ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

LABORATORIOS DE TELEFONÍA IP

ELABORACIÓN DE PRÁCTICAS DE LABORATORIO APLICADAS AL ASEGURAMIENTO Y CALIDAD DE SERVICIO DE LA INFRAESTRUCTURA DE VOZ SOBRE IP.

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN TELECOMUNICACIONES

ALEJANDRA PRISCILLA SILVA GARCIA
alejandra.silva@epn.edu.ec

DIRECTOR: Ph.D. FELIPE LEONEL GRIJALVA ARÉVALO
felipe.grijalva@epn.edu.ec

DMQ, Octubre 2022

CERTIFICACIONES

Yo, ALEJANDRA PRISCILLA SILVA GARCIA declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento

ALEJANDRA PRISCILLA SILVA GARCIA

Certifico que el presente trabajo de integración curricular fue desarrollado por ALEJANDRA PRISCILLA SILVA GARCIA, bajo mi supervisión

Ph.D. FELIPE LEONEL GRIJALVA ARÉVALO
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el producto resultante del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

ALEJANDRA PRISCILLA SILVA GARCIA

Ph.D. FELIPE LEONEL GRIJALVA ARÉVALO

DEDICATORIA

Dedico este trabajo a mis padres Marcelo y Priscilla, que siempre fueron el pilar fundamental para lograr culminar esta etapa de mi vida, a mis tres hermanas Andrea, Milena y Valeria que siempre con su apoyo, palabras y amor estuvieron siempre conmigo, a mi enamorado, Anndy R. por todo su apoyo incondicional,paciencia, a mis abuelos paterno, Virgilio y Zoila que desde el cielo me cuidan, una dedicatoria especial porque a pesar de que físicamente no estuvieron conmigo en este largo camino, siempre los llevo en mi corazón.

A mi abuela materna, Tala que más que mi abuela siempre fue como una segunda madre para mi, por su paciencia y amor y a todas las personas que estuvieron a mi lado para brindarme palabras de aliento, apoyo o consejos en esta etapa de mi vida que hoy finaliza de la mejor manera.

Alejandra Priscilla Silva García

AGRADECIMIENTOS

En primer lugar quiero agradecer a mis padres, Marcelo S. y Priscilla G.un eje fundamental en mi formación academica y personal en mi vida, que sin su apoyo y dedicación no hubiera podido culminar esta etapa de mi vida, a mis hermanas, Andrea, Milena y Valeria que para mi son las personas mas importantes en mi vida, gracias por su paciencia, comprensión, ánimos y noches de desvelo a mi lado, a mi abuela, Chari por siempre darme sus bendiciones, sus buenas vibras y por todos los días sacarme una sonrisa.

A mi mejor amiga del colegio Anabel E. que a pesar de que tomamos rumbos diferentes nunca dejo de alentarme y apoyarme, a mis amigos de la universidad, Carolina Q., Sebastian Y., Jefferson M., Frank C. que estuvieron en cada paso, en cada prueba, cada sonrisa y tristeza que nos dejaba la universidad, sin ellos de igual manera no lo hubiera podido lograr, a mis amigas que me dejó el fútbol, un agradecimiento especial a ”Las Mosas de tu Ñaño”quienes no solo me dieron la alegría de formar parte de este grupo de mujeres luchadoras si no también varios triunfos y dentro de esta gran familia, quiero agradecer especialmente a Daniela Valverde una mujer luchadora, fuerte,excepcional con la que siempre pude contar en este largo camino.

Quiero realizar un agradecimiento especial al Ph.D Felipe Grijalva que ha sido una guía y un gran apoyo durante el desarrollo del presente trabajo. Siempre con sus palabras de aliento, buenas ideas, sustos, conocimientos para mejorar cada una de las partes del trabajo y finalmente poder culminarlo de la mejor manera.

ÍNDICE DE CONTENIDO

CERTIFICACIONES I
DECLARACIÓN DE AUTORÍA II
DEDICATORIA III
AGRADECIMIENTO IV
ÍNDICE DE CONTENIDO V
RESUMEN VI
ABSTRACT VIII
1. INTRODUCCIÓN 1
1.1. OBJETIVO GENERAL 2
1.2. OBJETIVO ESPECÍFICOS 2
1.3. ALCANCE 3
1.4. MARCO TEÓRICO 4
1.4.1. VoIP 4
1.4.2. Herramientas 10
2. METODOLOGÍA 12
2.1. Estructura 12
2.2. Tópicos de las Prácticas de Laboratorio 14
2.2.1. Práctica 1:Aseguramiento de capa 2 en Telefonía IP 15
2.2.2. Práctica 2: Cifrado de Trafico VOIP 19
2.2.3. Práctica 3:Servicios Diferenciados en VOIP. 20
2.2.4. Práctica 4: VPN en VOIP 24
2.2.5. Práctica 5:Configuración de Auto QoS. 28

3. RESULTADOS 29
3.1. Resultados 29
3.1.1. Práctica 1: Aseguramiento de capa 2 en Telefonía IP. 29
3.1.2. Práctica 2: Cifrado de Trafico VOIP 30
3.1.3. Práctica 3: Modificación de clases de mapeo. 35
3.1.4. Práctica 4: VPN en VOIP 39
3.1.5. Práctica 5: Configuración de AutoQos. 40
4. CONCLUSIONES y RECOMENDACIONES 42
4.1. Conclusiones 42
4.2. Recomendaciones 44
5. REFERENCIAS BIBLIOGRÁFICAS 45
6. ANEXOS 47

RESUMEN

El continuo desarrollo y avance tecnológico con el pasar de los años ha modificado el ambiente laboral en el sector empresarial. Gracias a estos cambios las empresas han podido tener un crecimiento significativo, así mismo ha aumentado la necesidad de tener una mejor comunicación con sus clientes, hablando de la calidad que se brinda a sus clientes, pero también el cómo brindar seguridad y una buena calidad, que estas dos características vayan siempre de la mano.

Gracias a esto se generaron herramientas destinadas a cubrir todas las necesidades de los clientes, una de estas son mecanismos de protección, comandos de configuración en dispositivos específicos que se pueden tener en el ambiente laboral, para que todas estas especificaciones puedan funcionar hoy en día se tienen software como *Issabel*,que permite tener llamadas unificadas en un ambiente mucho más simple en cuanto a la configuración y la administración, siendo hoy en día un software muy cotizado en el sector empresarial ya que ayuda también con las necesidades de seguridad ante los datos de los usuarios, Calidad y servicio *QoS*, mientras que en cuanto a los comandos que brindan calidad y servicio y temas de seguridad también se tienen emuladores como son *GNS3* el mismo que posee un ambiente de simulación de vida real, lo que hoy en día se está buscando para cubrir todas estas necesidades y probar cuales son las mejores alternativas para lograr el objetivo.

Por esta razón es necesario que los estudiantes de la carrera de Ingeniería en Telecomunicaciones estén familiarizados con el funcionamiento y la forma de implementar *Issabel* y el emulador *GNS3* orientado principalmente a la seguridad y la calidad y servicio *QoS*.

Este componente propone un conjunto de prácticas de laboratorio desarrolladas en la plataforma *Notion*, que desde cero incorpora los aspectos más básicos, comandos de configuración, factores avanzados que brinda estos softwares. Con un total de cinco prácticas de laboratorios se busca que el estudiante de la Escuela Politécnica Nacional, específicamente de la carrera de Ingeniería en Telecomunicaciones se encuentre familiarizado con un entorno lo más cercano a la vida real sobre los riesgos, mejoras y configuración.

Las guías de laboratorio tienen una actividad para que el estudiante pueda expandir y afirmar sus conocimientos sobre los conceptos planteados en cada práctica.

PALABRAS CLAVE: Calidad y Servicio, Comandos, Configuración , GNS3, Ingeniería en Telecomunicaciones, Issabel, Notion, Seguridad.

ABSTRACT

The continuous development and technological advance over the years has modified the work environment in the business sector. Due to technological development, companies have been able to have significant growth, as well as the need to have better communication with their clients regarding the quality that is provided and how it should be provided, to maintain safety and good quality always go hand in hand.

Seeking to keep these two characteristics together, tools were created to cover all customer needs, protection mechanisms, configuration commands on specific devices that can be had in the work environment, software programs like Issabel are currently used so that all these specifications can work; Issabel allows you to have unified calls in a much simpler environment in terms of configuration and administration. Due to this, it is a highly valued software in the business sector since it also helps with the security needs of user data, Quality and QoS service, regarding the commands that provide quality and service and security issues, there are emulators such as GNS3, which has a real-life simulation environment. So currently, it seeks to cover these needs and what are the best alternatives to achieve the objective. Due to this, for this reason it is necessary that the students of the Telecommunications Engineering career are familiar with the operation and how to implement Issabel and the GNS3 emulator, oriented mainly to security and quality and QoS service. This component proposes a set of laboratory practices developed on the Notion platform. It includes the most basic aspects such as configuration commands to advanced factors.

This component has a total of five laboratory practices whose objective is for the student at the National Polytechnic School, specifically from the Telecommunications Engineering career, to become familiar with an environment closer to real life on the risks, improvements, and configuration.

The laboratory guides have an activity so that the student can expand and affirm their knowledge about the concepts raised in each practice.

KEYWORDS: Quality and Service, Commands, Configuration, GNS3, Telecommunications Engineering, Issabel, Notion, Security.

1. INTRODUCCIÓN

VoIP (Voice Over Internet Protocol) es un servicio que permite la transmisión de voz en forma de paquetes por medio de la red de datos haciendo uso del protocolo de Internet. Su uso se da principalmente en ambientes empresariales, una de las razones es dado que la instalación del servicio por medio de la telefonía IP, se simplifica. Es decir, el antiguo cableado de par de cobre, típico en telefonía tradicional, se omite [1].

Al igual que otros servicios que se basan en paquetes, como la transferencia de datos y video, VoIP debe estar implementado de tal forma que cumpla con los requerimientos de QoS (Quality of Service) o Calidad de Servicio, cuyos factores como el jitter, pérdida de paquetes, ancho de banda y retardo deben estar dentro de un valor definido. Este último factor suele ser el más crítico, por ejemplo los valores recomendados se consideran adecuados cuando se encuentran alrededor de 150 ms o menos [2].

En los últimos años VOIP ha sido una de las tendencias emergentes más importantes en telecomunicaciones [3]. por lo que los estudiantes necesitan verificar y comprobar el conocimiento teórico adquirido en cuanto a la infraestructura, funcionamiento, equipos, problemática, y ventajas.

Por otro lado, en la actualidad se han incrementado los ataques informáticos y VOIP no es la excepción [4]. por lo que es importante que los estudiantes conozcan sobre el aseguramiento de esta nueva tendencia tecnológica que viene de la mano con QoS (Quality of Service).

La actual problemática que se presenta en una de las materias dictadas en la carrera de Ingeniería en Telecomunicaciones de la Escuela Politécnica Nacional, específicamente en la materia de Telefonía IP, consiste en la falta de un componente práctico que permita al estudiante analizar, diseñar y evitar problemas, enfocados a la Telefonía IP en entornos reales, como son empresas e industrias.

Dado lo antes mencionado , el presente componente tiene como propósito resolver la falta de un material práctico para la materia de Telefonía IP, para así lograr complementar los conocimientos de los estudiantes y permitir un mejor desenvolvimiento en el campo laboral. De forma específica se definen 5 prácticas de laboratorio, las cuales cuentan con el soporte de plataformas digitales, cuyo objetivo general es enseñar y entrenar a los estudiantes en temas de gran relevancia , como es el Aseguramiento y Calidad de Servicio (Quality of Service), en el contexto de la Telefonía IP.

Una vez finalizado este componente se podrá tener el suficiente material de apoyo, lo que

brindará a los estudiantes una mejor visión en cuanto a las configuraciones utilizadas para implementar esta tecnología, lo que les permitirá obtener a futuro una experiencia más real que ayude en el desenvolvimiento de su formación profesional.

En la Facultad de Ingeniería Eléctrica y Electrónica se tiene trabajos similares Uno de ellos se lo puede leer en [5]. el cual tiene como propósito la implementación de calidad de servicio en una red convergente (video, datos y voz) usando el protocolo IPv6 para una empresa PYME con la ayuda de dos escenarios, el primero una red con calidad y servicio y la misma sin calidad y servicio en los cuales se analizaran varios parámetros los cuales se detallan en el primer capítulo así como también conceptos básicos de IPv6, dicha implementación de los escenarios se los realizó en el laboratorio de la Universidad Politécnica Nacional La diferencia radica en el uso del protocolo ya que en este proyecto dicho parámetro se definirá en el proceso de la práctica , también solo se plantea un solo escenario que es demostrar la calidad de servicio en la infraestructura de VOIP y finalmente el uso de varios software que permiten el análisis y simulación de un ambiente controlado. También existe otro trabajo que se asemeja al proyecto que se encuentra en [6], en donde se realiza el Análisis de Vulnerabilidades, Investigación Forense y Política de Seguridad para Sistemas de Telefonía IP basados en Asterisk con la ayuda de un prototipo de telefonía IP local que permitirá determinar las debilidades y realizar pruebas de explotación en un ambiente controlado que beneficie en la propuesta de una guía de buenas prácticas para la protección de sistemas de telefonía IP basado en Asterisk. La diferencia se da que solo se va a basar en Asterisk mientras que la guía de seguridad en telefonía IP se llevará a cabo en varias plataformas de acuerdo al nivel de dificultad con el que se vaya realizando las prácticas, otra diferencia es que no se analiza las vulnerabilidades sino más bien se aplicará seguridad para comprobar la infraestructura de la telefonía IP

1.1. OBJETIVO GENERAL

Elaborar prácticas de laboratorio aplicadas al aseguramiento y la calidad de servicio de la infraestructura de Voz sobre IP.

1.2. OBJETIVO ESPECÍFICOS

- Investigar el funcionamiento de la Telefonía IP implementando el aseguramiento y el *QoS*.

- Implementar 5 prácticas de laboratorio para el aseguramiento y *QoS*.
- Resolver las prácticas de telefonía IP en un ambiente lo más real posible.

1.3. ALCANCE

Se desarrollará un conjunto de cinco prácticas de laboratorio orientadas al aseguramiento y QoS, con el objetivo de entregar a los estudiantes de la Escuela Politécnica Nacional una guía de estudios en la cual se pueda complementar la parte teórica con la práctica. Para el desarrollo de este material se hará uso de diversas herramientas principalmente GNS3 y Cisco Packet Tracer, y pueda explotar las características principales de aseguramientos y QoS mediante diseño de topologías con la respectiva comprobación mediante pruebas de funcionamiento.
Para la implementación de este componente se tiene 3 etapas, que son:

1. **Fase de investigación e instalación.**

   En esta fase se realiza un proceso de investigación sobre los parámetros que afecta al QoS y cómo estos influyen en las redes, de igual manera los mecanismos,configuraciones de los diferentes parámetros que involucra la seguridad en una red cuando se tiene Telefonía IP. .Al mismo tiempo se analiza cuál es la mejor herramienta para poder tener el entorno adecuado en cada una de las prácticas, finalmente la fase se termina con la instalación de los diferentes herramientas que se necesita para el diseño de cada topología, en donde se incluye instalación de imágenes los para GNS3, instalación de máquinas virtuales, softphones con sus respectivos comandos de configuración„ software que permitan medir el ancho de banda,

2. **Fase de elaboración de prácticas de laboratorio.**

   En esta fase se elaboran 5 hojas guías con los principales parámetros que involucran obtener buena seguridad y QoS, para el desarrollo de las guías de laboratorio se utilizó la herramienta Notion, la cual permite generar de una manera más didáctica las prácticas incluyendo imágenes animadas, bloques, tablas, etc. Cada una de las hojas guías consta de un procedimiento paso a paso de la configuración de cada elemento que forma parte de la topología en cada práctica conjuntamente con la parte teórica de los elementos utilizados en cada guía de laboratorio.

