ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTÓNICA

ESCUELA DE INGENIERIA EN SISTEMAS

“PROTECCIÓN DE TRÁFICO SIP EN REDES DE TELEFONÍA IP A TRAVÉS DEL ANÁLISIS DE TÉCNICAS DE SEGURIDAD EN REDES CORPORATIVAS”

TESIS DE GRADO

Previa la obtención del título de

INGENIERO EN SISTEMAS INFORMÁTICOS

Presentado por:

DIANA CAROLINA CHAPALBAY SANTILLÁN

Riobamba – Ecuador

2011

Agradezco a Dios por darme la vida, la constancia y perseverancia para alcanzar mis objetivos planteados, de manera especial a mis padres porque me han apoyadoincondicionalmente y me han guiado para continuarcon mis estudios superiores, a mis hermanas Erika y Tatiana y a Vinicio por estar siempre cuando los necesité, A mi director, Ingeniero Alberto Arellano y al Ingeniero Patricio Morenocolaborador de tesis por sus enseñanzas y el tiempo brindado para culminar mi carrera y a todos quienes me brindaron su apoyo para sobrellevar esta dura tarea.

A mis padres por el esfuerzo, que han realizado para que yo pudiera seguir esta carrera, a mis hermanas por el apoyo que me han brindado durante mi vida estudiantil a Vinicio por las palabras de aliento y comprensión ya que con ello he alcanzado un objetivo más en mi vida.

NOMBRE	FIRMA	FECHA
Ing. Iván Ménes **DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	----------	----------
Dr. Raúl Rosero **DIRECTOR ESCUELA DE INGENIERÍA EN SISTEMA**	----------	----------
Ing. Alberto Arellano **DIRECTOR DE TESIS**	----------	----------
Ing. Patricio Moreno **MIEMBRO DEL TRIBUNAL**	----------	----------
Ing. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACIÓN**	----------	----------

NOTADE TESIS _____

Yo Diana Carolina Chapalbay Santillán soy la responsable de las ideas, doctrinas y resultados expuestos en esta: Tesis, y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo.

_____

Diana Carolina Chapalbay Santillán

ÍNDICE DE ABREVIATURAS

AH: Authentication Header

ARP: Address Resolution Protocol

DoS: Denegación de servicio

ESP: Encapsulated Security Payload

ESPOCH: Escuela Superior Politécnica de Chimborazo

HTTP: Hypertext Transport Protocol

IETF: Internet Engineering Task Force

IKE: Internet Key Exchange

IP: Internet Protocol

IPsec: Internet Protocol security

MAC: Control de Acceso al medio

MitM: Man-in-the-middle

NS: Network Server

OSI: Open Systems Interconnection. Interconexión de Sistemas Abiertos

RTP:Real-time **T**ransport **P**rotocol (Protocolo de Transporte de Tiempo real)

SA: Security Association (Asociación de Seguridad)

SDP: Session Description Protocol

SIP: Session Initiation Protocol

SPI: Índice de parámetros de seguridad

SSH:Secure **SH**ell

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

TLS: Transport Layer Security - Seguridad de la Capa de Transporte

UA: Agente de Usuario o User Agent

UAC: Agente de Usuario Cliente

UAS: Agente de Usuario Servidor

UDP: User Datagram Protocol, protocolo de datagrama de usuario

ÍNDICE GENERAL

CAPÍTULO III

Protocolo de Comunicación SIP

CAPITULO IV

Análisis Comparativo

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En los últimos años el interés por las redes de paquetes IP como soporte de tráfico multimedia ha experimentado un crecimiento muy elevado.

SIP permite implementar, sobre redes IP, servicios telefónicos básicos y avanzados.

Su sencillez es uno de los factores que ha contribuido en ser un protocolo sumamente aceptado en el medio y aplicado en Telefonía IP, su único defecto es que no brinda seguridad por lo que es de vital importancia analizar técnicas que proporcionen seguridad para el protocolo SIP y garanticen seguridad en su uso en redes IP.

La telefonía IP surge como una alternativa a la telefonía tradicional, brindando nuevos servicios al cliente y una serie de beneficios económicos y tecnológicos.

Para cumplir con el propósito de analizar técnicas que garanticen la seguridad en telefonía IP es necesario implementar un escenario de prueba en la Academia Local de Redes Cisco ESPOCH.

La tesis se halla dividida en capítulos cada uno hace relación a una parte importante que permitirá llegar a garantizar la confidencialidad e integridad de la voz en la comunicaciones en telefonía IP.

El capítulo uno describe la problematización, los objetivos, las técnicas que permite la seguridad en la comunicaciones usando el protocolos SIP.

El capítulo dos hace referencia a conceptos básicos que se usan en el desarrollo de la tesis.

El capítulo tres describe cada uno de los aspectos importantes del protocolo SIP, las técnicas que ayudan a la seguridad de la telefonía IP.

El capítulo cuatrohace referencia al escenario de prueba implementado en la Academia de Redes Locales Cisco-ESPOCH en el cual se implementó cada una de las técnicas estudiadas para la seguridad en telefonía IP, además se realizó un análisis de las características más relevantes de las técnicas que ayudan a la seguridad de la telefonía IP, además se evalúa el rendimiento de las tecnologías a través de las características en común para lo que se utiliza la Técnica del Benchmaking.Una vez obtenidos los resultados y seleccionada la técnica que más se adapta a las necesidades, requerimientos para garantizar le confidencialidad e integridad de la voz.

Mediante el uso del protocolo TLS se garantiza la confidencialidad e integridad de la voz de esta manera se comprueba la hipótesis planteada para el desarrollo de la Tesis.

CAPITULO I

ENFOQUE

Se realiza un enfoque general de la problematización, las vulnerabilidades que presenta el protocolos SIP empleado para la comunicación de VoIP en redes Corporativas, las técnicas que ayudan a proteger el tráfico SIP para hacer más segura la comunicación evitando que intrusos capturen la información y esta sea reproducida con fines maliciosos y afecten la integridad de la misma, provocando inseguridad para la transmisión de voz en la red, los objetivos planteados para alcanzar este propósito y la hipótesis para el desarrollo de la Tesis.

1.1 MARCO REFERENCIAL

1.1.1. Antecedentes

1.1.1.1. Problematización

La Escuela Superior Politécnica de Chimborazo ha creído conveniente hacer uso de la Telefonía IP en las comunicaciones dentro de la Institución ya que esto posibilita una rápida comunicación a través del uso del Protocolo SIP, pero este se ve afectado ya que este protocolo no posee un mecanismo de seguridad incorporado, por lo que es necesario usar técnicas que garanticen la comunicación segura.

El protocolo SIP es usado en los sistemas de telefonía IP para crear, modificar y terminar sesiones de comunicación de VoIP entre uno o más usuarios pero no es del todo seguro por lo que es necesario usar técnicas que posibiliten mantener la integridad de los datos transmitidos.

La telefonía IP reúne la transmisión de voz y datos, lo que posibilita la utilización de las redes informáticas para efectuar llamadas telefónicas siempre y cuando las terminales que se encuentra comunicándose posean características similares para establecer una comunicación adecuada y puedan entenderse.

La información trasportada es dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete. Estos paquetes pueden perderse, y además no hay una garantía sobre el tiempo que tardan en llegar de un extremo al otro de la comunicación.

Las vulnerabilidades que posee el protocolo SIP son las que a continuación se detallan:

- Denegación de servicio (DoS). . La denegación de servicio son intentos malintencionados de degradar seriamente el rendimiento de la red o un sistema
- Acceso no autorizado

a) Suplantación
b) Escucha de tráfico
c) Secuestro

- Footprinting
- Escaneado

Los ataques a los que esta propenso la comunicación en redes de telefonía IP son:

- Man-in-the-middle que consiste en envenenar el cache tanto en el cliente como del servidor SIP de manera que nos lleguen los paquetes que se envían para el registro en SIP y de reenviar dichos paquetes a sus destinatarios originales.
- Eavesdropping es la interceptación de las conversaciones VoIP por parte de individuos que no participan en la conversación.
- Hopping, consistente en la conexión del cable Ethernet que llega al terminal de voz directamente a un ordenador, pudiendo a partir de entonces realizar los ataques eavesdropping y MitM.
- Ataques a los dispositivos

a) Son muy frecuentes los ataques de fuzzing con paquetes malformados que provocan cuelgues o reboots en los dispositivos cuando procesan dicho paquete.

b) Otros ataques de denegación de servicio llamados “flooders” tienen como objetivo los servicios y puertos abiertos de los dispositivos VoIP.

- Descubrimiento de objetivos. De este modo en las primeras etapas el atacante realizará un **footprinting** u obtención de toda la información pública posible del objetivo
- Registration Hijacking. Este ataque se basa en que un atacante secuestra la información de registro de un usuario legítimo.
- Proxy Impersonation. Un atacante para situarse entre dos proxys mediante DNS Spoofing o ARP spoofing
- Message Tampering.Este tipo de ataques se produce cuando un usuario consigue acceso a cualquiera de los componentes SIP, UAs, proxy
- Session Tear Down. Consiste en el envío de mensajes BYE que provocan que se cierren las conexiones

Las conversaciones que se dan en redes de telefonía IP pueden ser captados a través de un sniffer como Wireshark, que permitirán que la información pueda ser reproducida con fines maliciosos que afecten la integridad de la misma, provocando inseguridad para la transmisión de voz en la red.

1.1.1.2. Formulación

¿Existen Técnicas que aseguran el transporte del tráfico SIP en Telefonía IP en redes Corporativas?

1.1.1.3. Sistematización

¿Cuáles son las características que presente el protocolo SIP?
¿Cuáles son las vulnerabilidades del protocolo SIP?
¿A qué ataques es propenso el protocolo SIP?
¿El protocolo SIP presenta fallos de seguridad?
¿Qué técnicas existen para implementar seguridad del tráfico SIP de Telefonía IP en redes Corporativas?
¿Qué técnica es la más adecuada para la seguridad del tráfico SIP en Telefonía IP en redes Corporativas?

1.1.2. Justificación

1.1.2.1. Justificación Teórica

Debido a que la seguridad de la comunicación es uno de los factores primordiales en la actualidad ya que puede sufrir ataques que comprometan la integridad de la misma es necesario que se realice un análisis exhaustivo de las técnicas que permitan que el protocolo SIP sea seguro en la transmisión de la información dentro de la Institución.

Ya que SIP fue diseñado de modo que sea un protocolo extensible y sus funciones pudiesen ser ampliadas mediante nuevos mensajes, esto permitirá solucionar algunas características propias de los nuevos servicios de movilidad, presencia, control de llamadas e interoperabilidad con los sistemas telefónicos actuales.

Para garantizar que la información trasmitida en la telefonía IP sea segura, SIP deberá hacer uso de técnicas que conserve la integridad de la información para ello puede usar:

- Autenticación criptográfica.
- Encriptación
- Protocolos seguros de la capa de transporte

- Mecanismos de seguridad de HTTP.

1.1.2.2. Justificación Metodológica

Mediante el análisis de las técnicas existentes que permitan implementar seguridad de tráfico SIP en Telefonía IP en redes Corporativas se pretende definir una propuesta metodológica de seguridad del protocolo SIP en la red de Telefonía de la ESPOCH.

1.1.2.3. Justificación Práctica

En la actualidad la ESPOCH cuenta con redes de Telefonía IP pero no se ha realizado un análisis de las técnicas que proporcionen seguridad en la comunicación.

Por tal motivo se analizarán las técnicas existentes para implementar seguridad y se establecerá la técnica adecuada para garantizar la integridad de los datos transmitidos en Telefonía IP en redes Corporativas, se harán las pruebas necesarias en un escenario de prueba implementado en el Laboratorio de la Academia Local de Redes Cisco-ESPOCH.

1.1.3. Objetivos

1.1.3.1. Objetivo General

Proteger el tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en redes Corporativas.

1.1.3.2. Objetivos Específicos

- Estudiar las características del Protocolo SIP.
- Identificar los fallos de seguridad inherentes en el protocolo SIP.
- Analizar y comparar las técnicas de seguridad SIP. Autenticación criptográfica, encriptación, protocolos de la capa de transporte y establecer la más adecuada para mantener la seguridad de la información transmitida en Telefonía IP en redes Corporativas.
- Implementar el escenario de pruebas y evaluar sus resultados.

- Definir una propuesta metodológica de solución de seguridad del tráfico SIP, en la Academia Local de Redes Cisco de la ESPOCH.

1.1.4. Hipótesis

La protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas conseguirá confidencialidad e integridad en la comunicación de voz.

CAPITULO II

CONCEPTOS BÁSICOS

Hoy en día la conversación se puede mantener entre dos puntos cualesquiera, ocupando una conexión de área local por lo cual es necesario conocer conceptos que sonimportantes dentro del desarrollo de la Tesis, los protocolos que ayudan a que se establezca la comunicación, la central elastix, los códec que son utilizados en la comunicación de la voz, todos ellos constituyen un pieza fundamental para la comprensión adecuada de la misma.

2.1 Telefonía Tradicional

Los sistemas de telefonía tradicional están guiados por un sistema muy simple pero ineficiente denominado conmutación de circuitos. En este sistema cuando una llamada es realizada la conexión es mantenida durante todo el tiempo que dure la comunicación.

