le port 10 ont été ventilées dans quatre files d'attente de priorité différente, en fonction d'informations de priorité déterminées par le commutateur, ou déjà intégrées dans les trames entrantes. Les paquets de la file de priorité haute 6/7 seront traités en priorité ; puis ce seront ceux de la file de priorité medium "4/5" ; puis ceux de la file de priorité normale "0/3" et enfin, ceux de la priorité la plus basse "1/2". [18]

Cette priorisation prendra tout son sens dans les cas de congestion du commutateur, avec pour un port de sortie donné, un nombre de paquets entrant à un rythme plus élevé que le rythme de traitement des paquets à sortir. Il se produit alors une mise en file d'attente des paquets. [19]

La décision de placement en file d'attente de priorité N peut être prise selon différents critères. Par exemple :

- Le VLAN d'origine du paquet, ce qui permet de donner une priorité à un VLAN par rapport à un autre ;
- Le port UDP/TCP du paquet IP, ce qui revient à donner la priorité à une application par rapport à une autre;
- Une adresse IP source ou de destination, ce qui revient à donner la priorité à un équipement de réseau par rapport à d'autres (un serveur IPBX par exemple);
- Une interface d'entrée dans le commutateur, ce qui revient à donner la priorité à un segment de réseau, ou un équipement;
- Des informations de priorité déjà présentes dans l'entête d'une trame ou d'un paquet entrant.

II.4/ Algorithme de priorité

Parmi les algorithmes de gestion de priorités entre les files d'attente on note principalement [18] :

- Priority Queuing (PQ) : Tant qu'il ya des paquets prioritaires dans la file d'attente, ils seront traités avant de passer aux autres moins prioritaires, son principe c'est qu'une file de priorité N est vidée entièrement avant les files de priorité N-1. La configuration de Priority Queuing se fait par 3 étapes :

  1-Définir une liste de priorités.
  2- Affectation de la liste de priorités à une interface.
  3- La surveillance de la liste (Optionnel).

- First In First Out (FIFO) : Celle-ci n'impose aucune priorité sur les paquets, et ceux-ci sont transmis dans l'ordre où ils sont reçus. D'un point de vue technique, cette méthode est toujours utilisée par défaut sur les interfaces.

- Weighted Fair Queuing (WFQ): Priorité à certains trafics par rapport à d'autres, cet algorithme consiste à privilégier le trafic à faible volume sur celui à fort volume pour cela chaque flux est identifié avec son adresse IP source et adresse IP destination et des ports TCP/UDP (source et destination).

II.5/ Les standards de la QoS aux niveaux 2 et 3

II.5-1/ Standard 802.1p - niveau 2

Cette norme 802.1p est une extension du protocole 802.1q (vue dans le premier chapitre), elle est utilisée soit sur des Switch de niveau 2 ou de niveau 3 (Switch gérant des fonctions de routage inter VLAN) [18]. Elle propose d'insérer, dans le TAG de la trame Ethernet, un champ définissant la priorité de cette trame, comme elle permet de gérer des files d'attente au niveau des Switch. Le protocole 802.1p ne peut être opérationnel que dans un contexte 802.1q. [15]

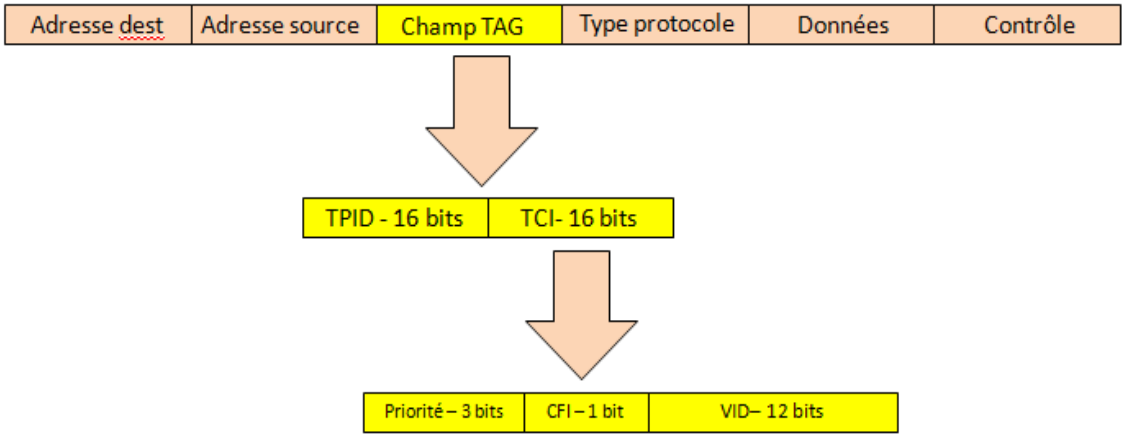


Figure II-2 : Localisation du champ dans la trame Ethernet

Ce champ de 32 bits est inséré après l'adresse MAC source de la trame. Il comprend un champ TPID (Tag Protocol Identifier) qui permet d'indiquer le type de protocole (ici 802.1q) et le champ TCI (Tag Control Information) qui se décompose lui-même en trois parties :

- Le champ de priorité, sur 3 bits, permettant de définir 8 niveaux de priorité ;
- Le champ CFI indiquant si nous sommes en Token Ring ou Ethernet ;
- Le champ VID donnant le numéro de VLAN (sur 12 bits) permettant 4094 VLANs.

II.5-2/ L'entête IP et le champ ToS/CoS - niveau 3 :

La priorisation des flux peut se définir et s'utiliser également au niveau du paquet IP, dans le champ appelé ToS (Type of Service) ou CoS (Class of Service) présent dans l'entête d'un paquet IP.

Le champ ToS permet de distinguer différentes qualités de service différenciant la manière dont les paquets sont traités. Composé de 3 bits de priorité (donc 8 niveaux) et trois indicateurs permettant de différencier le débit, le délai ou la fiabilité. [19]

Ce champ a été peu utilisé et il est désormais généraliser par le champ DSCP (Differentiated Service Code Point) sur 6 bits et d'un champ CU (Currently Unused) de 2 bits,

et donc remplacé, dans le modèle DiffServ (Differentiated Services), par le champ CoS, toujours de 8 bits.

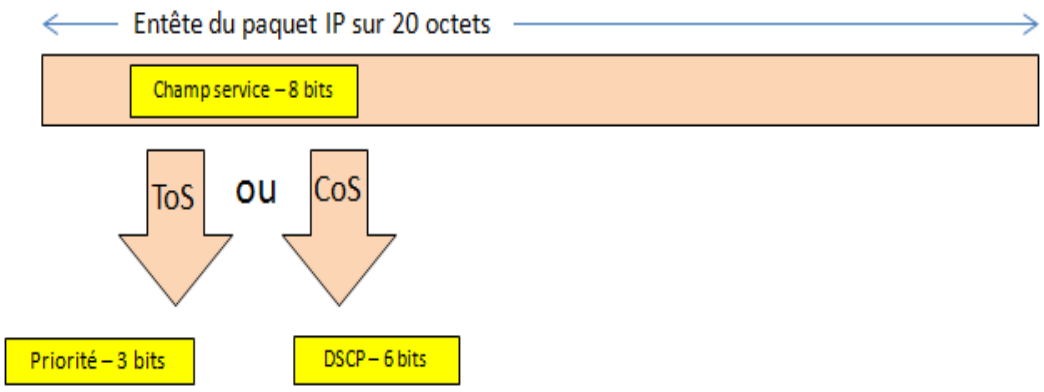


Figure II-3 : Entête du paquet IP

La priorisation se définira et s'utilisera ainsi en fonction des valeurs prises par ce champ DSCP. Cette priorisation fonctionne donc dans un environnement non "802.1q". Elle est gérée au niveau 3 du modèle OSI, possiblement moins rapidement qu'une priorisation gérée au niveau 2.

Les valeurs possibles du champ CoS sont les suivantes [18] :
1 : arrière plan
2 : service économique ou standard
0 : service best effort
3 : service maximum (business critical)
4 : streaming application à charge contrôlée
5 : multimédia interactif (voice)
6 : voix interactive
7 : critique (network critical)

II.6/ Configuration de la QoS

II.6-1/ Configuration de la QoS au niveau du Switch

Le Switch centralise les flux de données et de voix, c'est grâce à la technologie CoS que nous allons donner une priorité au flux VOIP.

La QoS n'est pas définis sur le Switch par défaut, elle doit être activé par la commande « mls qos »

Exemple de configuration d'un Switch : [19]

```
Switch>enable
Switch#configure terminal
Switch (config)#mls qos
Switch (config)#interface fastEthernet0/3
Switch (config-if)#mls qos trust cos
Switch (config-if)#mls qos cos 5
Switch (config-if)#switchport priority extend cos 5
Switch (config-if)#no shu
Switch (config-if)#exit
```

Figure II-4 : Activation de la QoS

- mls qos : active globalement la fonctionnalité de la qos en fonction du niveau de priorité configuré,
- qos trust : On accepte la priorité annoncée par le téléphone,
- cos 5 : On affecte un niveau de priorité (CoS = 5) aux données provenant du port f0/3

Nous pouvons vérifier la configuration de l'interface par la commande "show interface":

```
Switch#show interface f0/3
Unknow unicast bloked : disabled
Unknown multicast blocked : disabled
Appliance trust : 5
```

Figure II-5 : Vérification de l'interface f0/3

Comme nous pouvons vérifier la configuration de l'activation de la QoS par la commande "show mls qos interface":

```
Switch#show mls qos interface f0/3
FastEthernet0/3
Trust state : trust cos
Trusted mode : trust cos
Trust enabled flag : ena
COS override : dis
Default COS : 5
DSCP Mutation Map : Default DSCP Mutation Map
Trust device : cisco-phone
Qos mod : port-based
```

Figure II-6: Vérification de l'activation de la QoS

II.6-2/ Configuration de la QoS au niveau du Routeur

La procédure de mise en place de la QoS dans les environnements Cisco est la suivante:

Définition d'une ou plusieurs classes de flux, en fonction de paramètres divers, comme par exemple le protocole concerné par le flux.

Définition d'une politique de QoS dans laquelle chaque classe de flux se voit attribuer un niveau de priorité.

Application de cette politique sur une interface, en entrée ou en sortie. [18]

Premier exemple : QoS en fonction d'une interface source

```
Routeur#configure terminal
Routeur (config)#class-map match-all prio-sur-interface
Routeur (config-cmap)#match input-interface fa1/0
Routeur (config-cmap)#exit
Routeur (config)#
```

Figure II-7: Déclaration de classes de flux [18]

Nous avons donc déclaré une classe "prio-sur-interface". Pour appartenir à cette classe, le flux doit provenir exclusivement de l'interface fa1/0.

La clause "match-all" indique que, pour appartenir à la classe, un paquet doit vérifier tous les critères déclarés. La clause "match-any" signifie qu'il faut en vérifier au moins un. Si nous ne déclarons qu'un seul critère d'appartenance, "match-all" et "match-any" sont équivalents.

Nous pouvons vérifier la déclaration de la classe par la commande "show classmap":

```
Routeur# show class-map
Class Map match-any class-default (id 0)
Match any Class Map match-all prio-sur-interface (id 1)
```

Figure II-8: Vérification de la déclaration de la classe [18]

Nous voyons qu'il y a une classe par défaut, "classe-default", dont font partie tous les paquets. [19]

```
Routeur (config)#policy-map ma-politique-qos
Routeur (config-pmap)#class prio-sur-interface
Routeur (config-pmap-c)#set ip dscp cs7
Routeur (config-pmap-c)#exit
Routeur (config-pmap)#exit
Routeur (config)#
```

Figure II-9: Déclaration d'une politique de QoS [19]

Si la politique "ma-politique-qos" n'existait pas encore, elle est créée. Si elle existait, les commandes "class" vont la compléter.

Une priorité sur champ DSCP est définie pour les paquets de la classe "prio-sur-interface" avec le code "cs7", équivalent à un DSCP de "111000" et donc une priorité haute de "7" (voir le tableau de correspondance code/DSCP plus bas).

```
Routeur (config)#interface fa0/1
Routeur (config-if)#service-policy output ma-politique-qos
Routeur (config-if)#exit
Routeur (config)#exit
```

Figure II-10: Application de la politique de QoS sur une interface [19]

Nous avons donc appliqué la politique consistant à attribuer une priorité haute aux flux qui étaient entrés par l'interface fa1/0. Les paquets correspondants voient leur champ DSCP passer à "111000" quand ils sortent par l'interface fa0/1.

Nous pouvons vérifier la déclaration de la politique de QoS par la commande "show policy-map" :

```
Routeur# show policy-map
Policy Map ma-politique-qos
Class prio-sur-interface
set ip dscp cs7
```

Figure II-11: Vérification de la déclaration de la politique de QoS [19]

Nous pouvons également vérifier que la priorisation en sortie d'interface fa0/1 a changé et qu'elle n'est plus en mode "FIFO", mais en mode "class-based queueing" :

```
Routeur #show interfaces fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Lance, address is 0001.c996.9902 (bia 0001.c996.9902)
Internet address is 172.20.0.254/16
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: Class-based queueing
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 1/1 (allocated/max allocated)
Available Bandwidth 75000 kilobits/sec
```

Figure II-12: Vérification du mécanisme de traitement de la file d'attente en sortie de l'interface fa0/1. [19]

Second exemple : QoS en fonction du protocole

```
Routeur (config)#class-map match-all prio-sur-ftp
Routeur (config-cmap)#match protocol ftp
Routeur (config-cmap)#exit
Routeur (config)#
```

Figure II-13: Déclaration d'une nouvelle classe de flux [19]

Nous avons donc déclaré une classe "prio-sur-ftp". Pour appartenir à cette classe, le flux doit être de protocole FTP, quelle que soit sa source IP ou son interface source.

```
Routeur (config)#policy-map ma-politique-qos
Routeur (config-pmap)#class prio-sur-ftp
Routeur (config-pmap-c)#set ip dscp cs1
Routeur (config-pmap-c)#exit
Routeur (config-pmap)#exit
Routeur (config)#
```

Figure II-14: Elargissement de la politique de QoS [19]

Ici, on complète la politique "ma-politique-qos" en y ajoutant la classe "prio-sur-ftp" à laquelle on attribue une priorité basse de type "cs1", soit un DSCP "001000" correspondant à une priorité "1".

II.6-3/ Configuration automatique de la QoS

```
Routeur (config-if)#auto qos voip
```

Figure II-15: Active la QoS automatique pour VoIP [20]

```
Routeur (config-if)#auto qos classify
```

Figure II-16: Active la QoS automatique pour la classification [20]

```
Routeur (config-if)#auto qos trust
```

Figure II-17: Active la QoS automatique pour les interfaces approuvées [20]

II.7/ Conclusion :

Pour permettre d'améliorer la qualité de service VOIP, on a donné plus de priorité au service de la voix par rapport aux autres données. Au début de la configuration les switchers et les routeurs sont initialement configurés en FIFO (first in first out) le premier qui entre le premier qui sort.

Pour les paquets de la voix ce sont en temps réel (n'accepte pas le retard) parce que l'oreille humaine très sensible aux pertes ou le retard des paquets.

CHAPITRE III

Technologie WAN et Sécurité

Chapitre III : Technologie WAN et Sécurité

III.1/ Introduction :

Au niveau de la couche Accès Réseau deux grands types de technologies se distinguent: les technologies LAN (Local Area Network) et les technologies WAN (Wide Area Network). Elles couvrent les couches physiques (L1) et la couche Liaison de données (L2) du modèle OSI [21].

Les technologies WAN sont diverses dans le monde pour des accès et dans les infrastructures des opérateurs.

La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu [22].

Dans ce chapitre en va évoquez quelque technologie du WAN et la sécurité informatique, ses objectifs et de leur impact sur les réseaux.

III.2/ Technologie WAN :

III.2-1/ Frame-Relay :

Le relayage de trames (ou FR, pour l'anglais Frame Relay) est un protocole à commutation de paquets situé au niveau de la couche de liaison (L 2) du modèle OSI, il a été développée à l'origine en tant qu'extension du RNIS.

Les commutateurs Frame Relay créent des circuits virtuels permettant de connecter des réseaux locaux distants à un WAN. Les PVC (Circuit virtuel permanent) s'identifient au niveau des interfaces des DTE et DCE grâce à des DLCI (Data Link Connection Identifiers) afin de pouvoir distinguer les flux provenant des différents PVC. Les DLCI sont généralement des numéros d'identification à valeur uniquement locale (à une interface) qu'on assimile à une sous-interface dans certains contextes : sur un routeur par exemple, chaque PVC d'une interface pourra ainsi avoir sa propre adresse IP associée. [23]

Frame Relay réduit le trafic en implémentant de la détection plutôt que de la correction d'erreur en utilisent le mécanisme de détection d'erreur appelé CRC (cyclic redundancy check)... [24]

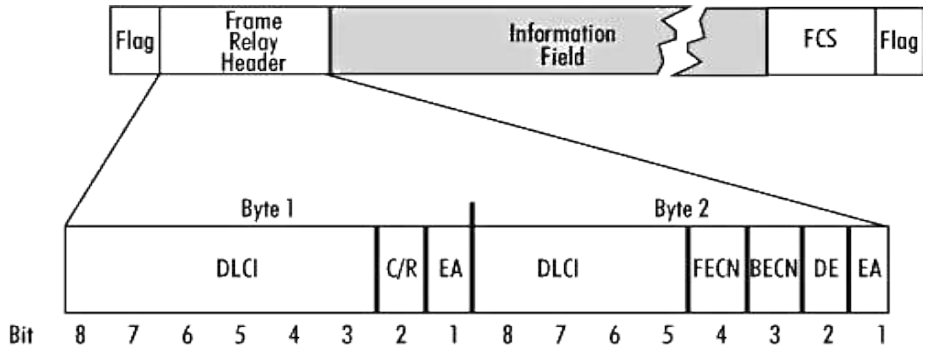


Figure III-1 : Entête Frame Relay

- Flag : synchronisation de valeur 0111111 0
- Header : DLCI (10-23 bits), 3bits (FECN, BECN, DE), 3 bits taille adresse
- C/R (commande/Réponse) transmis de bout en bout, afin d'identifier, si nécessaire, les trames de commande et de réponse.
- Data : 0-4096 octets max.
- FCS : CRC-16. [25]

Il existe deux modes de configuration d'une interface frame relay qui sont :

- Point à point :

Une sous-interface point à point établit une connexion par circuit virtuel permanent à une interface physique ou une sous-interface d'un routeur distant.

Chaque paire de routeurs point à point réside sur son propre réseau informatique et chaque sous-interface point à point ne dispose que d'un DLCI. Dans ce cas, le découpage d'horizon n'intervient pas.

- Multipoint :

Une seule sous-interface établit plusieurs connexions de circuit virtuel permanent à plusieurs interfaces physiques ou sous-interfaces sur des routeurs distants. Tous les circuits virtuels multipoint appartiennent au même sous réseau. [26]

III.2-2/ Protocole PPP (Protocole point-à-point) :

PPP (Protocole point-à-point) est le meilleur protocole à mettre en œuvre sur une connexion commutée WAN série. Un protocole de transport décrit par le standard RFC 1661permet d'établir une connexion entre deux hôtes sur une liaison point à point et fournit des fonctions de détection d'erreurs. Il fait partie de la couche liaison de données (couche 2) du modèle OSI [27].

Le protocole PPP comporte un processus d'authentification par CHAP ou PAP. Il peut être utilisé sur différents médias physiques, notamment les câbles à paires torsadées, la fibre optique ou la transmission par satellite. [28]

Le protocole PPP s'appuie sur trois composants:

- L'encapsulation des datagrammes.
- Le protocole de contrôle de liaison (LCP : Link Control Protocol) – Utilisé pour négocier et configurer les options de contrôle sur la liaison de données WAN.
- Le protocole de contrôle réseau (NCP : Network Control Protocol) – Utilisé pour configurer les divers protocoles de couche réseau.