   En la fase de elaboración se desarrollará un total de cinco prácticas de laboratorio cuyos temas son:

- Práctica 1: Aseguramiento de capa 2 en Telefonía IP.
- Práctica 2: Cifrado de tráfico VOIP.
- Práctica 3: Servicios Diferenciados en VOIP.
- Práctica 4: VPN en VOIP.
- Práctica 5: Configuración de Auto QoS.

3. **Fase de elaboración de actividades propuestas para el estudiante.**

   En esta fase se encontrará al final de la resolución de cada hoja guía correspondiente a cada práctica de laboratorio, en donde se propone una actividad que debe realizar el estudiante. Dicha actividad tiene como objetivo verificar los conocimientos alcanzados por el estudiante sobre cada tema que se imparte en cada práctica. Esta actividad se la hace en base a la modificación de parámetros o ciertas configuraciones que se destacan en las hojas guías.

   Una vez finalizada la implementación del componente, se entregará como resultado final las 5 hojas guías en la plataforma Notion. De igual manera se entregará la resolución de actividades propuestas en cada práctica, así como las máquinas virtuales y las topologías correspondientes.

1.4. MARCO TEÓRICO

1.4.1. VoIP

Voice over Internet Protocol o VoIP por sus siglas en inglés es la tecnología que permite obtener la comunicación de voz y vídeo utilizando el envió de paquetes sobre el protocolo IP [7]. En otras palabras, gracias a la digitalización principalmente de la voz y también se puede realizar llamadas a toda la red. De esta solo depende únicamente de la cobertura de Internet mas no de la infraestructura de una antena.

Desde el punto de vista de la seguridad y QoS durante el resto del documento se intentará dar una explicación y una visión más general de que con la ayuda de la evolución de las tecnologías se puede solucionar estos problemas críticos.

En la actualidad la seguridad en las redes IP es una característica difícil de implementar, para esto se debe tener recursos necesarios y garantizar tanto la calidad y servicio, la confidencialidad, la integridad y la disponibilidad de la información [8].

Para garantizar también la seguridad es importante tener técnicas de seguridad, por mencionar que se tienen algunas, como son:

- **Autenticación Criptográfica:** Se basa en que se necesitan tener identidades personales relacionadas a un perfil, con un identificar único con el cual se puede identificar a cada persona que decide tener acceso a cualquier tipo de información.
- **Encriptación:** Simplemente consiste en una manera de codificar la información para que terceros no puedan tener acceso. Dentro de esta técnica existe un protocolo, que se llama IPsec, el mismo cuya función es asegurar las comunicaciones sobre IP, implementando cifrado.
- **Protocolos seguros de la capa de transporte:** Aquí lo que se quiere lograr es una conexión segura de que cualquier ataque pueda cambiar o interceptar la comunicación.

Componentes de VoIP

Entre los componenetes que posee VoIP se tienen:

- **Cliente**: Principal elemento que tiene como características hacer y recibir llamadas telefónicas de voz, las mismas que son codificadas para ser enviadas y decodificadas para que en el destino puedan ser reproducidas exitosamente [9].
- **Servidores**: Este elemento se encarga de ejecutar enrutamiento, recolección, inscripción de clientes y manejo del servicio IP.

  Los servidores de VoIP se los conoce como Switches de telefonía IP o IP-PBX [9]. Actualmente se tienen varios IP-PBX en el mercado que son: Elastix, FreePBX, Issabel, etc.
- **Gateways**: Elementos que actúa como un puente para conectar todos los usuarios finales Una de las funciones más importantes es de aceptar peticiones de llamadas entre diferentes terminales y conversiones al establecimiento y liberación de la comunicación en los dos extremos de la red. [10].

Ventajas de VoIP

VoIP tiene como ventaja que no posee ningún vinculo con las antenas de la red telefónica convencional, generando un beneficio muy grande que es que tiene banda ancha en telefonía permitiendo obtener una mejor calidad de la voz. [11]. VOIP también tiene otras ventajas:

- *Menor costo en equipos*: A comparación de telefonía tradicional que el costo de sus equipos es elevado, para VOIP es mucho más bajo. Esto se debe a que posee una interoperabilidad entre sus diferentes equipos por la utilización de IP y con esto la mayoría de sus equipos se encuentran estandarizados lo que ayuda a reducir significativamente los precios. [12]

- *Mejor uso de recursos*: La diferencia de VOIP con la telefonía tradicional es que esta solo existe cuando se tenga la transmisión de información. También, con las nuevas técnicas de codificación y el uso de VOIP se tiene un menor ancho de banda lo que ayuda a tener mayor eficiencia en el uso total del ancho de banda.

- *Movilidad*: El uso de telefonía IP ha facilitado el aspecto de la movilidad, con el hecho de tener una conexión a Internet, que pida un acceso con un nombre de usuario y su respectiva contraseña esto permite a cualquier dispositivo con una cuenta realizar llamadas con otras personas. A diferencia de la telefonía tradicional que no permite desplazarse de un lugar a otro ya que su conexión es fija con un dispositivo en concreto [11].

En base a las ventajas ya mencionadas y al avance tecnológico que tiene VoIP viene de la mano también varias amenazas que posee por esta razón es muy importante la implementación de la seguridad en VoIP.
Los conceptos asociados a la seguridad y a la protección de información son: [13].

- *Confidencialidad*: Permite tener acceso a la información solo por personas autorizadas, evitando así el acceso a terceros. Para evitar este tipo de violación se utiliza técnicas de encriptación y contraseñas robustas de seguridad.

- *Integridad*: Verifica que no se ejecuten cambios no autorizados en la información y si se ve afectado en ese caso se debe alertar, para evitar la vulnerabilidad de la integridad se puede hacer uso de bits de paridad para verificar que el mensaje no ha sido modificado.

- *Disponibilidad*: Permite que los recursos estén disponibles para que cada usuario autorizado pueda tener acceso a la misma, para reducir estas vulneraciones se utiliza la redundancia ya que al garantizar la disponibilidad se tiene un correcto funcionamiento del sistema.

Protocolos de VoIP

Entre los protocolos más utilizados se tienen:

- *Session Initiation Protocol*:SIP (Session Initiation Protocol),es un protocolo de señalización utilizado para establecer la conexión entre dos o más participantes, modificar y posteriormente terminar la sesión. [14]

  SIP está basado en un texto y es de estándar abierto, tiene varas similitudes con el protocolo HTTP, posee una rápida resolución de errores gracias a su mecanismo de petición- respuesta.

- *H.323*: El protocolo H.323 tiene gran similitud con el protocolo SIP ya antes mencionado, mediante el cual se puede configurar, administrar y terminar una sesión. Este protocolo es más antiguo que SIP, más parecido a HTTP/SMTP pero menos complejo, H323 es un protocolo binario lo que lo hace menos accesible a poder resolver problemas así como también el tiempo que necesita para ser definido e implementado [15]. Por estas razones H.323 ha sido absorbido por completo por SIP a lo largo del tiempo.

- *Real Time Transport Protocol*: El Protocolo de Transporte en Tiempo Real o RTP por sus siglas en inglés, este definido en el RFC 1889, publicado en 1996 por primera vez, posee un formato de paquetes para que se pueda enviar la voz y el vídeo sobre Internet [16]. RTP es utilizado en medios de transmisión como telefonía, videoconferencias, servicio web y servicios de TV, etc.

  Es importante tomar en cuenta que RTP va conjuntamente con el protocolo de Control (RTCP), este último es el encargado de tener una buena gestión en cuánto a la calidad tanto en la transmisión como en los servicios que posee la comunicación. RTP también se lo puede utilizar con el protocolo SIP en el establecimiento de la sesión de comunicación a través de la red.

- *Real Time Transport Control Protocol*: El protocolo RTCP como ya se mencionó anteriormente trabaja con el RTP, este definido en el RFC 3550 [17]. Su función consiste en el envío de paquetes de control a los usuarios, con la finalidad de gestionar y elegir los parámetros de la calidad de servicio. Una de las desventajas de RTCP es que no posee encriptación o método de autenticación en su desarrollo.

Calidad y servicio en VoIP

La calidad y servicio **QoS** (Quality of Service) es la capacidad que brindar un buen servicio cuando se transmite la voz o el video, para esto se necesitan mecanismos que den prioridad ya que las conversaciones se dan en tiempo real. [18].

Para la calidad y servicio existen indicadores de la calidad de voz, que son:

- Ancho de Banda
- Latencia
- Jitter
- Perdida de Paquetes
- Eco

Pues bien cuando se quiere hablar de calidad y servicio, se hace referencia a clases de servicio diferenciados con la ayuda de mecanismo de políticas de tráfico, estas políticas permiten determinar cómo serán manejadas las clases de tráfico a medida que pasan por la red. [18].

Desde que el Internet necesito una mayor integración en los servicios de red se ha implementado un mecanismo de Calidad de Servicio (QoS de sus siglas en inglés) que permita mejorar el servicio, con el pasar de los años los servicios se han incrementado y han llegado a tener una integración de datos, voz y multimedia, estos servicios pueden ser proporcionados por mecanismos de Calidad de Servicio ya que permite separar los servicios y asignarles prioridad de uso en la red para garantizar el servicio a los usuarios con un costo menor [19].

Aquí surgió los Servicios Integrados (InterServ) que consiste en gestionar recursos para tener una Calidad y Servicio (QoS), tratando cada flujo de manera independiente ya que funciona de extremo a extremo realizando una reserva de recursos en los elementos de la red.

Debido a esto surgió los servicios diferenciados Diffserv cuya función principal es diferenciar el tráfico en distintas clases, este servicio ayuda a proporcionar mecanismo de QoS para que en la red no se tenga sobre carga.

Esta arquitectura posee escalabilidad gracias a funciones como: [20].

- Agregación de tráfico.
- Condicionamiento y comportamiento de saltos
- Campo DS usado en marcación de paquetes.

En cuanto a la marcación de paquetes, se lo hace con un código especifico llamado DSCP (Diffserv CodePoint). Como se muestra en la siguiente figura 1.1, su campo consta de 6

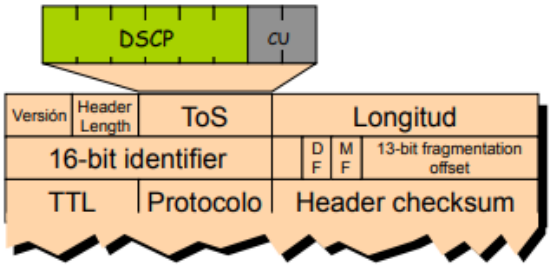

Figura 1.1: Código DSCP.

bits que posee 64 diferentes valores binarios, dos bits sin usar CU (Currently Unused), cada Code Point es la probabilidad de que se reenvió a tiempo el paquete.
Para poder tener la diferenciación de servicios se lo realiza mediante un PHB (Per Hop Behavoir) conocido como el comportamiento específico para cada clase definidos en: [21]

- **Expedited Forwading "EF":** Este ofrece mayor prioridad en QoS garantizando que las pérdidas de paquetes, jitter y de retardo disminuyan. El valor en DSCP es de "101110".
- **Best Effort "BE":** No brinda ninguna seguridad de que los paquetes puedan ser entregados.
- **Assured Forwarding "AF":** No garantiza retardos ni ancho de banda, consta de 4 grupos AF1x, AF2x, AF3 y AF4x independientes.

VPN en VoIP

VPN o como su nombre en inglés (Virtual Private Network) es una tecnología que permite extender la red local en una red pública utilizando la encapsulación y encriptación, en el cual los paquetes de datos se envían remotamente mediante un túnel a diferentes destinos remotos en una red de transporte publica, hablando del acceso remoto, la VPN le permite al usuario a la red empresarial dándole direcciones y permisos de la misma aunque la conexión se haya realizado mediante un Internet público. [22]
Las ventajas de configurar VPN en telefonía IP son muchas, aquí se destacan las más importantes: [23]

- Comunicación segura de principio a fin.
- Ahorro en las llamadas.
- Conectividad se la realiza por un acceso remoto.

1.4.2. Herramientas

Para la realización del presente trabajo se tiene varias herramientas que fueron utilizadas como son. tiene.

Notion

Notion es una plataforma que permite la creación de escritos como proyectos utilizados en el campo laboral o en la vida personal [24]. Esta plataforma web tiene como ventaja que puede ser utilizada solo con tener una computadora, teléfono celular o un navegador web.

La plataforma Notion ofrece una gran ventaja al momento de la realización de los diferentes documentos, ya que permite tener un documento con cambios realizados por cada usuario, dándole un toque personal al mismo. Gracias a que posee diferentes tipos de bloques permitiendo agregar: tablas, índice de contenido, títulos, subtítulos, videos, subpáginas, pestañas sincronizadas, pedazos de código, entre otros. Brindando la posibilidad de elaborar documentos didácticos como informes, planes de trabajo, planes personales, calendarios, cronogramas, entre otros.(ver Fig. 1.2).

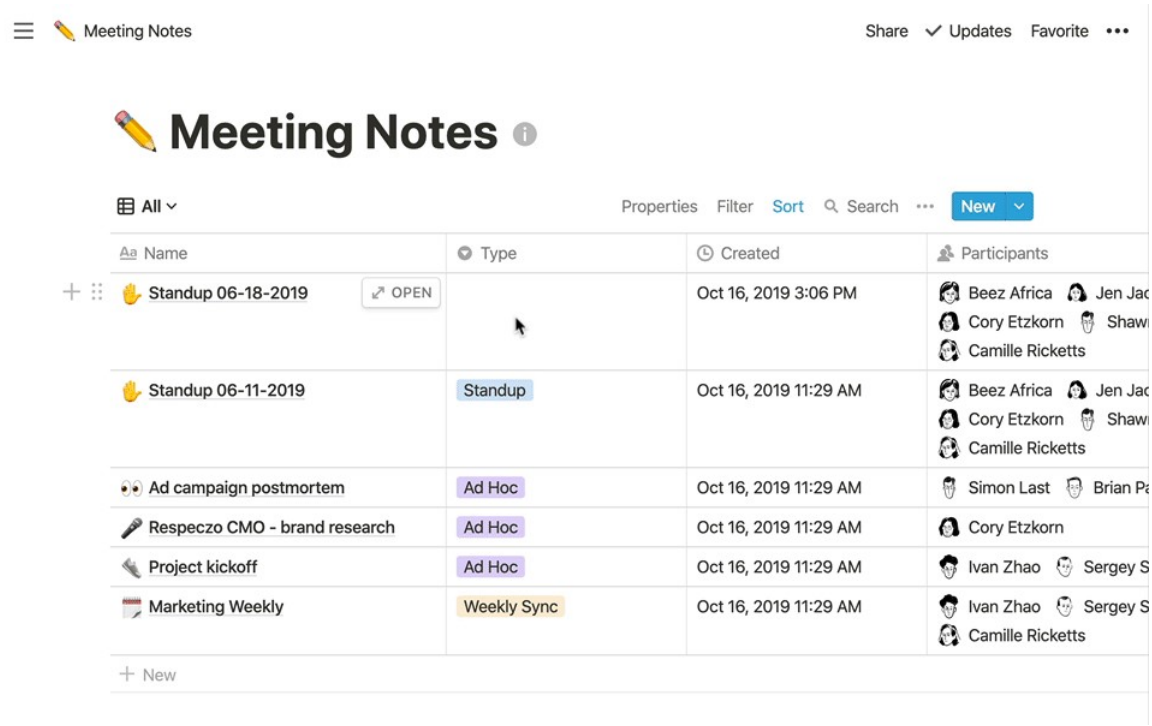

Figura 1.2: Ejemplo de Notas de reuniones [24]

GNS3

El software GNS3 es utilizado para configurar, emular y solucionar problemas de redes mediante la creación de topologías que se caracteriza por la composición de dispositivos como router, switch, teléfonos, PC. la ventaja de este software es que usa un código abierto y es gratuito, lo que lo hace más llamativo e interesante para estudiantes, ingenieros y varias empresas. [25]
Posee dos componentes que son:

- Software todo en uno (GUI)
- Máquina Virtual (VM).