2.1.1 Funcionamiento de la Red Tradicional

- Se levanta el teléfono y se escucha el tono de marcado. Esto deja saber que existe una conexión con el operador local de telefonía.
- Se disca el número de teléfono al que se desea llamar.
- La llamada es transmitida a trabes del conmutador (switch) de su operador apuntando hacia el teléfono marcado.
- Una conexión es creada entre tu teléfono y la persona que se está llamando, entremedio de este proceso el operador de telefonía utiliza varios conmutadores para lograr la comunicación entre las 2 líneas.
- El teléfono suena a la persona que estamos llamando y alguien contesta la llamada.
- La conexión abre el circuito.
- Uno habla por un tiempo determinado y luego cuelga el teléfono.
- Cuando se cuelga el teléfono el circuito automáticamente es cerrado, de esta manera liberando la línea y todas las líneas que intervinieron en la comunicación.

2.2 VoIP

VoIP es un método por el cual tomando señales de audio analógicas se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección IP determinada.

2.2.1 Funcionamiento de VoIP

La Voz sobre IP es una tecnología de telefonía que puede ser habilitada a través de una red de datos de conmutación de paquetes, vía el protocolo IP (Protocolo de

Internet). La ventaja real de esta tecnología es la transmisión de voz de forma gratuita, ya que viaja como datos.

2.3 Telefonía IP

La telefonía IP surge como una alternativa a la telefonía tradicional, permite integrar en una misma red comunicaciones de voz y datos que se basan en el protocolo IP, esto ha posibilitando hacer uso de redes informáticas para efectuar llamadas telefónicas.

Figura II. 1. Telefonía IP

Según Quarea (1) Telefonía IP es una tecnología que permite integrar en una misma red, basada en protocolo IP las comunicaciones de voz y datos.

Según la Universidad de Chile (2) Telefonía IP reúne la transmisión de voz y de datos, lo que posibilita la utilización de las redes informáticas para efectuar llamadas telefónicas.

Según la Universidad Sergio Arboleda (3) Telefonía IP convierte el computador en un teléfono. Es un servicio que permite realizar llamadas desde redes que utilizan el protocolo de comunicación IP (Internet Protocol), es decir, el sistema que permite comunicar computadores de todo el mundo a través de las líneas telefónicas. Esta tecnología digitaliza la voz y la comprime en paquetes de datos que se reconvierten de nuevo en voz en el punto de destino.

Ref [1]:http://www.quarea.com/tutorial/que_es_telefonia_IP

Ref [2]:http://www.telefoniaip.uchile.cl/capacitacion_telefonia.htm

Ref [3]:http://www.usergioarboleda.edu.co/grupointernet/telefonia.htm

Similitudes

- Permite integrar en una red datos y voz.
- Utilizan redes informáticas.

Diferencias

- Convierte un computador en teléfono.

2.3.1 Ventajas de la Telefonía IP

Las ventajas de la telefonía IP son:

Reducción de costos

- **Simplificación de la infraestructura**: Una única plataforma técnica para voz y datos: Menor inversión, mantenimiento y formación.
- **Simplificación cableado** de red: unificación del cableado voz y datos en Ethernet y posibilidad de compartir un único punto de red entre PC y Teléfono.
- **Menores costos** de gestión: Las extensiones se pueden reubicar simplemente cambiando los teléfonos IP de sitio y punto de red. Los cambios de configuración se pueden hacer en remoto.
- **Llamadas internas gratis** entre sedes de una empresa.
- Fácil acceso a proveedores **VoIP**, con llamadas muy económicas y otros servicios avanzados de gran valor pero muy asequibles a cualquier empresa.

Ventajas competitivas

- Las aplicaciones y servicios IP mejoran la productividad y la atención al cliente.
- Un menor tiempo para añadir nuevos usuarios a la red.
- Rápida instalación de nuevos servicios.

Mejoras funcionales

- **Unificación** del sistema de Telefonía entre sedes

- Plan de numeración integrado
- Llamada directa extensión a extensión sin costo.
- Centralización/Diversificación del puesto de operadora: Las llamadas entrantes pueden dirigirse a cualquier operadora independientemente de su ubicación, siguiendo criterios de disponibilidad o carga de trabajo.
- Gestión centralizada del sistema de telefonía.

- **Mejora en laAtención a Clientes**

  - Música en espera basada en archivos tipo MP3.
  - Operadora Automática (IVR)
  - CTI: Integración con sistemas de gestión (CRM), para llamadas automáticas o identificación datos del cliente por su CLID.
  - ACD: Distribución de llamadas entrantes entre agentes comerciales.
  - IPCC: Aplicaciones especificas para centros de llamadas (Call Centers) o departamentos comerciales.

- **Incremento de productividad del empleado**

  - Sistema de correo vocal (Voice Mail) integrado con correo electrónico y directorio.
  - Movilidad: posibilidad de acceder a su extensión telefónica (IP) en cualquier punto:
  - Reubicación en la red corporativa, en cualquier delegación
  - Acceso para Teletrabajo

- **Terminales Duales** SIP-GSM: Teléfonos móviles que disponen de interfaz WIFI con protocolo SIP, pudiendo logarse a centralita SIP.

2.3.2 Formas de Acceder

- Comunicación entre usuarios de PC conectados a Internet. Mediante el uso de computadoras multimediales y un programa adecuado se puede entablar una conversación en tiempo real con otra computadora similar ubicada en cualquier parte del planeta.

- La segunda modalidad es la que posibilita la comunicación entre dos usuarios, aunque uno de ellos no esté conectado a Internet. Una persona conectada a través de su PC con Internet puede llamar a un teléfono fijo.
- La tercera modalidad, y la más reciente, permitió ampliar las comunicaciones. Dos teléfonos fijos pueden comunicarse entre sí por medio del protocolo IP; uno de ellos llama a una central conectada a Internet y ésta lo comunica con el otro teléfono fijo de manera similar a la descrita anteriormente.

2.3.3 Funcionamiento de la Telefonía IP

La telefonía IP convierte el computador en un teléfono, es un servicio que permite realizar llamadas desde redes que utilizan el protocolo IP, permite comunicar computadores de todo el mundo a través de las líneas telefónicas.

Los pasos que tiene lugar en una llamada a través de internet son conversión de la señal de la voz analógica a formato digital y comprensión de la señal a protocolo de internet para su transmisión.

En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

Cuando hacemos una llamada telefónica por IP, nuestra voz se digitaliza, se comprime y se envían en paquetes de datos IP, estos paquetes se envían a través de internet a la persona con la que estamos hablando. Cuando alcanza su destino, son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original.

2.3.4 Arquitectura

Uno de los beneficios que aporta VoIP es la arquitectura desde el punto de vista de su distribución, puede ser centralizada o distribuida.

Se define tres elementos fundamentales en su estructura:

- Terminales: son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

- Gatekeepers: son el centro de toda la organización VoIP, y serían el sustituto para las actuales centrales. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.
- Gateways: se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

Protocolos de VoIP: son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

2.4 Códec

Un Códec, viene de abreviar codificación-decodificación, convierte una señal de audio analógico en un formato de audio digital para transmitirlo y luego convertirlo nuevamente a un formato descomprimido de señal de audio para poder reproducirlo. Esta es la esencia del VoIP, la conversión de señales entre analógico-digital.

Los códec de audio de la Telefonía IP son:

G722. Es un códec wideband, consume de 32 a 64 kbit/s de ancho de banda y muestrea la señal a 16khz (el doble de lo normal) con lo que consigue más claridad y calidad. Se utiliza en conexiones de alta calidad.

G711u. Proporciona una gran calidad de audio y es el que menos CPU consume, aunque es el que más ancho de banda necesita (aprox 64 kbps). Es el más recomendable para conexiones a Internet rápidas, pero hay que tener en cuenta que es el más susceptible a variaciones en el ancho de banda debido a su consumo.

G711a. El códec g711 tiene dos versiones conocidas como alaw (usado en Europa) y ulaw (usado en USA y Japón). Es preferible usar el G711u ya que es más compatible.

G729.G.729 se usa mayoritariamente en aplicaciones de Voz sobre IP por sus bajos requerimientos en ancho de banda (8Kbps) y su buena calidad, aunque tiene un elevado consumo de CPU para comprimir el audio.

GSM. Es el utilizado por la mayoría de los teléfonos móviles, su calidad es buena y tiene un consumo de ancho de banda reducido (3Kb/s).

iLBC. Buena calidad de sonido y bajo consumo de ancho de banda. Ideal para conexiones a internet lentas, compartidas o si queremos consumir poco ancho de banda, alrededor de 3kb/s.

SPX. La calidad de sonido es aceptable y es el códec con menor consumo de ancho de banda, (aproximadamente 8 Kbps). Es posible mantener conversaciones de audio incluso con módems de 56Kbps.

G726. G.726 es un códec ITU-T de voz que opera a velocidades de 16-40 kbit/s. El modo más utilizado frecuentemente es 32 kbit/s, ya que es la mitad de la velocidad del G.711, aumentando la capacidad de utilización de la red en un 100%. G.726 se basa en tecnología ADPCM. ITU estandarizó G.726 por primera vez en 1984. Luego se hicieron algunas adiciones al mismo estándar, que incluyen modos adicionales (originalmente G.726 era el único con 32 kbit/s) y la eliminación de todos los códigos cero. Es el códec estándar de los teléfonos DECT.

2.5 Centralitas PBX

Una centralita PBX es un dispositivo de telefonía que actúa como conmutador de llamadas en una red telefónica. Es utilizada en la mayoría de las medianas y grandes empresas ya que permite a los usuarios compartir un determinado número de líneas externas para hacer llamadas telefónicas entrantes o salientes, así mismo establecer comunicaciones internas entre los dispositivos que dependen de la PBX, una ventaja que ofrece una PBX es que es una solución menos cara ya que proporciona a cada usuario una línea telefónica interna, además proporciona versatilidad en los dispositivos que se pueden conectar.

2.6 Modelo OSI

El modelo se denomina Modelo de Referencia OSI (Open Systems Interconnect), esta constituido por 7 capas que definen las funciones de los protocolos de

comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia.

Figura II. 2. Modelo OSI

Características

Las características del modelo OSI son:

- La división en niveles especifica funciones y servicios diferentes en la transferencia de datos desde un equipo hacia otro a través del cableado de red.
- El modelo OSI define cómo se comunica y trabaja cada nivel con los niveles inmediatamente superior e inferior.
- Antes de pasar los datos de un nivel a otro, se dividen en paquetes, o unidades de información, que se transmiten como un todo desde un dispositivo a otro sobre una red.
- Evita los problemas de incompatibilidad
- Los cambios de una capa no afectan las demás capas y éstas pueden evolucionar más rápido
- Simplifica el aprendizaje
- Normaliza los componentes de red y permite el desarrollo por parte de diferentes fabricantes

2.7 TCP/IP

TCP/IP (Transfer Control Protocol/Internet Protocol) se agrupa un paquete de protocolos de comunicación de datos. El paquete toma este nombre por dos de los protocolos que lo integran, el TCP, o Protocolo de Control de Transferencia, y el IP, o Protocolo de Internet, esta formado por 4 capas:

Figura II.3. TCP/IP

2.7.1 Características

Los protocolos TCP/IP presentan las siguientes características:

- Son estándares de protocolos abiertos y gratuitos. Su desarrollo y modificaciones se realizan por consenso, no a voluntad de un determinado fabricante. Cualquiera puede desarrollar productos que cumplan sus especificaciones.
- Independencia a nivel software y hardware Su amplio uso los hace especialmente idóneos para interconectar equipos de diferentes fabricantes, no solo a Internet sino también formando redes locales. La independencia del hardware nos permite integrar en una sola varios tipos de redes
- Proporcionan un esquema común de direccionamiento que permite a un dispositivo con TCP/IP localizar a cualquier otro en cualquier punto de la red.
- Son protocolos estandarizados de alto nivel que soportan servicios al usuario y son ampliamente disponibles y consistentes.

2.8 Protocolos

Internet Protocol (IP)

El protocolo IP trabaja a nivel de red, las comunicaciones se basan en paquetes (también llamados *datagramas*). Permite enviar paquetes especificando la forma deseada de enrutado: por la vía menoscongestionada, por la vía más corta, o por la vía más segura, sin garantizar que eso vaya acumplirse. Además permite especificar el número máximo de nodos que visita un paquete antes de eliminarlo, la longitud máxima de un paquete: 64Kb.

El protocolo IPv4 o simplemente IP (Internet Protocol) asigna a cada máquina una o varias direcciones únicas de 4 bytes, expresables en notación punto.

Clases de direcciones IP

- Clase A. 7 bits para red, 3 bytes para el nodo; 128 redes con 16 millones de nodos c.u.
- Clase B. 14 bits para la red, 2 bytes para el nodo; 16384 redes con 65536 nodos c.u.
- Clase C. 21 bits para la red, 1 byte para el nodo; 2 millones de redes con 256 nodos c.u.
- Clase D. 28 bits para multicasting. Clase E. 27 bits reservados para uso futuro.

Transfer Control Protocol(TCP)

El protocolo TCP (Transport Control Protocol) permite establecer conexiones seguras (sinpérdida ni duplicación de datos) entre nodos.Puede implantarse sobre IP o sobre otros protocolos de red.El flujo de datos a través de una conexión puede verse como un flujo ordenado de bytes,llamado circuito virtual.

El usuario emisor envía datos hacia una conexión TCP, en trozos de longitud variable. Elprotocolo los recibe y los almacena hasta alcanzar un tamaño dado (normalmente, undatagrama), y luego los envía al destino. El trozo de bytes que pueden almacenarse se llamasegmento.