➢ LCP (Link Control Protocol)

PPP utilise le sous-protocole LCP pour accepter automatiquement des options de format d'encapsulation, telles que :

- L'authentification : en utilisant soit le protocole d'authentification du mot de passe (PAP pour Password Authentication Protocol), soit le protocole d'authentification à échanges confirmés (CHAP pour Challenge Handshake Authentication Protocol) ;
- La compression ;
- La détection ;

L'établissement d'une session PPP se déroule en trois phases. Ces phases sont l'établissement de la liaison, l'authentification et la phase de protocole de couche réseau.

➢ NCP (Network Control Protocol)

Network Control Protocol (NCP) est une catégorie de protocole qui négocie des paramètres de couche 3 pour son propre compte.

a. Configuration du protocole PPP :

```
(config)#interface s0/0
(config-if)#encapsulation ppp
```

III.2-3/ Le protocole CHAP (Challenge-Handshake Authentication Protocol)

Le protocole CHAP (Challenge-Handshake Authentication Protocol), défini par la RFC 1994, est utilisé pour vérifiez périodiquement l'identité de l'homologue au moyen d'une négociation en trois étapes [29]. Ceci est fait lors de l'établissement initial de la liaison, et peut être répété à tout moment après que le lien a été établi.

- Une fois la phase d'établissement de liaison terminée, l'authentificateur envoie un message "challenge" à l'homologue.

- L'homologue répond avec une valeur calculée à l'aide d'une "réponse unidirectionnelle". hash "fonction.
- L'authentificateur compare la réponse à son propre calcul de la valeur de hachage attendue. Si les valeurs correspondent, l'authentification est reconnue; sinon la connexion DEVRAIT être résiliée. [29]

À intervalles aléatoires, l'authentificateur envoie un nouveau défi à l'homologue et répète les étapes 1 à 3.

L'objectif de CHAP est d'assuré une authentification sans échange de mot de passe en clair sur le réseau et sans que l'échange puisse être rejoué par un tiers à l'écoute. [30]

✓ **Configurer PPP CHAP :**

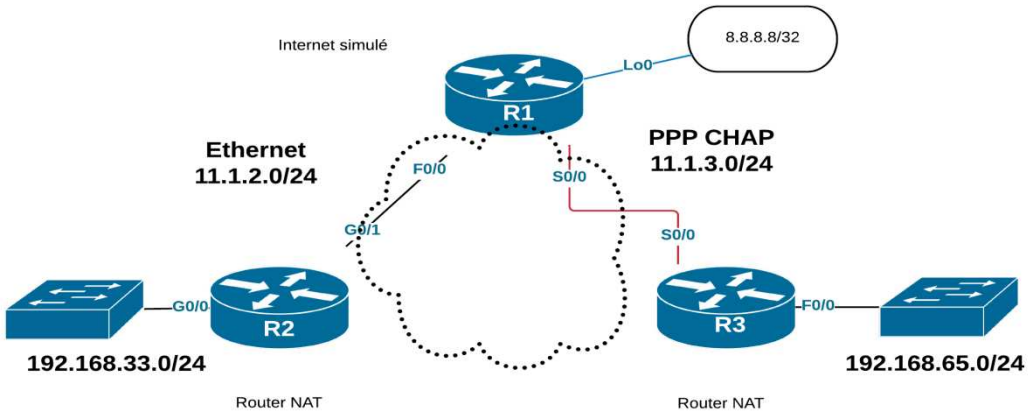


Figure III-2 : Exemple de configuration du protocole PPP CHAP

✓ **Activation de PPP CHAP entre R1 et R3.**

```
R1(config)#username R3 password testtest
R1(config)#int s0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
```

```
R3(config)#username R1 password testtest
R3(config)#int s0/0
R3(config-if)#encapsulation ppp
R3(config-if)#ppp authentication chap
```

III.2-4/ le protocole PPPoE

PPPoE a été développé parce que les liaisons Ethernet ne supportent pas nativement PPP. Comme le montre la Figure III-3, PPPoE permet l'envoi de trames PPP encapsulées dans des trames Ethernet [31].

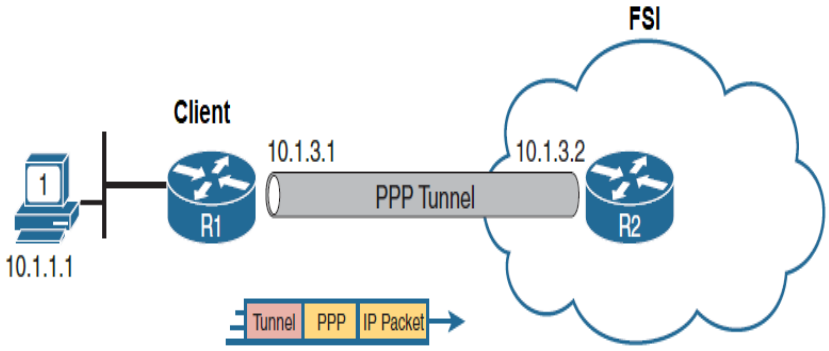


Figure III-3 : Construction d'un tunnel PPP à l'intérieur d'Ethernet

✓ **Configuration PPPoE**

Pour mettre en œuvre PPPoE, suivez les étapes suivantes :

Étape 1 : Créez un tunnel PPP à l'aide d'une interface de numérotation, qui est un type d'interface virtuelle. Configurez PPP et l'adressage sur l'interface du numéroteur. En règle générale, le FSI attribue automatiquement l'adressage IP.

Étape 2 : Configurez PPP CHAP pour effectuer l'authentification avec le FSI.

Étape 3 : Activez PPPoE sur l'interface physique avec la commande pppoe enable. L'interface du numéroteur est reliée à l'interface Ethernet avec la commande pppoe-client, suivie du numéro utilisé pour créer le pool de numéroteurs à l'étape 2.

Le numéro d'interface du numéroteur ne doit pas nécessairement correspondre au numéro de pool du numéroteur.

Étape 4 : L'unité de transmission maximale (MTU) doit être fixée à 1492, contre 1500 par défaut, pour tenir compte des en-têtes PPPoE. Ceci permet d'éviter la fragmentation des paquets, ce qui entraîne un retard dans la transmission [32].

III.3/ Sécurité :

III.3-1/ Réseau privé virtuel VPN :

Les VPNs (Virtual Private Network), ou réseaux privés virtuels, forment une classe particulière de réseaux partagés. Dans de tels réseaux, les ressources d'un réseau réel peuvent se trouver distribuées à un instant donné entre plusieurs réseaux, de telle sorte que chaque sous-réseau puisse croire que le réseau réel a appartient à lui seul. Un VPN est un tunnel

sécurisé permettant la communication entre deux entités y compris au travers des réseaux peu sûrs comme peut l'être le réseau Internet. [33]

Le VPN est ne représente donc qu'un concept. Plusieurs moyens techniques peuvent être utilisés et couplés pour mettre en œuvre des VPN : le chiffrement, l'authentification, le contrôle d'intégrité et les tunnels.

- **Chiffrement** : Utilisé dans le contexte du VPN pour garantir la confidentialité des données circulant sur le réseau public. En effet, le réseau privé n'est que virtuellement coupé du réseau public.
- **Authentification** : On veut garantir qu'a chaque instant de la communication, on parle au bon interlocuteur.
- **Contrôle d'intégrité** : il garantit que les données transmit entre les interlocuteurs n'ont pas été modifié.
- **Tunnel** : le tunnel consiste à établir un canal entre 2 points sans ce soucié des problématiques d'interconnexion (de façon transparente). Nous verrons plus en détail cet aspect important du VPN.

✓ **Avantages et inconvénients du VPN:**

Les principaux avantages de cette solution sont :

- une indépendance quasi-totale vis-à-vis des opérateurs, ce qui fait que la solution peut être bâtie avec des opérateurs différents selon les sites.
- pas de contrat à signer, à dénoncer pour la mise en place et la suppression de ces VPN.
- pas de frais mensuels autres que ceux de l'abonnement internet servant de support à ces VPN.
- une grande souplesse pour déplacer les tunnels, en changer les périmètres ou contrôler le trafic y circulant.
- maitrise des protocoles de sécurité (authentification, cryptage, filtrage ……).
- Mais il y'a quelques inconvénients :
- aucune garantie de temps de rétablissement en cas de défaillance.
- aucune garantie de performances puisque ces VPN ont pour support un lien internet. [34]

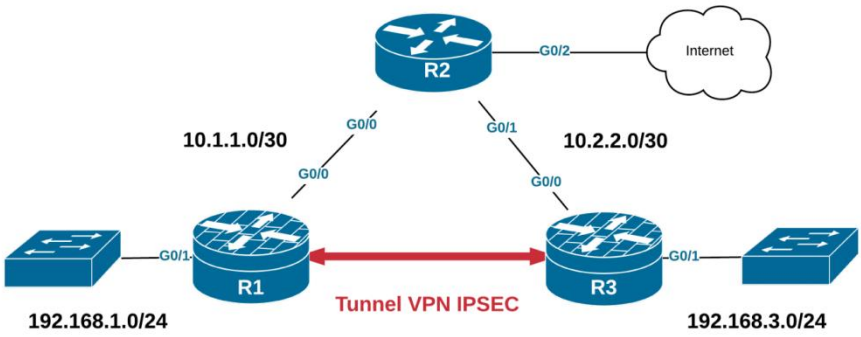


Figure III-4 : Tunnel VPN

Ce dernier s'appuie sur le protocole IPSec et offre la possibilité de se connecter à distance au réseau informatique.

III.3-2/ IPsec (IP sécurisé)

IPSec est un protocole défini par l'IETF (RFC 2401) permettant de sécuriser les échanges au niveau de la couche réseau. La solution IPsec introduit des mécanismes de sécurité au niveau du protocole IP, de telle sorte qu'il y ait indépendance des fonctions introduites pour la sécurité dans IPsec vis-à vis du protocole de transport. Le rôle de ce protocole est de garantir des services de sécurité comme la confidentialité, l'intégrité et l'authenticité de données échangées.

Pour cela, une signature électronique est ajoutée au paquet IP. Véritable extension de IP, IPSec repose sur les protocoles AH (Authentication Header) et ESP (Encapsulation Security Payload). [35]

✓ Les mécanismes AH et ESP :

IPsec fait appel à deux mécanismes de sécurité pour le trafic IP, les 'protocoles' AH et ESP, qui viennent s'ajouter au traitement IP classique :

- Authentication Header (AH) est conçu pour assurer l'intégrité et l'authentification des datagrammes IP sans chiffrement des données (i.e.confidentialité).
- Le principe de AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme.
- Encapsulating Security Payload (ESP) a pour role premier d'assurer la confidentialité aussi assurer l'authenticité des données.
- Le principe de ESP est de générer ; à partir d'un datagramme IP classique, un nouveau datagramme dans lequel les données et éventuellement l'en-tête original chiffrés.

Ces mécanismes peuvent être utilisés seuls ou combinés pour obtenir les fonctions de sécurité désirées.

✓ **Modes de fonctionnement :**

On distingue deux modes différents, selon le type de sécurisation et de connexion utilisés Mode transport et Mode tunnel :

- Mode Transport: Dans ce mode, IPsec s'intercale entre le protocole réseau(IP) et le protocole de transport, seules les données des protocoles de niveau supérieur (TCP,UDP…) transportées par le datagramme IP, sont protégées sans toucher à l'en-tête .Il est réservé aux connexions entre équipements terminaux (postes clients, serveurs).
- Mode Tunnel: Ce mode permet la création de tunnels par encapsulation de chaque paquet IP dans un nouveau paquet (IP in IP) .Ainsi, la protection porte sur tous les champs des paquets IP arrivant à l'entrée d'un tunnel, y compris sur les champs des en-têtes(adresses source et destination par exemple). Donc l'en-tête IP est également protégé et remplacé par un nouvel en-tête qui permet juste au paquet de traverser le tunnel de sécurité, à la sortie du quel l'en-tête original est rétabli.

➢ Le protocole d'authentification AH (Authentification Header)

❖ *Mode transport* :

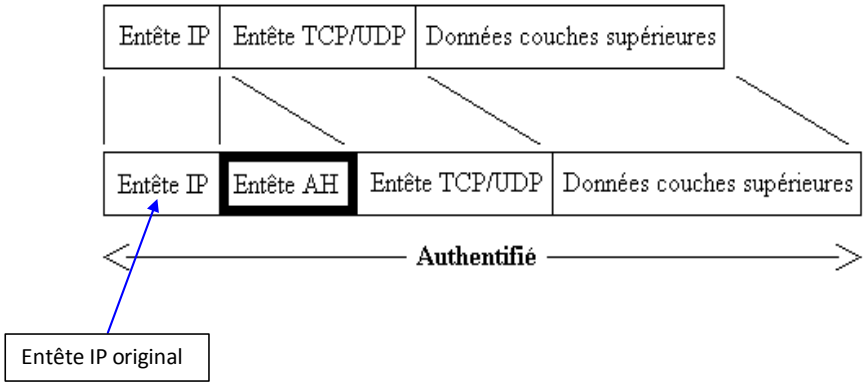


Figure III-5 : AH en mode transport

❖ *Mode tunnel* :

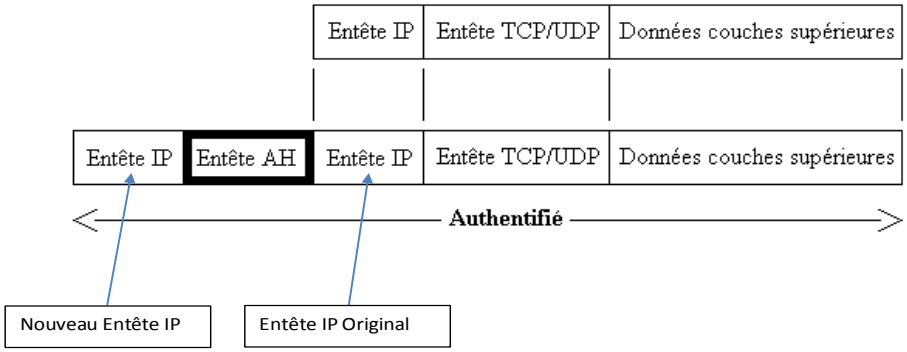


Figure III-6 : AH en mode tunnel

➢ Le protocole de confidentialité ESP (Encapsulating Security Payload)

❖ *Mode transport* :

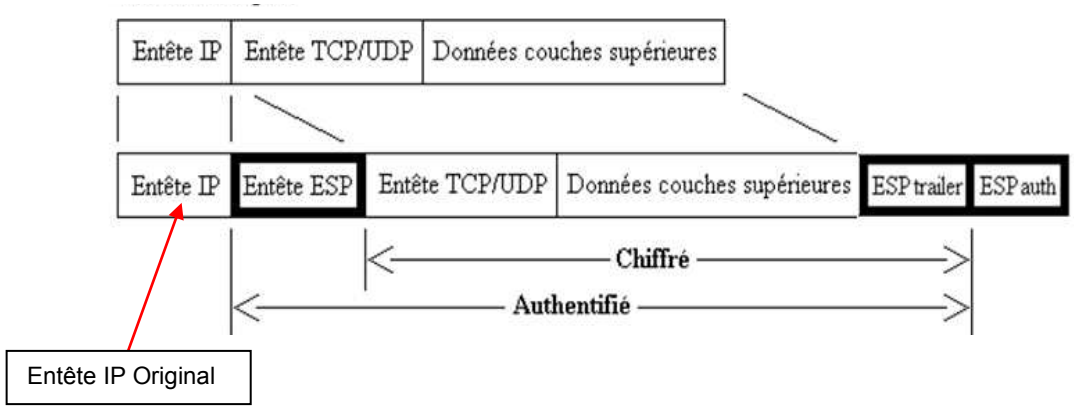


Figure III-7 : ESP en mode transport

❖ *Mode tunnel* :

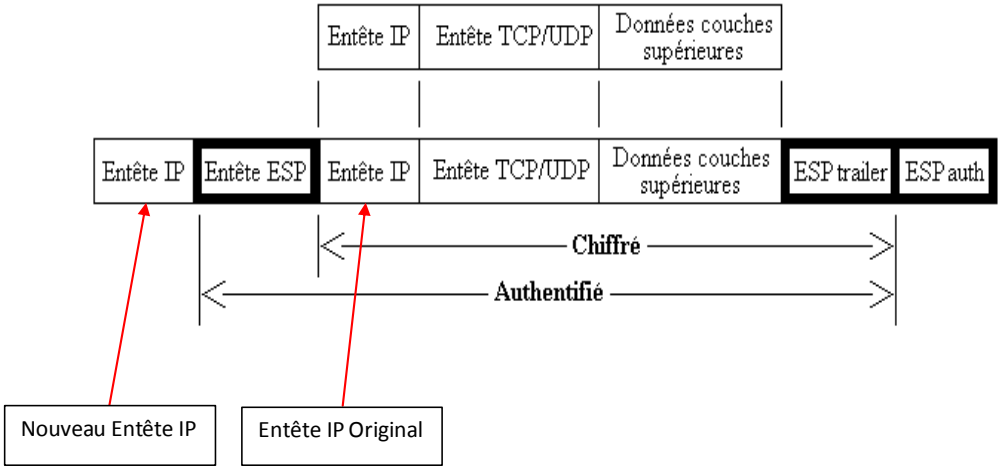


Figure III-8 : ESP en mode tunnel. [34]

III.3-3/ SSH (Secure Shell) :

La commande SSH est une version sécurisée de RSH (Remote Shell) et rlogin. Elle se situe au niveau de la couche application du modèle OSI et permet d'obtenir un interprète de commande (shell) distant sécurisé avec un système cible donné.

Comme l'illustre la figure III-9, d'autres applications peuvent utiliser une session SSH. Le protocole SSH s'insère entre les couches applicatives et la couche réseau TCP afin d'offrir ses services de sécurité. Il reste possible de ne pas utiliser le protocole SSH. Les couches applicatives se connectent alors directement à la couche réseau TCP.

Ce protocole était souvent utilisé pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son essor est limité à la fois par le succès grandissant de SSL/TLS et par son champ d'application plus restreint. Néanmoins il reste encore un protocole à considérer pour certains usages. [36]

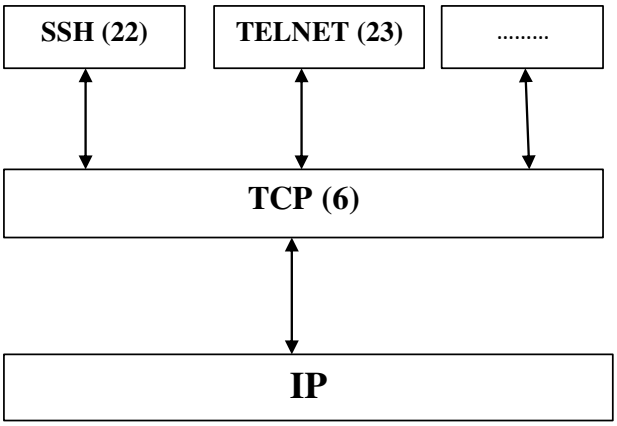


Figure III-9 : Représentation en couches du protocole SSH

III.3-4/ ACL (Access Control List) :

ACL (Access Control List) est la liste de contrôle d'accès. Elle désigne la liste des conditions qui sont appliquées généralement au trafic circulant via une interface de routeur tel que montre la Figure III-10.