Al momento de crear las topologías existen tres opciones del servidor.

1. Servidor local GNS3.
2. Máquina virtual local GNS3.
3. Máquina virtual remota GNS3.

Por recomendación es necesario utilizar la VM GNS3 cuando se quiere realizar topologías mucho más avanzadas que necesiten dispositivos como Cisco VIRL u otros dispositivos que requieren Qemu.

Máquinas virtuales

Una máquina virtual o también llamada Virtual Machine es una computadora virtual, la diferencia que posee con una computadora física es el hardware ya que necesita de un código para realizar todas sus funciones. [26]
Para poder levantar una máquina virtual se realiza el proceso llamada virtualización, él mismo consiste en tomar elementos del CPU como memoria y almacenamiento, mencionando que los cambios que se hagan en la máquina virtual no afectan a la maquina física, es decir son independiente una de la otra.

2. METODOLOGÍA

Es importante mencionar que para desarrollar las diferentes prácticas de laboratorio, se crearon un conjunto de hojas guías que permitirán al estudiante tener una noción de cuáles serán los temas a tratar en las cinco prácticas que se plantean, las mismas que se llevaran a cabo en la plataforma Notion, una herramienta que brinda un conjunto de instrumentos sencillos, dinámicas y especificaciones para lograr que cada practica sea implementada de manera didáctica, recreativa y amigable para los estudiantes.

2.1. Estructura

La segmentación de las prácticas de laboratorio en *QoS y Seguridad* se realizó en base de cuatro parámetros: La *Seguridad* en las diferentes topologías a implementar, la *QoS* en la simulación de las topologías, la complejidad para ejecutar y llevar acabo el funcionamiento de las pruebas y por último, la verificación del tiempo que requiere realizar las configuraciones. A partir de esto, se dividió el tema de *QoS y Seguridad* en cinco prácticas, las cuales son:

- Práctica 1: Aseguramiento de capa 2 en Telefonía IP.
- Práctica 2: Cifrado de Tráfico VOIP.
- Práctica 3: Servicios Diferenciados en VOIP.
- Práctica 4: VPN en VOIP.
- Práctica 5: Configuración de Auto QoS.

Prerrequisitos

Los prerrequisitos son las herramientas indispensables, que necesariamente se debe tener instaladas antes de iniciar las prácticas de laboratorio; de estas se destacan softphones, software, máquinas virtuales, servidores de telefonía IP, etc. Estos elementos son de neta importancia ya que siempre se utilizarán en las diferentes practicas o en algún momento puntual de cada una de las mismas. Sin estas herramientas no se lograrán culminar con el desarrollo de la práctica.

En cada hoja guía se incluye la forma en la cual se puede instalar alguna herramienta necesaria acorde a cada tema de las diferentes prácticas, y también se tiene el link para descargar

en caso de ser necesario o como se debe configurar, con el fin de ayudar al estudiante a ahorrar tiempo.

Tópicos del Laboratorio

Esta sección está compuesta por los tópicos a tratarse durante el desarrollo de los laboratorios. En este punto se tiene una introducción y definición de cada tema, así como los diferentes parámetros o elementos que se utilizarán. Por ejemplo, si en una práctica uno de sus subtemas es configuración de VPN, se escribirá una pequeña definición de VPN, de igual manera se explicará las opciones que se tienen dentro de la configuración, con el fin de no tener un laboratorio de forma mecánica y que el estudiante sepa que es lo que está realizando en cada paso y de donde viene cada definición, parámetro, configuración y cuando lo puede aplicar en un futuro.

Actividad

Esta sección trata de una pequeña modificación a la práctica de forma teórica o práctica, para el caso de las 4 primeras son de forma práctica y la última practica será una modificación teórica para el estudiante, esto ayudará a evaluar el conocimiento en el transcurso del laboratorio. Por lo general, está orientada a la configuración de algún parámetro explicado durante la hoja guía u otro elemento que se pueda configurar y comprobar su funcionamiento para garantizar el objetivo de la práctica.

Cada hoja guía elaborada tiene una pequeña actividad con un rendimiento de medio a alto, lo que permitirá tener un conocimiento mucho más avanzado que se puede desarrollar a nivel empresarial.

Las actividades propuestas para cada estudiante en las diferentes prácticas de laboratorio serán presentadas como resultado en este trabajo de integración curricular.

En cada laboratorio se encuentra definidos los nombres de las actividades como se observa en la Tabla 2.1.

Tabla 2.1: Nombres de las actividades propuestas

Práctica de Laboratorio	Actividad
Práctica 1	Cambio del protocolo (ICMP) en la asignación del ACL.
Práctica 2	Captura de la llamada sin cifrado y con cifrado en wireshark.
Práctica 3	Configuración de prioridad de los protocolos FTP y Telnet
Práctica 4	Bloqueo del puerto 21 (FTP) a usuario remotos
Práctica 5	Consulta del equivalente de AutoQoS en Huawei y Juniper.

2.2. Tópicos de las Prácticas de Laboratorio

Para el desarrollo de las diferentes topologías se utiliza la herramienta de comunicaciones Issabel y el emulador GNS3. En esta herramienta se realizarán las configuraciones de los elementos mientras que en GNS3 se realiza la ejecución de comandos que ayuden a la aplicación de los diferentes temas en seguridad y QoS.

Se tomó Issabel como la herramienta más importante ya que posee varios bloques, los mismos que permiten copiar todos los componentes que existen dentro de un centro de llamadas con la finalidad de obtener buenos resultados en cuanto a características de Seguridad y Qos, permitiendo así obtener una guía de laboratorio lo más completa posible para el estudiante con la ayuda del emulador GNS3 que permite realizar las configuraciones necesarias lo más cercanas a la realidad.

En Issabel se destacan bloques que permiten tener una relación con el módulo *Seguridad* se encuentran: cortafuegos, fail2Ban, auditoría, claves débiles, configuraciones avanzadas y certificado HTTPS (Let's Encrypt) como se observa en la Figura 2.1.

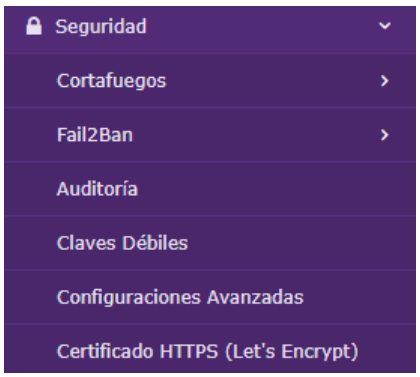

Figura 2.1: Estructura general del módulo destacado.

Estos tópicos conjuntamente con su tiempo de ejecución se pueden observar en la Tabla 2.2.

Tabla 2.2: Nombres de las prácticas propuestas y su tiempo de ejecución

Práctica de Laboratorio	Nombre de la Práctica	Tiempo de ejecución
Práctica 1	Aseguramiento de capa 2 en Telefonía IP	1h30min
Práctica 2	Cifrado de Trafico VOIP	1h30min
Práctica 3	Servicios Diferenciados en VOIP	1h
Práctica 4	VPN en VOIP	1h30min
Práctica 5	Configuración de Auto QoS	1h

2.2.1. Práctica 1:Aseguramiento de capa 2 en Telefonía IP

La finalidad de la practica número uno de laboratorio es desarrollar la configuración básica de seguridad mediante la aplicación de un ACL a todo el tráfico de la red para posteriormente comprobar su funcionamiento mediante los comandos ping y telnet.

En Telefonía IP se tiene el intercambio de información que puede ser datos, voz, video en el cual un papel muy importante es tener una adecuada protección para esta información por ende se debe tener mecanismos de seguridad que ayuden a que el intercambio de la misma no sea vulnerada o accedida por terceras personas ya que no solo el contenido de una conversación (que puede llegar a ser altamente confidencial) sino también la información y los datos de la propia llamada, que, utilizados de forma maliciosa, permitirán acceder a los registros de conversaciones entrantes o salientes, configurar y redirigir llamadas, grabar datos, llevar a cabo robo de identidad.

Entonces son muchas las amenazas que se tiene por una falta de cifrado y técnicas permiten que un atacante con esnifer pueda alterar la confidencialidad, integridad y disponibilidad del servicio. Por tal motivo es importante empezar esta serie de laboratorios adentrándose con varios métodos de seguridad, específicamente el que se va a detallar a continuación que es ACL (Access Control List), tomando en cuenta que existen más métodos de seguridad que en posteriores laboratorios se explicara. ACL (Access Control List) es un conjunto de reglas que sirve para filtrar el tráfico entrante, saliente en una interfaz. El ACL tiene varias ventajas que ayudan a mejorar el rendimiento de la red, reduce la carga.
Los ACL constan de los siguientes campos:

- **Numero de secuencia:** Permite procesar en orden las líneas que se ejecutan de los ACL.
- **Dirección:** Indica la dirección en que se va a aplicar el ACL, estas son entrante, saliente y cualquiera.
- **ACL de entrada:** Verifican los paquetes antes de llegar a la interfaz de salida, lo que ayuda a la sobrecarga de paquetes.
- **ACL de salida:** Se dirigen a la interfaz de salida para posteriormente ser procesados mediante el ACL de salida.
- **Any:** Se aplica en las dos direcciones entrada o salida.

Nota: La única dirección y máscara que se debe utilizar al seleccionar Any para la dirección es 0.0.0.0/0.0.0.0 (Any), esta dirección solo se debe utilizar en situaciones específicas para permitir o bloquear un puerto, protocolo en las dos direcciones.

- **Mascara y dirección IP de origen**
- **Mascara y dirección IP de destino**
- **Protocolo:** Especifica que protocolo se va a bloquear o permitir trafico.
  TCP (protocolo IP 6)
  UDP (protocolo IP 17)
  ICMP (protocolo IP 1)
  ESP (protocolo IP 50)
  AH (protocolo IP 51)
  GRE (protocolo IP 47)
  IP (protocolo IP 4 IP 6)
  Eth Over IP (protocolo IP 97)
  OSPF (protocolo IP 89)
  Otro (especificar)
- **Puerto Dest:** Puerto al cual se debe entregar el ACL.
- **Acción:**Se tiene dos acciones permit o deny, permit reenvía el paquete y deny bloquea el paquete.

Este laboratorio tiene como topología general la Fig. 2.2.

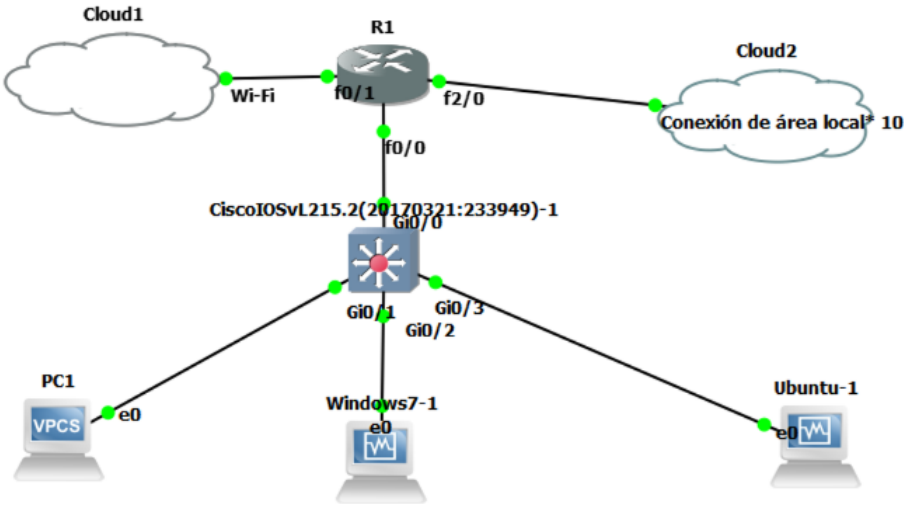

Figura 2.2: Topología general Práctica 1.

Dentro de esta topología se puede evidenciar que se tiene una PC que nos brinda GNS3, la misma que se utilizara para verificar el ACL, dos máquinas virtuales, en una de ellas se registraran dos diferentes dispositivos (softphones).

Gracias al esquema planteado se puede generar dos VLANs, una para datos y otra para voz esta permitirá dividir el tráfico y utilizar los ACLS para que solo se pueda denegar o permitir el tráfico a los datos o a la voz en el switch, con los siguientes comandos.

vlan database

vlan 10 name DATOS

vlan 20 name VOZ

NOTA: Estos tres comandos se deben correr en el modo privilegiado.

Estas dos VLANs una vez creadas se las debe generar en la interfaz de interés, en este caso la interface FastEthernet 0/0, mediante los siguientes comandos.

interface FastEthernet0/0.10

encapsulation dot1Q 10

NOTA: Estos dos comandos se deben correr en el modo global.

Antes de configurar los ACLs se debe tener conectividad entre la máquina física y las maquinas virtuales, se realiza la configuración de rutas estáticas, en este caso dos, una para cada maquina virtual, esta configuración es sencilla.

En primer lugar se debe abrir un CMD en modo administrador y ejecutar el siguiente comando

route add 192.168.10.0 mask 255.255.255.0 192.168.100.40

route add 192.168.20.0 mask 255.255.255.0 192.168.100.40 , tal como se ve en la Fig. 2.5.

```
  192.168.20.0    255.255.255.0   192.168.100.40       1
     10.0.0.0  255.255.255.252   192.168.100.40       1
  192.168.10.0    255.255.255.0   192.168.100.40       1
```

Figura 2.3: Rutas estáticas.