Las conexiones son full-dúplex, se permiten múltiples destinos u orígenes (procesos) en una misma conexión.

En cada nodo de red se pueden definir puntos extremos de conexión a los que pueden referirselos procesos remotos para establecer conexiones. Un punto extremo consta de la dirección IP delnodo más un número de puerto.

Si el emisor no recibe la señal de reconocimiento en un tiempo máximo, reenvía elsegmento.

Los segmentos contienen un número de secuencia que permite reconstruirlos en el ordenadecuado en el nodo receptor.

Para evitar la congestión en la red, los nodos usan temporizadores para monitorizar la tasade datos presentes en ella, y ajustan sus parámetros a ésta.

User Datagram Protocol (**UDP**)

Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

UDP es generalmente el protocolo usado en la transmisión de vídeo y voz a través de una red. Esto es porque no hay tiempo para enviar de nuevo paquetes perdidos cuando se está escuchando a alguien o viendo un vídeo en tiempo real.

Protocolo de Transporte en Tiempo Real (RTP)

El protocolo RTP es el encargado de transportar tanto audio como video en tiempo real. Utiliza UDP como protocolo de transporte, para cumplir su función hace uso de un número de secuencia, marcas de tiempo, envío de paquetes sin retransmisión, identificación del origen, identificación del contenido, sincronización. Además permite identificar el tipo de información transmitida, controlar la llegada de los paquetes.

Protocolo de Control de Tiempo Real (RTCP)

RTCP es el encargado de monitorizar el flujo de los paquetes RTP. Obtiene estadísticas sobre el jitter, RTT, latencia, pérdida de paquetes. Se relaciona fundamentalmente con la calidad de servicio, su desventaja radica en que no posee un mecanismo para reservar ancho de banda o control de la congestión.

EIGRP

Los protocolos de enrutamiento son los protocolos que utilizan los routers para comunicarse entre sí a fin de intercambiar información de forma dinámica acerca de las redes que pueden alcanzar y de la conveniencia de las rutas disponibles.

EIGRP suministra una eficiencia de operación superior y combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector distancia.

Características EIGRP:

Las características del protocolo EIGRP son:

- Métrica por defecto: Ancho de banda + retardo.
- Posee una distancia administrativa de 90 interno y 170 externo.
- Soporta hasta 255 saltos (100 por defecto).
- Utilización del algoritmo DUAL para actualizaciones y rápida convergencia.
- Actualizaciones parciales desencadenadas por eventos.
- Soporta IP, IPv6, IPX y AppleTalk.
- Soporta direccionamiento sin clase, VLSM y resumen de rutas arbitrario.

Tablas EIGRP

Las tablas que maneja el protocolo EIGRP son:

- **Tabla de Vecinos:** En esta tabla EIGRP guarda las rutas hacia los routers vecinos (directamente conectados).

- **Tabla de Topología:** En esta tabla EIGRP guarda las rutas de los destinos de sus routers vecinos.
- **Tabla de Enrutamiento:** En esta tabla con la información de la “Tabla de Topología” EIGRP selecciona la mejor ruta hacia cada destino.

Funcionamiento EIGRP

Los routers adyacentes (vecinos) del mismo Sistema Autónomo intercambian sus “Tablas de Vecinos”, arman la “Tabla de Topología” y generan la “Tabla de Enrutamiento” con las mejores rutas hacia los destinos (sucesor). En caso de fallas EIGRP tiene la capacidad de utilizar rutas alternativas (sucesor factible) precalculadas hacia un destino.

VPN

Una red privada virtual o VPN es una tecnología de red que permite una extensión dela red local sobre una red pública o no controlada. Estatecnología permite mediante encapsulación y encriptación el tráfico de paquetes de la redprivada sobre la red pública, dando unas garantías de seguridad, integridad y confidencialidad.

Características

- Proporciona el medio para usar una infraestructura de red públicacomo un canal apropiado para comunicaciones privadas de datos.
- Permite a los usuarios remotos conectarse de forma transparente y segura.
- Con las tecnologías de cifrado y encapsulación adecuadas, una VPNconstituye un túnel cifrado y/o encapsulado através de Internet.
- Proporciona los servicios de las redes privadas (confianza)
- Utiliza conexiones temporales (virtuales)
- Es una combinación de hardware y/o software.
- La información que atraviesa la red se encapsula en paquetes de un protocolo de forma que el contenido resulta invisible hasta llegar a su destino, donde se desencapsula el paquete.

CAPÍTULO III

PROTOCOLO DE COMUNICACIÓN SIP

En la actualidad la necesidad de una comunicación segura en tiempo real es un factor importante por lo cual se utiliza protocolos que ayudan a que la comunicación se establezcaen tiempo real, así el protocolo SIPes uno de ellos y maneja el establecimiento, control y terminación de sesiones de comunicación de VoIP, a la vez que es fundamental que se emplee técnicas que proporcionen seguridad en la comunicación para evitar que la información sea alterada y sustraída con fines maliciosos.

Se hace una descripción detallada del protocolo SIP, cada una de las vulnerabilidades, ataques que puede sufrir el protocolo SIP en la comunicación, a la vez se describe cada una de las técnicas que permiten asegurar la integridad y confidencialidad de la información transmitida en redes de telefonía IP.

3.1 PROTOCOLO SIP

SIP es un protocolo de señalización a nivel de aplicación que maneja el establecimiento, control y terminación de las sesiones de comunicación de VoIP.

Tiene la responsabilidad de iniciar una sesión después de marcar un número, una vez se ha establecido la llamada se produce el intercambio de paquetes RTP que transportan la voz en tiempo real. Encapsula también otros protocolos como SDP utilizado para la negociación de las capacidades de los participantes, tipo de codificación, etc.

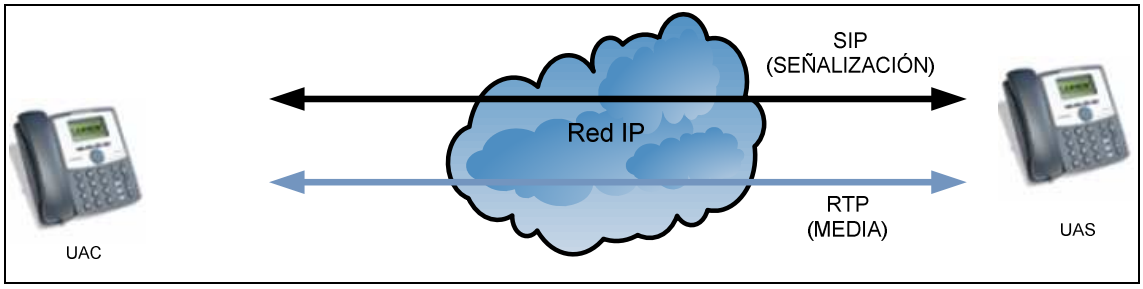


Figura. III.4. Protocolo SIP

El protocolo SIP permite llevar un control de las llamadas permitiendo la iniciación, modificación y finalización de sesiones interactivas de manera sencilla de usuarios haciendo uso de elementos multimedia como voz, imágenes, datos. Para ello SIP hace uso de los Agentes de Usuario y los Servidores cada uno de ellos con funciones propias para establecer la llamada.

Según IETF (4) SIP es un protocolo que permite crear, modificar y finalizar sesiones multimedia con uno o más participantes y sus mayores ventajas recaen en su simplicidad y consistencia.

Ref [4]:
https://www.tlm.unavarra.es/investigacion/seminarios/slides/20080516_Juanra_Apuntes_de_Seguridad_en_SIP.pdf

Según Javier Cortés Peña, Gonzalo Pérez Noguerol, Alvaro Sarmiento Losada (5) SIP es Protocolo de señalización para el establecimiento de sesiones sobre redes IP.

Según Josep Artigas, Manuel Méndez y Mohamed El Harrak (6) SIP es un protocolo de control de nivel de aplicación, creado para la señalización y el control de llamadas.

Según Software based PBX for Windows (7) SIP es un protocolo de señalización de telefonía IP utilizado para establecer, modificar y terminar llamadas VOIP

Según Wikipedia (8) SIP es un protocolo desarrollado con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

Similitudes:

- Es un protocolo de señalización.
- Crea, modifica y finaliza sesiones.
- Hace uso de elementos multimedia voz, datos.

Diferencias:

- Es un protocolo desarrollado para ser un estándar.
- Es un protocolo de nivel de aplicación.

Ref [5]:http://trajano.us.es/~fornes/RSR/2005/SIP/PresentacionSIP.ppt

Ref [6]:http://locortes.net/Vicenc/Telematica/Enginyeria%20de%20Xarxes/Protocolo%20SIP.pdf

Ref [7]:http://www.3cx.es/voip-sip/sip.php

Ref [8]:http://es.wikipedia.org/wiki/Session_Initiation_Protocol

3.1.1. Arquitectura

La arquitectura del protocolo SIP es la siguiente:

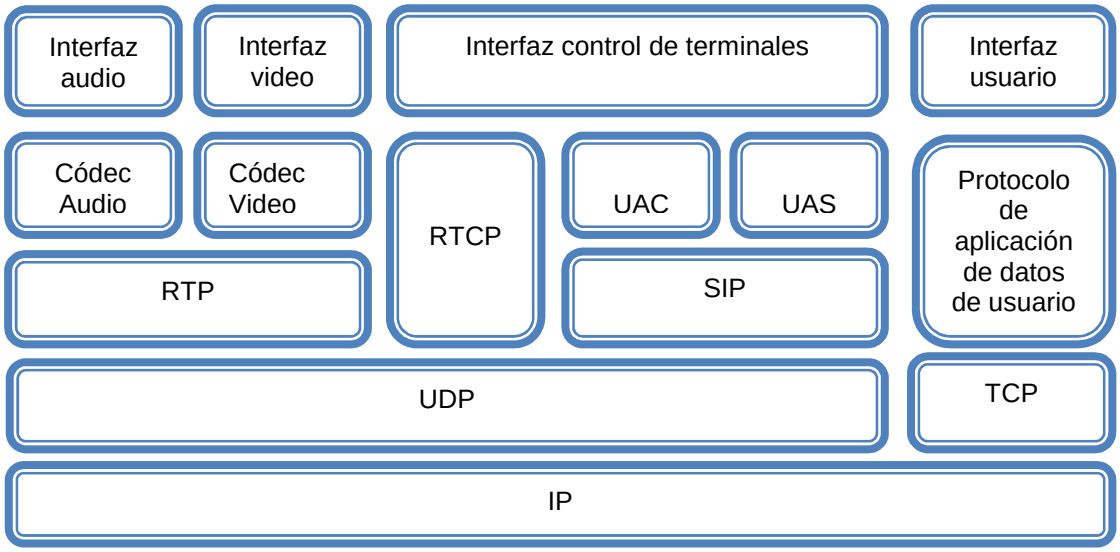


Figura III. 5. Arquitectura del protocolo SIP

3.1.2. Características

El protocolo SIP presenta algunas características que lo hacen muy recomendable para la comunicación de VoIP.

- SIP es un protocolo basado en el modelo cliente-servidor.
- SIP es un protocolo abierto y ampliamente soportado que no depende de ningún fabricante.
- Su simplicidad, escalabilidad y facilidad para integrarse con otros protocolos y aplicaciones lo han convertido en un estándar de la telefonía IP.
- SIP es un protocolo de aplicación y funcionará tanto sobre UDP como TCP.
- SIP permite implementar servicios telefónicos básicos y avanzados sobre redes IP.
- Proporciona escalabilidad entre los dispositivos telefónicos y los servidores.
- Una llamada SIP es independiente de la existencia de una conexión en la capa de transporte.
- SIP define un número reducido de tipos de mensajes denominados métodos a las solicitudes y códigos de respuestas a las respuestas.

- SIP soporta movilidad de usuarios y de terminales, sesiones con múltiples interlocutores, identificación de usuarios con URI's, cualquier sintaxis en el cuerpo de sus mensajes.
- Los terminales SIP pueden establecer llamadas de voz directamente sin la intervención de elementos intermedios.

3.1.3. Elementos Funcionales

SIP presenta cuatro elementos funcionales y son los siguientes:

- **Localización de usuarios:** SIP posee la capacidad de poder conocer en todo momento la localización de los usuarios, de esta manera no importa en que lugar se encuentre un determinado usuario. La movilidad de los usuarios no se ve limitada
- **Negociación de los parámetros:** Posibilidad de negociar los parámetros para la comunicación puertos para el tráfico SIP, así como el tráfico media, direcciones IP para el tráfico media, códec, etc.
- **Disponibilidad del usuario:** SIP permite determinar si un usuario está disponible o no para establecer la comunicación.
- **Gestión de la comunicación:** Permite la modificación, transferencia, finalización de la sesión activa. Además informa el estado de la comunicación que se encuentra en progreso

3.1.4. Componentes

Dentro de una red SIP se va a encontrar tres componentes principales los mismos que permiten que se produzca la comunicación y son los siguientes:

3.1.4.1. Agentes de Usuario (UA)

Son aplicaciones que se encuentran en terminales SIP. Estos agentes pueden por si solos, realizar una comunicación sin un servidor de por medio o utilizando un sistema de registro en algún servidor de red.

- Las direcciones SIP son identificadas mediante los denominados URI (Uniform Resource Identifiers), que sigue la estructura user@host, donde user corresponde

con un nombre, identificador o número telefónico y host es el dominio al que pertenece el usuario o dirección de red.