Le but d'une liste d'accès est de définir le trafic qui devrait être autorisé ou pas à franchir le routeur, d'où le choix du terme « accès », alors qu'elle pouvait être nommés liste de contrôle de trafic, puisqu'il faut bien constater que tous les paquets ne sont pas légitimes sur le réseau, les paquets considérés comme illégales ou illégitimes doivent être interdit par le routeur. Afin de mettre en place ce filtrage, les listes d'accès représentent le moyen favorisé par les administrateurs réseaux. [37]

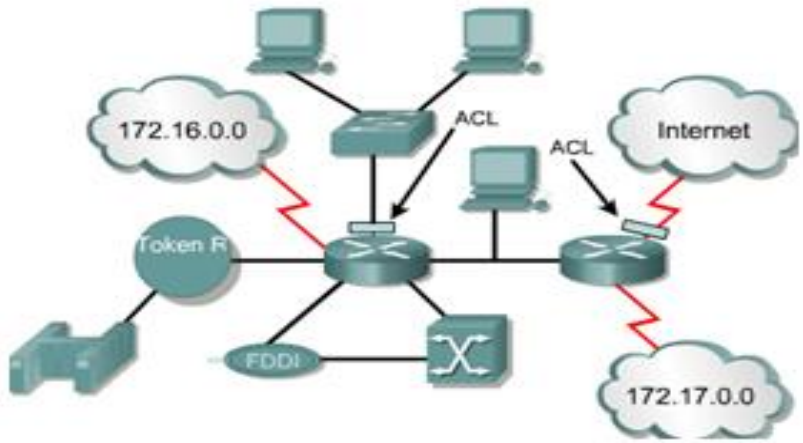


Figure III-10 : ACL

III.4/ Conclusion :

Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre la technologie WAN, où nous avons décrit quelque technologies, et en deuxième lieu de comprendre les concepts et objectifs de la sécurité informatique, et plus particulièrement la sécurité des réseaux où nous avons présenté brièvement les différentes politiques sécuritaires, tel que IPSec, SSH et les ACLs.

CHAPITRE IV

Configuration

Chapitre IV : Configuration

IV-1/ Introduction:

Dans ce chapitre, nous allons passer à la dernière étape qui est la configuration. Nous proposerons un schéma réalisable pour l'interconnexion dans une entreprise, nous implémenterons quelque notion dictée dans les chapitres précédents tels que la VOIP, VPN, et la sécurité. Pour ce faire nous commencerons par la présentation du simulateur utilisé, puis nous expliquerons en détail les différentes étapes suivies pour la réalisation de notre architecture proposée.

IV-2/ Présentation du simulateur « Cisco Packet Tracer »

Packet Tracer est un simulateur de matériel réseau Cisco (Routeur et Switchs). C'est l'outil idéal pour s'introduire dans le domaine des réseaux et se familiariser avec les équipements du constructeur Cisco, en les simulant sans matériel. [38]

Pour notre travail nous avons utilisé la version 7.2.

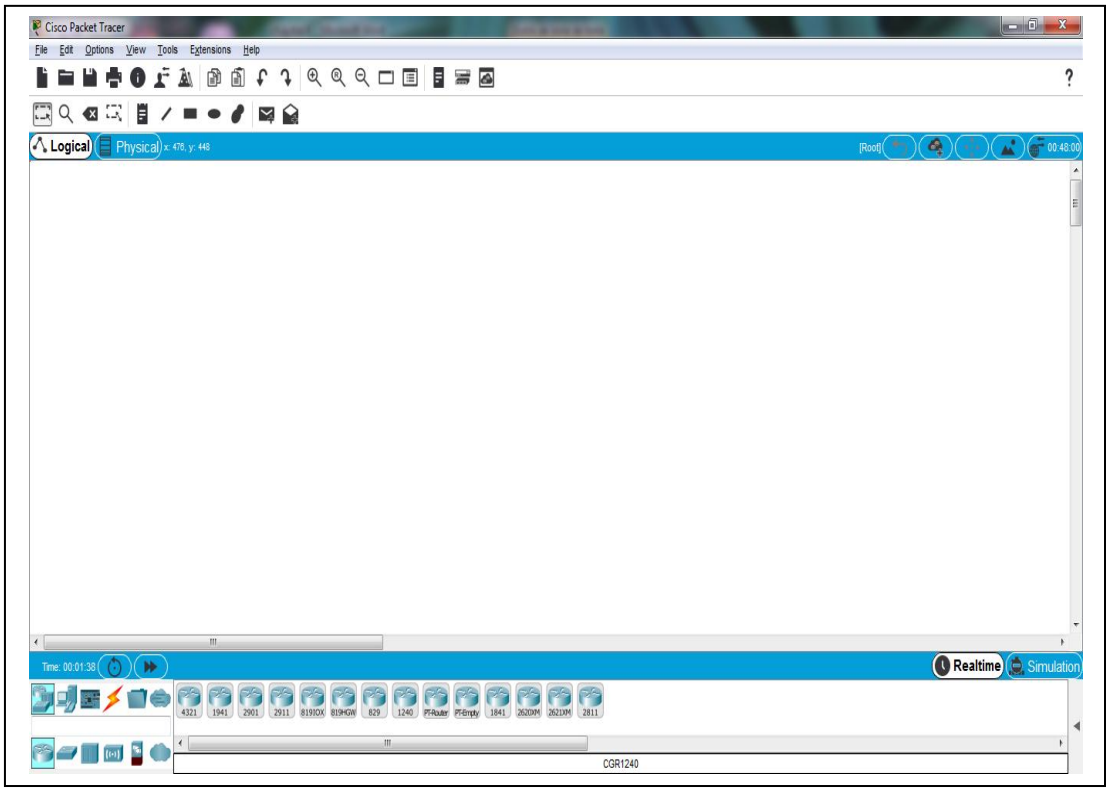


Figure IV-1 : Interface Packet Tracer 7.2.

IV -3/ Equipement utilisé :

Table IV-1 : Equipements utilisés [39], [40], [41], [42], [43], [44], [45]

Nom d'équipement	Description
Router	Un élément intermédiaire dans un réseau informatique assurant le routage des paquets entre réseaux indépendants
Switch	Un matériel d'interconnexion de type concentrateur réseau mais il fractionne le réseau en domaines de collision indépendants.
Cloud	désigne un ensemble de processus qui consiste à utiliser la puissance de calcul et/ou de stockage de serveurs informatiques distants à travers un réseau, généralement Internet.
Point Access	Un appareil se connecte à un routeur filaire, commutateur ou hub par câble Ethernet et délivre un signal Wi-Fi à une zone dédiée.
PC	Un ordinateur est un appareil, une machine qui permet de réaliser, d'exécuter des opérations, des calculs, c'est un calculateur.
PC Portable	Un ordinateur portable peut être utilisé au bureau, à la maison, en déplacement, Le principal avantage d'un ordinateur portable est la mobilité grâce à sa petite taille.
IP Phone	Un téléphone bien particulier avec des ports ethernet permettant de se connecter sur le port réseau afin d'utiliser internet comme support de communication.

IV -4/ Plan d'adressage :

Un plan d'adressage détermine l'adresse IP du réseau, du sous-réseau et donc des équipements qui composent le réseau de l'entreprise ou de l'établissement. [46]

L'élaboration d'un plan d'adressage nécessite la prise en considération de certaines règles, telles que la classe d'adressage, la définition de sous-réseau, l'attribution statique et/ou dynamique des adresses. Pour notre projet on a propose un plan d'adressage comme il est illustre dans la Table si dessous. [47]

Table IV-2 : Plan d'adressage

Réseaux	Plan d'adressage	Réseaux	Plan d'adressage
LAN-A	130.20.0.0/24	LAN-H	167.0.0.0/18
LAN-B	130.20.16.0/24	LAN-I	10.0.1.0/24
LAN-C	130.20.32.0/24	LAN-J	10.0.2.0/24
LAN-D	200.5.6.0/24	LAN-K	10.0.3.0/24
LAN-E	201.1.1.0/24	FRAME-RELAY	192.168.1.0/24 – 192.168.2.0/24 – 192.168.3.0/24
LAN-F	10.0.0.0/24	VPN	198.2.2.0/30 – 199.3.3.0/30
LAN-G	180.20.20.0/24		

IV -5/ Architecture réalisée :

Nous proposerons un schéma réalisable pour l'interconnexion d'un réseau LAN-WAN dans une entreprise quelconque, formalisant toute les technologies vue au par avant dans les chapitres précédents. La Figure IV-2 illustre l'Architecture réalisée.

V -6/ Méthode de configuration des équipements :

Toutes les configurations des équipements du réseau seront réalisées au niveau de la CLI (Commande Langage Interface) (Figure IV-2).CLI est une interface de simulateur Cisco Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commande. [48]

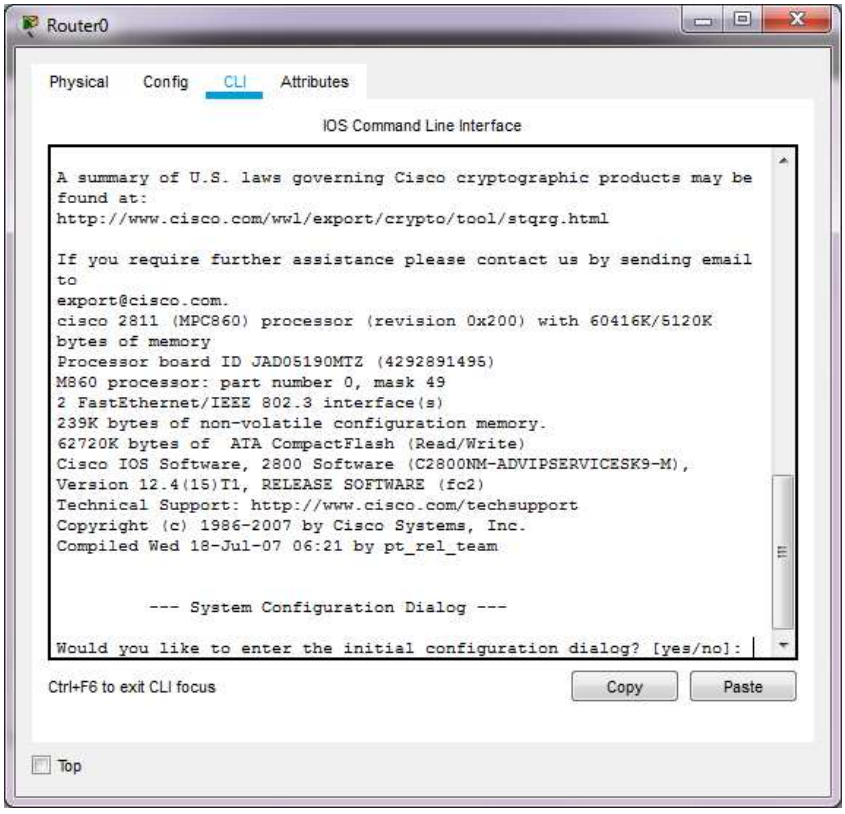


Figure IV-3 : Interface CLI

IV -6-1/ Configuration des équipements :

On va lance des séries des configurations sur tous les équipements du réseau avec un exemple configuré.

On va suivre les étapes de configuration illustrées comme suit :

a. Configuration DHCP au niveau des routeurs R2, R9, R10, R11 et R12,
b. Configuration du routage RIP au niveau de tous les routeurs,
c. Configuration de la VoIP au niveau du routeur R2 et R9,

d. Configuration de la VPN entre les routeurs R5 et R12,
e. Configuration du Frame relaye entre les routeurs R4, R10 et R11,
f. Configuration de l'encapsulation PPP sur liaison série (authentification PAP ou CHAP) entre les routeurs R3 et R9
g. Configuration de l'encapsulation PPPoE sur liaison ADSL (authentification PAP ou CHAP) entre PC7 et le routeur R6 ;
h. Configuration de l'accès distant par SSH (authentification sur serveur Radius) ;
i. Configuration des Laptots.

a) Configuration du DHCP :

Le protocole DHCP (Dynamic Host Configuration Protocol) a pour fonctionnalité de fournir aux machines qui le demandent une configuration IP complète, adresse IPv4, masque de sous-réseau, passerelle par défaut, serveur DNS… [49]

- Au niveau routeur :

On va réalisée la configuration des routeurs R2, R9, R10, R11 et R12 en serveur DHCP, on prend en exemple le routeur R11.

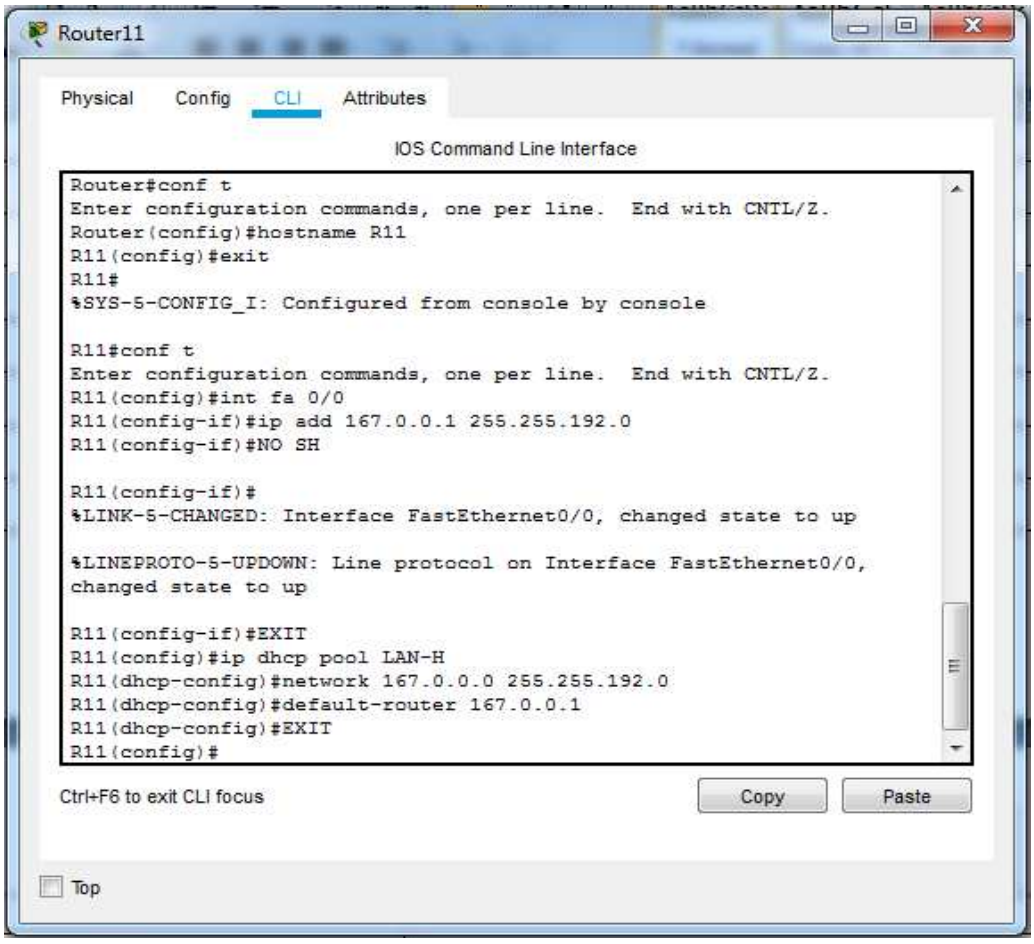


Figure IV-4 : Configuration DHCP au niveau routeur R11.

b) Configuration du routage RIP

Dans chaque routeur on active le routage RIP et on déclare les réseaux connectés directement au routeur.

Pour cette configuration on prend en exemple le routeur R10.

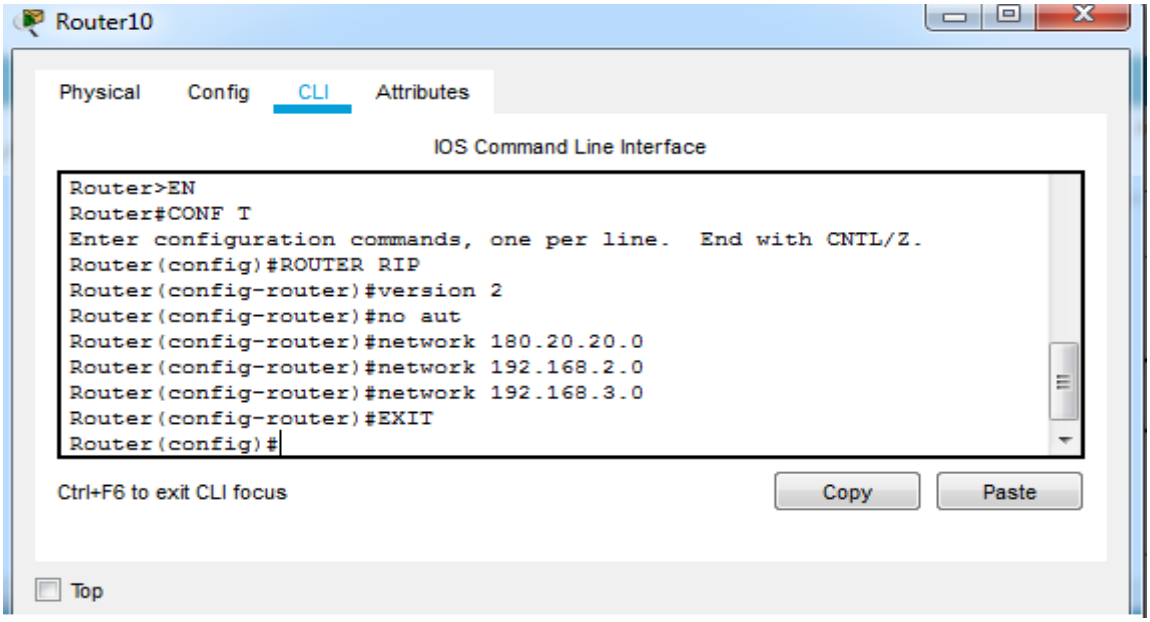


Figure IV- 5 : Configuration du protocole de routage RIP.

c) Configuration de la VOIP :

Configuration du routeur R 9. Après la configuration des interfaces et du routage on entame la configuration de la VOIP comme suit :

Nous créons et configurons le serveur DHCP utilisé pour distribué une adresse IP à chaque terminal IP du réseau.

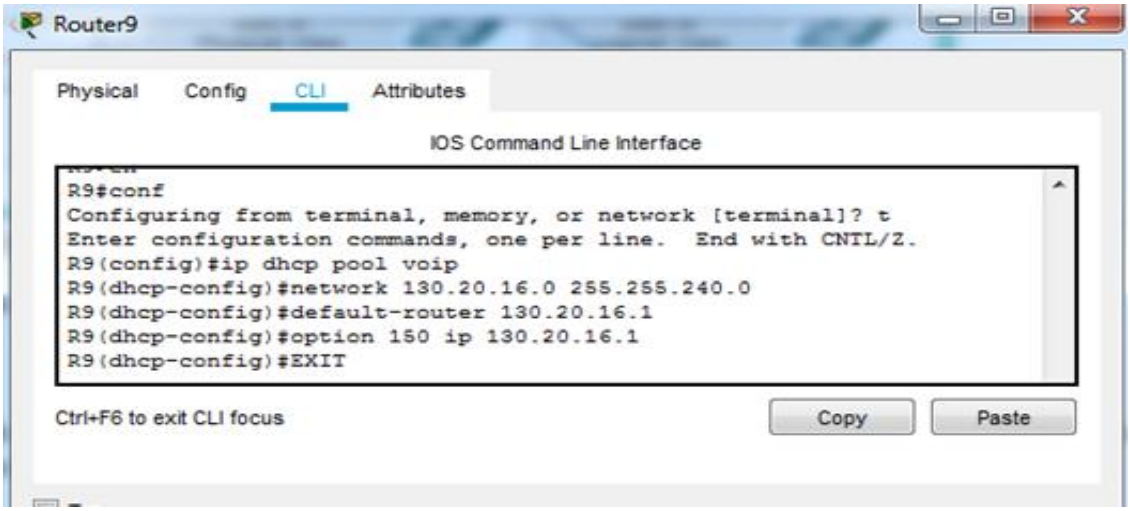


Figure IV- 6 : Configuration du serveur DHCP.