Para finalmente ejecutar el comando de la configuración de los ACL, la misma que consta de:

- Número de ACL
- Tipo de comandos, en este caso deny, accept, drop
- Tipo de Protocolo
- Host

tal como se ve en la Fig. 2.4.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#acc
R1(config)#access-list 101 deny tcp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.$
```

Figura 2.4: Comando para ACL.

Una vez se haya ejecutado los comandos mas importantes en este caso la configuración del ACL en el emulador GNS3, se procede a realizar las pruebas de funcionamiento con el uso del protocolo TELNET, donde se podrá verificar la correcta configuración del ACL en cuanto al envió de datos mientras tanto que la comprobación de telefonía IP se lo realiza mediante la llamada entre softphones, las cuales no se vieron afectadas al aplicar las reglas de ACL entre las dos redes, tal como se ve en la Fig. 2.5.

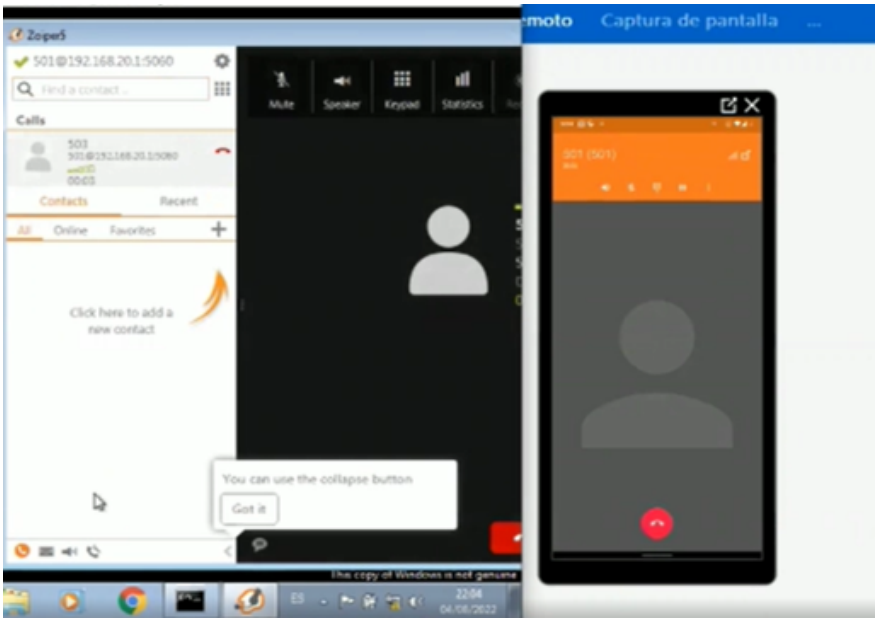

Figura 2.5: Llamada exitosa.

2.2.2. Práctica 2: Cifrado de Trafico VOIP

En la segunda práctica de laboratorio se tiene como objetivo realizar la configuración de certificados TLS para asegurar el cifrado de voz y comprobar el funcionamiento de los elementos configurados mediante las llamadas entre softphones después de configurar los certificados en la máquina virtual Issabel y finalmente se utiliza el software Wireshark el que permite visualizar el resultado final de que la llamada fue cifrada y no se puede diferencias ningún tipo de información.

El presente laboratorio tiene como fin familiarizarse con el cifrado para garantizar la seguridad en el tráfico de voz.

En donde se incluye la creación de certificados, clave pública, clave privada, las cuales son utilizadas para realizar, la autenticación, proteger, encriptar, desencriptar y administrar conexiones seguras. Hay que tomar en cuenta que el servidor necesita de dos archivos, el certificado de CA y la clave privada del servidor mientras que el cliente solo necesita el certificado de CA y la clave pública. Dichos elementos tienen archivos de configuración dentro del Issabel que se pueden configurar para que tengan un buen funcionamiento, y de igual se toma en cuenta que dentro del módulo de extensiones se debe habilitar la opción de transporte *TLS Only* y de igual manera la opción encryption en el mismo modulo.

Por tal motivo es importante empezar este laboratorio con las características principales del protocolo que se va a utilizar que en este caso es TLS *Transport Security Layer*. Así mismo es importante familiarizarse con la infraestructura que posee y cuáles son las etapas para establecer la comunicación.

Hay que tomar en cuenta que gracias a Issabel se es más fácil la configuración del cifrado ya que posee un módulo el cual consta de los archivos necesarios para habilitar las configuraciones en el servidor y posteriormente en cada extensión tener la opción de habilitar dos parámetros fundamentales en este caso el tipo de transporte y la opción en **YES** en la encriptación.

La topología general de la Práctica 2 se puede observar en la Fig. 2.6.

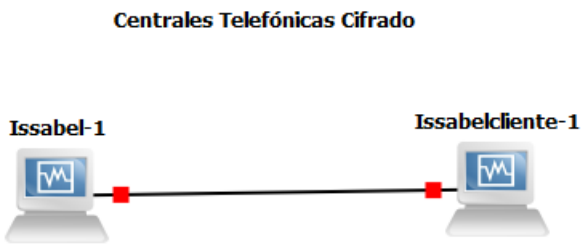

Figura 2.6: Topología general Práctica 2.

Dentro de la topología se puede evidenciar que se tiene dos máquinas virtuales, las cuales serán registradas en diferentes dispositivos (softphones).

Se puede evidenciar que se crearán dos certificados, tanto para el servidor y el cliente, los mismos que serán utilizados por las dos extensiones ya previamente creadas. Dichos certificados tendrán su configuración, permiso para que puedan realizar las llamadas encriptadas entre las extensiones que se encuentran en cada máquina virtual, en la cual los flujos tienen información en caracteres especiales.

2.2.3. Práctica 3:Servicios Diferenciados en VOIP.

En la práctica número tres de esta guía de laboratorio se tiene como objetivo emular un ambiente de dos LAN en la cual los diferentes paquetes que se envíen de una LAN a otra tenga configurado marcación de paquetes mediante la aplicación de QoS en tres diferentes

tipos de protocolos.

Los protocolos que se van a implementar para verificar la configuración correcta de Qos son: HTTP y ICMP para datos, mientras que para voz se tiene RTP.
Por tal motivo es importante empezar este laboratorio con las definiciones necesarias para entender cuál es el fin.
Los mecanismos de QoS son importante al momento de querer tener conexiones seguras y que permitan al usuario tener una experiencia agradable esto gracias a la asignación de prioridad en el uso de la red para que el usuario al tener la garantía de una buena calidad la adquiera a un costo menor, esto nos permite la configuración de varios comandos dentro de la topología asignada.

Debido a esto se va a implementar servicios diferenciados *Diffserv* cuya función principal es diferenciar el tráfico en distintas clases, este servicio ayuda a proporcionar mecanismo de *QoS* mediante comandos que habiliten dentro de este laboratorio la marcación de paquetes. Con la ayuda del emulador GNS3 se puede observar el funcionamiento de los diferentes comandos de QoS a cada uno de los routers, en donde se crean clases de mapas seguida de una política que permita reconocer el protocolo que se quiere configurar y hacer match junto con la misma configuración en el otro router que permita que se tenga esta coincidencia de los protocolos que se crearon en la clase y se puedan evidenciar la marcación de paquetes en el destino.

Esta marcación se la realiza identificando un código, llamado DSCP *Diffserv CodePoint* que es el campo que posee la cabecera de los paquetes, cada uno con un código diferente para poder diferenciar los 3 protocolos que se utilizó en esta práctica.

Esta arquitectura posee escalabilidad gracias a funciones como:

- Agregación de tráfico.
- Condicionamiento y comportamiento de saltos.
- Campo DSC usado en marcación de paquetes.

En este laboratorio se va a implementar la marcación de paquetes, la cual se lo hace con un código especifico llamado DSCP (Diffserv CodePoint). Como se muestra en la siguiente

figura, su campo consta de 6 bits que posee 64 diferentes valores binarios, dos bits sin usar CU (Currently Unused), cada *Code Point* es la probabilidad de que se reenvió a tiempo el paquete.