- Entre los User Agent podemos encontrar los **agentes de usuario clientes (UAC)** que son los que inician las peticiones de llamada y los **agentes de usuario servidor (UAS)** que reciben las peticiones del UAC.

3.1.4.2. Servidores de Red

También conocidos como NS (Network Server) son los encargados de procesar peticiones SIP provenientes de los UA y generar alguna respuesta.

Encontramos básicamente cuatro tipos de servidores:

- **Servidor Proxy SIP**: Realiza las funciones intermediador entre le UAC y el UAS. Una vez que le llega una petición de inicio de llamada de UAC decide a que servidor debería ser enviada y entonces retransmite la petición, que en algunos casos pude llegar a atravesar varios proxys SIP antes de llegar a su destino.
- **Servidor de Redirección:** Es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.
- **Servidor de Registro:** es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.
- **Servidor de Localización:** Facilita información al Proxy o al de Redirección sobre la ubicación del destinatario de una llamada.

3.1.4.3. Mensaje SIP

Son en texto plano y emplean el formato de mensaje genérico así:

- Una línea de inicio.
- Campos de cabecera (header)
- Una línea vacía (indica el final del campo de cabeceras)
- Cuerpo de mensaje (opcional)

Líneas de Inicio

Peticiones SIP: tienen una línea de solicitud (Request-Line), cuyo formato es el siguiente:

Tabla III. I. Formato de Línea de Solicitud

MÉTODO	SP	REQUEST-URI	SP	SIP VERSION	CRLF

Fuente: Tesis Doctoral de Manuel moreno Martín de la Universidad Politécnica de Madrid.

Métodos. Corresponde a la acción que desea realizar, se define 6 métodos:

Tabla III. II. Métodos

Método	Explicación
REGISTER	Petición de registro
INVITE	Permite invitar un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente.
ACK	Confirma el establecimiento de una sesión
OPTION	Solicita información sobre las capacidades de un servidor
BYE	Indica la terminación de una sesión
CANCEL	Cancela una petición pendiente de llamada.

SP es el carácter “espacio” y “CRLF” es la secuencia de “retorno del carro y una nueva línea”.

Request-URI corresponde a un SIP o SIPS URI que indica el usuario o servicio al cual va dirigida la petición.

SIP Versión: Indica la Versión del Protocolo.

Respuestas SIP: tienen una línea de estado (Status-Line), cuyo formato es el siguiente:

Tabla III. III. Formato de la Línea de Estado

SIP VERSION	SP	STATUS-CODE	SP	REASON-PHRASE	CRLF

Fuente: Tesis Doctoral de Manuel Moreno Martín de la Universidad Politécnica de Madrid.

SIP-Version: Versión del Protocolo

Status-Code es un entero de 3 dígitos que se genera como el resultado de una petición. El primer dígito define la clase de la respuesta. Se definen los siguientes:

Tabla III. IV. Resultado de las peticiones

Código	Significado
1xx	Provisional, solicitud recibida y se está procesando
2xx	Solicitud exitosa. La solicitud fue recibida de forma adecuada, comprendida y aceptada.
3xx	Solicitud fue redireccionada. Más acciones deben ser consideradas para completar la solicitud.
4xx	Error del cliente. La solicitud contiene mal la sintaxis o no puede ser resuelta en el servidor.
5xx	Error del servidor. El servidor ha errado en la resolución de una solicitud aparentemente válida.
6xx	Fallo global. La solicitud no puede ser resuelta en servidor alguno.

Fuente: Tesis Doctoral de Manuel Moreno Martín de la Universidad Politécnica de Madrid.

Reason-Phrase. Representa una descripción corta y textual del Status-Code.

Cabeceras de los mensajes SIP

- Los campos de cabecera especifican cosas como llamada, emisor de la llamada, la trayectoria del mensaje, tipo y largo del cuerpo del mensaje entre otras características.
- El número total de cabeceras definidas en el protocolo SIP son 46.
- Los distintos tipos de cabeceras SIP se pueden dividir en cuatro tipos:
  - **Cabeceras generales:**se utilizan en todos los mensajes
  - **Cabeceras de entidad:** definen información sobre el cuerpo del mensaje. Si el cuerpo no está presente, sobre los recursos identificados por la petición.
  - **Cabeceras de solicitud:** actúan como modificadores de solicitud. Permiten que el cliente pase información adicional sobre la solicitud o sobre si mismo.
  - **Cabeceras de respuesta:** permiten al servidor agregar información adicional sobre la respuesta cuando no hay lugar en la línea de inicio (Status-Line), brinda información del servidor y también respecto al recurso identificado por el campo Request-URI.

Cabeceras de los Mensajes SIP

Las seis cabeceras SIP más significativas, que no deben faltar en un mensaje de solicitud son:

- **Call-ID:** Identifica una sesión de manera unívoca
- **CSeq:** Identifica cada solicitud, se incrementa por cada nueva solicitud, excepto en los métodos ACK y CANCEL:
- **From:** Identifica el origen de la solicitud.
- **To:** Identifica el destino de la solicitud.
- **Via:** Se emplea para el encaminamiento de los mensajes SIP, y posibilitar a los servidores de res reenviar las respuestas por la misma ruta seguida por la solicitud. Esta cabecera es una de las potencialidades más importantes del protocolo.
- **Max-Forwards:** Se utiliza para indicar el número máximo de saltos que un mensaje de solicitud puede dar antes de alcanzar al UAS, su valor se decrementa en uno por cada servidor proxy que reenvía dicha solicitud.

Cuerpo del Mensaje

El cuerpo es opcional, sin embargo muchas veces es utilizado para describir las sesiones con SDP, pero puede ser cualquier otro contenido en forma clara o cifrada. Este contenido es solo de interés para UAS, no para los servidores de red.

Protocolo RTP(Real-time Transport Protocol)

Una vez establecida una llamada, la conexión es manejada por el protocolo RTP.Es un protocolo de nivel de aplicación utilizado para la transmisión de información en tiempo real, comoaudio, video, videoconferencia. Es la base en la industria VoIP y se integra con el protocolo SIP.

3.1.5. Vulnerabilidadesdel Protocolo SIP

Se debe tomar en cuenta las vulnerabilidades que afectan las comunicaciones de voz en una red IP, ya que aprovecha de las debilidades del protocolo SIP, así encontramos:

3.1.5.1. Denegación de servicio (DoS)

Afectan a la disponibilidad del servicio de VoIP. La denegación de servicio son intentos malintencionados de degradar seriamente el rendimiento de la red o un sistema, incluso llegando al punto de impedir la utilización del mismo por parte de usuarios legítimos. Se considera como el agotamiento de recursos al recibir gran cantidad de paquetes.

Otra forma de denegación de servicio es atacar al servicio DHCP que suministra la información de configuración de red a los terminales IP, agotando todas las direcciones previstas para su entrega, y dejando a los terminales sin posibilidad de operar.

Algunas técnicas se basan en el envío de paquetes especialmente construidos para explotar alguna vulnerabilidad en el software o en el hardware del sistema, saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos.
Las aplicaciones y los dispositivos de telefonía IP suelen trabajan sobre ciertos puertos específicos, bombardear dichos puertos con tráfico innecesario pero aparentemente "real" puede causar una denegación de servicio y que usuarios legítimos no puedan hacer uso del sistema.

3.1.5.2. Acceso no autorizado

Pueden terminar afectando a la confidencialidad del servicio

a) Suplantación

El robo o suplantación de identidad (del destinatario de la llamada o de algún otro dispositivo VoIP) generalmente deriva en una denegación de servicio.
En redes VoIP basadas en el protocolo SIP, es posible enviar mensajes CANCEL, GOODBYE o ICMP Port Unreacheable, con el objetivo de desconectar ciertos usuarios de sus respectivas llamadas o evitar que se produzcan, no permitiendo la correcta configuración inicial de la llamada (señalización).

La información sobre una llamada es tan valiosa como el contenido de la voz. Por ejemplo, una señal comprometida en un servidor puede ser usada para configurar y dirigir llamadas, del siguiente modo: una lista de entradas y salidas de llamadas, su duración y sus parámetros. Usando esta información, un atacante puede obtener un mapa detallado de todas las llamadas realizadas en tu red, creando grabaciones completas de conversaciones y datos de usuario.

b) Escucha de Tráfico

La conversación es en sí misma un riesgo y el objetivo más obvio de una red VoIP. Consiguiendo una entrada en una parte clave de la infraestructura, como una puerta de enlace de VoIP, un atacante puede capturar y volver a montar paquetes con el objetivo de escuchar la conversación. O incluso peor aún, grabarlo absolutamente todo, y poder retransmitir todas las conversaciones sucedidas en tu red.

c) Secuestro

Las llamadas también son vulnerables al “secuestro”, un atacante puede interceptar una conexión y modificar los parámetros de la llamada. Se trata de un ataque que puede causar bastante pavor, ya que las víctimas no notan ningún tipo de cambio. Las posibilidades incluyen la técnica de spoofing o robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo.

Los teléfonos y servidores son blancos por sí mismos. Aunque sean de menor tamaño o nos sigan pareciendo simples teléfonos, son en base, ordenadores con software. Obviamente, este software es vulnerable con los mismos tipos de agujeros de seguridad que pueden hacer que un sistema operativo pueda estar a plena disposición del intruso. El código puede ser insertado para configurar cualquier tipo de acción maliciosa.

3.1.5.3. Footprinting

Se conoce como footprinting el proceso de acumulación de información de un entorno de red especifico, es donde el atacante obtiene, reúne y organiza toda la información posible sobre su objetivo o su víctima, mientras más información obtiene con mayor

precisión puede lanzar un ataque, este procesose realiza antes de hacer un ataque a alguna empresa.

Las principales tareas del footprinting es detectar información y ubicar el rango de red.

3.1.5.4. Escaneado

La identificación: del sistema operativo de la máquina, los puertos abiertos que presenta, tipos de servicios, y huellas identificativas de la pila TCP/IP.

Una vez que se ha escaneado los puertos de la máquina y se ha obtenido información suficiente, es capaz de identificar de una forma suficientemente fiable sistema del que se trata.

A la hora de escáner la red objetivo para identificar sistemas VoIP se debería tener en cuenta que los dispositivos SIP usualmente responden a los puertos 5060-5061 tanto en UDP como en TCP.

3.1.6. Ataquesde las Comunicaciones en redes de Telefonía IP

Los ataques a los que son propensas las comunicaciones en redes de Telefonía IP son:

3.1.6.1. Man-in-the-middle (MitM)

Existe alguien en medio de la comunicación entre el origen y el destino. Una infraestructura de red insegura puede facilitar el trabajo del intruso a la hora de acceder a la red VoIP para lanzar sus ataques.

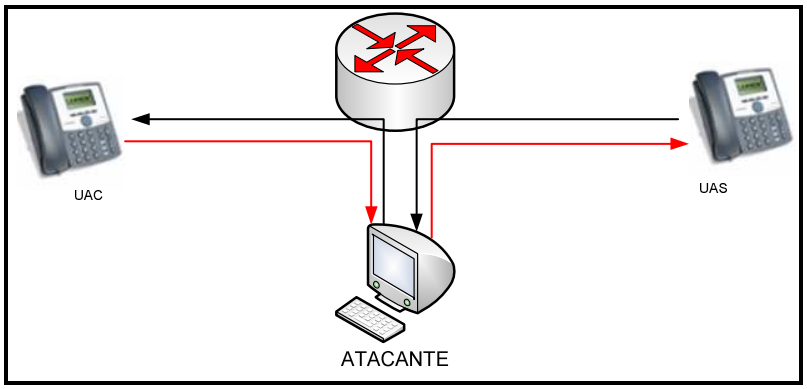


Figura III.6. Ataque MitM

El atacante puede observar, interceptar, modificar y retransmitir la información, lo que da origen a los siguientes posibles ataques posteriores:

Sniffing

- Leer credenciales enviadas. (Users, Passwords, Cookies, Ccs...)
- Leer informacion enviada. (Archivos, chat, paginas...)
- Observar el comportamiento del usuario en base al tráfico de red.

Spoofing

- El atacante puede enviar datos como si fuera el origen.
- Realizar operaciones con los datos del cliente.
- Mostrar páginas falsas.
- Enviar los datos a un destino diferente.

Negación de Servicio

- El atacante puede interrumpir la comunicación.
- Bloquear el acceso a ciertas páginas.

3.1.6.2. Eavesdropping

Eavesdropping es la interceptación de las conversaciones VoIP por parte de individuos que no participan en la conversación.

El impacto de esta técnica es más que evidente, interceptando comunicaciones es posible obtener toda clase información sensible y altamente confidencial. Y aunque en principio se trata de una técnica puramente pasiva, razón por la cual hace difícil su detección, es posible intervenir también de forma activa en la comunicación insertando nuevos datos, redireccionar o impedir que los datos lleguen a su destino.

3.1.6.3. Hopping

Hopping, consistente en la conexión del cable Ethernet que llega al terminal de voz directamente a un ordenador, pudiendo a partir de entonces realizar los ataques eavesdropping y MitM.

3.1.6.4. Ataques a los dispositivos

Hay que tener en cuenta que los dispositivos VoIP son tan vulnerables como lo es el sistema operativo o el firmware que ejecutan. Son muy frecuentes los ataques de fuzzing con paquetes malformados que provocan cuelgues o reboots en los dispositivos cuando procesan dicho paquete.