Nous allons configurer Call Manager Express afin d'activer le support VOIP sur notre réseau.

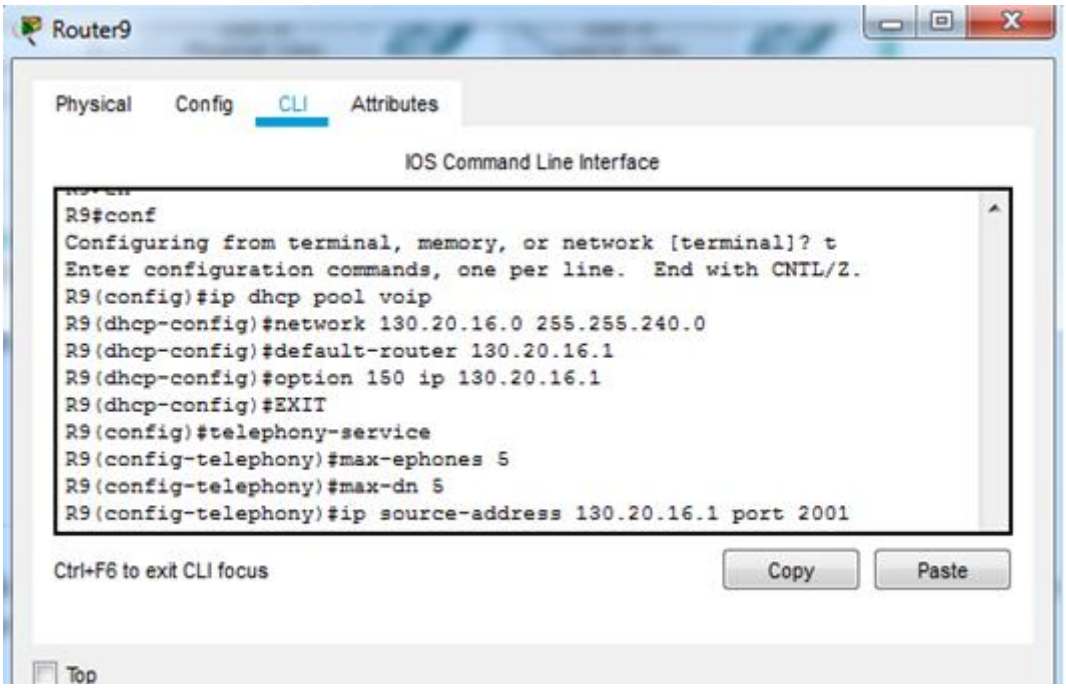


Figure IV- 7 : Configuration du service de téléphonie « Call Manager Express ».

Nous allons configurer les interfaces du Switch afin de séparer les données (transferts de fichiers par exemple) et les communications.

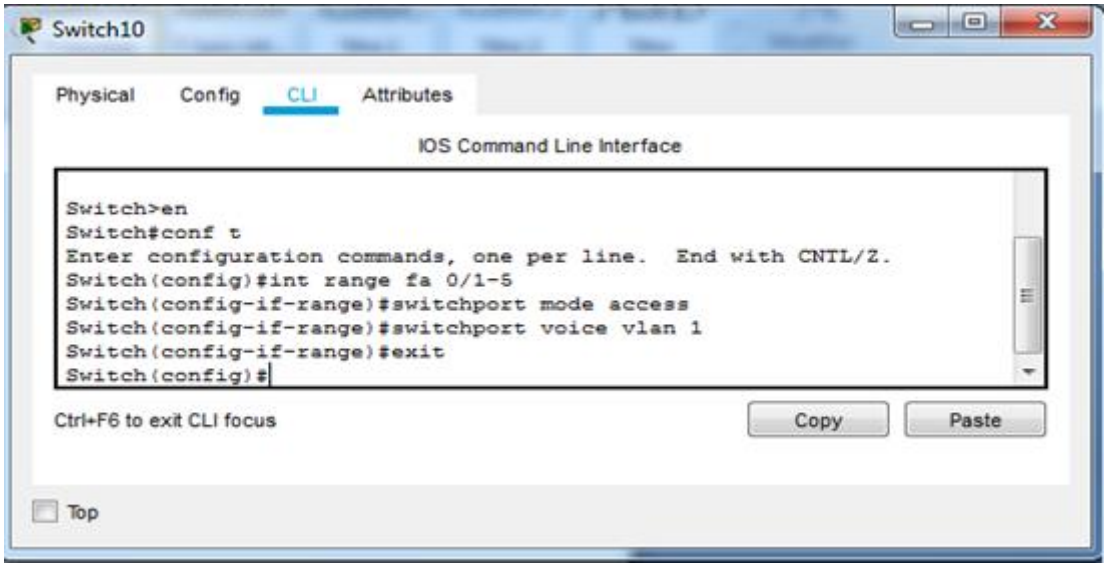


Figure IV- 8 : Configuration d'un Vlan Voice sur le Switch.

Nous allons assigner un numéro de téléphone afin de mettre les IP phones en relation.

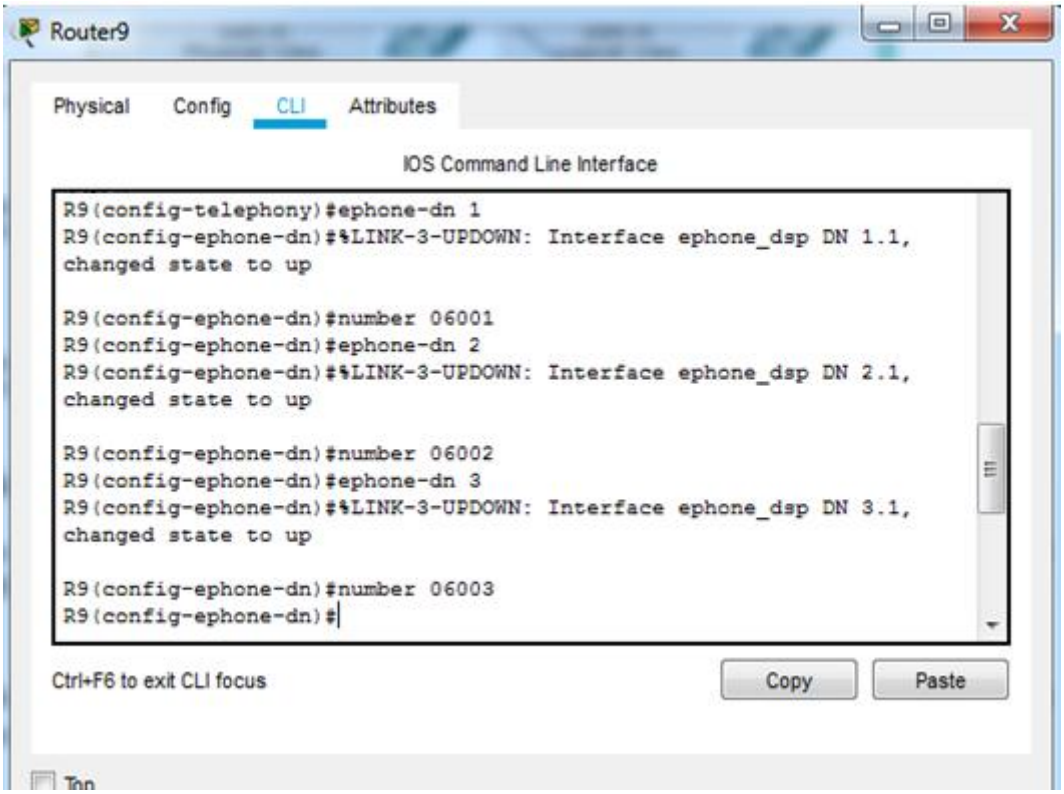


Figure IV- 9 : Configuration des IP phones sur le Routeur.

On entame la même configuration pour le routeur R2 on prenant en considération la plage d'adresse et numérotation des IP phones.

Activation de la VOIP entre les deux routeurs R2 et R9.

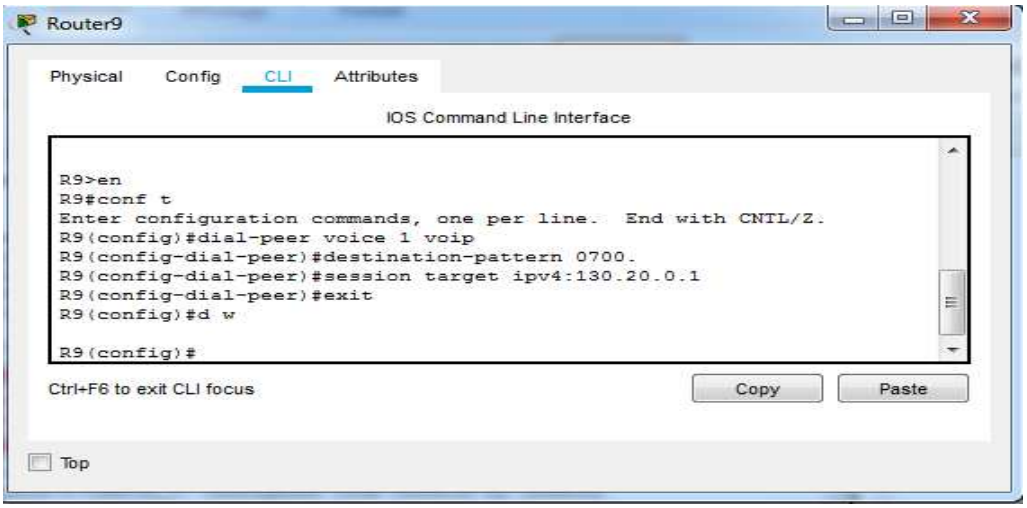


Figure IV- 10 : Activation de la VOIP sur R9.

d) *Configuration du VPN entre les routeurs R5 et R12 :*

Nous commencerons par la configuration de base des deux routeurs tels que les interfaces ainsi que le routage, ensuite on passe à la configuration du VPN qu'on va réalisée au niveau du routeur R5 et R12. [50]

Configuration du routeur R12 :

- Configuration des interfaces et du routage :

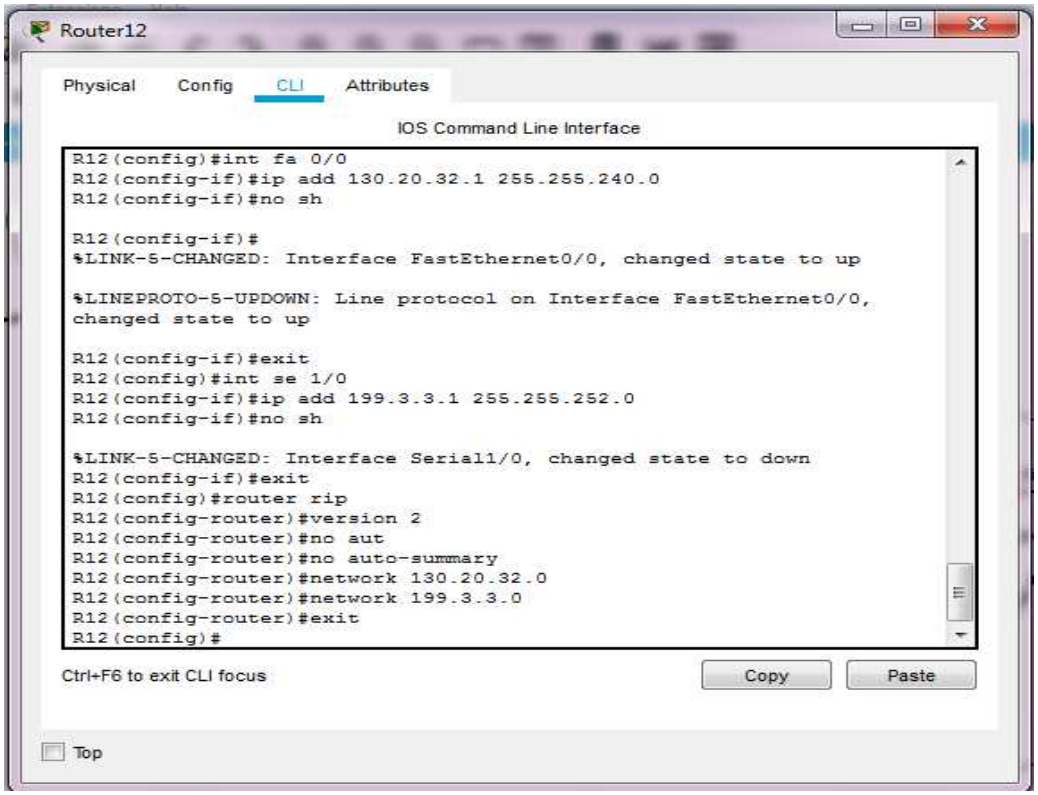


Figure IV- 11 : Configuration de base du routeur R12.

- Configuration du VPN :

On commence par active les fonctions crypto du routeur.

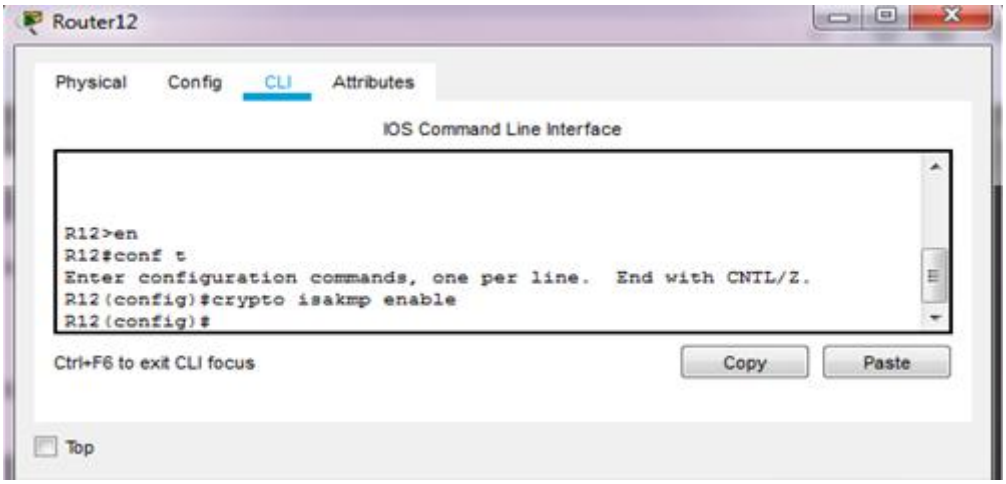


Figure IV- 12 : Activation des fonctions crypto du routeur.

Nous allons configurer la police qui détermine quelle encryptions on utilise, quelle Hash, quelle type d'authentification, etc.

Figure IV- 13 : Activation des fonctions crypto du routeur.

Ensuite on va configurer une clef d'accès au routeur R5.

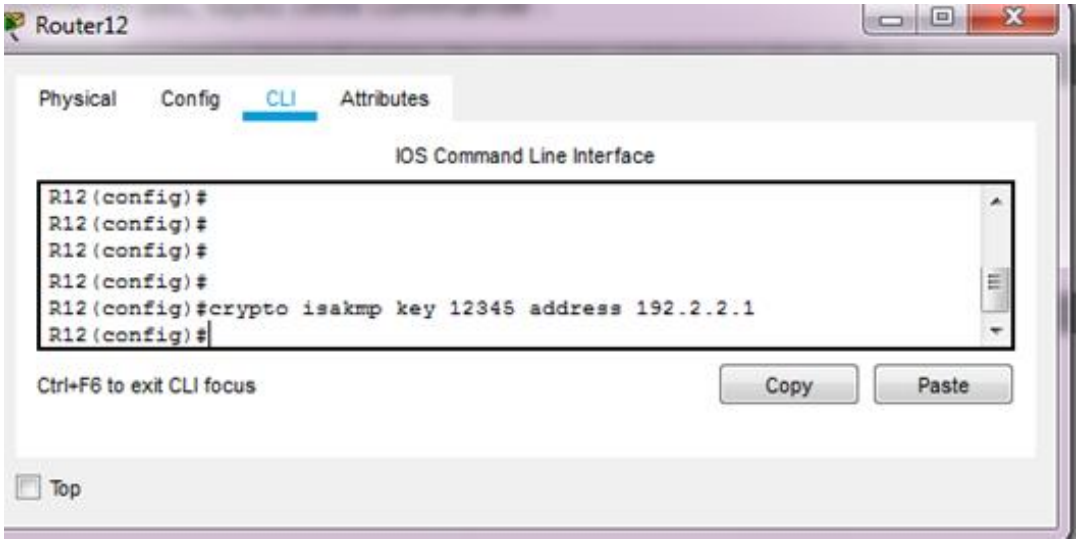


Figure IV- 14 : Configuration d'une clef d'accès.

Dans la quatrième étape on va configurer les options de transformation des données.

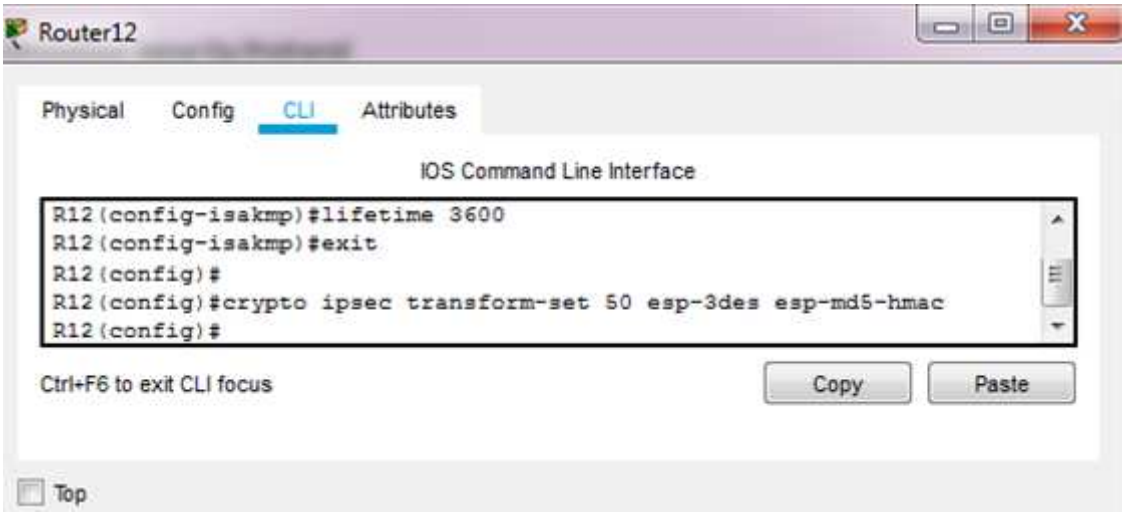


Figure IV- 15 : Configuration des options de transformation des données.

On fixe ensuite une valeur de lifetime.

Figure IV- 16 : Configuration de la valeur du lifetime.

Dans l'étape qui suit on va crées une ACL qui va déterminer le trafic autorisé.

Figure IV- 17 : Création de l'ACL.

Ensuite on va configurer la crypto map qui va associer l'ACL, le trafic et la destination.