La topología general del escenario del tercer laboratorio se observa en la Fig.
2.7.

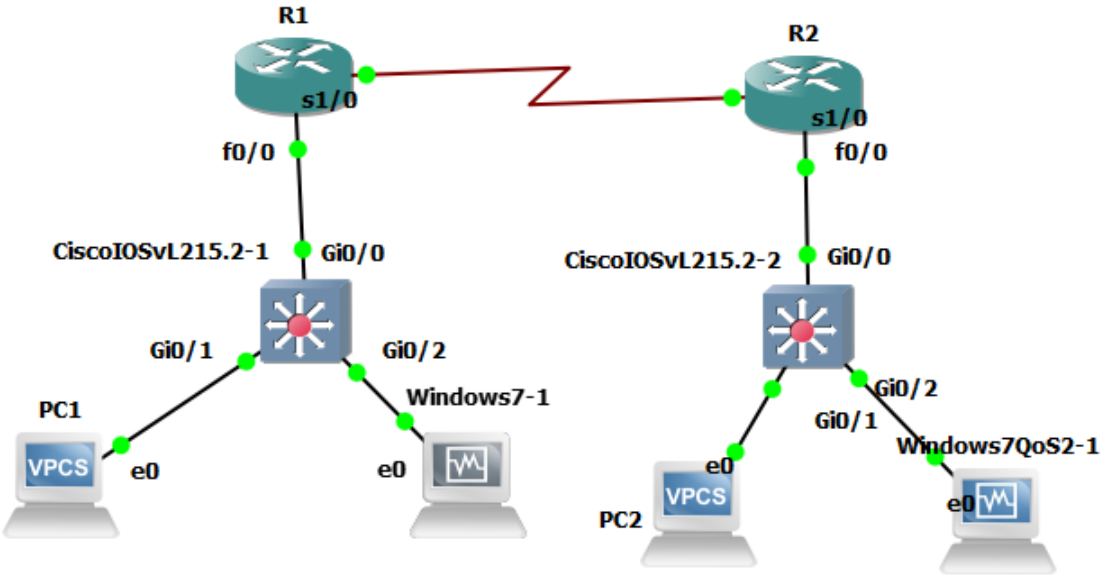

Figura 2.7: Topología general Práctica 3.

Una vez realizada la configuración mediante los comandos respectivos de QoS como son *class-map match-all* , seguido del protocolo, después se debe generar la política para cada clase con la ayuda del comando *policy-map*, seguido de un nombre que sea fácil de recordar, la siguiente línea de comando es la que permite asignar el código de DSCP, todas las configuraciones para QoS deben ser vinculadas a una interfaz especifica.

Para comprobar el funcionamiento de las configuraciones se hace uso del software Wireshark que permite capturar paquetes de acuerdo a las tres clases que se crearon, en este caso HTTP,ICMP y RTP, los mismo que se podrán visualizar con diferente tipo de prioridad tomando en cuenta que la de mayor importancia en este caso es la de RTP ya que hace referencia a la voz.

Para el protocolo HTTP se puede evidenciar el resultado tal como se ve en la Fig. 2.8.

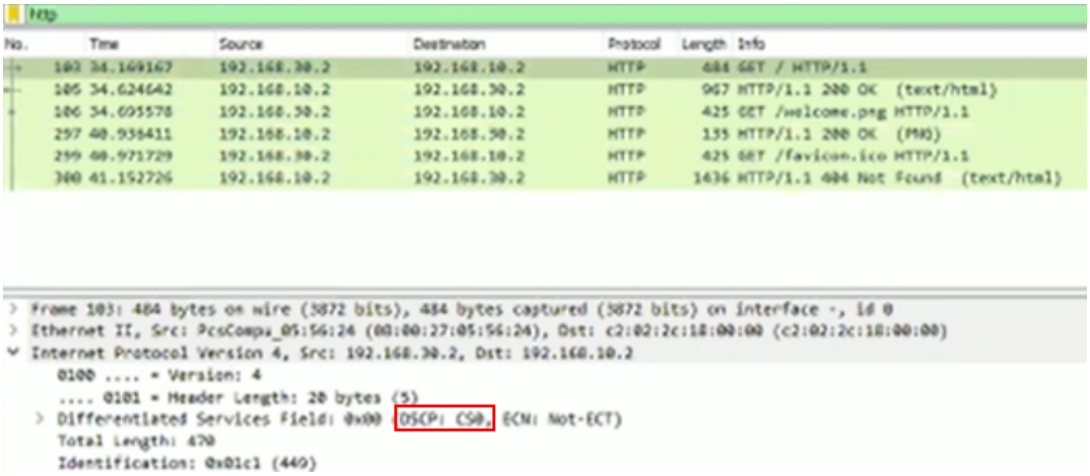

Figura 2.8: Captura del paquete HTTP.

Para el protocolo ICMP se puede evidenciar el resultado tal como se ve en la Fig. 2.9.

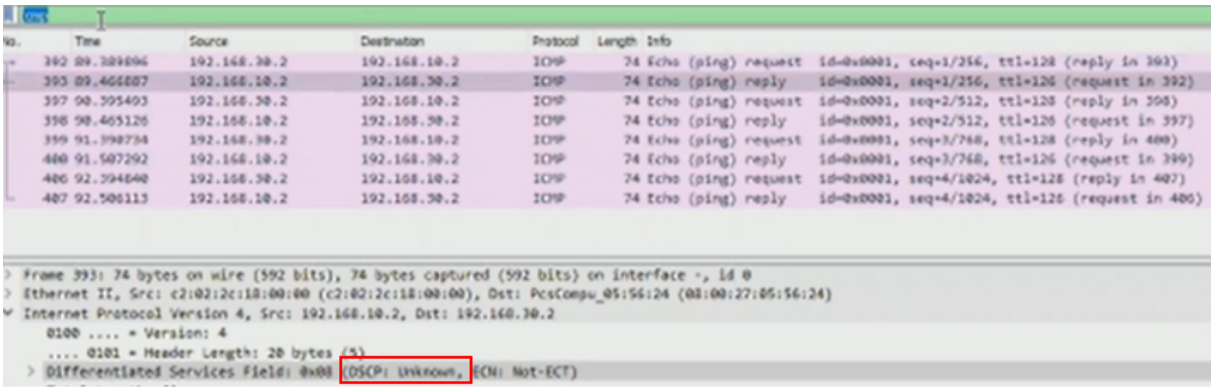

Figura 2.9: Captura del paquete ICMP.

Finalmente para el protocolo RTP se puede evidenciar el resultado tal como se ve en la Fig. 2.10.

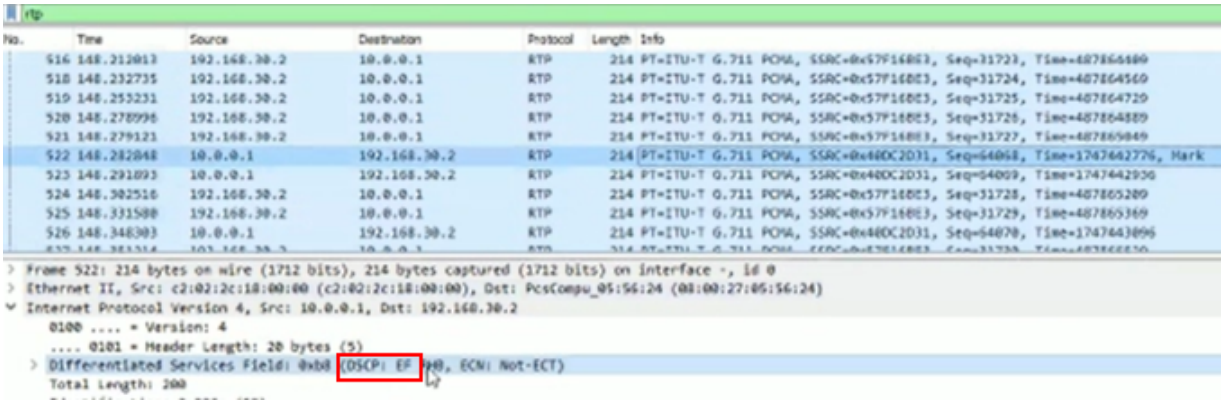

Figura 2.10: Captura del paquete RTP.

2.2.4. Práctica 4: VPN en VOIP

La práctica del laboratorio número cuatro tiene como finalidad la configuración de VPN en Issabel. Con esto se podrá observar el comportamiento de usuarios remotos mediante la ejecución de una llamada.

Pues bien, en este laboratorio se analizará otra manera de protección la red VoIP, no es simplemente bloquear el tráfico de datos externo que no se solicita, en buena hora se tiene varias herramientas que los administradores pueden utilizar para garantizar que su red este a salvo de amenazas.

Una de estas herramientas es el uso de la VPN *Virtual Private Network*, es una forma diferente de brindar seguridad, basada en el protocolo de internet IPsec , permite crear un túnel seguro entre el la IP PBX y el teléfono remoto.

De esta manera cuando un usuario quiera conectarse hacia la central lo tendrá que hacer mediante un túnel que se genera para garantizar seguridad en cuanto a las llamadas telefónicas. Esto se consigue con la ayuda de una herramienta que también se encuentra en Issabel, llamada Easy VPN, la cual permite habilitar las configuraciones para que la VPN funcione correctamente seguido de varias configuraciones en la creación de los dos usuarios remotos.

Gracias a esto, cuando una empresa quiera realizar teletrabajo en casos de emergencia como fines de semana que no se tiene acceso al trabajo, diferente ubicación o en pandemias mundiales, en los cuales no se puede tener acceso al trabajo con facilidad, se puede hacer uso de esta implementación.

Por estas razones es importante dedicar un laboratorio exclusivo a la configuración y creación de VPNs. Incluyendo su configuración previa para su correcto funcionamiento para posteriormente concluir con las respectivas pruebas de funcionamiento. En las pruebas de funcionamiento se espera realizar llamadas exitosas entre usuarios remotos que se crearon en la central telefónica. Todo esto será posible gracias a la configuración del módulo Easy VPN dentro de Issabel.

La topología general del cuarto laboratorio se observa en la Fig 2.11.

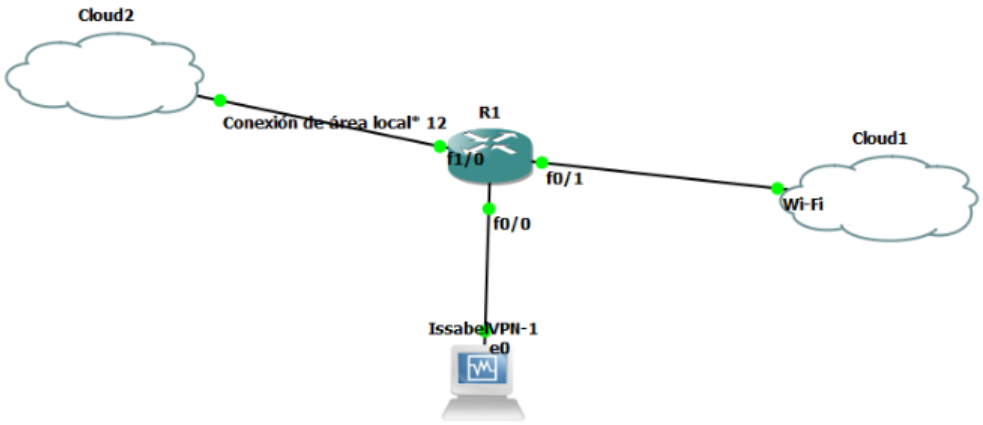

Figura 2.11: Topología general Práctica 4.

En esta topología se puede evidenciar que se tiene dos nubes, una de ellas sera la que permita tener acceso a la VPN como tal y la otra permitirá administrarla.

Para la realización de esta práctica se debe construir un certificado el miso que permita tener acceso a la VPN.
Los campos más importantes para la configuración del servidor son:

- **IP or HOST:** IP o Host que la Open VPN se tiene que conectar puede ser publica o la misma IP del servidor de Issabel.
- **Listening Port:** Puerto por defecto que escucha 1194.
- **Protocol:** Protocolo a utilizar, en este caso UDP.
- **Server Network:** Segmento de la red que utilizara la VPN.
- **Server Mask:** Mascara que utilizara la red.

- **Timeout:** Periodo de tiempo que tiene en respuesta.

Toda esta configuración se la realiza en la opción de *Seguridad>OpenVPN.*
Después de la creación de los certificados para los dos usuarios remotos gracias a la configuración en Issabel del OpenVPN, es muy importante configurar el NAT en la misma máquina virtual en la pestaña de *PBX >Edit Settings*, habilitando el NAT y colocando la IP del servidor, tal como se ve en la Fig. 2.12.

Figura 2.12: Configuración de NAT

Una vez descargados los dos certificados y habilitado el NAT se debe realizar la configuración de cada uno de ellos en los dispositivos (softphones) que se van a utilizar, estos son dos X-Lite que se encuentra en la computadora y Zoiper en el celular.
Primero se va a cargar el certificado en el cliente celular, seleccionando el certificado en la carpeta en donde se haya guardado, para verificar que este cargado correctamente se despliega una pantalla, tal como se ve en la Fig. 2.13.

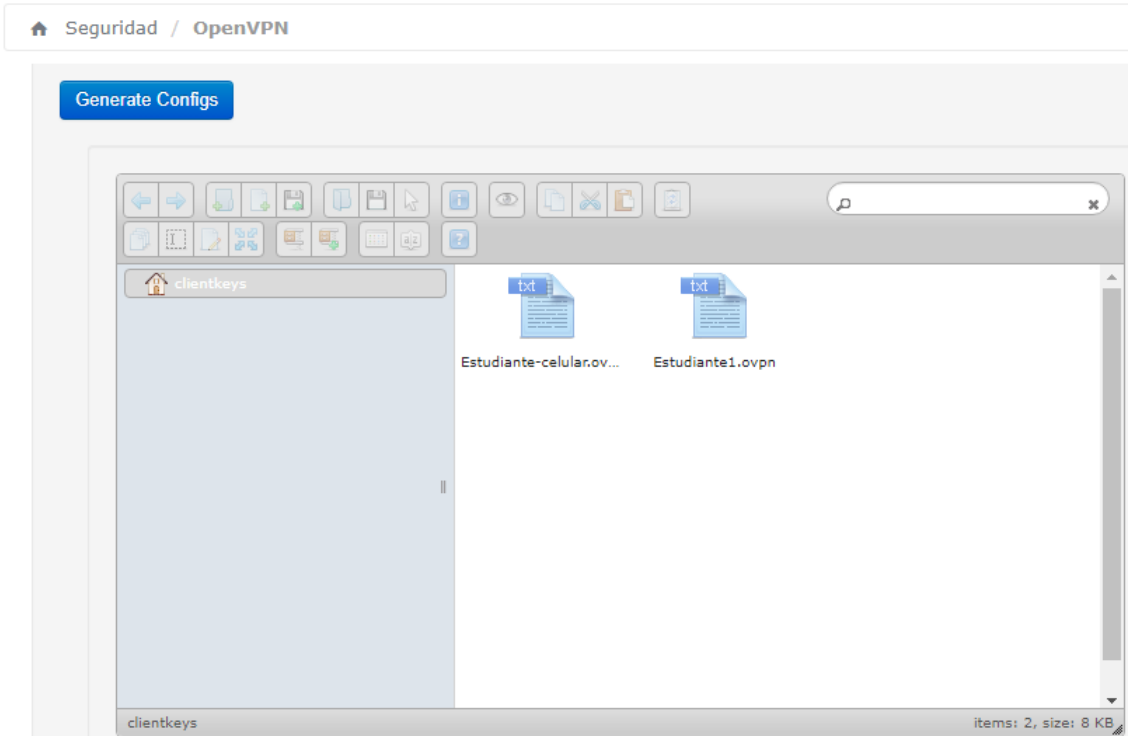

Figura 2.13: Certificados.

Adicionalmente se agregara un paso, con el final de poder comprobar que los dos dispositivos remotos se encuentran en la VPN, se debe dirige a la pestaña *Seguridad >OpenVPN >Status* lo mismo que va a permitir visualizar que los dos dispositivos tienen la IP que pertenece a la VPN ,tal como se observa en la siguiente Fig. 2.14

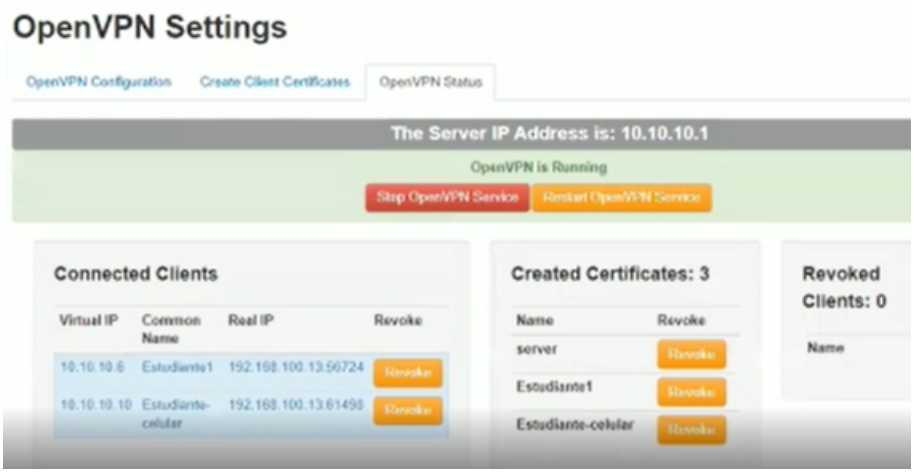

Figura 2.14: Verificación de dispositivos remotos en la VPN.

Finalmente se realiza la prueba de la llamada entre los dos dispositivos remotos, después de toda la configuración de la VPN, la cual se realizó de manera exitosa.

2.2.5. Práctica 5:Configuración de Auto QoS.