Otros ataques de denegación de servicio llamados “flooders” tienen como objetivo los servicios y puertos abiertos de los dispositivos VoIP.

Otro aspecto que hace muchas veces de los dispositivos un punto débil dentro de la red son configuraciones incorrectas. A menudo los dispositivos VoIP trabajan con sus configuraciones por defecto y presentan gran variedad de puertos abiertos. Los servicios por defecto corren en dichos puertos y pueden ser vulnerables a ataques de DoS, desbordamientos de buffer o cualquier otro ataque que pueden resultar en el compromiso del dispositivo VoIP.

El intruso a la hora de penetrar en la red tendrá en cuenta estos aspectos e intentará explotarlos. Buscará puertos por defecto y servicios innecesarios, comprobará passwords comunes o los que usa por defecto el dispositivo, etc.

No hay que olvidarse de los dispositivos VoIP que utiliza el usuario directamente, los teléfonos. A pesar de ser dispositivos más pequeños obviamente son igual de vulnerables que cualquier otro servidor de la red, y el resultado de comprometer uno de ellos puede llegar a ser igual de negativo.

3.1.6.5. Descubrimiento de objetivos

Una vez que el hacker ha seleccionado una red como su próximo objetivo, sus primeros pasos consistirán en obtener la mayor información posible de su víctima. Cuando el intruso tenga información suficiente evaluará sus siguientes pasos eligiendo el método de ataque más adecuado para alcanzar su objetivo.

Normalmente el método de obtención de información se realiza con técnicas de menos a más nivel de intrusión. De este modo en las primeras etapas el atacante realizará un **footprinting** u obtención de toda la información pública posible del objetivo. Más adelante una de las acciones más comunes consiste en obtener la mayor información posible de las máquinas y servicios conectados en la red atacada. Después de tener un listado de servicios y direcciones IP consistente, tratará de buscar agujeros de seguridad, vulnerabilidades y obtener la mayor información sensible de esos servicios (enumeración) para poder explotarlos y conseguir una vía de entrada.

3.1.6.6. Registration Hijacking

Este ataque se basa en que un atacante secuestra la información de registro de un usuario legítimo. Un atacante puede aprovecharse de que normalmente en los registros se utilizan mensajes UDP que son más fáciles de falsear que las conexiones TCP, de que a veces se utilizan autenticaciones básicas enviando los datos del usuario y la contraseña en texto plano, o de que aunque se envíe la contraseña encriptada, el atacante podría realizar un ataque por fuerza bruta basado en directorio para obtenerla, a partir de un intento de conexión escuchado, o bien conociendo el nombre de usuario y realizando intentos de conexión contra el servidor, ayudado por la inoperancia de algunos proveedores que no generan logs o si los generan no los controlan.

Como resultado el atacante podría pasar a tener el control de la conexión del usuario, impidiéndole las conexiones, cerrándoselas arbitrariamente, limitándose a escuchar en el medio.

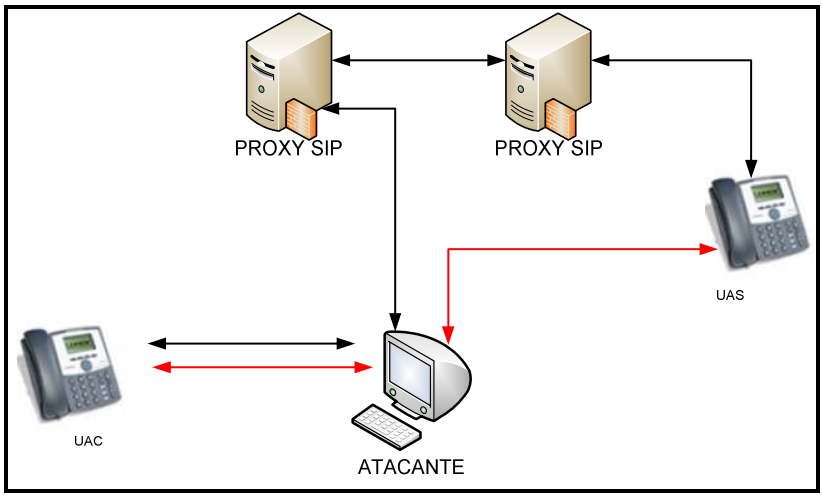


Figura III.7. Ataque Registration Hijacking

3.1.6.7. Proxy Impersonation

Los proxys se comunican entre sí mediante mensajes UDP y normalmente por canales no seguros. Esta situación la podría aprovechar un atacante para situarse entre dos proxys mediante DNS Spoofing o ARP spoofing, tomando el control de todas las comunicaciones entre ellos.

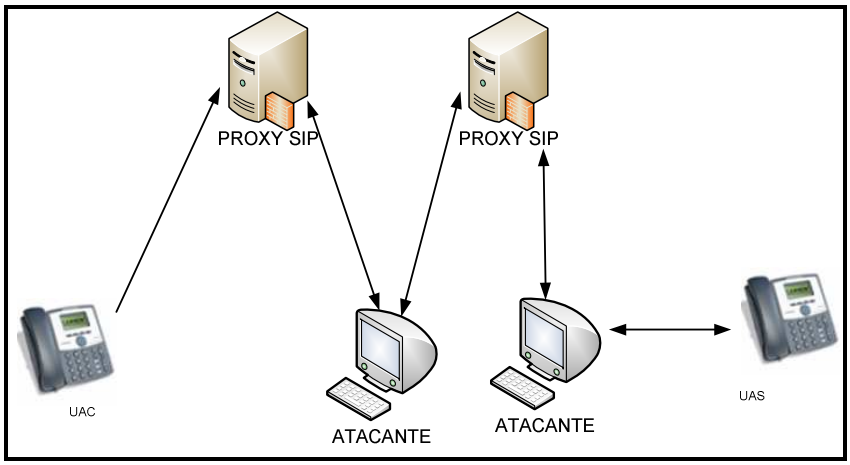


Figura III.8. Ataque Proxy Impersonation

DNS Spoofing (Suplantación de Identidad por Nombre de Dominio)

Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables. Las entradas falseadas de un servidor DNS son susceptibles de infectar (envenenar) el caché DNS de otro servidor diferente (DNS Poisoning).

ARP spoofing (Suplantación de identidad por falsificación de tablade Address Resolution Protocol)

El ataque denominado ARP Spoofing hace referencia a la construcción de tramas de solicitud y respuesta ARP modificada con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima, de forma que en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.

El protocolo Ethernet trabaja mediante direcciones MAC, no mediante direcciones IP. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda establecerse; para ello cuando un host quiere comunicarse con una IP emite una trama ARP-Request a la dirección de Broadcast pidiendo la MAC del host poseedor de la IP con la que desea comunicarse. El ordenador con la IP solicitada responde con un ARP-Reply indicando su MAC.

Los Switches y los hosts guardan una tabla local con la relación IP-MAC llamada "tabla ARP". Dicha tabla ARP puede ser falseada por un ordenador atacante que emita tramas ARP-REPLY indicando su MAC como destino válido para una IP específica.
Una manera de protegerse de esta técnica es mediante tablas ARP estática (siempre que las IPs de red sean fijas), lo cual puede ser difícil en redes grandes.

Otras formas de protegerse incluyen el usar programas de detección de cambios de las tablas ARP (como Arpwatch) y el usar la seguridad de puerto de los switches para evitar cambios en las direcciones MAC.

3.1.6.8. Message Tampering

Este tipo de ataques se produce cuando un usuario consigue acceso a cualquiera de los componentes SIP, UAs, proxy, por ejemplo mediante otro ataque tipo Registration Hijacking o Proxy Impersonation. El atacante podría interceptar estos mensajes y modificarlos, pudiendo inhabilitar las conexiones de los usuarios, cambiar las características de las conexiones, producir ataques DoS.

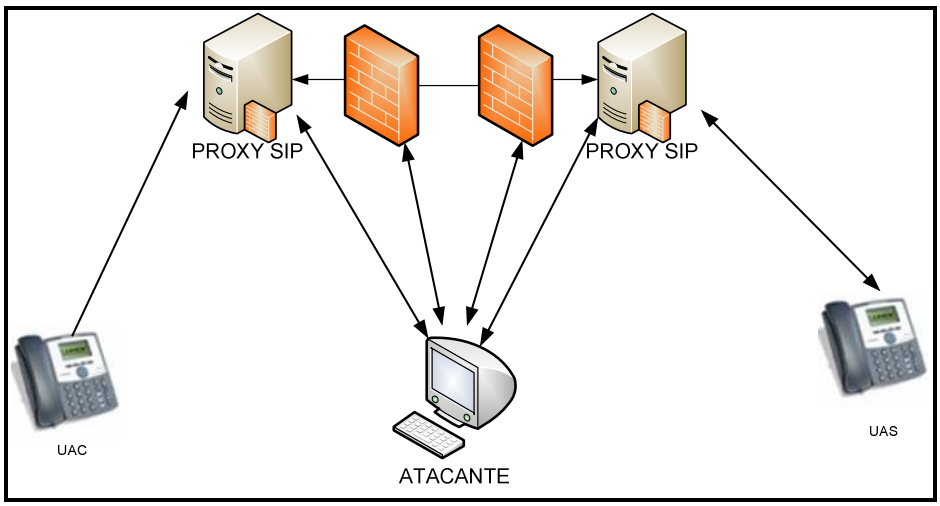


Figura III.9. Message Tampering

3.1.6.9. Session Tear Down

Consiste en el envío de mensajes BYE que provocan que se cierren las conexiones. Así por ejemplo, si un atacante conoce la existencia de un UA siempre activo, puede enviarle mensajes BYE para cerrar sus conexiones. Otra modalidad de ataque consiste en inundar los firewall o proxys con estos mensajes provocando un ataque DoS a la vez que la desconexión masiva de sesiones. Hay que tener en cuenta que la desconexión de un UA sin pasar por el proxy supone que la conexión se termine pero sin que el proxy se de cuenta, por lo que su registro de llamadas, normalmente utilizado luego para la facturación, ya no sería consistente.

Hay otra variante de este tipo de ataque consistente en enviar mensajes RE-INVITE en vez de BYE para modificar las propiedades de la conexión, por ejemplo para enviar la información multimedia a una dirección de broadcast, produciendo un ataque DoS.

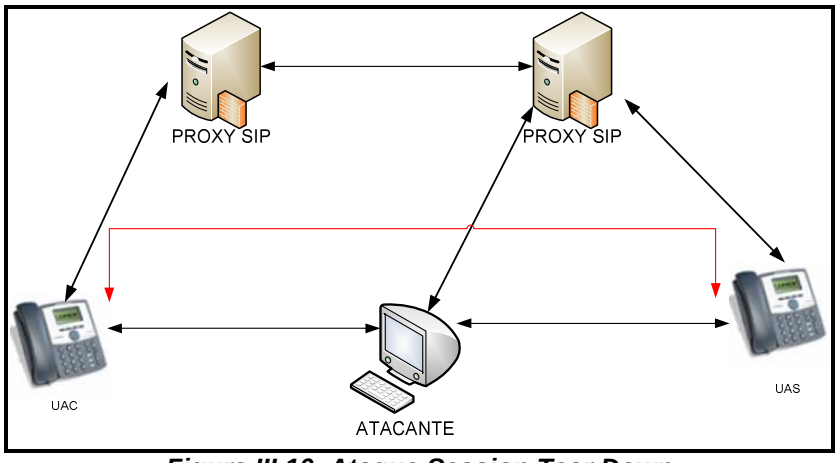


Figura III.10. Ataque Session Tear Down

3.1.4. Técnicas de Seguridad del Tráfico SIP en redes de Telefonía IP

Es evidente que la seguridad es un aspecto crítico a la hora de integrar servicios en una red IP, por ello debemos disponer de recursos y esfuerzo en garantizar, no sólo calidad de servicio, sino disponibilidad, confidencialidad e integridad de la información, para ello se emplea técnicas que colaboren con este propósito.

Las técnicas de seguridad poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

3.1.4.1. Autenticación criptográfica

La autenticación se considera uno de los tres pasos fundamentales para la seguridad de datos en las redes.

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser, para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización yauditoría oportunos.

El primer elemento necesario por tanto para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único. Los identificadores de usuarios pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como **login**.

El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no

3.1.4.2. Encriptación

Encriptar es una manera de codificar la información para protegerla frente a terceros.

3.1.4.2.1. IPsec

IPsec(Internet Protocol security) es un estándar del IETFdefinido en el RFC 4301, se encuentra constituido por un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP). Este protocolo implementa cifrado

a nivel del protocolo IP, por lo que todos los protocolos por encima de IP se pueden utilizar con IPSec de forma transparente.

IPsec está diseñado para proveer seguridad basada en criptografía, de alta calidad e interoperable para Ipv4 e Ipv6.

Servicios de Seguridad

IPsec se introdujo para proporcionar servicios de seguridad tales como:

- Confiabilidad de datos.- Los paquetes enviados son cifrados antes de ser enviados a través de la red.
- Integridad de datos.- El que recibe los paquetes puede autentificar al que envía y asegurarse que el paquete no haya sido modificado.
- Autentificación de los datos de origen.- El que recibe los datos puede autentificar el origen de los paquetes IPsec enviados.
- No repetición.- El que recibe los paquetes IPsec puede detectar y rechazar paquetes retransmitidos.