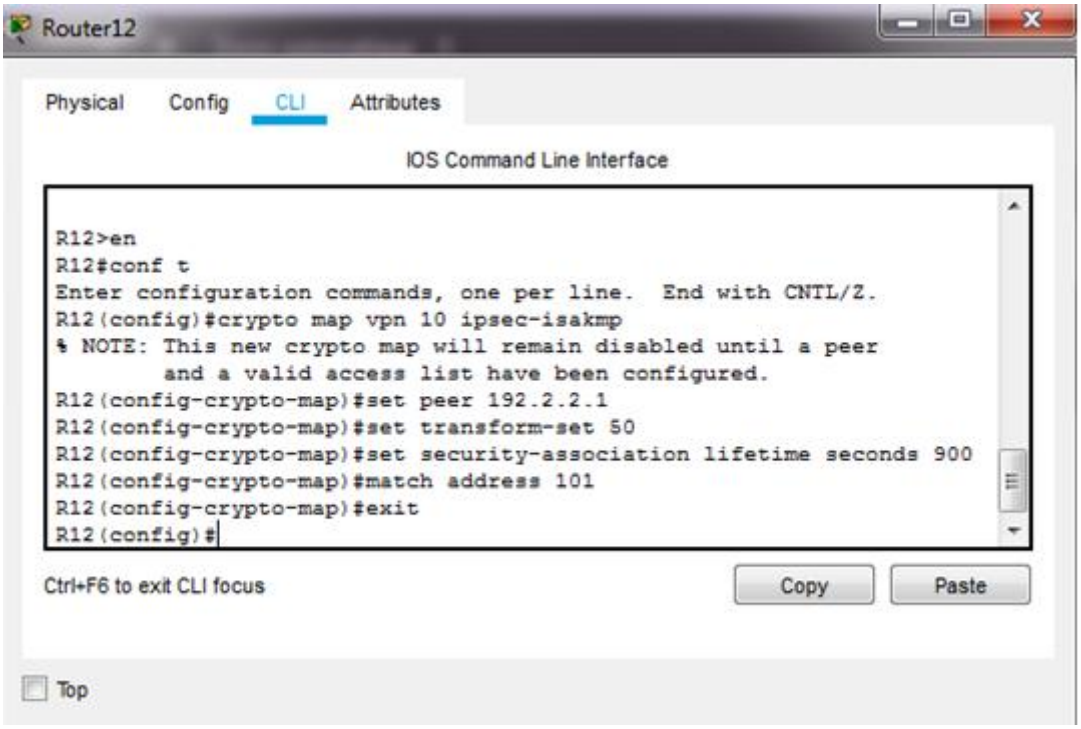


Figure IV- 18 : Configuration de la crypto map.

Dans cette dernière partie on va appliquer la crypto map sur l'interface de sortie qui est dans notre cas l'interface Se1/0.

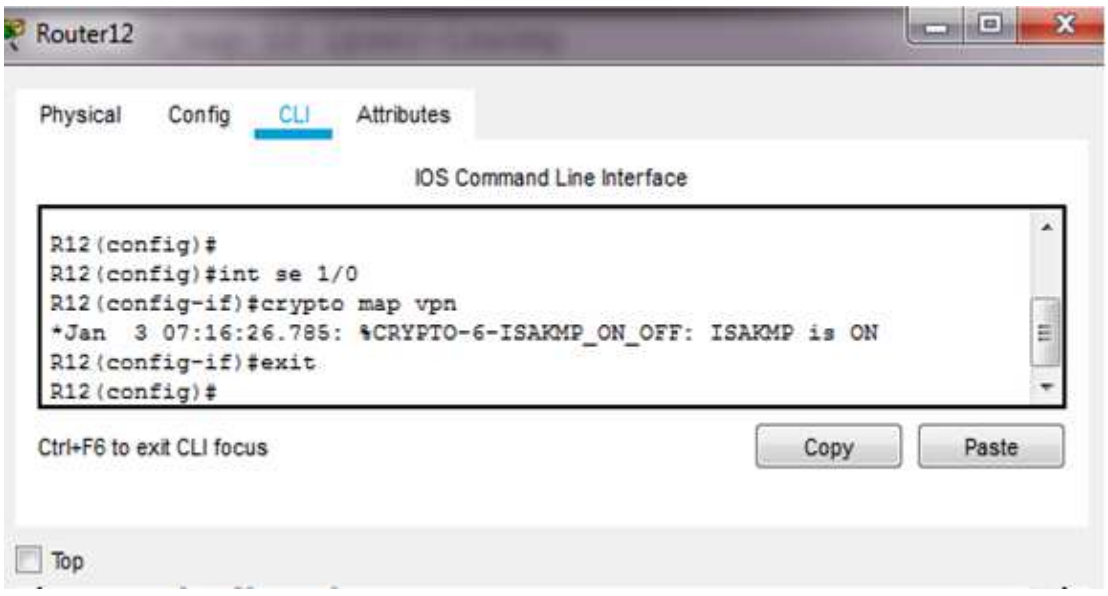


Figure IV- 19 : Application de la crypto map sur interface Se1/0.

On refait la même configuration pour le routeur R5.

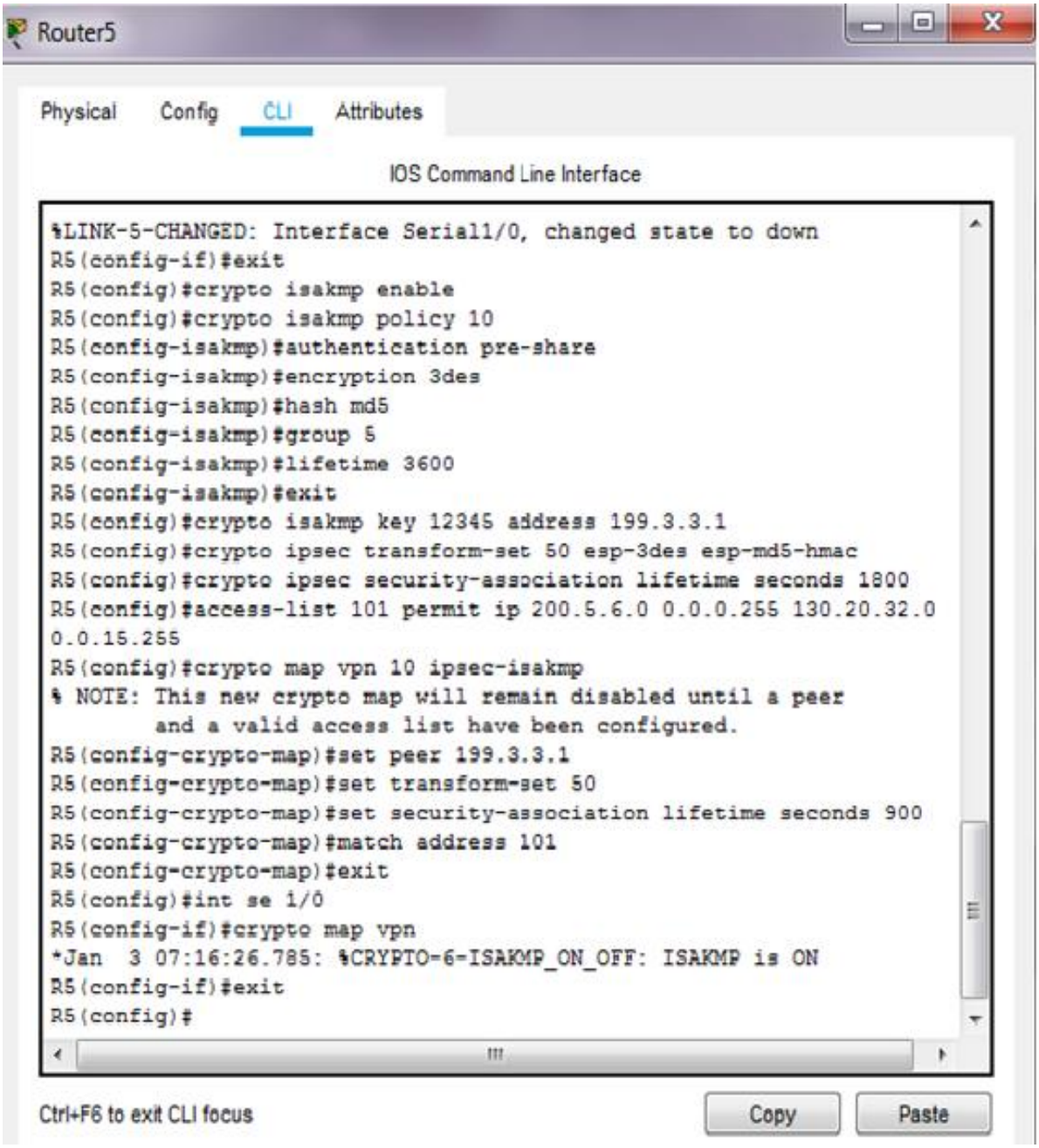


Figure IV- 20 : Configuration du VPN su le routeur R5.

e) Configuration du Frame relaye

- Au niveau du Cloud

Nous allons commencer par la configuration des interfaces du Cloud on déclarant les DLCI.

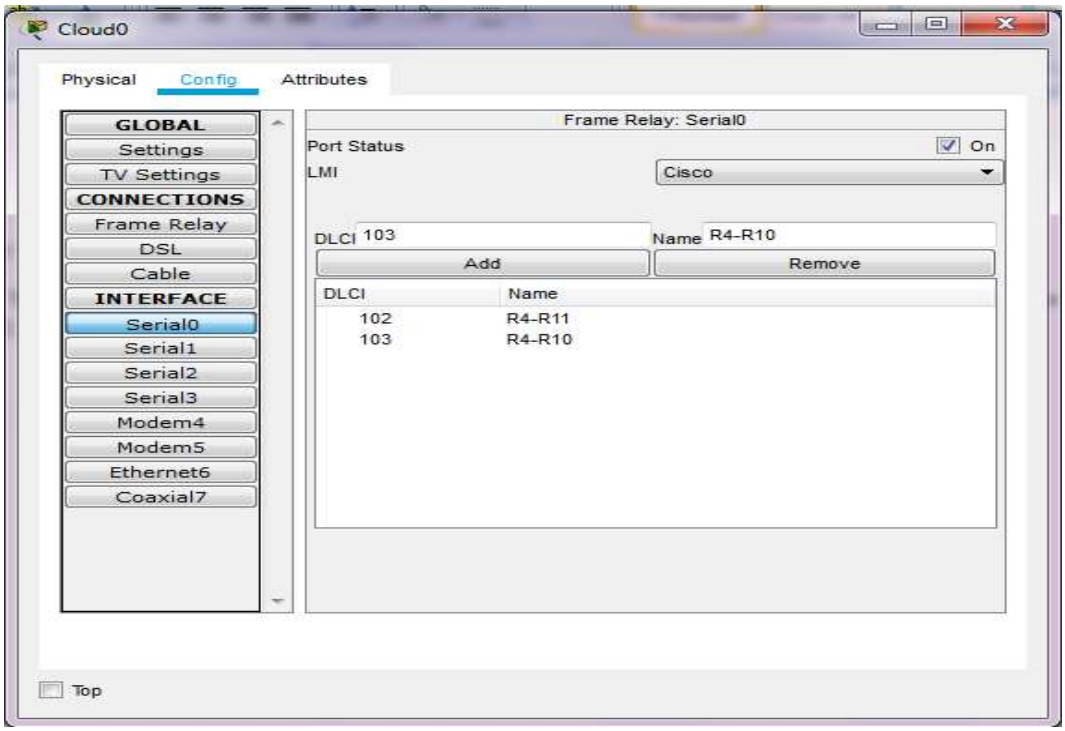


Figure IV- 21 : Attribution des DLCI aux interfaces du Cloud.

Même configuration pour les interfaces Serial1 et Serial2, en suite nous allons configurer le frame-relay.

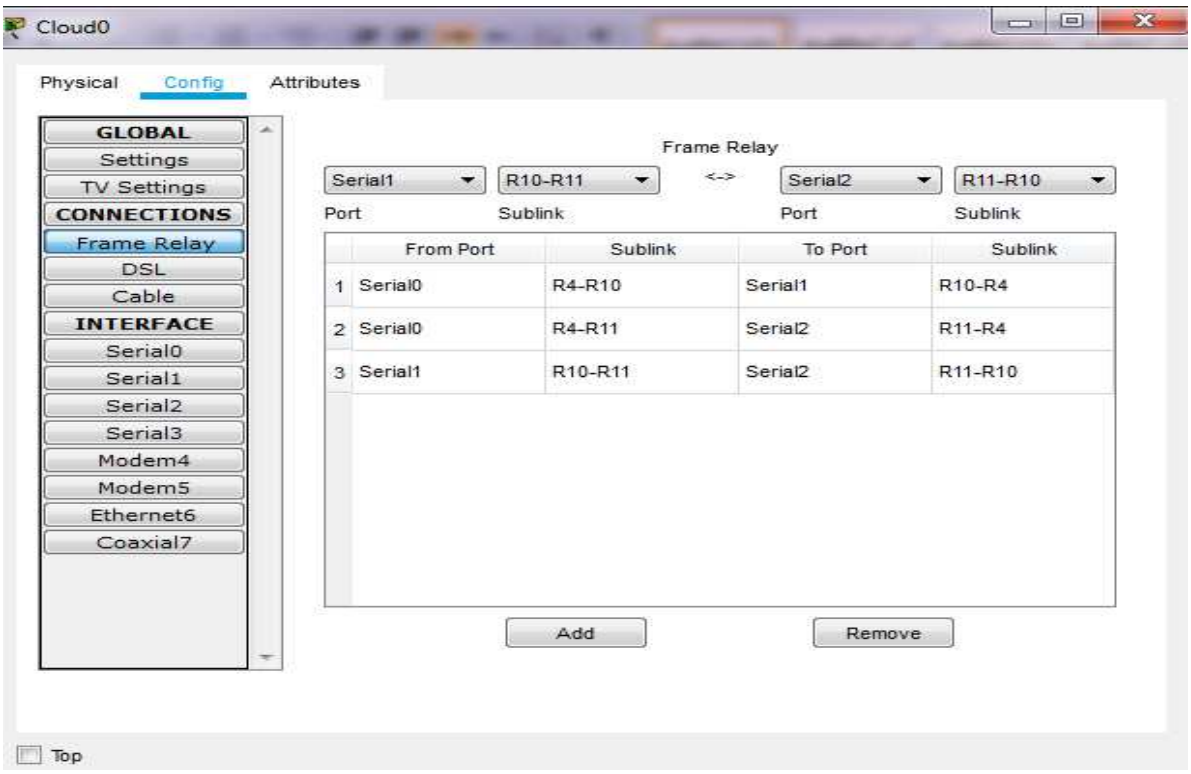


Figure IV- 22 : Configuration du frame-relay sur le Cloud.

- Au niveau routeurs

Pour cette étape on va configurer les sous interfaces frame-relay du routeur R4 comme exemple.

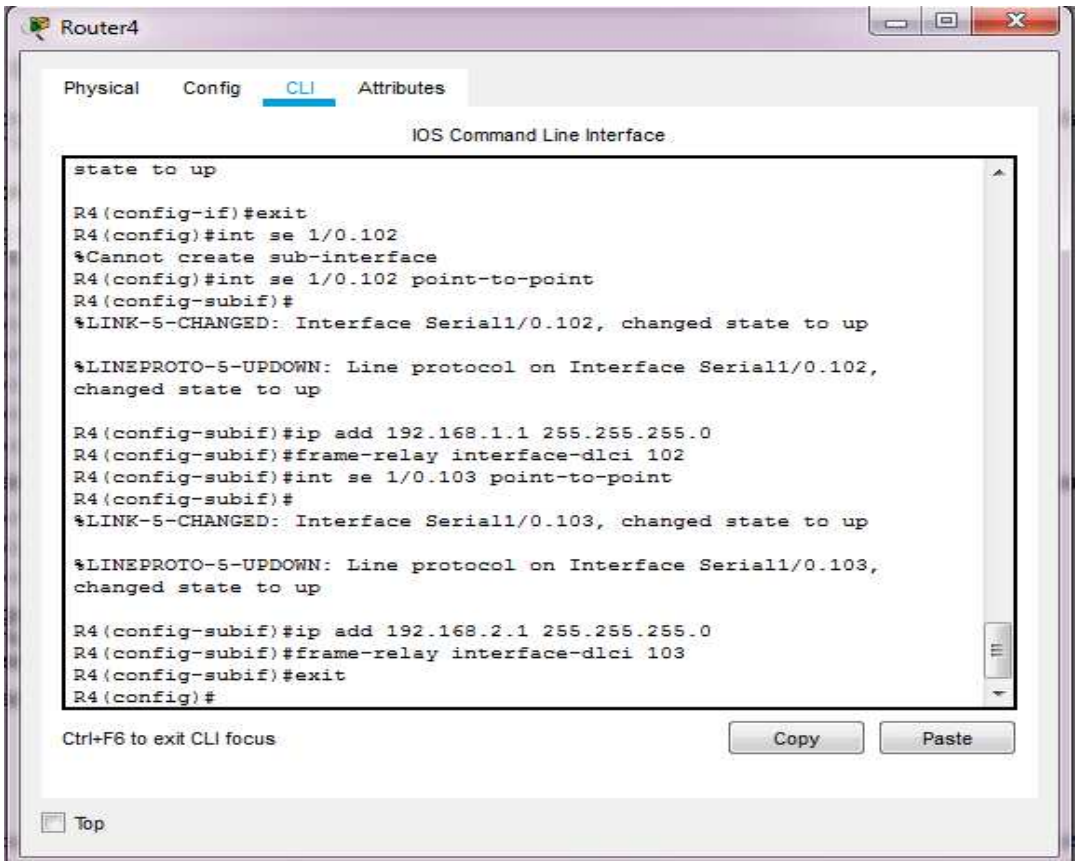


Figure IV- 23 : Configuration des sous interfaces frame-relay sur le routeur R4.

f) Configuration de l'encapsulation PPP sur liaison série

On va réaliser cette configuration entre les routeurs R3 et R9 on utilisant une authentification CHAP.

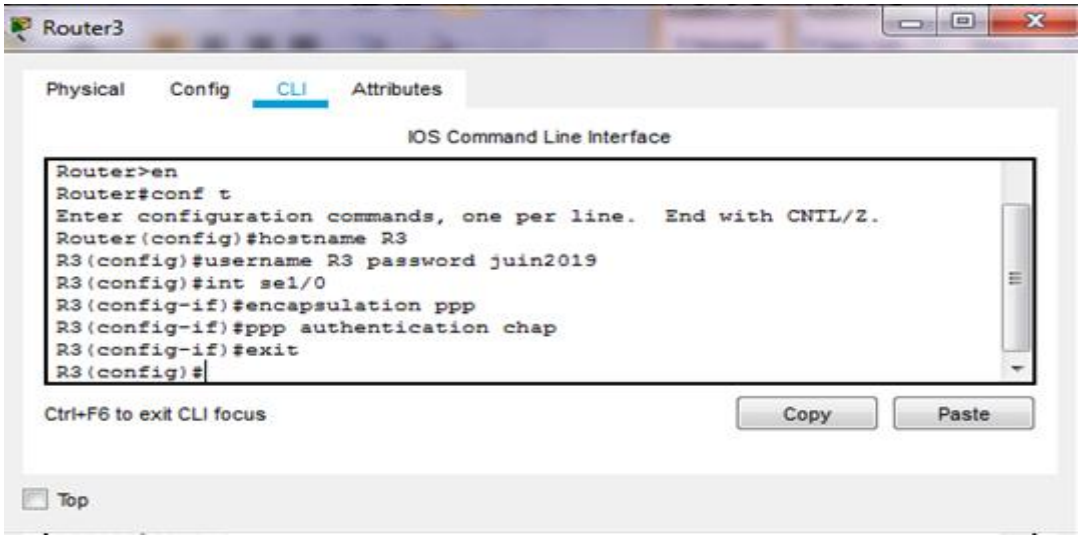


Figure IV- 24: Configuration de l'encapsulation PPP sur le routeur R3.

Les mêmes étapes seront effectuées sur le routeur R9.

g) Configuration de l'encapsulation PPPoE sur liaison ADSL

Cette configuration se réalise sur le routeur R6.