La práctica del laboratorio número cinco tiene como objetivo general la configuración del Auto QoS por defautl que ofrece el router y finalmente la comprobación de la correcta configuración mediante una llamada entre extensiones que se encuentran en la central telefónica mediante el uso de dos dispositivos que se cargaron correctamente en una máquina virtual.

La topología del laboratorio de la práctica número cinco se observa en la Fig. 2.15.

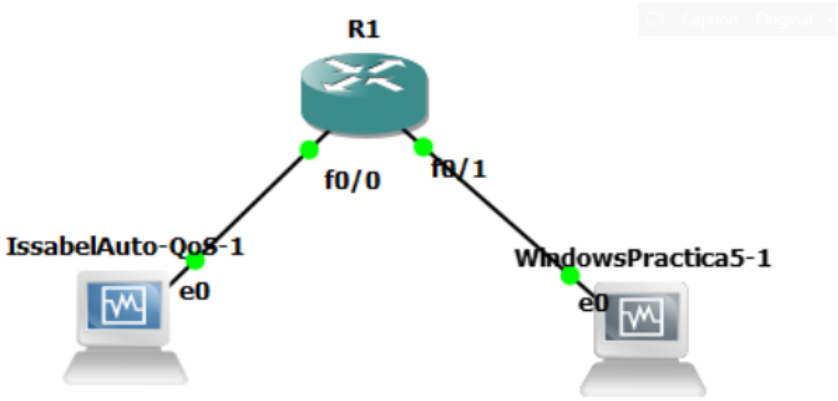

Figura 2.15: Topología general Práctica 5.

Para iniciar con esta práctica de laboratorio se debe hacer un énfasis en que es un desarrollo más avanzado de la practica 3 ya que en el desarrollo de este laboratorio se utilizaran comandos que permiten verificar lo que se configuro en la práctica número tres.
En esta práctica es importante delimitar el ancho de banda en cada interfaz con la ayuda del comando *bandwidth* seguido del número 2(MHz).

Como se mencionó antes en esta práctica solo se va a utilizar un solo comando, *auto qos voip*, es importante que la ejecución de este comando se la realice en cualquier interfaz dentro de la topología ya mencionada.

Gracias a la ejecución del único comando para este laboratorio se puede comprobar el correcto funcionamiento con la ayuda del comando *show running config*, el mismo que permitirá observar un conjunto de configuraciones en base al QoS como son *class-map*, este permite generar clases que ayuden a identificar el tráfico que se le asigna a cada clase mediante una lista de acceso, el otro comando es *policy-map* encargado de asignar prioridades a las clases ya anteriormente creadas.

3. RESULTADOS

3.1. Resultados

En este apartado se encuentran definidas las resoluciones de las actividades que fueron realizadas para los estudiantes al finalizar cada una de las prácticas. Como se ha mencionado anteriormente estas actividades tienen como finalidad ayudar a evaluar los conocimientos que pudieron capturarlos estudiantes en el desarrollo de cada práctica.

3.1.1. Práctica 1: Aseguramiento de capa 2 en Telefonía IP.

El enunciado de la actividad de la práctica de laboratorio 1 es: *Cambio del protocolo (ICMP) en la asignación del ACL.*

De acuerdo a lo indicado, la actividad consta de la ejecución de varios comandos los mismos que permitirán que el protocolo ICMP no se pueda realizar con éxito en las VLANs.

Para el desarrollo de esta actividad se debe hacer uso de la sección Configuración de ACL, en este caso la regla que se genera es con la ayuda de siguiente comando. *access-list 102 deny icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255*.

Este comando consta del número del access-list, la orden que en este caso es *deny* y las redes a las cuales se quiere negar el tráfico.

Después de la creación del ACL se debe asignar a la interfaz correcta, en este caso la que posee las dos VLANs, para este caso es la fasEthernet 0/0.10 y la fasEthernet 0/0.20, con la ayuda del siguiente comando.
ip access-group 102 in

Una vez asignada a la interfaz correcta ahora lo único que sigue es comprobar mediante ping en un CMD en las dos máquinas virtuales.
Es importante tomar en cuenta que la opción siempre será IN.El resultado final se lo observa en la Fig. 3.1.

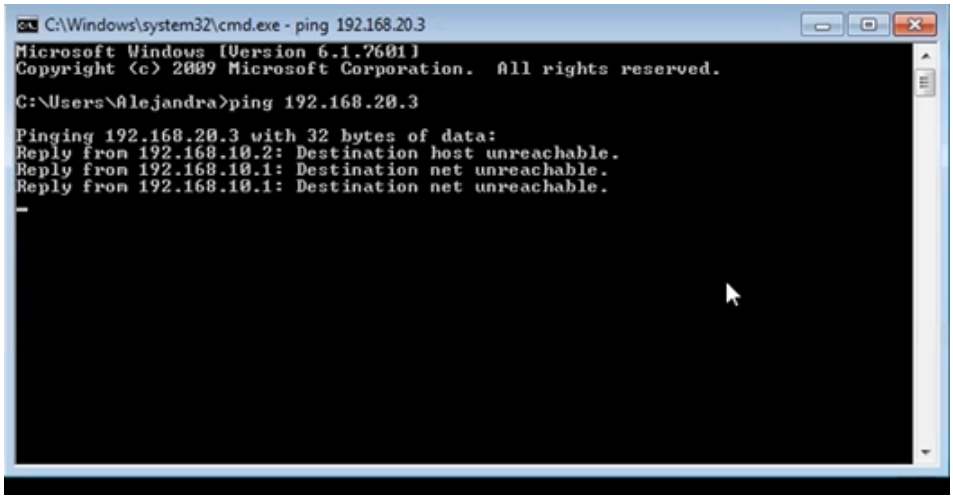

Figura 3.1: Protocolo ICMP denegado.

También se lo puede verificar desde la otra máquina virtual que en este caso es un Ubuntu, ejecutando el mismo comando, ping a la IP de la maquina Windows, el resultado final se lo observa en la Fig. 3.2.

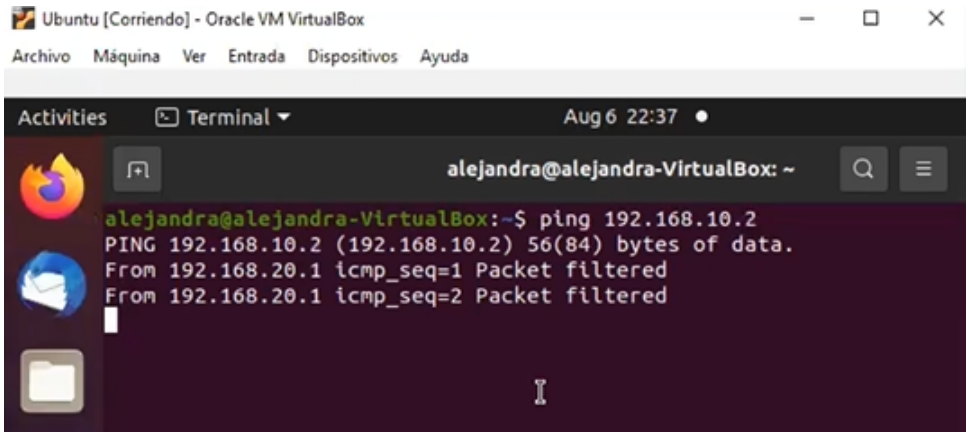

Figura 3.2: Protocolo ICMP denegado.

3.1.2. Práctica 2: Cifrado de Trafico VOIP

El enunciado de la actividad de la práctica de laboratorio 2 es: *Capturar la llamada sin la configuración del cifrado y escuchar la voz del estudiante para después configurar el cifrado y verificar que no se puede escuchar. Por último, verificar cual es el resultado con la ayuda de la visualización de flujos UDP y TLS en cada caso.*

De acuerdo a lo mencionado, la actividad tiene varios tópicos. Una de ellas consiste en realizar la modificación del certificado en el servidor, el transporte, el número de puerto y la

opción de encriptar. Se debe indagar y configurar cada uno de estos parámetros correctamente ya que si no se encuentran en las dos centrales de la misma manera no se podrá tener una llamada exitosa.

El primer para para la ejecución de la actividad es acceder al softaware Wireshark, después ejecutar la llamada entre extensiones y colocar el filtro en primer lugar seria UDP para poder escuchar la llamada.

Para esto se da clic en cada paquetes y se dirige a la opción de **Seguir >Flujo UDP** y se activa la opción y se despliega una pantalla emergente con la información que tiene cada paquete, tal como se muestra en la Fig. 3.3.

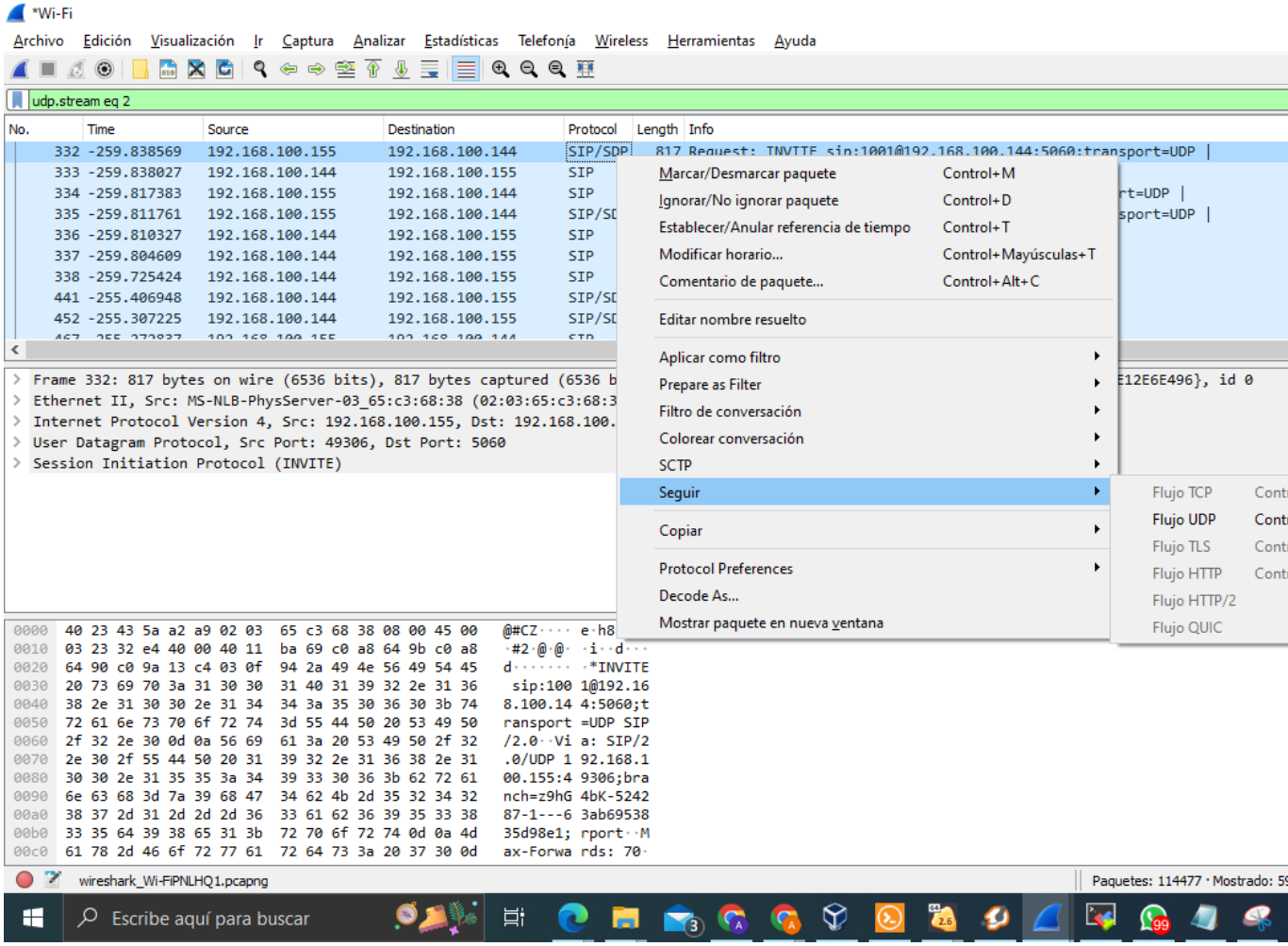

Figura 3.3: Visualización de la información de cada paquete.

Una vez dentro de esta opción se puede visualizar la información correcta, como la IP que se registra, la IP destino que en este caso es el servidor, el tipo de transporte, el número del puerto, numero de extensión, el tipo de cifrado, etc., tal como se muestra en la Fig. 3.4.

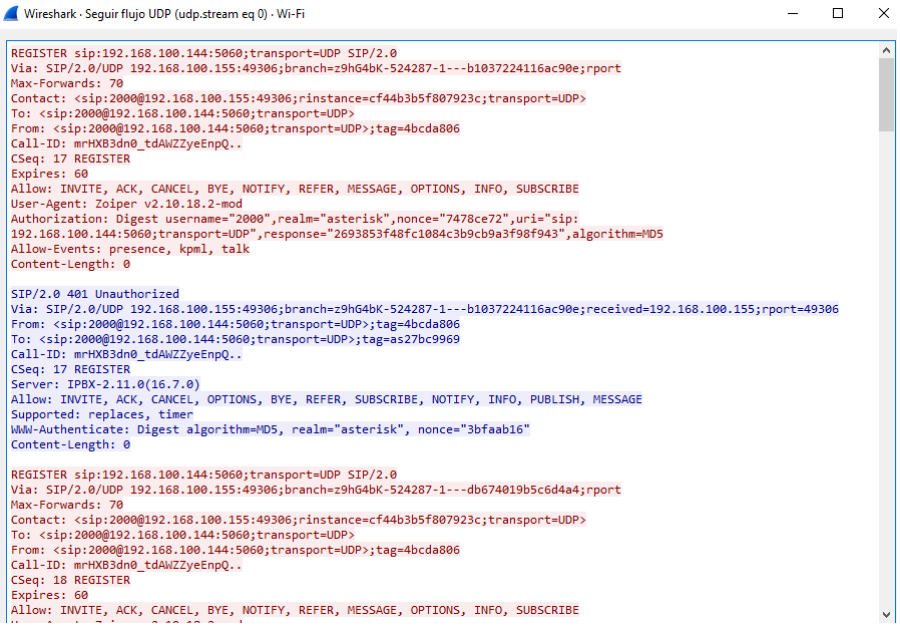

Figura 3.4: Flujo UDP.

Con solo capturar unos pocos datos del usuario o los HASH se pueden utilizar herramientas que fácilmente ayuden a descifrar las claves que posee y esto permita a los hackers que sea mucho más fácil obtener información valiosa que puede tener un costo muy grande.

En esta parte de la actividad también se puede tener la opción de escuchar que es o que se dijo en la llamada, esta opción se tiene en el Wiresahrk, en la pestaña de **Telefonía >RTP >Flujo RTP**, tal como como se como se muestra en la Fig. 3.5.

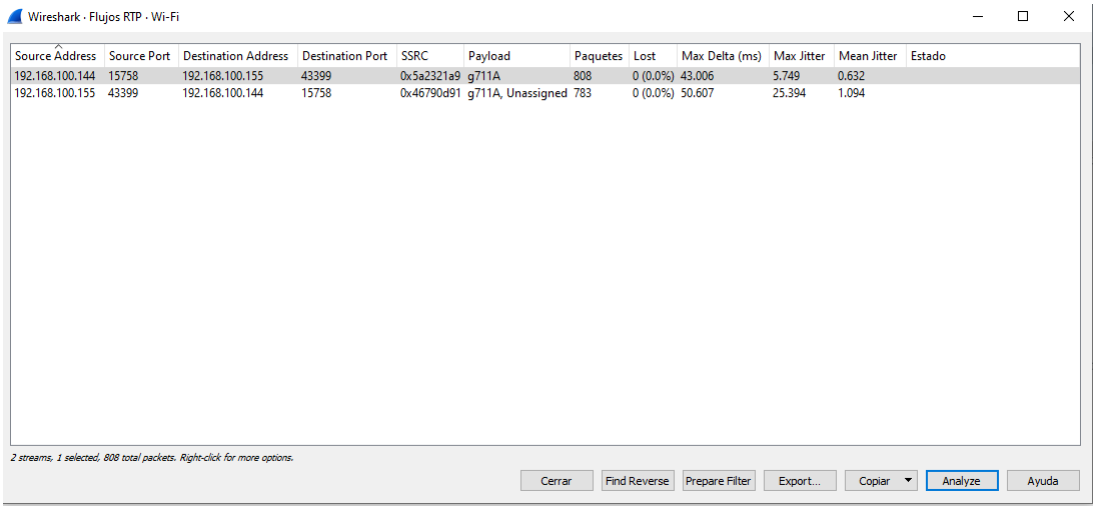

Figura 3.5: Flujo RTP.

Continuando con la parte final de la actividad, finalmente se dirige a al opción **Analyze**, desplegando así otra ventana emergente, tal como como se como se muestra en la Fig. 3.6.

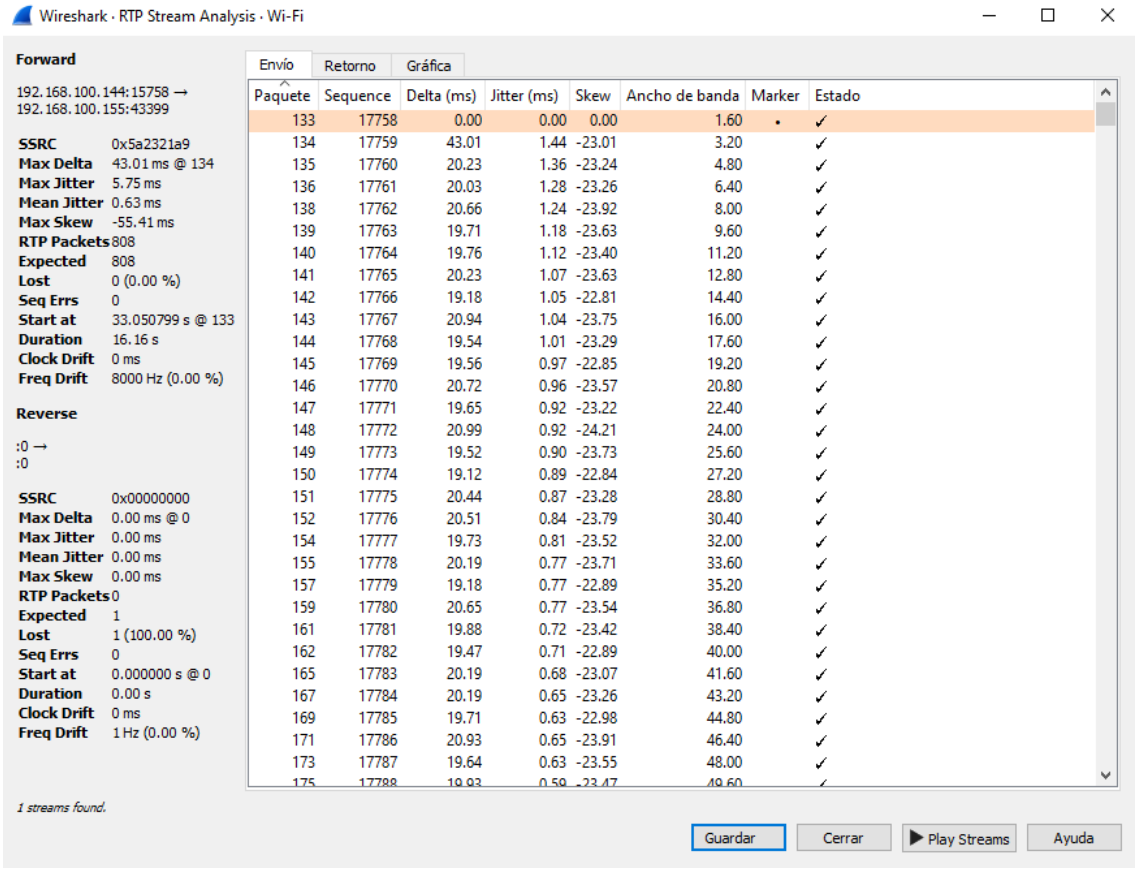

Figura 3.6: Análisis del Flujo RTP.