Características

Las características principales de IPsec son:

- IPsec es un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía.
- IPsec proporciona integridad como servicio añadido al cifrado de datos o como servicio independiente.
- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el costo de líneas dedicadas.
- El conjunto de protocolos de seguridad que utiliza IPsec y la forma en que son empleados estará determinado por requerimientos del sistema y de seguridad de los usuarios y aplicaciones.
- Los mecanismos utilizados por IPsec están diseñados para ser independientes de los algoritmos empleados. Esta modularidad permite la selección de diferentes conjuntos de algoritmos sin afectar las otras partes del sistema.

- Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública, algoritmos de cifrado, algoritmos de hash y certificados digitales.

Componentes de IPsec

Los componentes principales de IPsec son:

- Dos protocolos de seguridad de tráfico: IP Authentication Header **(AH)** e IP Encapsulating Security Payload **(ESP)** que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un protocolo de gestión de claves Internet Key Exchange **(IKE)** que permite a dos nodos negociarlas claves y todos los parámetros necesarios paraestablecer una conexión AH o ESP.

Protocolos de Seguridad

Existen dos protocolos de seguridad de IPsec que son AH y ESP:

El Encabezado de Autenticación- AH (Authentication Header)

Es el procedimiento dentro de IPsec que proporciona autenticación de datos, una integridad sólida y protección de repetición para los datagramas IP.
AH protege la mayor parte del datagrama IP. Se inserta entre el encabezado IP y el encabezado de transporte,que pueden ser un mensaje TCP, UDP o ICMP, oincluso un datagrama IP completo
Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables.

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete. La cabecera AH es la siguiente:

Tabla III. V: La cabecera AH

Siguiente Cabecera	Longitud del Contenido del Paquete	Reservado
Índice de Parámetro de Seguridad (SPI)		
Número de Secuencia		
Código de resumen para la autenticación de mensaje (HMAC)		

La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados. Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bit protege frente a ataques por repetición. Finalmente, los últimos 96 bit almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network address translation - Traducción de direcciones de red, también conocido como Enmascaramiento de direcciones) reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción.

ESPEncapsulating Security Payload

La carga de seguridad encapsuladora provee cifrado y protección limitada contra análisis de flujo de datos. ESP puede ser usado para proveer los mismos servicios de seguridad, y también provee un servicio de encriptación. La principal diferencia entre la seguridad provista por ESP y AH es el alcance de la protección.

Específicamente, ESP no protege ningún campo del encabezado IP (excepto en modo túnel, donde los datos encriptados por ESP corresponden a otro paquete IP).

Encapsulated Security Payload (ESP), protege los datos del paquete IP de interferencias de terceros, cifrando el contenido utilizando algoritmos de criptografía simétrica (DES).

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes como se indica en la siguiente figura:

Tabla III. VI. Cabecera de ESP

<table>
<tr><td colspan="4">Índice de Parámetros de Seguridad (SPI)</td></tr>
<tr><td colspan="4">Número de Secuencia</td></tr>
<tr><td colspan="4">Vector de Inicialización (IV)</td></tr>
<tr><td rowspan="2"></td><td colspan="3">Datos de Aplicación</td></tr>
<tr><td>Relleno (0-255 bytes)</td><td>Longitud de Relleno</td><td>Siguiente cabecera</td></tr>
<tr><td colspan="4">HMAC</td></tr>
</table>

Los primeros 32 bits de la cabecera ESP especifican el Índice de Parámetros de Seguridad (SPI). Este SPI especifica qué SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPsec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytesque especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT-Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

Protocolos de Gestión

Es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios.

Internet Security Association Key Management Protocol (ISAKMP)

Es utilizado por AH y ESP para la administración de claves. ISAKMP no define por si mismo los algoritmos de generación de claves, sino que permite el uso de distintos tipos de algoritmos, aunque el estándar pide un set mínimo en las implementaciones.

Para el intercambio de claves, se utiliza el protocolo IKE (Internet Key Exchange), esto se hace por separado para independizar el método de intercambio de claves del protocolo IPsec. La estandarización de IKE permite la interoperabilidad entre distintos sistemas.

IKE

Es un protocolo estándar de gestión de claves, el objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPsec. El protocolo de intercambio de claves de Internet (IKE) gestiona automáticamente la administración de claves. También puede administrar las claves manualmente con el comando ipseckey.

Dicha negociación se lleva a cabo en dos fases:

Fase I

La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC.

Los gateways negocian un canal bidireccional (SA) que se utilizará para crear los canales de la siguiente fase. Se presentan los algoritmos de cifrado probables, y las claves de autenticación para armar los túneles IPsec.

Fase II

Usando el canal generado en la fase uno, se establece un par de SAs (unidireccionales, uno para cada sentido) con los parámetros de refresco de claves, método de cifrado, y el protocolo a usar: AH o ESP

Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD. Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transportes estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.

El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros

de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

Filtrado de paquetes IPsec

Los protocolos AH y ESP están implementados sobre la capa IP, AH es el protocolo IP 51 y ESP es el protocolo IP 50. El protocolo ISAKMP usa el puerto UDP 500 para envío y recepción. En el caso en que se tenga un firewall delante del gateway de seguridad, habrá que tener en cuenta estos protocolos para su filtrado.

Arquitectura de Seguridad

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP.Una asociación de seguridad (SA) IPsec especifica las propiedades de seguridad que se reconocen mediante hosts comunicados. Una única SA protege los datos en una dirección.

La protección es para un solo host o para una dirección de grupo (multidifusión).Dado que la mayoría de la comunicación es de igual a igual o de cliente-servidor, debe haber dos SA para proteger el tráfico en ambas direcciones.

Los tres elementos siguientes identifican una SA IPsec de modo exclusivo:

- El protocolo de seguridad (AH o ESP)
- La dirección IP de destino
- El índice de parámetros de seguridad (SPI)

El SPI, un valor arbitrario de 32 bits, se transmite con un paquete AH o ESP.Se utiliza un valor de suma de comprobación de integridad para autenticar un paquete. Si la autenticación falla, se deja el paquete.

Las asociaciones de seguridad se almacenan en una base de datos de asociaciones de seguridad (SADB). Un motor de administración basado en sockets, la interfaz PF_KEY, permite a lasaplicaciones privilegiadas administrar la base de datos. Por la aplicación IKE usa la interfaz de socket PF_KEY.

Modos de Operación de IPsec

Los modos de operación de IPsec son:

Modo Transporte

En este modo IPsec protege el tráfico (los datos de las capas superiores que se transportan en el paquete IP), el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPsec.

El SA se hace entre dos nodos del final y define el cifrado o la autentificación para la carga útil de todos los paquetes del IP para esa conexión.

Modo Túnel

IPsec en este modo encapsula el paquete IP original con una nueva cabecera IP y opera entre hosts y routers o puertas de enlace, protege completamente la cabecera interna (cabecera del usuario) y partes de la cabecera externa. En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPsec.

El modo túnel es empleado principalmente por los gateways IPsec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPsec en un equipo. El modo túnel también es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales (RPV) a través de redes públicas, es decir,

interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en Internet.

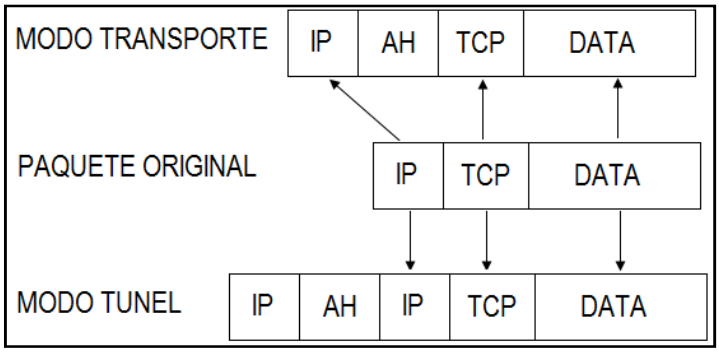


Figura III. 11. Modos de Operación de IPsec

Ventajas

- IPsec permite la confidencialidad de datos que protege a los paquetes de suplantación, la autenticación asegura que solo el emisor y el receptor tienen acceso a la información y no un tercero, y la integridad de datos que garantiza que no se han modificado los paquetes durante el trayecto.
- IPsec puede trabajar en diferentes modos según se requiera y se configure, puede proteger el paquete completo IP o solo su cabecera.
- Su diseño es flexible
- Este protocolo implementa cifrado a nivel del protocolo IP, por lo que todos los protocolos por encima de IP se pueden utilizar con IPsec de forma transparente.
- Trabaja con otros protocolos AH, ESP, IKE

3.1.4.3. Protocolos seguros de la capa de transporte

La función de los protocolos que proporcionan seguridad en la capa de transporte es garantizar una conexión segura entre dos puntos de la red cualquiera, sin preocuparse de que cualquier posible atacante pueda interceptar la comunicación o modificarla.

3.1.4.3.1. SSL

SSLSecure Sockets Layer. Protocolo de Capa de Conexión Segura. Es un protocolo desarrollado por Netscape,proporciona autentificación, integridad y privacidad de la

información entre cliente y servidor. Encripta la comunicación que viaja entre un cliente y un servidor.

Componentes

SSL está formado por dos componentes:

- SSL Record Protocol. Está ubicada sobre algún protocolo de transporte confiable como TCP y es usado para encapsular varios tipos de protocolos de mayor nivel.
- SSL Handshake Protocol. Es uno de los posibles protocolos que pueden encapsularse sobre la capa anterior y permite al cliente y al servidor autenticarse mutuamente, negociar un algoritmo de cifrado e intercambiar llaves de acceso.

Las conexiones realizadas por medio de este protocolo tienen las siguientes propiedades básicas:

- Privada. Después de un proceso inicial de "handshake" en el cual se define una clave secreta, se envía la información encriptada por medio de algún método simétrico (DES, RC4).
- Segura. La identidad de cada extremo es autenticada usando métodos de ciftrado asimétricos o de clave pública (RSA, DSS).
- Confiable. El transporte del mensaje incluye un control de la integridad del mismo usando una MAC cifrada con SHA y MD5.

Servicios

El protocolo SSL proporciona:

- Seguridad Criptográfica. Debe ser usado para establecer una conexión segura entre dos partes.
- Interoperatividad. Programadores independientes deben poder desarrollar aplicaciones que, utilizando SSL, permitan intercambiar en forma exitosa parámetros de cifrado sin tener conocimiento del código utilizado por el otro.

- Flexibilidad. Debe ser una base sobre la cual puedan incorporarse nuevos métodos de cifrado. Esto trae aparejado dos objetivos más: evitar la creación de un protocolo nuevo y la implementación de una nueva biblioteca de seguridad
- Eficiencia. Dado que las operaciones de cifrado consumen gran cantidad de recursos, en especial CPU, incorpora ciertas facilidades que permiten mejorar este aspecto, además de mejorar el uso de la red.

Características

SSL ofrece algunas características de interés:

- **Separación de responsabilidades.-** Utiliza algoritmos independientes para la encriptación, autenticación e integridad de datos, con claves diferentes (claves secretas) para cada función.
- **Eficiencia.-** Aunque la fase de saludo utiliza algoritmos de clave pública, la operativa de intercambio de datos se realiza mediante encriptación y des-encriptación de clave privada. Los algoritmos de clave privada son más rápidos. Además la fase de saludo no tiene que repetirse para cada comunicación entre un cliente y un servidor, la ''clave secreta'' negociada puede conservarse entre conexiones SSL. Esto permite que las nuevas conexiones SSL inicien la comunicación segura de inmediato, sin necesidad de realizar lentas operaciones de clave pública.
- **Autenticación con base en certificados.-** Se utilizan certificados X.509 para la autenticación. Los certificados de servidores son obligatorios, mientras que los de cliente son opcionales.
- **Independiente de protocolos.-** Aunque SSL se diseño para funcionar sobre TCP/IP, puede hacerlo sobre cualquier protocolo confiable orientado a conexiones.
- **Protección contra ataques.-** SSL protege frente a ataques de MitM. En un ataque MitM, el atacante intercepta todas las comunicaciones entre las dos partes, haciendo a cada una de ellas creer que se comunica con la otra. SSL protege contra estos ataques mediante certificados digitales que nos garantizan con quien se está hablando.
- **Soporte a algoritmos heterogéneos.-** aunque depende de las implementaciones, SSL suele dar soporte a diversos algoritmos:

  - Intercambio de claves (RSA y Diffie - Hellman).
  - Compendio (MD5, SHA-1).
  - Encriptación (RC2, RC4, DES, Triple DES, Idea, Fortezza).
- **Soporte de compresión.-** SSL permite comprimir los datos del usuario antes de ser encriptados mediante múltiples algoritmos de compresión.
- **Compatibilidad hacia atrás con SSL v2.-** Los servidores de SSL v3 pueden recibir conexiones de clientes SSL v2 y manejar el mensaje de manera automática.