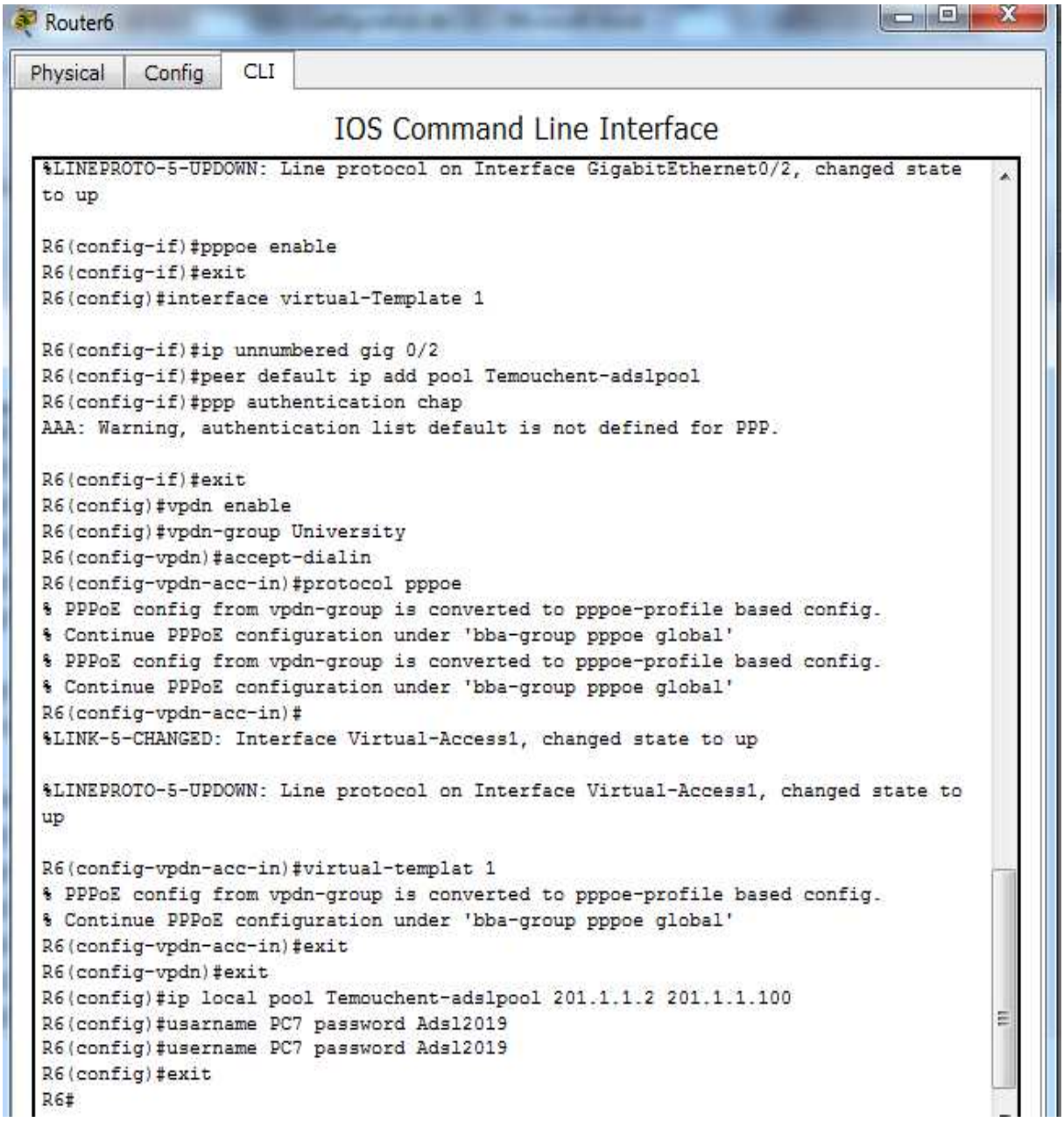


Figure IV- 25: Configuration de l'encapsulation PPPoE sur le routeur R6.

h) Configuration de l'accès distant par SSH

- Configuration du serveur Radius

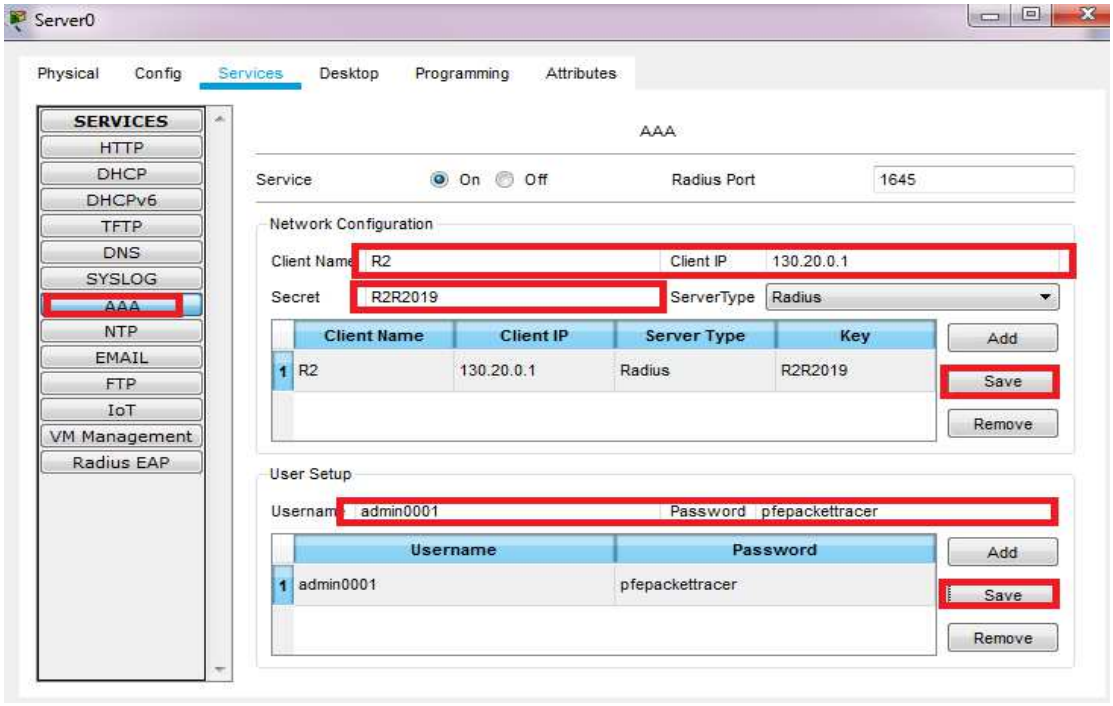


Figure IV- 26: Configuration du serveur Radius.

- Configuration du routeur R2

Nous allons configurer le protocole SSH

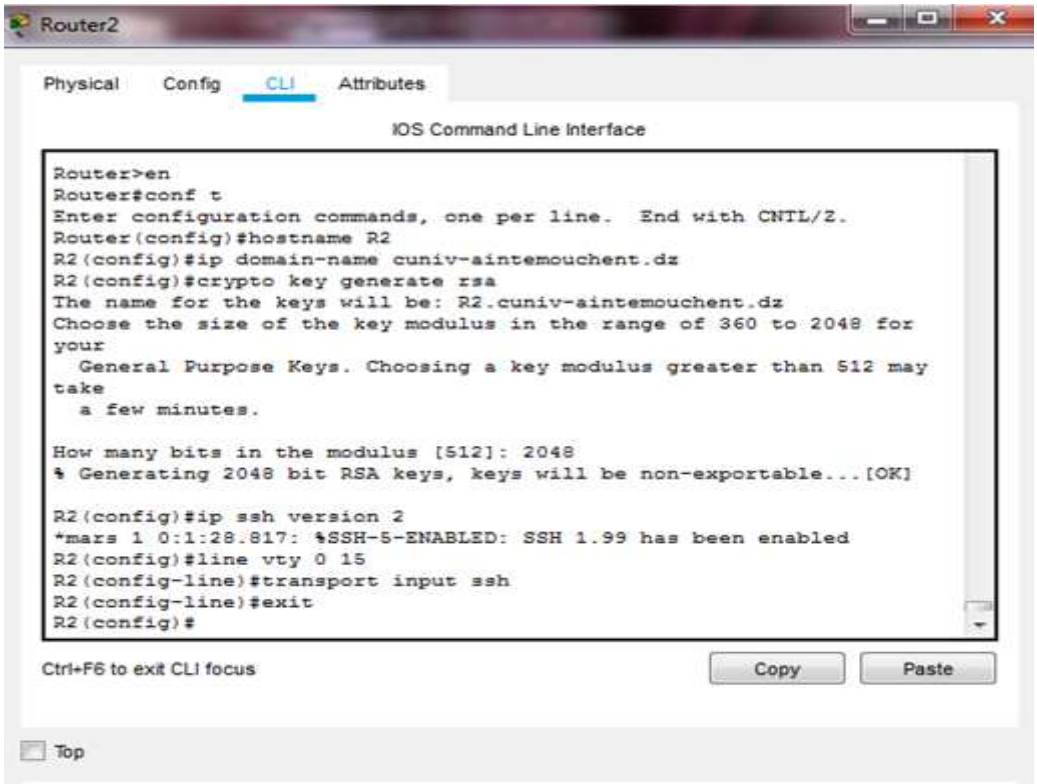


Figure IV- 27: Configuration du protocole SSH.

Ensuite on configure l'authentification radius sur R2.

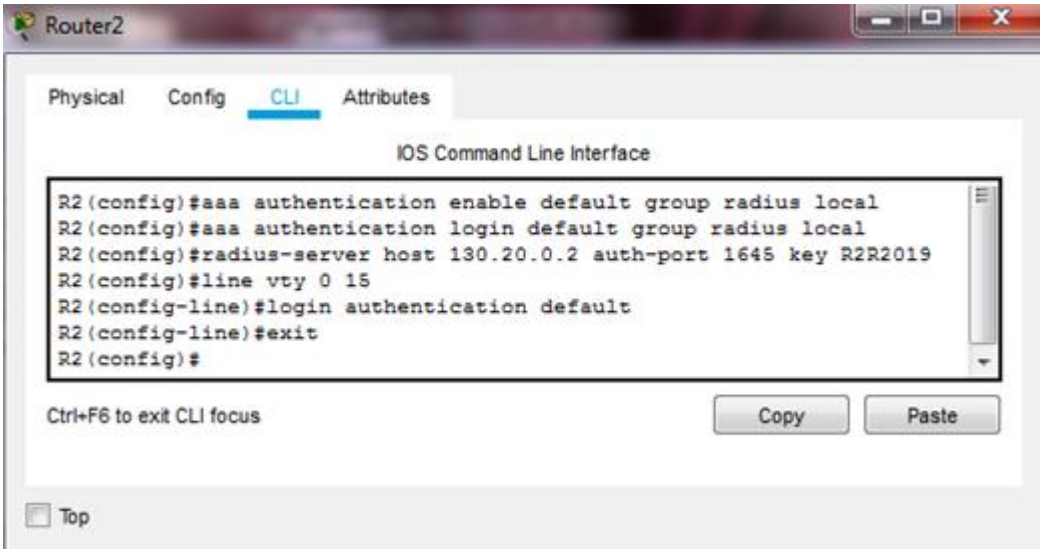


Figure IV- 28: Configuration de l'authentification radius.

i) Configuration du réseau sans fil :

- Au niveau point d'accès :

Dans l'angle configuration, port 1, on entre le nom du point d'accès puis on active l'authentification WPA2-PSK Pass Phrase. Pour notre configuration on va choisir le point d'accès 0(2) sous le nom AP3 et comme mot de passe : 123456789AP3.

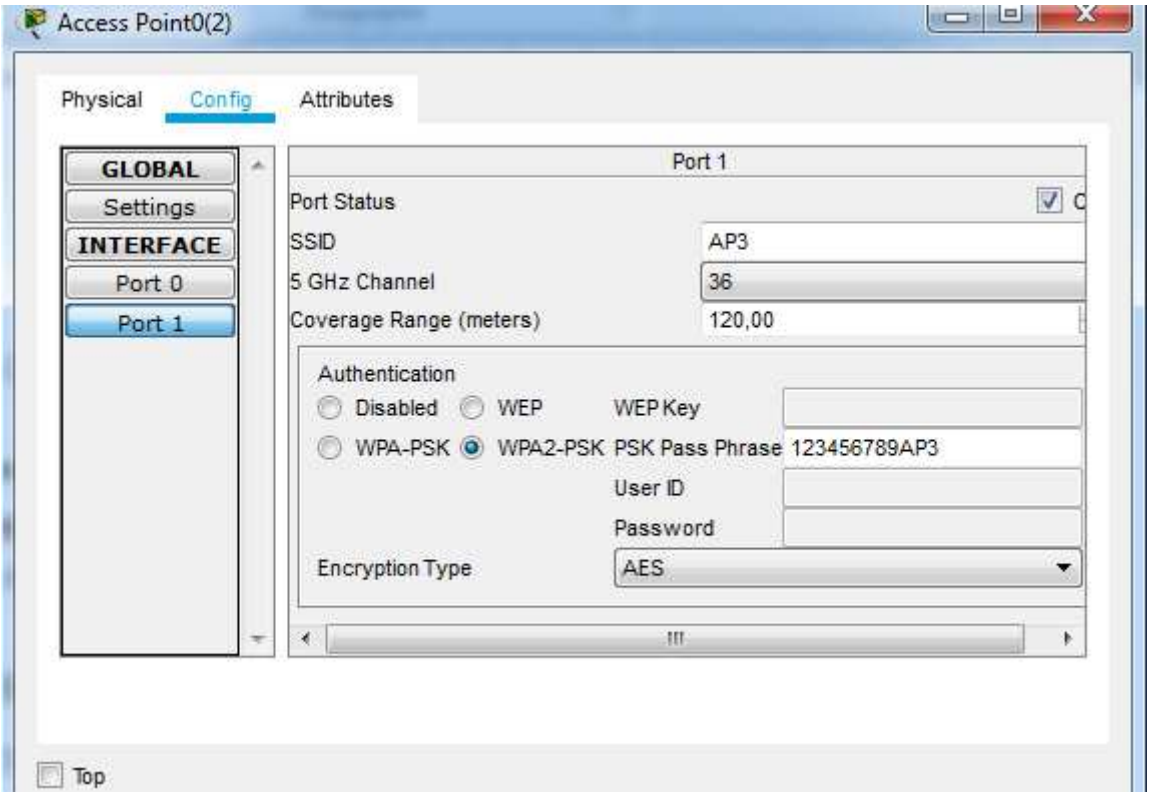


Figure IV- 29: Configuration du point d'accès.

➢ Au niveau laptop :

Dans l'angle Physical on arrête le Laptop ensuit on Change le port réseau (RJ45) par WPC300N, on démarre le Laptop.

Dans l'angle Desktop, PC Wireless, Profiles, Edit on Choisi le Wireless Network Name puis Connect, ensuit on entrer la clé, en fin Connect.

Figure IV- 30: Configuration du laptop.

IV -7/ Vérification de la configuration et de la connectivité

IV -7-1/ Vérification du DHCP :

Au niveau du routeur R10 on exécute au mode privilégier la commande « show ip dhcp binding » on obtient le résultat suivant :

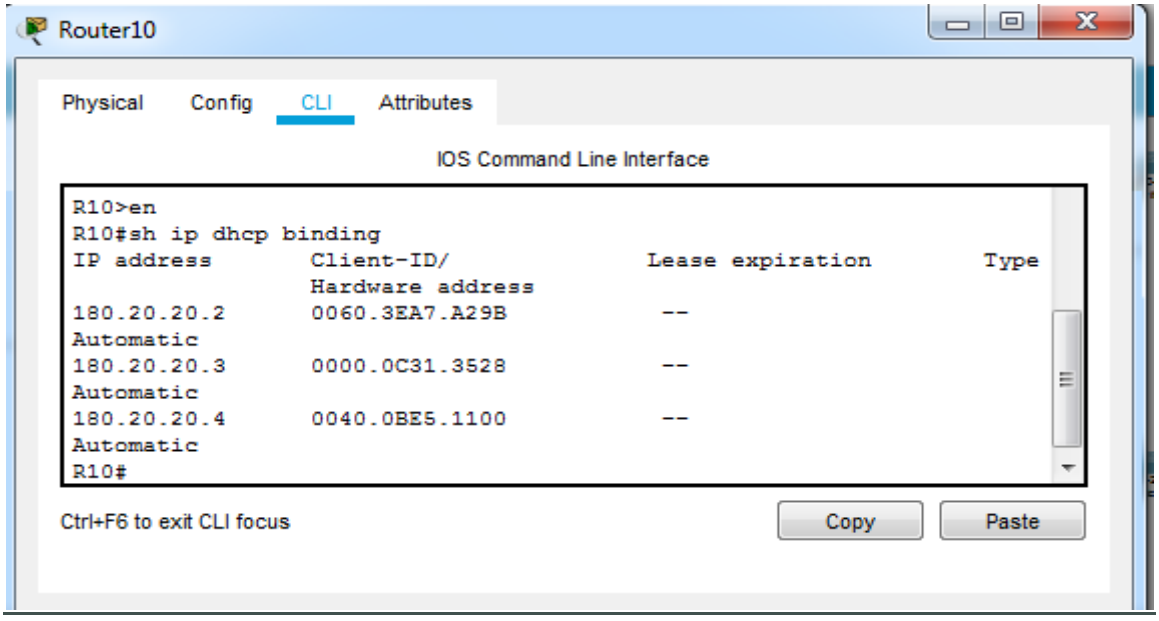


Figure IV- 31: Vérification du DHCP sur R10.

Nous voyons les adresses IP associées aux adresses MAC automatiquement après l'activation du DHCP au niveau PCs.

IV -7-2/ Vérification du fonctionnement de la VOIP :

- Au niveau IP phone :

Obtention d'une adresse automatiquement ip : 130.20.16.3/20 et d'un numéro de téléphone : 06002

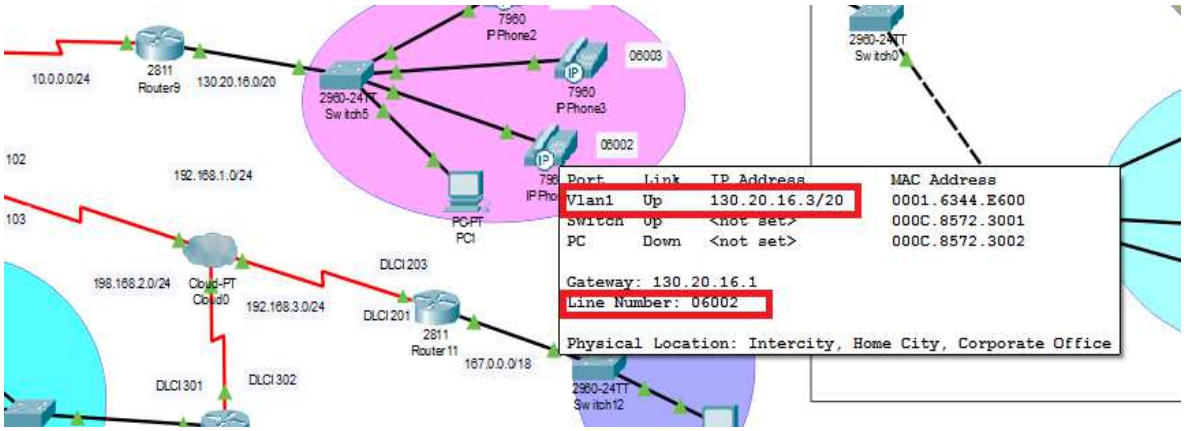


Figure IV- 32 : Vérification de la configuration du IP Phone 4.