Finalmente se debe dar clic en la opción **Play Streams**, la misma que despliega la última pantalla emergente en la que se puede visualizar un audio, dicho audio es lo que se pudo capturar al momento de realizar la llamada, se visualiza tal como se muestra en la Fig. 3.7 en la que se tiene un flujo continuo de la voz que realizo en este caso el usuario, la cual se va a proceder a escuchar para verificar que sin certificado no se tiene la seguridad correspondiente y exitosa.

Figura 3.7: Audio de la llamada.

Al igual que en el apartado anterior para comprobar el correcto funcionamiento del cifrado se debe utilizar las configuraciones correctas en el servidor de Issabel.

El único cambio que se realiza es en la pestaña **PBX>Configuración de PBX >Extensiones** dentro de la máquina virtual o central telefónica Issabel, en donde se dirigen a la lista de extensiones y se debe configurar de igual manera la opción de **transporte**, que en este caso sería TLS, **número de puerto**, será 5061 y **encryption.**, la cual debe ser habilitada o colocada como **YES.**

Hecha dicha configuración, para comprobar el correcto funcionamiento de la misma, se puede acceder mediante otra extensión si así el estudiante lo desea con estas nuevas configuraciones o con las mismas que anteriormente ya fueron configuradas para verificar que todo fue correctamente ejecutado.

En donde se podrá evidenciar de igual manera que en el apartado anterior el primer paso es correr el programa Wireshark, una vez con el programa en su pantalla de inicio se deberá dar clic y seleccionar **Seguir** para que se despliegue la pantalla emergente con la información en este caso del flujo TCP. Para finalmente verificar que lo único que se puede observar son

caracteres sin sentido, también se puede verificar que el protocolo que se está utilizando es TLS dentro de la pantalla de la captura de paquetes del Wireshark, tal como se como se muestra en la Fig. 3.8.

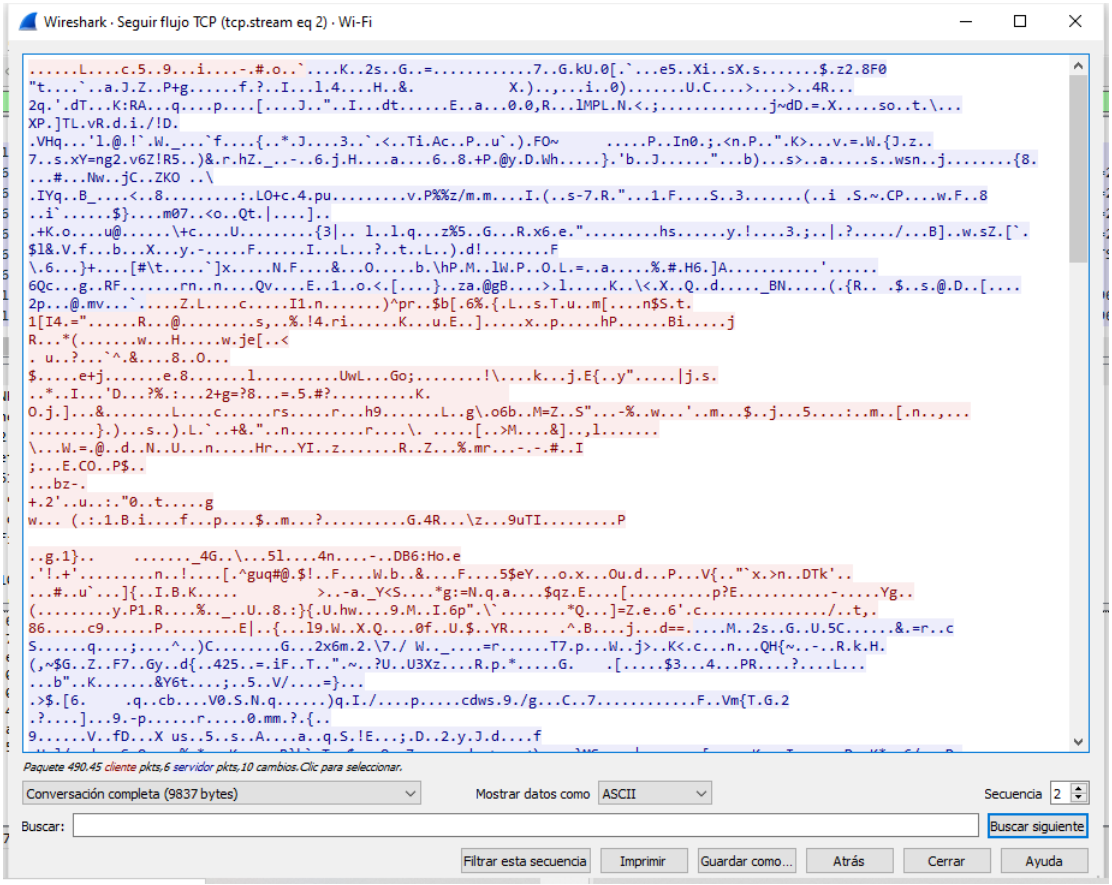

Figura 3.8: Flujo TCP.

3.1.3. Práctica 3: Modificación de clases de mapeo.

El enunciado de la actividad de la práctica 3 es: *Dentro de la práctica de laboratorio realizar la creación de dos clases de mapeo, con la configuración de la prioridad que se le quiere asignar a los protocolos FTP y TELNET respectivamente. Comprobar en la captura de paquetes el marcado asignado.*

Esta actividad permitirá emular un ambiente mucho más real, en donde se puede administrar diferentes protocolos se les pueda asignar una prioridad de acuerdo a un cuadro mencionado ya anteriormente que permite asignar el respectivo código y que los paquetes puedan ser enviados y recibidos correctamente. De esta los usuarios no tendrán sobre cargo en la red y que esto genere problemas para las empresas que brindan estos servicios y problemas

como estos les genere perdidas de dinero.

Para lograr esto es necesario realizar una configuración de prioridad que se le debe asignar a cada clase de mapeo que se crea para cada protocolo que se colocó para que el estudiante pueda realizar la actividad. Es necesario tomar en cuenta que la configuración se la realiza de igual manera en el router que da paso al intercambio de paquetes.

La configuración de dicha prioridad se lo realiza mediante varios comandos. El comandos que permitirá cumplir con la actividad es **set ip dscp código**. Este comando se utiliza para dar prioridad mediante un código que se lo modifica en la cabecera de cada paquete y es el que marca los paquetes desde el más importante al menos importante.

Este mismo comando se lo realiza al otro lado de la red pero en este caso se utiliza el siguiente comando **set precedence numero** este hace match con la prioridad a los diferentes protocolos que se tiene en la red ya configurados en la primera parte de la topología, permitiendo así finalmente que la voz que siempre va a tener prioridad uno, sea el que se verifique primero.

Al finalizar toda la configuración anteriormente mostrada, se procede a efectuar las pruebas de funcionamiento respectivas. Para lo cual se utiliza el software Wireshark mediante la opción en cada interface en el GNS3, tal como se como se muestra en la Fig. 3.9.

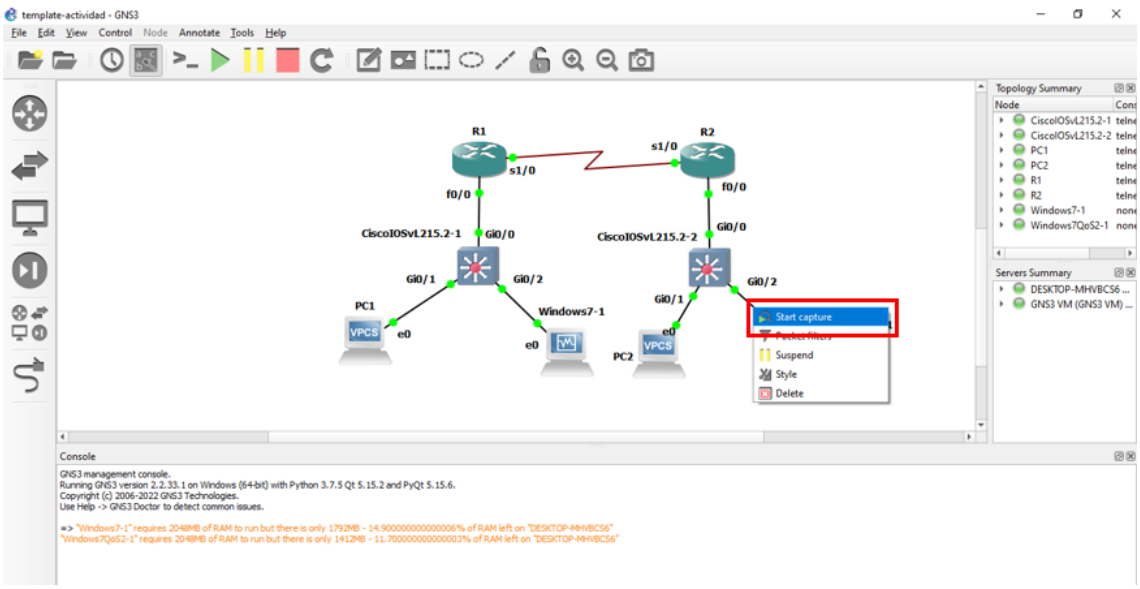

Figura 3.9: Captura de paquetes.

Para esta parte de la actividad se debe utilizar el putty colocando la ip del servidor **(192.168.10.2)**,el cual permitirá tener acceso mediante el protocolo telnet, una vez abierta la conexión, tal como se como se muestra en la Fig. 3.10.

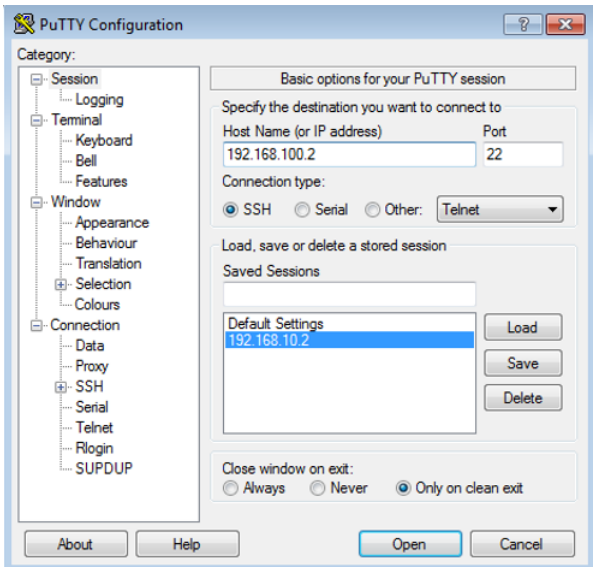

Figura 3.10: Captura de paquetes.

Después se despliega una pantalla emergente solicitando el usuario y la contraseña que tiene la máquina virtual, una vez dentro de la maquina se puede capturar los paquetes con el filtro del protocolo que se colocó en el putty, en este caso telnet, tal como se como se muestra en la Fig. 3.11.

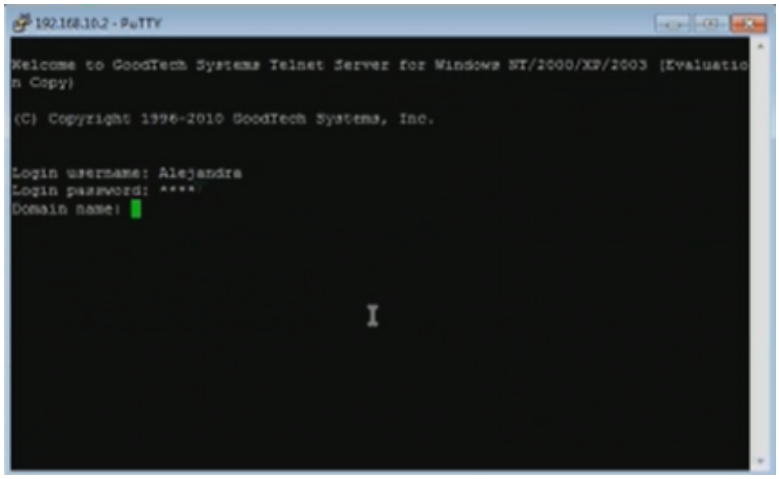

Figura 3.11: Acceso mediante Telnet.

Para que finalmente se observe que la conexión fue exitosa y se puede capturar ya tráfico y observar que prioridad obtiene si se accede mediante telnet tal como se configuro anteriormente, tal como se como se muestra en la Fig. 3.12.

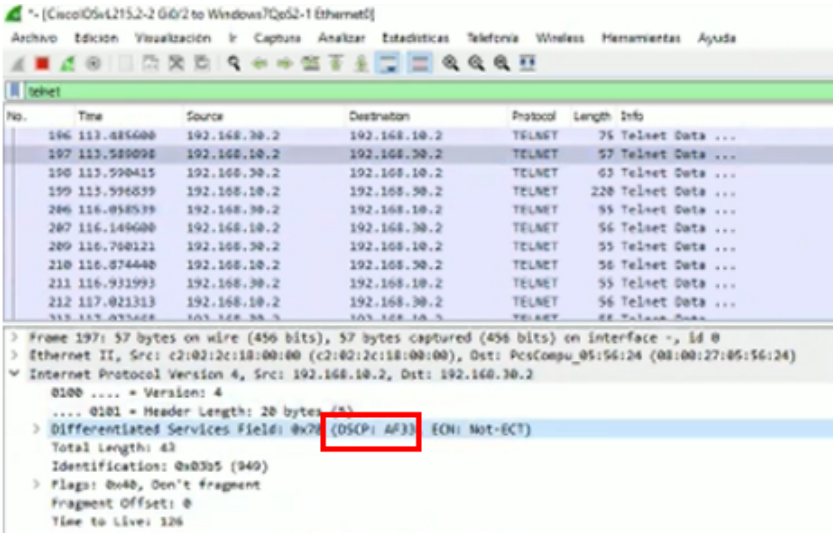

Figura 3.12: Visualización de prioridad del protocolo Telnet.

Para finalizar la actividad también se comprueba la prioridad del protocolo FTP, en este caso se utiliza WinSCP para poder tener una conexión FTP, tal como se como se muestra en la Fig. 3.13.

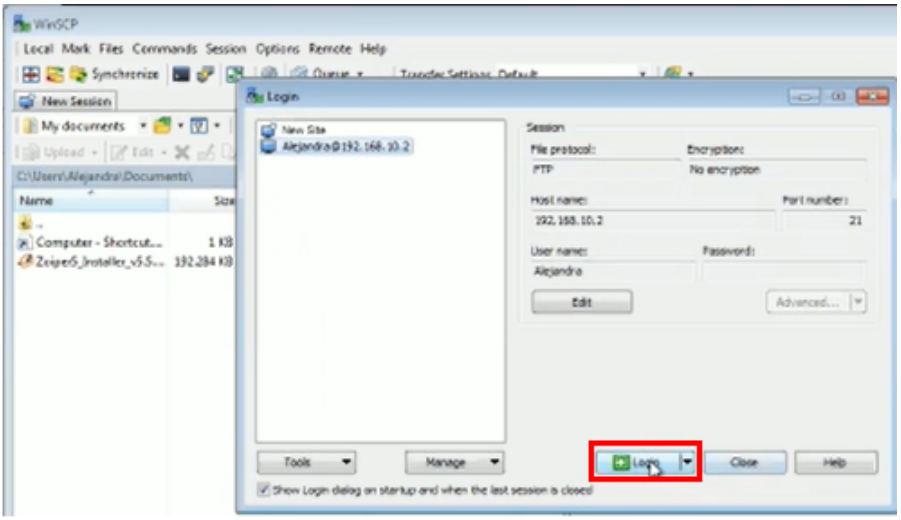

Figura 3.13: Conexión FTP.

Finalmente se aplica el filtro ftp en Wireshark y se observa cual es el resultado de la configuración para la prioridad, tal como se como se muestra en la Fig. 3.14.

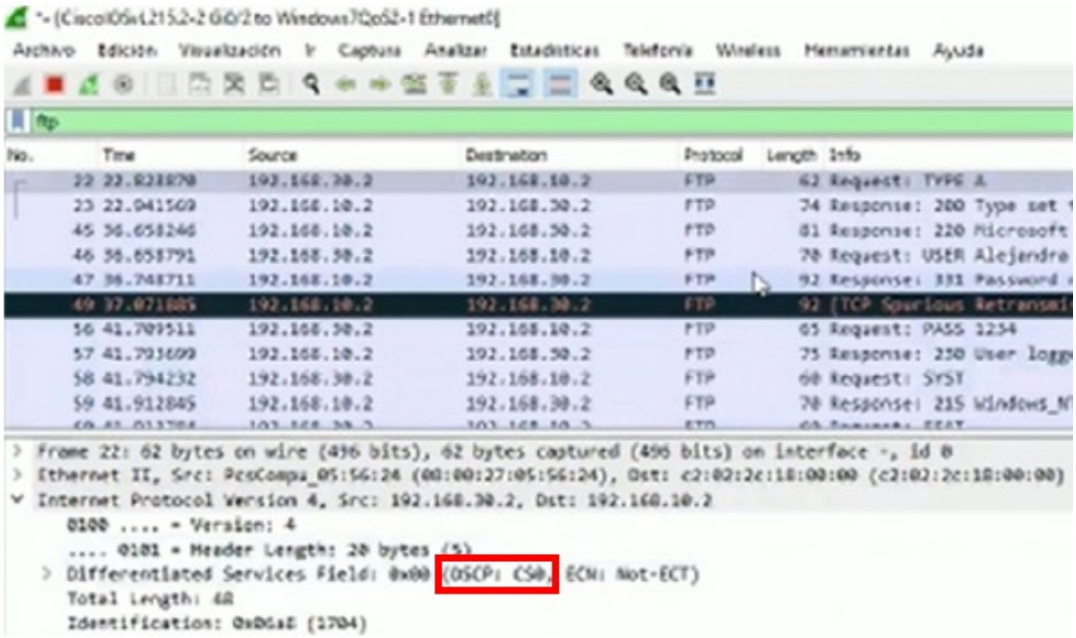

Figura 3.14: Visualización de prioridad del protocolo FTP.

3.1.4. Práctica 4: VPN en VOIP

El enunciado de la actividad de la práctica de laboratorio 4 es: *Mediante la creación de reglas en el Firewall, mediante comandos en consola en la máquina virtual para poder bloquear el puerto FTP (21) a los usuarios remotos. Comprobar que esta regla esta correcta mediante el acceso a telnet desde un usuario remoto y un local. Finalmente comprobar que la llamada aún se pueda realizar con éxito:*

Para realizar esta actividad se parte de la verificación de que el puerto 21 se encuentre escuchando, en este caso se utiliza el comando.