SSL permite:

1. Que el cliente compruebe la identidad de la máquina servidor, si el servidor tiene habilitado SSL. Un cliente que soporte SSL puede utilizar técnicas de la criptografía de llave pública para comprobar que el certificado y la identidad de un servidor están validados por una Autoridad de Certificación (CA). El cliente confía en los certificados emitidos por unas CA concretas. Esta comprobación puede ser interesante si el cliente, por ejemplo, está enviando un número de la tarjeta de crédito y desea controlar la identidad del servidor.
2. Que el servidor compruebe la identidad del usuario cliente. Con las mismas técnicas de la autentificación del servidor, el servidor con SSL puede comprobar que el certificado y la identidad del usuario cliente están validados por una CA.
3. Permite que entre ambas máquinas se establezca una conexión cifrada o segura. Todos los datos enviados a través de una conexión cifrada SSL viajan no solamente cifrados sino protegidos con un mecanismo para detectar alteraciones, es decir, para detectar automáticamente si los datos se han modificado en tránsito.

El protocolo de transporte seguro SSL trabaja sobre el TCP/IP y da servicio a protocolos de alto nivel tales como HTTP, SMTP, IMAP.

Fases del Protocolo SSL

Las fases del protocolo SSL son:

Fase de negociación:

- El cliente envía al servidor el número de versión del SSL, ciertas propiedades del cifrado y un dato generado aleatoriamente.

- El servidor envía al cliente el número de versión del SSL, ciertas propiedades del cifrado, un dato generado aleatoriamente y su propio certificado. Si se usa autentificación del cliente, el servidor pide el certificado del cliente.

Fase de creación de llaves simétricas:

- El cliente usa la información proporcionada por el servidor para comprobar su identidad. Si no se puede comprobar la identidad del servidor el usuario es avisado del problema.
- Usando la información intercambiada el cliente crea un secreto de sesión temporal. Lo cifra con la llave pública del servidor, forma parte del certificado, y lo envía al servidor. Si se usa autentificación del cliente, el cliente también envía su certificado.
- Si todo el proceso ha sido correcto, incluida la comprobación de la identidad del cliente, el cliente y el servidor usan el secreto temporal para generar el secreto de la conexión, con el que crearán las llaves simétricas de cifrado de la sesión.

Fase de intercambio:

- Tanto el cliente como el servidor envían un primer mensaje cifrado para indicar al otro que todo el proceso se ha realizado correctamente.
- A partir de este momento todo el intercambio de datos entre el cliente y el servidor será cifrada.

Solicitud de SSL:

Típicamente este proceso ocurre en el momento que un cliente accede a un servidor seguro, identificado con "https://...". La comunicación se establecerá por un puerto distinto al utilizado por el servicio normalmente. Luego de esta petición, se procede al SSL Handshake.

SSL Handshake:

En este momento, servidor y cliente se ponen de acuerdo en varios parámetros de la comunicación. Se puede dividir el proceso en distintos pasos:

- Client Hello: El cliente se presenta. Le pide al servidor que se presente (certifique quien es)y le comunica que algoritmos de encriptación soporta y le envía un número aleatorio para el caso que el servidor no pueda certificar su validez y que aun así se pueda realizar la comunicación segura.
- Server Hello: El servidor se presenta. Le responde al cliente con su identificador digital encriptado, su llave pública, el algoritmo que se usará, y otro número aleatorio. El algoritmo usado será el más poderoso que soporte tanto el servidor como el cliente.
- Aceptación del cliente: El cliente recibe el identificador digital del servidor, lo desencripta usando la llave pública también recibida y verifica que dicha identificación proviene de una empresa certificadora segura. Luego se procede a realizar verificaciones del certificado (identificador) por medio de fechas, URL del servidor, etc. Finalmente el cliente genera una llave aleatoria usando la llave pública del servidor y el algoritmo seleccionado y se la envía al servidor.
- Verificación: Ahora tanto el cliente y el servidor conocen la llave aleatoria (El cliente la generó y el servidor la recibió y desencriptó con su llave privada). Para asegurar que nada ha cambiado, ambas partes se envían las llaves. Si coinciden, el Handshake concluye y comienza la transacción.

Intercambio de Datos:

Desde este momento los mensajes son encriptados con la llave conocida por el servidor y el cliente y luego son enviados para que en el otro extremo sean desencriptados y leídos.

Terminación de SSL

Cuando el cliente abandona el servidor, se le informa que terminara la sesión segura para luego terminar con SSL.

Ventajas

- Proporciona autentificación, integridad y privacidad de la información entre cliente y servidor.

- Utiliza algoritmos independientes para la encriptación, autenticación e integridad de datos, con claves diferentes para cada función.
- Puede trabajar con cualquier protocolo orientado a las conexiones a pesar de haber sido creado para trabajar con TCP.
- Utiliza navegadores Web estándar, no clientes específicos.
- Permite control de acceso aplicación por aplicación.
- Requiere menor esfuerzo de administración.

3.1.4.3.2. TLS (Transport Layer Security)Seguridad de la Capa de Transporte

El protocolo TLS es una evolución del protocolo SSL (Secure Sockets Layer). Se ejecuta sobre una capa de transporte definida, pero no determinada, esto indica que puede ser utilizado para cualquier tipo de comunicaciones.

Sirve para proporcionar comunicaciones seguras usando un modelo de autenticación y privacidad de la información entre extremos mediante criptografía.

Normalmente el servidor es el único que es autenticado, garantizando así su identidad, pero el cliente se mantiene sin autenticar, ya que para la autenticación mutua se necesita una infraestructura de claves públicas (o PKI) para los clientes.

Estos protocolos permiten prevenir escuchas (eavesdropping), evitar la falsificación de la identidad del remitente y mantener la integridad del mensaje en una aplicación cliente-servidor.

Servicios

Los servicios que brinda TLS son:

- **Seguridad criptográfica**. El protocolo se debe emplear para establecer una conexión segura entre dos partes.
- **Interoperabilidad**. Aplicaciones distintas deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca el código de la otra.

- **Extensibilidad**. El protocolo permite la incorporación de nuevos algoritmos criptográficos.
- **Eficiencia**. Incluye un esquema de cache de sesiones para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).

Conceptos

El protocolo TLS se fundamenta en dos conceptos:

- **Conexión:** son relaciones par a par o peer-to-peer, las cuales son temporales y están asociadasa una sesión.
- **Sesión:** una sesión TLS es una asociación entre un cliente y un servidor. Estassesiones son creadas por el protocolo Handshake. Una sesión define un conjunto de parámetros criptográficos que pueden ser compartidas entre conexiones.

Fases

El protocolo TLS se basa en tres fases básicas:

- **Negociación**: los dos extremos de la comunicación (cliente y servidor) negocian que algoritmos criptográficos utilizarán para autenticarse y cifrar la información. Actualmente existen diferentes opciones:
  - Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.
  - Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
  - Con funciones hash: MD5 o de la familia SHA.
- **Autenticación y Claves**: los extremos se autentican mediante certificados digitales e intercambian las claves para el cifrado, según la negociación anterior.
- **Transmisión Segura**: los extremos pueden iniciar el tráfico de información cifrada y autentica.

Componentes

El protocolo está compuesto por dos capas: Protocolo de registro TLS y Protocolo de mutuo acuerdo TLS

Protocolo de registro TLS (TLS Record Protocol)

El de más bajo nivel es el Protocolo de Registro, que se implementa sobre un protocolo de transporte fiable como el TCP.

Elprotocolo de registro se emplea para encapsular varios protocolos de más alto nivel, uno de ellos, el protocolo de mutuo acuerdo, permite al servidor y al cliente autentificarse mutuamente y negociar un algoritmo de encriptación y sus claves antes de que el protocolo de aplicación transmita o reciba datos.

El protocolo proporciona seguridad en la conexión con dos propiedades fundamentales:

- **La conexión es privada**. Para encriptar los datos se usan algoritmos de cifrado simétrico. Las claves se generan para cada conexión y se basan en un secreto negociado por otro protocolo (como el de mutuo acuerdo). El protocolo también se puede usar sin encriptación.
- **La conexión es fiable**. El transporte de mensajes incluye una verificación de integridad para lo cual define una clave utilizada para generar un código de autenticación de mensajes (MAC), usando funciones como SHA.

El protocolo toma los mensajes a ser enviados, divide el contenido en bloques de datos, comprimelos datos opcionalmente, genera un MAC, cifra y transmite el resultado. Los datos recibidos son descifrados, verificados, descomprimidos y rearmados,para ser entregados a la capa superior.

Protocolo de mutuo acuerdo TLS (TLS Handshake Protocol)

El protocolo de mutuo acuerdo proporciona seguridad en la conexión con tres propiedades básicas:

- La identidad del interlocutor puede ser autentificada usando criptografía de clave pública. Esta autentificación puede ser opcional, pero generalmente es necesaria al menos para uno de los interlocutores.
- La negociación de un secreto compartido es segura.
- La negociación es fiable, nadie puede modificar la negociación sin ser detectado por los interlocutores.

Esta capa del protocolo TLS está compuesta por tres sub-protocolos, los cuales son utilizadospara alcanzar acuerdos de parámetros de seguridad entre interlocutores, autenticación, iniciar la negociación de parámetros de seguridad, y reportar errores ocurridos. Estos tres sub-protocolosson: Change cipher spec , Alert y Handshake.

El Protocolo Handshake está encargado de establecer una sesión, lo que incluye:

- Identificar cada sesión por medio de una secuencia de bytes escogida.
- Autenticación por medio de certificados digitales.
- Establecer el algoritmo de compresión a utilizar, y el simétrico para el cifrado de datos.

La clave utilizada es definida por el Protocolo Handshake. Este protocolo también puedeutilizarse sin esta propiedad

- Elegir los algoritmos criptográficos.
- Compartir el secreto maestro (master secret) de 48 bits entre el cliente y servidor.
- Indicar por medio de una bandera (flag) si la conexión es reiniciable o no.

Características

Las características del protocolo TLS son:

- TLS está basado en SSL y son muy similares en su forma de operar, encriptando la comunicación entre el servidor y cliente mediante el uso de algoritmos
- Estandarizado por IETF mediante el RFC-4279.

- Comunicación segura entre cliente y servidor.
- Autenticación del servidor
- Corre debajo de los protocolos usuales HTTP, FTP, POP
- Numera todos los registros y usa el número de secuencia en MAC.
- Algoritmos negociados

Ventajas

- Es transparente a protocolos de más alto nivel
- Popular en la Web
- Utiliza navegadores estándar
- Estos protocolos permiten prevenir escuchas (eavesdropping), evitar la falsificación de la identidad del remitente y mantener la integridad del mensaje en una aplicación cliente-servidor.
- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.

CAPITULO IV

ANÁLISIS COMPARATIVO

Se realiza el análisis y comparación de las Técnicas disponibles en el medio que proporcionen seguridad en la comunicación en el tráfico de SIP en Telefonía IP en redes Corporativas, para lo cual se implementó un escenario de prueba en los Laboratorios de la Academia de Redes Locales Cisco de la Escuela Superior Politécnica de Chimborazo, éste análisis se lo realiza mediante la metodología benchmarking con la cual se escoge la técnica más adecuada que cumpla con éste propósito en base a los resultados obtenidos mediante determinados factores de comparación.

4.1. Implementación del Escenario de Prueba

Para la implementación del escenario de prueba se utilizó tanto software como hardware, este escenario permitirá implementar cada una de las técnicas que proporcionen seguridad en la comunicación de voz en redes de telefonía IP.

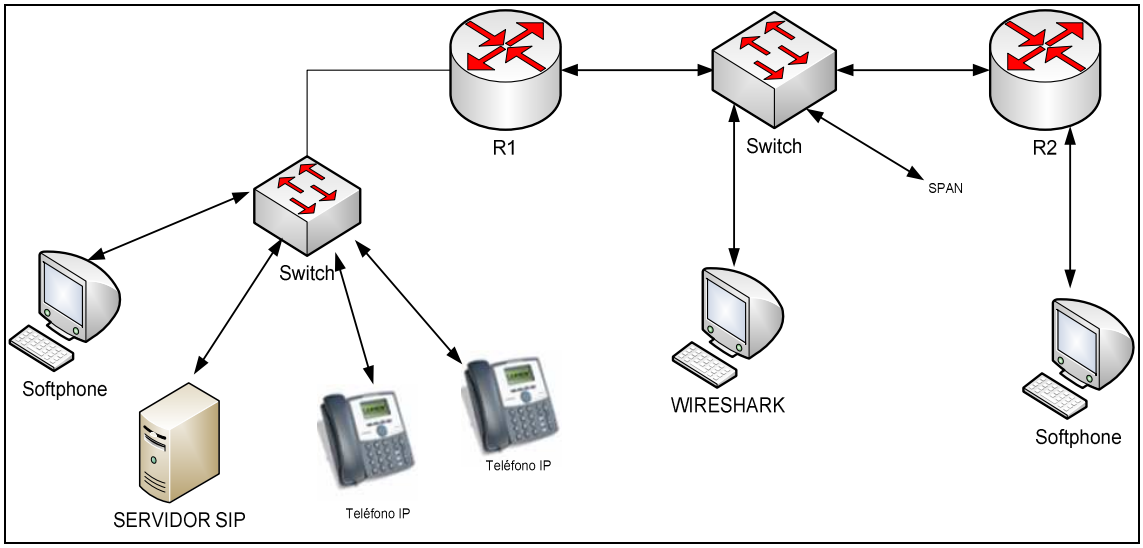


Figura IV.12. Escenario de Prueba

4.1.1. Requerimientos Hardware

- 2 Router Cisco 2800 Series
- 2 switch Cisco Catalyst 2560
- Dos teléfonos IP Grandstream Budgetone-201
- Cinco Computadoras:

  1 equipo. Instalar elastix

  2 equipo. Instalar el sniffer

  3 equipo. Ayudará en la configuración de elastix en forma gráfica al acceder a través de un navegador web a la dirección del servidor elastix

  4 y 5 equipo. Instalar los softphone PhonerLite 1.86, los clientes vpn, y configurar los routers

4.1.2. Requerimientos Software

- Sofware Elastix 2.0.3

- Sniffer Wireshark
- Softphone PhonerLite 1.86
- Cliente VPN-GUI
- IOS Seguridad Cisco
- Openssl
- Openvpn

Se utilizó una máquina para el software Elastix el cual es el servidor sip, en éste se registran los usuarios de la central PBX.