- Teste connectivite entre deux IP phone dans le même réseau

On effectue un appel du IP phone 2 vers IP phone 3 on obtient le résultat illustré dans la figure IV-33. On voit apparaitre « Connected » sur l'écran des deux téléphones qui signifie que le service de téléphonie est fonctionnel.

Figure IV- 33 : Teste connectivite entre deux IP phones.

➢ Teste connectivite entre deux IP phone dans deux réseaux différents :

On effectue un appel du IP phone 0 vers IP phone 2 on obtient le résultat illustré dans la figure IV -34. On voit apparaitre « Connected » sur l'écran des deux téléphones qui signifie que le service de téléphonie est fonctionnel.

Figure IV- 34 : Teste connectivite entre deux IP phones de deux réseaux différents.

IV -7-3/ Vérification du fonctionnement du VPN :

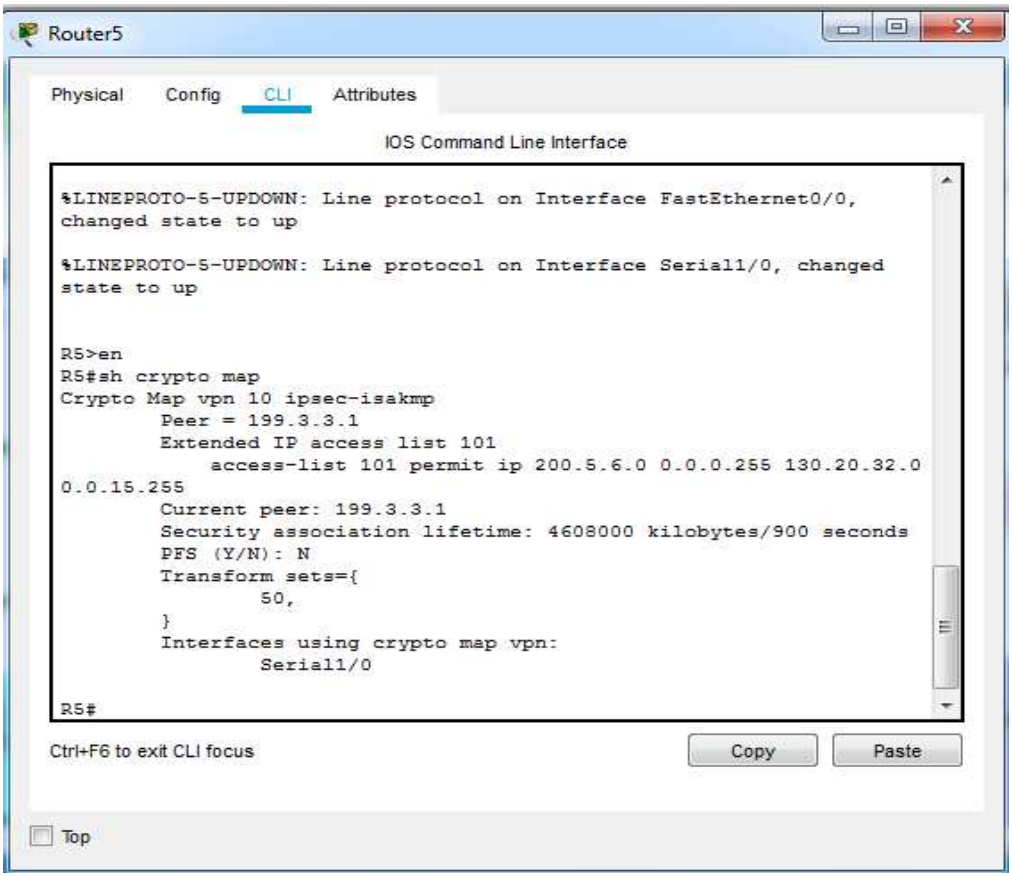


Figure IV- 35 : Vérification de la map VPN.

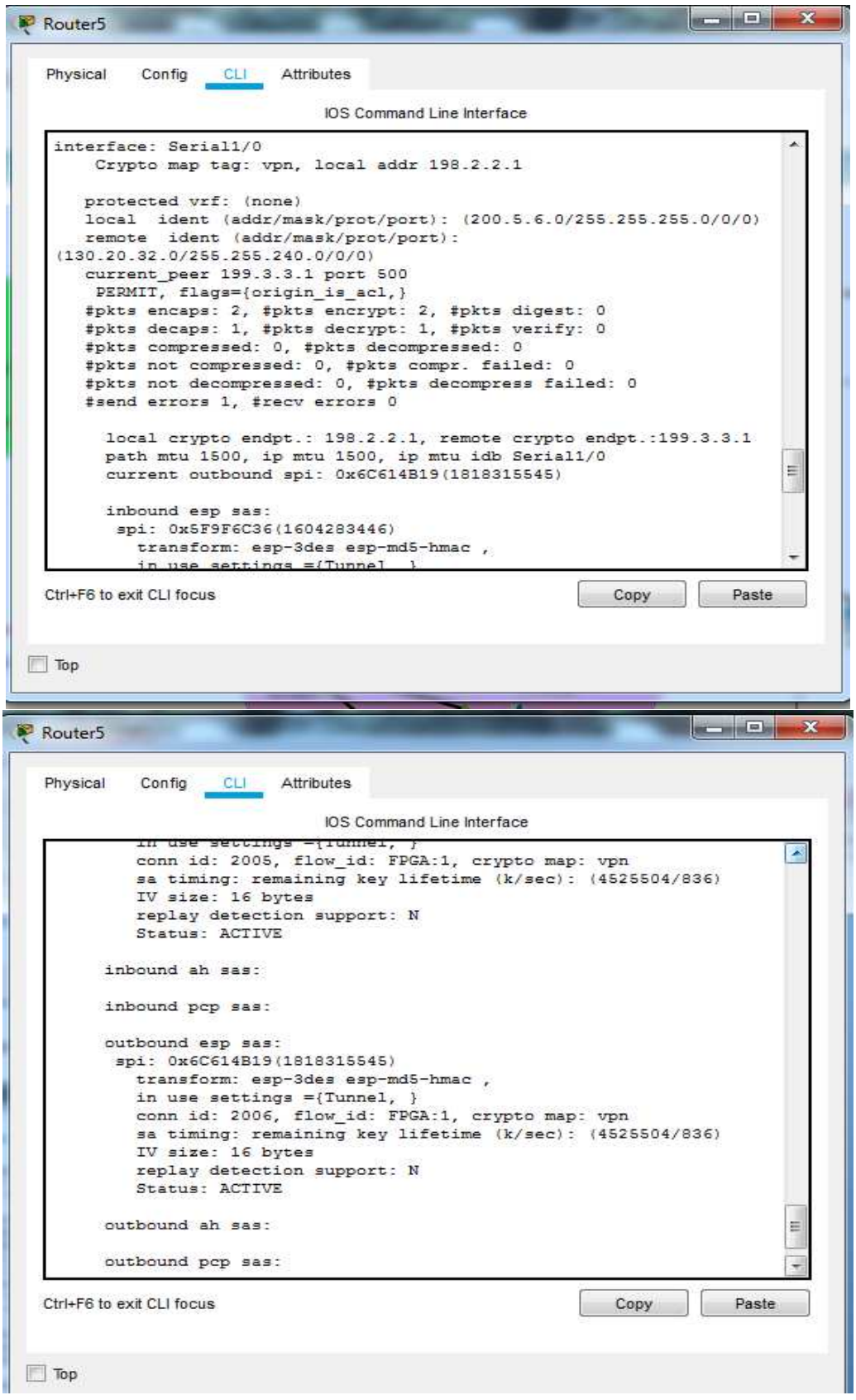


Figure IV- 36 : Vérification des opérations IPsec.

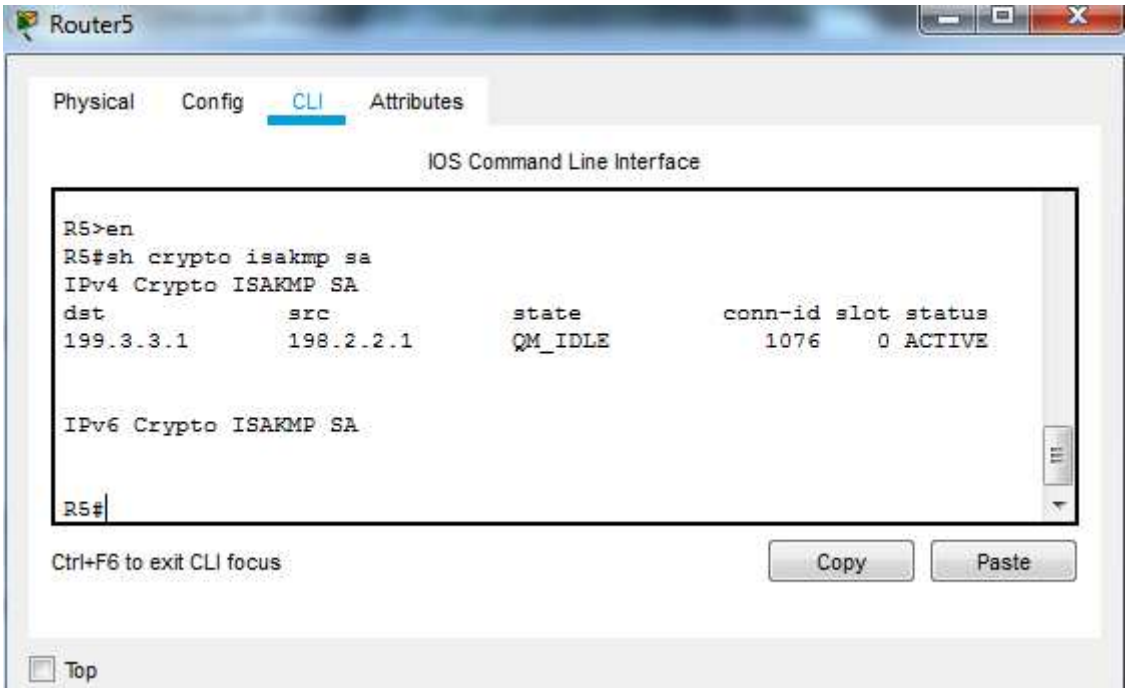


Figure IV- 37 : Vérification des opérations Isakmp.

IV -7-4/ Vérification du fonctionnement du frame-relay :

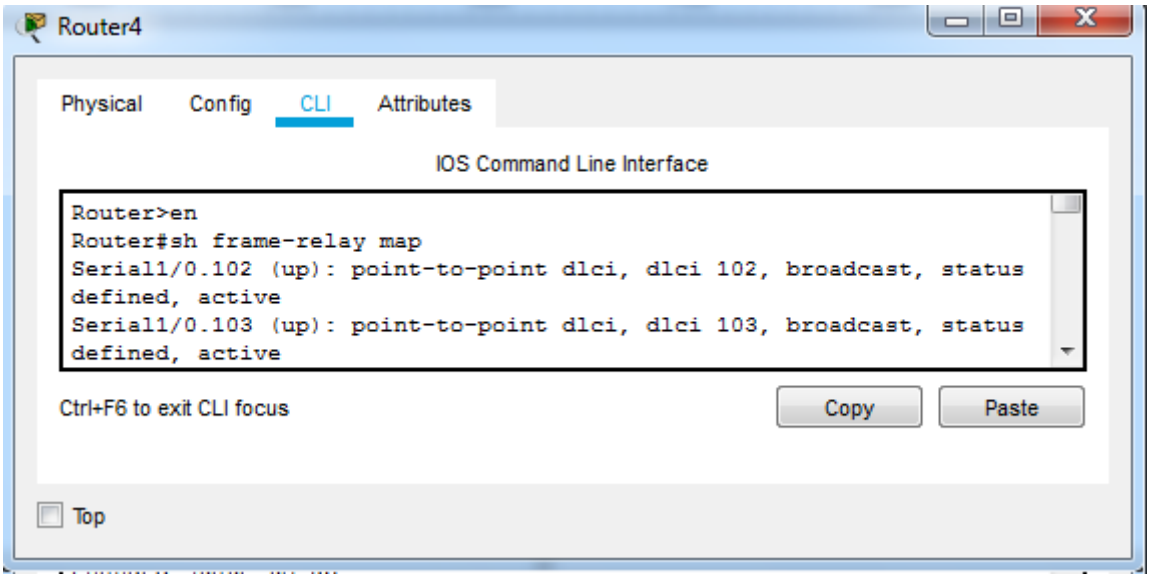


Figure IV- 38 : Vérification de frame-relay map.

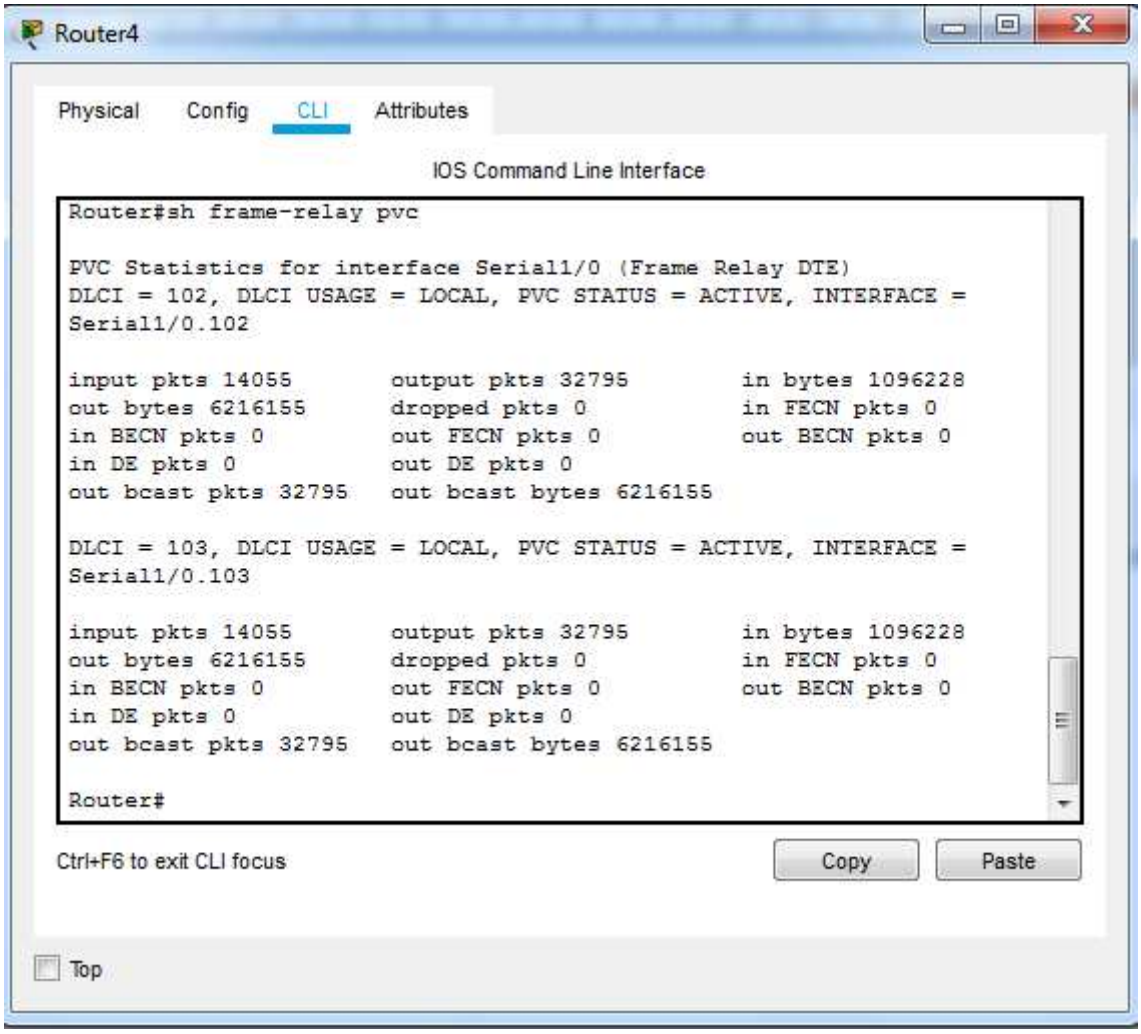


Figure IV- 39 : Vérification de frame-relay pvc.

IV -7-5/ Vérification de l'encapsulation du PPP entre le R3 et R9 :

En premier temps on va effectuer un Ping entre deux PC situe de part et d'autre des routeurs R3 et R9.

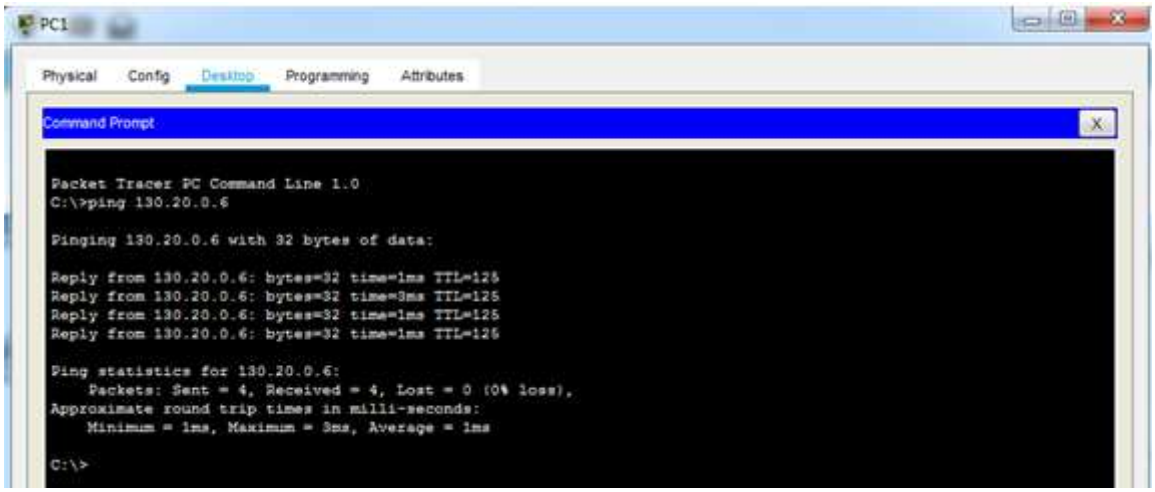


Figure IV- 40 : Test de Ping entre PC.