```
netstat -tapn
```

Si el caso es que el puerto no esta levantado se debe utilizar el comando

```
rpm -qa | grep ftpd
```

El mismo que realiza una búsqueda para verificar que versión de FTP se tiene instalado en la máquina.

Una vez verificado que versión se tiene, se debe habilitar con la ayuda del siguiente comando.

```
iptables -R ISSABEL\_INPUT 13 -p tcp -m tcp --dport 21:21 -j ACCEPT
```

Después de esto se debe bloquear a la interfaz **tun** por la cual pasa la VPN, utilizando el comando.

```
iptables -i tun0 ISSABEL\_INPUT 12 -p tcp -m tcp --dport 21:21 -j ACCEPT
```

Para finalmente guardar los cambios con la ejecución del comando

```
iptables-save > /etc/sysconfig/iptables
```

Para verificar las reglas que se han aplicado hasta e momento y realizar la prueba de funcionamiento que el puerto 21 fue bloqueado para usuarios remotos, el primer paso es utilizar el comando

```
iptables -nvL
```

Y la prueba de funcionamiento es abrir un CMD (Command Prompt) y realizar telnet al puerto 21, tal como se como se muestra en la Fig. 3.15.

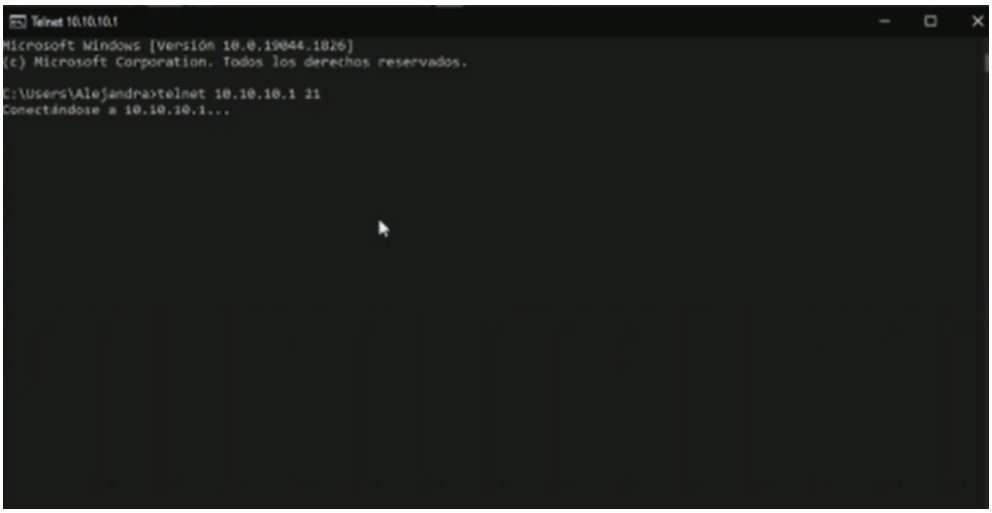

Figura 3.15: Puerto FTP Bloqueado.

3.1.5. Práctica 5: Configuración de AutoQos.

El enunciado de la actividad de la práctica de laboratorio cinco es: *Consultar cuales son los equivalentes de los comandos de Auto Qos para Routers Huawei y Juniper*.
En los routers Juniper se puede visualizar las configuraciones predeterminadas mediante el comando *show-of-service*, que es un comando de modo operativo.

Ahora si no se aplica los comandos para la creación de clases de reenvió, de manera automática se crea un conjunto de clases predeterminadas, como también el 100 porciento del

ancho de banda a la salida del puerto donde están las clases predeterminadas.

Hay que tomar en cuenta que las clases de reenvió es transparente. Las semejanzas que tiene con los comandos Cisco es que este también posee los mismos códigos de prioridad. Mientras tanto en Huawei se realiza una comparación mediante una tabla, que tiene los comandos que se puede utilizar tanto en Cisco como en Huawei, verificando los más importantes que se tenían para verificar las semejanzas y diferencias entre la ejecución de los comandos y tener una comparativa de cual es mucho más fácil entender y aprender.

Comando en Cisco	Comando en Huawei
match ip precedence	if-match ip-precedence ip-precedence-value
priority percent percentage	queue ef bandwidth pct percentage
set [ip] precedence ip-precedence	remark ip-precedence ip-precedence
service[policy policy name	traffic-policy policy-name
set ip dscp dscp-name	remark dscp dscp-name
class-map {match-any| match-all} classifier-name	traffic classifier classifier-name operator {or|and}
match precedence ip-precedence-value	if-match ip-precedence ip-precedence-value
bandwith percent percentage	queue af bandwith pct percentage
class class-name	traffic bahavior behavior-name classifier classifier-name behavior behavior-name

4. CONCLUSIONES y RECOMENDACIONES

4.1. Conclusiones

- La elaboración de un conjunto de prácticas de laboratorio enfocadas a la Calidad de Servicio *QoS* y seguridad ayudara a los estudiantes de la Escuela Politécnica Nacional de la carrera de Ingeniería en Telecomunicaciones en su vida profesional mediante la familiarización de varios escenarios que se dan a nivel empresarial y que con el pasar de los tiempos va cambiando constantemente.

- El uso de herramientas como Notion (que brinda un conjunto de bloques dinámicos) para la creación de las prácticas de laboratorio, genera una gran facilidad en la elaboración de una guía diferente, colaborativa, fácil de actualizar y sencilla de implementar ya que maneja perfiles de usuario.

- Con la implementación de reglas en cuanto al ACL se puede lograr la separación del tráfico de voz y el tráfico de datos sin perder la conectividad entre las redes lo que ayuda a conseguir una mayor administración y seguridad en la red.

- Se comprobó que en el escenario que se tenia al no aplicar los certificados TLS las llamadas pueden ser interceptadas y escuchadas de una forma clara lo que generara un alto riesgo en la comunicación mientras que en el escenario aplicando los certificados aun siendo interceptada la llamada, la comunicación no se entiende ya que se transmite de una forma cifrada lo que ayuda a la privacidad de datos de cada usuario.

- Se verificó que como en la red viajan paquetes de diferentes protocolos es necesario que estos sean identificados y marcados para darles prioridad con la finalidad de mejorar los servicios de la red, para brindar mejoras en el ancho de bandas, esto se consiguió aplicando configuraciones calidad y servicio (QoS).

- Con la implementación de una VPN, el estudiante puede entender la forma de trabajo remoto que en los últimos años que se han aplicado varias empresas por cuestiones de bioseguridad relacionadas al Covid 19, logrando conectar al usuario a la red LAN de la empresa y hacer uso del servicio de telefonía IP desde cualquier lugar o red que tenga acceso a Internet.

- Para facilitar la administración de los equipos activos de red, el tiempo que los usuarios emplean en la configuración y la investigación de los componentes que involucra la

calidad y servicio (QoS) existe la configuración automática, conocida como Auto QoS, la misma que implementa todos estos componentes en una sola línea de comandos.

4.2. Recomendaciones

- Se recomienda tener recursos de memoria y procesador,que permitan la correcta ejecución de todas las máquinas virtuales, software y emuladores en el desarrollo de cada una de las practica descritas en este componente.
- Se recomienda investigar otros emuladores de red diferentes a GNS3 tales como Eve-NG, VIRL o Netsim que permitan tener todas las opciones, comandos para un correcto funcionamiento, ejecución y administración de prácticas de laboratorio, las cuales se quiere tener un ambiente mucho mas real y profesional.
- Se recomienda utilizar nuevas reglas en la aplicación de ACL para generar mas métodos de seguridad en la red si fuera necesario en un ambiente empresarial.
- Para la ejecución de los diferentes archivos que consta en el presente trabajo se requiere que el software GNS3 que se utilizo en gran parte de las prácticas de laboratorio debe ser GNS3 versión 2.2.33 o superior.
- Para la elaboración de trabajos futuros se plantea que en cuanto a la ejecución de practicas de laboratorio enfocadas a al telefonía IP se las realiza en la nube, ya que esta brinda mayor seguridad y mayor cantidad de recurso para poder ser usados por los usuarios.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] y. D. G. C. P O. Hersent, J.-P. Petit, “Ip telephony: Deploying voice-over-ip protocols. john wiley sons,” no. 1, 2005.

[2] P. T. y A. Takanen, “Securing voip networks: Threats, vulnerabilities, and countermeasures,” no. 2, 2007.

[3] y. S. F. D. R. Kuhn, T. J. Walsh, “Security considerations for voice over ip systems,” 2005.

[4] A. D. Keromytis, “A look at voip vulnerabilities,” vol. 35, no. 1, pp. 41–50, 2010.

[5] M. A. V. Pilozo, “Implementacion de tecnicas de calidad y servicio (qos) en un prototipo de red convergente de datos, videos y telefonia usando ip6 en una empresa tipo pyme,” 2019. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/2027.

[6] M. A. C. Martínez, “Análisis de vulnerabilidades, investigación forense y política de seguridad para sistemas de telefonía ip basados en asterisk,” 2016. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/15155.

[7] Y. Fernández, “Voip: qué es y cómo funciona,” 2019. [Online]. Available: https://www.xataka.com/basics/voip-que-como-funciona

[8] S. D., “Protección de tráfico sip en redes de telefonía ip a través del análisis de técnicas de seguridad en redes corporativas.” 2012.

[9] M. F., “Elementos de la telefonia ip | voip,” 2016. [Online]. Available: http://www.servervoip.com/blog/elementos-de-la-telefonia-ip/.

[10] D. Aguilar, “Implementación de una central telefónica pbx basada en asterisk,” *Universidad del Azuay*, 2011.

[11] J. A. Carballar, “Voip la telefonía de internet,” *Paraninfo S.A.*, vol. 1, pp. 10–15, 2008.

[12] “Diseño y configuración de un sistema de voip para la etsit de la universidad politécnica de cartagena,” 2006. [Online]. Available: https://repositorio.upct.es/bitstream/handle/10317/231/pfc1825.pdf;sequence=1

[13] “Seguridad en voz sobre ip,” 2006.

[14] “Qué es sip – session initiation protocol,” *3CX*, 2021. [Online]. Available: https: //www.3cx.es/voip-sip/sip/

[15] “¿qué es h323?” *3CX*, 2021. [Online]. Available: https://www.3cx.es/voip-sip/h323/

[16] “Qué es rtp – real time transport protocol,” *3CX*, 2021. [Online]. Available: https://www.3cx.es/voip-sip/rtp/

[17] “¿qué es rtcp?” *3CX*, 2021. [Online]. Available: .https://www.3cx.es/voip-sip/rtcp/

[18] Z. T., “Modelos de configuraciÓn de calidad de servicios (qos). en el trÁfico de voz y su impacto en el sistema de telefonÍa ip de la empresa cemento chiimborazo c.a.” pp. 8–19, 2011.

[19] “Calidad de servicio qos (quality of service).” [Online]. Available: https://www. mundotelematico.com/calidad-de-servicio-qos-quality-of-service/

[20] “Servicios diferenciados (diffserv).” [Online]. Available: https://1library.co/article/ servicios-diferenciados-diffserv-modelos-calidad-servicio.z14l59vz

[21] “Tema2-9-diffserv.pdf.” [Online]. Available: https://www.tlm.unavarra.es/~daniel/ docencia/tar/tar12_13/slides/Tema2-9-DiffServ.pdf

[22] Galarza, “Introduccion (que es vpn,” 2021. [Online]. Available: https://www.ecotec.edu.ec/documentacion/investigaciones/estudiantes/trabajos_ de_clases/1580_TRECALDE_0033.pdf

[23] O. Loza, “Estudio y diseÑo de una red privada virtual para brindar el servicio de voip, adminitrado bajo el sstema operativo linux,” 2008. [Online]. Available: http://bibdigital.epn.edu.ec/handle/15000/261

[24] Notion, “What is notion?” 2022. [Online]. Available: https://www.notion.so/guides/ what-is-notion

[25] GNS3, “Primeros pasos con gns3,” 2021. [Online]. Available: https://docs.gns3.com/ docs/

[26] “What is a virtual machine (vm)?” *Azure Microsoft*, 2021. [Online]. Available: Whatisavirtualmachine(VM)?

6. ANEXOS

Los resultados del presente escrito están detallados en la resolución de las actividades de las cinco diferentes prácticas de laboratorio, el desarrollo de la práctica por ende se encuentra especificado en la sección de Anexos.
Es importante mencionar que todo el desarrollo, pruebas de funcionamiento, resoluciones de actividades se han realizado en la plataforma Notion con el uso de bloques animados,imágenes animadas, videos explicativos que no se evidencian en el presente escrito.
Para la correcta visualización de los laboratorios se puede acceder al enlace:

`https://pointy-whistle-142.notion.site/`
`Laboratorio-Seguridad-y-QoS-ebe5718419f24e2c8f3c45307f7e89e7`

En este link se detalla la lista de las cinco prácticas de laboratorio, videos y resolución de todas las actividades propuestas.

ANEXO I. Laboratorio 1: Aseguramiento de Capa 2 en Telefonía IP.

ANEXO II. Laboratorio 2: Cifrado de Trafico VoIP.

ANEXO III. Laboratorio 3: Servicios Diferenciados en VoIP.

ANEXO IV. Laboratorio 4: VPN en VoIP.

ANEXO V. Laboratorio 5: Configuración de Auto Qos.

ANEXO VII. Resolución de Actividades Laboratorios: Seguridad y QoS.