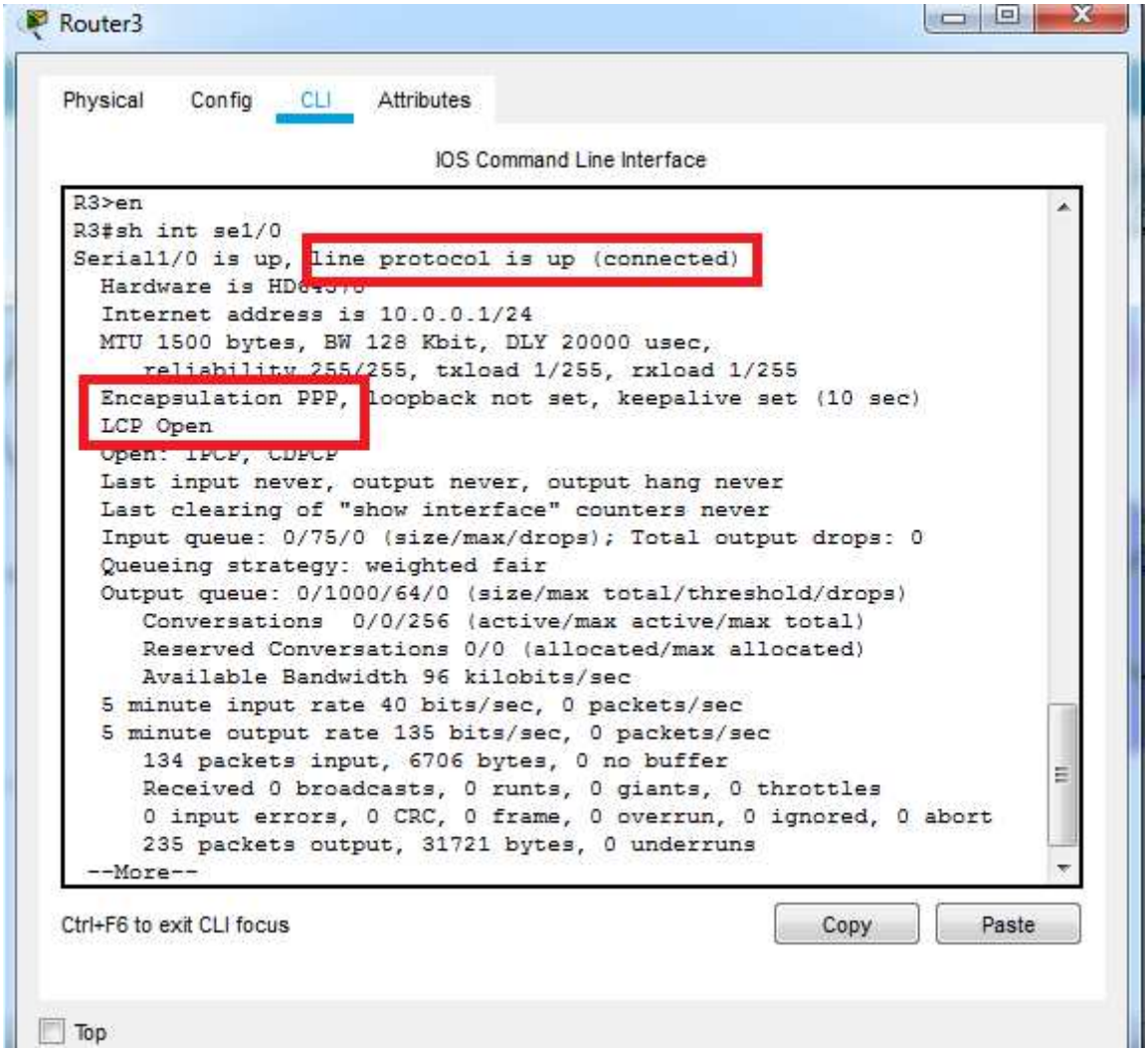


Figure IV- 41 : Vérification d'encapsulation du protocole PPP.

IV -7-6/ Vérification de l'encapsulation du PPPoP sur liaison ADSL :

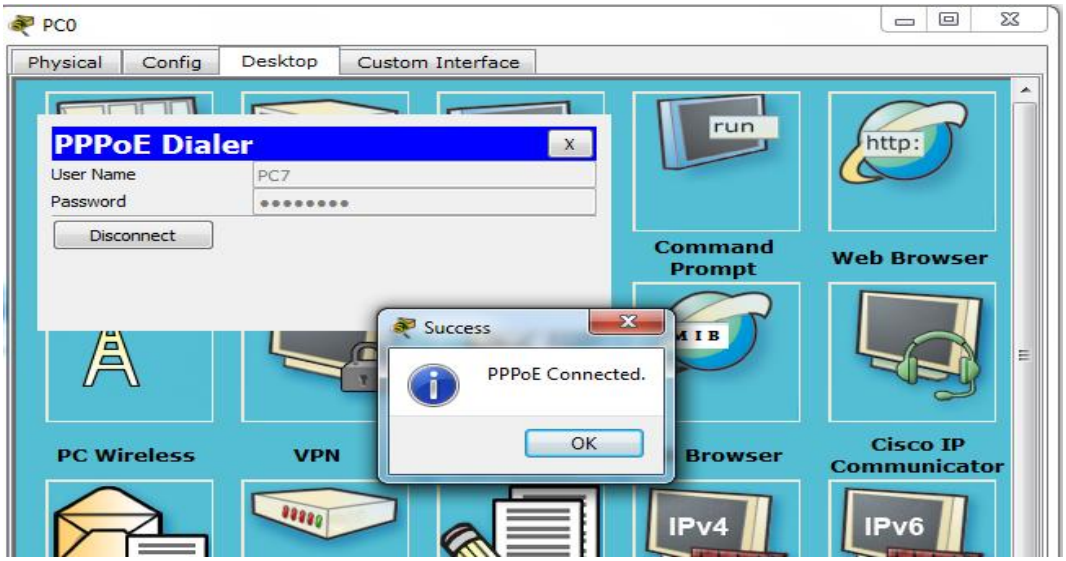


Figure IV- 42 : Test de vérification de l'encapsulation PPPoE.

IV -7-6/ Vérification de l'accès distant par SSH :

- A partir du pc on exécute la commande suivante afin d'accédé au Routeur R2:

« ssh –l admin0001 130.20.0.1 »

D'où 130.20.0.1 est l'adresse du routeur R2. On obtient le résultat qui suit :

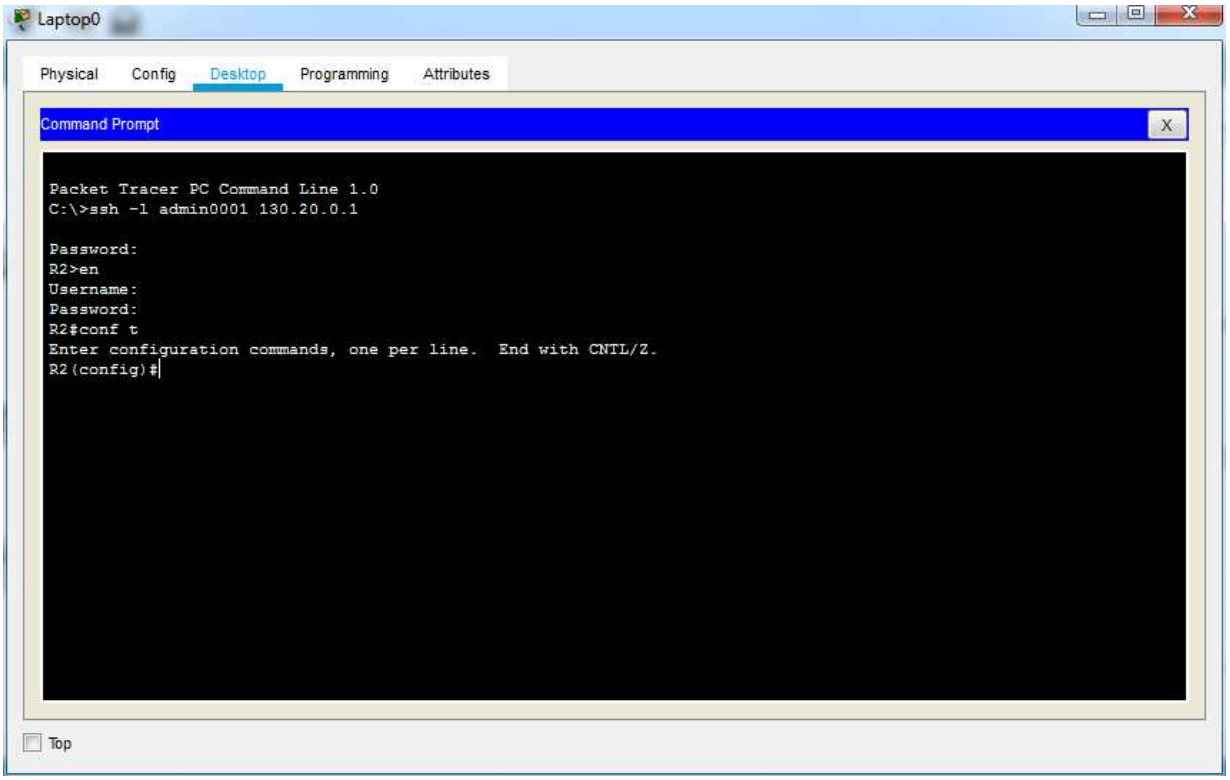


Figure IV- 43 : Test de l'accès distant du SSH.

IV -7/ Conclusion :

On a essayé dans ce chapitre d'effectué un ensemble de configuration pour la mis en place d'un réseau LAN-WAN où la topologie a été préparée d'une façon polyvalente : prise en charge du WiFi, Frame-Relay et PPP, de la QoS (VoIP) et de la sécurité (PPP CHAP, PPPoE, SSH, VPN). Une suite de tests de validation ont été conduits afin de prouver l'efficacité de ce réseau.

Conclusion générale

Conclusion Générale

Le rôle des réseaux informatiques a sensiblement évolué ces dernières années et ne se limite plus qu'aux transferts de l'information basique en toute sécurité. Le domaine de la sécurité informatique est considéré comme difficile pour sa complexité de mettre en œuvre une solution durable qui répond parfaitement aux besoins et exigences ressentis dans une entreprise, ce qui pousse les ingénieurs réseau à travailler sans relâche à fin d'arriver à une solution permettant l'amélioration de la sécurité de leur réseau.

En effet, Nous avons essayé à travers ce mémoire de concevoir une solution aidant une entreprise à préparer un dossier technique d'un projet, le maquettage et sa mise en œuvre.

Ce projet a traité en première partie les aspects des réseaux locaux virtuels ainsi que la norme 802.1q qui a été dédiée pour répondre à un besoin de normalisation sur le transport des VLANs, et une présentation du protocole d'administration et de gestion des VLAN nommé VTP. En deuxième partie La qualité de service de la VoIP dans une entreprise; la troisième partie dédié à la technologie WAN et sécurité VPN où nous avons basé notre étude de façon claire sur les notions, le fonctionnement ainsi que les différents protocoles utilisés pour la mise en œuvre d'un réseau VPN. Et en fin, nous avons consacré la dernière partie à la configuration du réseau où nous avons présenté l'outil de simulation Packet tracer ayant servi à l'élaboration du projet, tout en expliquant les étapes de configurations des différents équipements, nous avons également procédé à une série de tests pour évaluer l'efficacité de notre solution.

Ce projet nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour nous d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatiques.

Dans l'espoir que ce modeste travail contribue à l'enrichissement du fond documentaire pour la filière de Télécommunication et une base d'exploitation initiale, cette topologie a été préparée d'une façon polyvalente afin de servir de référence aux futurs étudiants.

Bibliographie

Bibliographie

[3] Memoire fin de cycle " Interconnexion et segmentation des sites distant –VPN et VLAN-Cas d'étude : SCS" réalisé par Melle OUHNIT Meriem et Melle SALMI Mounia, université de Bejaia année 2017/2018

[10] Mémoire fin cycle « proposition de solution de sécurité pour le réseau local de l'hopital d'Amizour » réalisé par Mr. Fares KHELOUFI et Mr. Yacine IKHLEF. 2015-2016

[13] Wikipédia Qualite de service

[14] Solutions réseaux pour la voix sur IP (VOIP)/ Netgear.

[15] Wikipédia Qualite de service

[16] Qualité de services dans les WLAN realize par: MOUNIR Assia, BOULLAILI Imane BAKKALI Asmae. Projet Réseaux Mobiles.ecole nationale des Scienses Appliquées de Tanger 2008-2009.

[17] Rapport de projet intetule L'implémentation des algorithmes de gestion de la QoS dans les routeurs Presente par Hajar OUAD Nasreddine LATRECHE Hajar BOUTKHIL Mostafa MOHIB.université d'AVIGNON. CERI-année 2015-2016.

[19] La Qualité de Service (QoS) Exemples de mise en application des principes de priorisation des flux dans des équipements de niveau 2 et 3.

[22] Sécurité des systems d'information/ Wikipedia.

[23] Rapport de stage «Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN» élaboré par Khaled TRABELSI et HaythemAMARA. UNIVERSITE VIRTUELLE DE TUNIS 201-2011.

[27] Point-To-Point wikipdia.

[33] Livre GUY pujolle 5eme édition les réseaux

[34] le livre Fonctionnement, mise en oeuvre et maintenance des Réseaux Privés Virtuels [2ième edition]

[36] Le Livre Tableaux. Bord.securité.réseau 2eme edition

[47] mémoire fin d'etude univ béjaia presente par BOURNANE Fazia et KHELFAOUI Yasmina sous le theme d'Etude et configuration d'un réseau de campus (SONATRACH Béjaïa)

[48] mémoire fin cycle proposition de solution de sécurité pour le réseau local de l'hopital d'Amizour réalisé par Mr. Fares KHELOUFI et Mr. Yacine IKHLEF, 2015-2016

[50] TP: Création d'un réseau virtuel privé (VPN) entre deux sites distants avec VPN IPsec. Centre Universitaire Belhadj Bouchaib - Ain Temouchent Master Réseaux de Télécommunications

Webliographie

[1] http://benhur.teluq.uquebec.ca/SPIP/inf1160/IMG/pdf/inf1160-notionsfondamentales.pdf Notions fondamentales.

[2] http://benhur.teluq.uquebec.ca/SPIP/inf1160/IMG/pdf/inf1160-notionsfondamentales.pdf Introduction les différents types de réseaux.

[4] https://fr.slideshare.net/eliebogning/chapitre-i-introduction-au-reseau-informatique./ Les réseaux informatiques.

[5] https://www.cours-gratuit.com/cours-reseau/formation-complet-sur-l-architecture-d-un-reseau-informatique

[6] https://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfmsov.pdf

[7] http://perso.modulonet.fr/~placurie/Ressources/BTS2-AMSI/Chap-10-%20Les%20VLAN.pdf

[8] (https://www.over-blog.com/Questce_que_le_VLAN_Trunking_Protocol_VTP-1095203942-art157378.html)

[9] https://www.academia.edu/12345147/Introduction_Aux_VLAN

[11] https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/

[12] http://www.ccnablog.com/ether-channel/

[18] http://www.mathieu-dubois.fr/E6SR/SISR3-DuboisMathieu-TP06-QoS.pdf/ Priorisation des flux et qualité de service. SISR3-TPN°6 Dubois Mathieu. 2018-2019.

[20] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/qos/configuration_guide/b_qos_152ex_2960-x_cg/b_qos_152ex_2960-x_cg_chapter_011.pdf

[21] Cours Cisco/ https://cisco.goffinet.org/ccna/ethernet/ Technologies LAN/WAN.

[24] http://fx.pottier.free.fr/rezo/Frame%20Relay.htm / Réseau et télécommunication

[25] http://perso.prism.uvsq.fr/~mogue/INI2/2_Cours.pdf / Cours Réseaux Haut Débit partie 3.

[26] http://www.coursnet.com/2014/11 / Cours : Le relais de trames (Frame Relay) en détails.

[28] http://info-technologie-cours.blogspot.com/2013/02 /Suite: Cours sur les réseaux Informatiques étendus WAN.

[29] https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html

[30] https://www.cisco.com/c/fr_ca/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.pdf

[31] https://cisco.goffinet.org/ccna/wan/ppp-pppoe-mlppp/

[32] https://coursreseaux.com/wan-ppp-pppoe-tunnel-gre-bgp-cisco/

[35] https://www.researchgate.net/publication/228818484_IPSEC_presentation_technique

[37] http://www.linux-france.org ACL Dernier accès juin 2016

[38] https://medium.com/@ElianisTech/introduction-au-cisco-packet-tracer-basique-476df253683c

[39] https://www.commentcamarche.net/faq/17446-qu-est-ce-qu-un-routeur

[40] https://www.commentcamarche.net/faq/17443-qu-est-ce-qu-un-switch

[41] https://www.quantic-support.fr/offres/cloudtech/description

[42] https://www.linksys.com/fr/r/amplificateur-de-signal/qu'est-ce-qu'un-point-d'acc%C3%A8s/

[43] https://www.imedias.pro/cours-en-ligne/informatique/ordinateur/qu-est-ce-qu-un-ordinateur/

[44] https://ordinateur.ooreka.fr/comprendre/ordinateur-portable

[45] https://www.commentcamarche.net/forum/affich-3769154-ip-phone-c-est-quoi

[46] http://www.siloged.fr cours les réseaux informatiques. Lycée Théodore DECK - NB2011..

[49] https://www.ciscomadesimple.be/2013/04/08/configuration_dhcp/

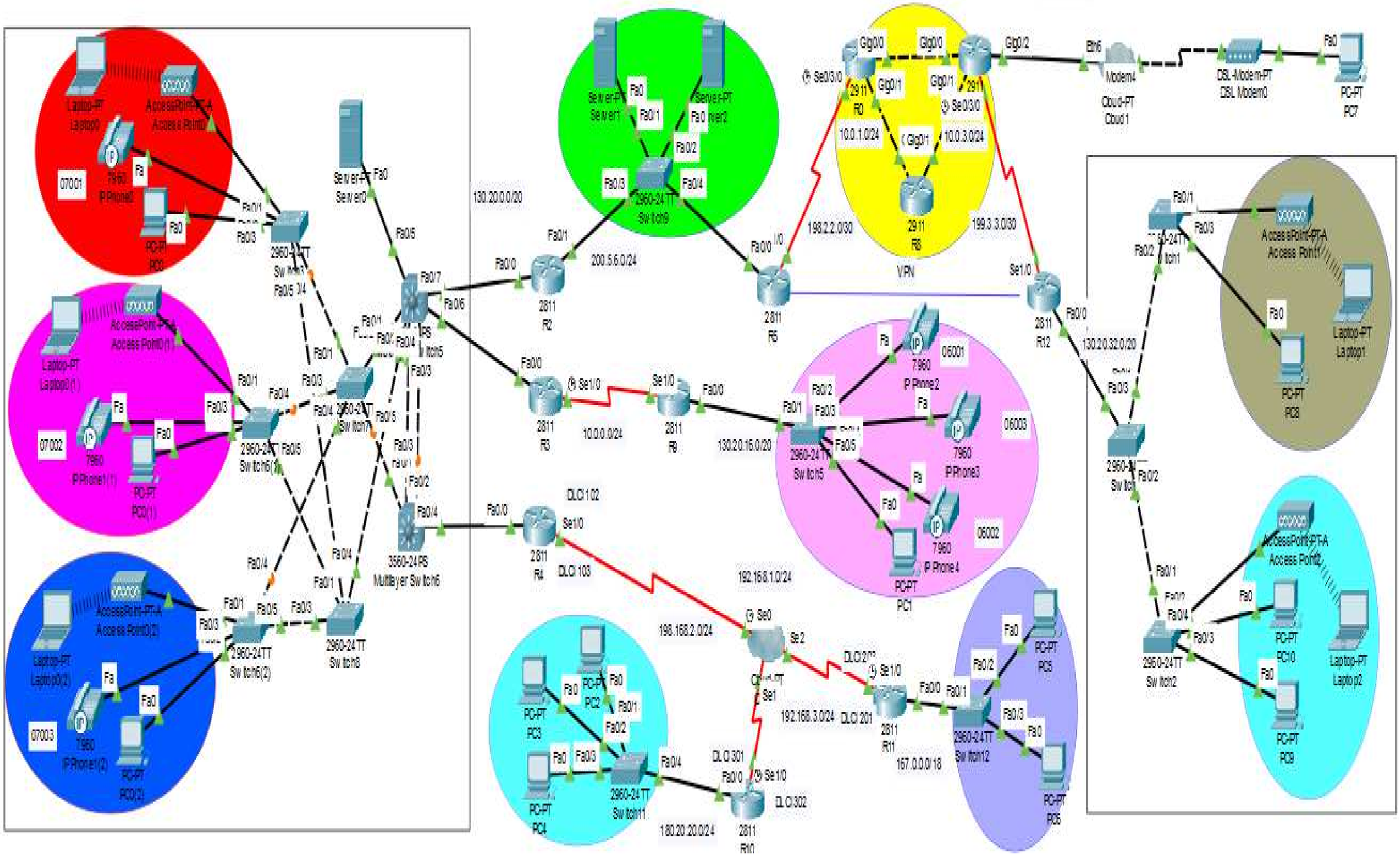


Figure IV-2 : Architecture réalisée.