4.2. Análisisde diferentes técnicas de seguridad para el protocolo SIP

La determinación de la técnica más adecuada para garantizar la integridad y confidencialidad en los datos transmitidos en telefonía IP mediante el protocolo SIP, se basa en un minucioso análisis de acuerdo a parámetros de comparación y a los resultados obtenidos en la implementación de cada una de las técnicas implementadas en el escenario de prueba.

El análisis se enfoca en las características principales de cada una de las técnicas tomando en cuenta los aspectos más relevantes de cada una de ellas para escoger la técnica que mejor cumpla con el propósito, para ello se seguirá la metodología benchmarking tipo competitivo para realizar el análisis, la misma que consta de seis fases.

4.2.1. Fases

Las fases que corresponden a la metodología Bencmarking son:

a) Fase I: Técnicas a Evaluar

Las técnicas a evaluar son las siguientes:

- IPsec
- SSL
- TLS

La implementación de cada una de las técnicas se lo realizó de la siguiente manera:

IPsec

La implementación de IPsec se realizó en los router cisco 2800 series, la implementación de esta técnica permitirá garantizar la confidencialidad e integridad de los datos transmitidos.

Los router deben poseer el IOS de seguridad de Cisco

Pasos para configurar IPsec

1. Verificar que los router contengan el IOS de seguridad mediante el comando show versión

2. Ingresar al modo de configuración con el comando **config**

3. Configurar las interfaces que permitirán conectar la red y guardar los cambios con el comando **no shutdown**

```
R1(config)# interface f0/0
R1(config-if)# ip address 192.168.37.1 255.255.255.0
R1(config-if)# no shutdown
R1(config)# interface f0/1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown

R2(config)# interface f0/0
R2(config-if)# ip address 192.168.37.2 255.255.255.0
R2(config-if)# no shutdown
R2(config)# interface f0/1
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)# no shutdown
```

4. Para mantener la conectividad de la red configurar EIGRP

```
R1(config)# router eigrp 1
R1(config-router)# no auto-summary
R1(config-router)# network 192.168.10.0
R1(config-router)# network 192.168.37.0

R2(config)# router eigrp 1
R2(config-router)# no auto-summary
R2(config-router)# network 192.168.20.0
R2(config-router)# network 192.168.37.0
```

5. Habilitar IKE con el comando **crypto isakmp enable**

```
R1(config)# crypto isakmp enable
R2(config)# crypto isakmp enable
```

6. Crear políticas IKE

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 5
R1(config-isakmp)# lifetime 3600

R2(config)# crypto isakmp policy 10
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption aes 256
R2(config-isakmp)# hash sha
R2(config-isakmp)# group 5
R2(config-isakmp)# lifetime 3600
```

7. Configurar las claves pre-compartidas

```
R1(config)# crypto isakmp key cisco address 192.168.37.2
```

R2(config)# crypto isakmp key cisco address 192.168.37.1

8. Configure ipsec

R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac ah-sha-hmac
R1(cfg-crypto-trans)# exit
R1(config)#

R2(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac ah-sha-hmac
R2(cfg-crypto-trans)# exit
R2(config)#

9. Configure el tiempo de vida de IPsec

R1(config)# crypto ipsec security-association lifetime seconds 1800

R2(config)# crypto ipsec security-association lifetime seconds 1800

10. Definir el tráfico creando listas de acceso

R1(config)# access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.00.0.0.255

R2(config)# access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.00.0.0.255

11. Crear y aplicar mapas Crypto

R1(config)# crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peerand a valid access list have been configured.
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set peer 192.168.37.2
R1(config-crypto-map)# set pfs group5
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900

R2(config)# crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peerand a valid access list have been configured.
R2(config-crypto-map)# match address 101
R2(config-crypto-map)# set peer 192.168.37.1
R2(config-crypto-map)# set pfs group5
R2(config-crypto-map)# set transform-set 50
R2(config-crypto-map)# set security-association lifetime seconds 900

12. Crear el sitio VPN para ello aplicar los mapas a las interfaces

R1(config)# interface fastethernet0/0
R1(config-if)# crypto map MYMAP

R2(config)# interface fastethernet0/0
R2(config-if)# crypto map MYMAP

13. Comprobar la configuración de IPsec

R1# show crypto ipsec transform-set
Transform set 50: { ah-sha-hmac }
will negotiate = { Tunnel, },
{ esp-256-aes esp-sha-hmac }
will negotiate = { Tunnel, },

R2# show crypto ipsec transform-set
Transform set 50: { ah-sha-hmac }
will negotiate = { Tunnel, },
{ esp-256-aes esp-sha-hmac }
will negotiate = { Tunnel, },

14. Use el comando show crypto map para verificar la creación de los mapas

R1# show crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
Peer = 192.168.37.2

Extended IP access list 101
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Current peer: 192.168.37.2
Security association lifetime: 4608000 kilobytes/900 seconds
PFS (Y/N): Y
DH group: group5
Transform sets={
50,
}
Interfaces using crypto map MYMAP:
FastEthernet0/0

R3# show crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
Peer = 192.168.37.1
Extended IP access list 101
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Current peer: 192.168.37.1
Security association lifetime: 4608000 kilobytes/900 seconds
PFS (Y/N): Y
DH group: group5
Transform sets={
50,
}
Interfaces using crypto map MYMAP:
FastEthernet0/0

15. Verificar el funcionamiento de IPsec
R1# show crypto isakmp sa
R1# show crypto ipsec sa

R2# show crypto isakmp sa
R2# show crypto ipsec sa

16. Depurar IPsec

R1# debug crypto isakmp
Crypto ISAKMP debugging is on
R1# debug crypto ipsec
Crypto IPSEC debugging is on

R2# debug crypto isakmp
Crypto ISAKMP debugging is on
R2# debug crypto ipsec
Crypto IPSEC debugging is on

17. Una vez configurado IPsec se procede a realizar las llamadas.

SSL

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket, de forma transparente al usuario y a las aplicaciones que lo usan.

SSL se introduce como una especie de nivel o capa adicional, situada entre la capa de Aplicación y la capa de Transporte, sustituyendo los sockets del sistema operativo, lo que hace que sea independiente de la aplicación que lo utilice

SSL proporciona servicios de seguridad a la pila de protocolos, encriptando los datos salientes de la capa de Aplicación antes de que estos sean segmentados en la capa de Transporte y encapsulados y enviados por las capas inferiores.

La implementación de SSL se realiza por medio de Openssl para generar los certificados y Openvpn para crear túneles

El servidor VPN **hace de pasarela** para que todos los clientes puedan estar **comunicados** a través del túnel OpenVPN,

Pasos para configurar el Túnel OpenVPN

Los pasos para configurar un túnel ssl son:

1. Activar el ip_forwarding en el servidor openvpn

Edite el archivo /etc/sysctl.conf y cambie ip_forwarding a 1 normalmente se encuentra en 0 a través del editor vi

```
[root@servidor /]# vi /etc/sysctl.conf_
```

Figura VI.13. Edición del archivo /etc/sysctl.conf

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1_

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
```

Figura VI.14. Cambio de ip_forward a 1

2. Ejecuta el siguiente comando para verificar los datos del ip_forward

sysctl –p

```
[root@servidor /]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 4294967295
kernel.shmall = 268435456
[root@servidor /]# _
```

Figura VI.15. Verificar información del ip_forward

3. Se creará una serie de claves y certificados iniciales para autenticar y encriptar la información que se transmitirá desde/hacia servidor/clientes. Para ello se debe copiar unos scripts que se encuentra en /usr/share/openvpn*/easy-rsa los cuales facilitarán para este proceso. Y luego cambiar de directorio

cp –a /usr/share/openvpn*/easy-rsa /etc/openvpn

cd /etc/openvpn/easy-rsa/2.0

```
[root@servidor /]# cp -a /usr/share/openvpn*/easy-rsa /etc/openvpn
[root@servidor /]# cd /etc/openvpn/easy-rsa/2.0
```

Figura VI.16. Copia de scripts al directorio /etc/openvpn/easy-rsa/2.0

4. Una vez dentro de este directorio se puede crear los Certificados para ello se ejecuta los siguientes comandos.

. varspermite inicializar variables de ambiente para poder trabajar con los siguientes scripts de shell para generar las variables.

sh clean-all permite inicializar el directorio de las claves

sh build-ca genera el certificado CA el cual se debe llenar información que solicita.

```
[root@servidor 2.0]# sh build-ca
Generating a 1024 bit RSA private key
.....++++++
.++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:EC
State or Province Name (full name) [CA]:Chimborazo
Locality Name (eg, city) [SanFrancisco]:Riobamba
Organization Name (eg, company) [Fort-Funston]:Tesis
Organizational Unit Name (eg, section) []:SSL
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:192.168.
10.2
Name []:servidor
Email Address [me@myhost.mydomain]:dcchs3490@yahoo.es
```

Figura VI.17. Creación del certificado de CA

5. Generar el certificado del servidor para ello ejecutamos:

sh build-key-server server

Ingrese la información que se solicita para generar el certificado como es el nombre del país, provincia, localidad, organización, unidad organizacional, dominio, email.

```
[root@servidor 2.0]# sh build-key-server server
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:EC
State or Province Name (full name) [CA]:Chimborazo
Locality Name (eg, city) [SanFrancisco]:Riobamba
Organization Name (eg, company) [Fort-Funston]:Tesis
Organizational Unit Name (eg, section) []:SSL
Common Name (eg, your name or your server's hostname) [server]:192.168.10.2
Name []:server
Email Address [me@myhost.mydomain]:dcchs3490@yahoo.es_
```

Figura VI.18. Creación del certificado del servidor

La parte más importante del certificado es el Common Name donde se debe indicar el dominio o IP que luego se usará para conectar los terminales SIP.

Una vez ingresada la información aparecerá la siguiente pantalla con los datos del certificado

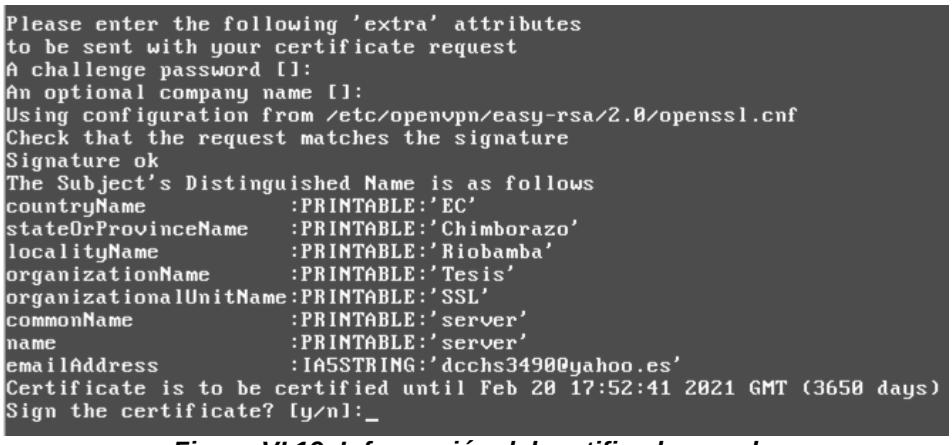


Figura VI.19. Información del certificado creado

6. Generar los certificados para cada uno de los clientes con la línea de comando **sh build-key usuario1**

Ingrese la información necesaria para crear el certificado

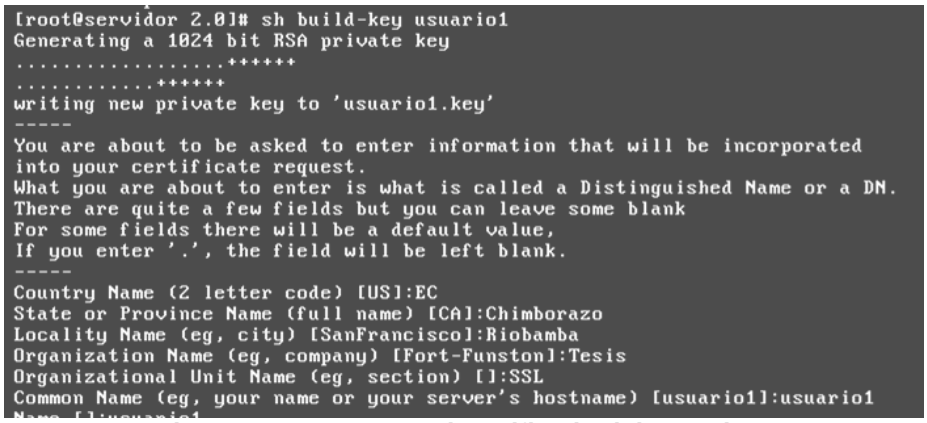


Figura VI.20. Generar el certificado del usuario 1

Una vez ingresada la información aparece la siguiente pantalla con la información del certificado, presione la letra y para guardar el certificado.

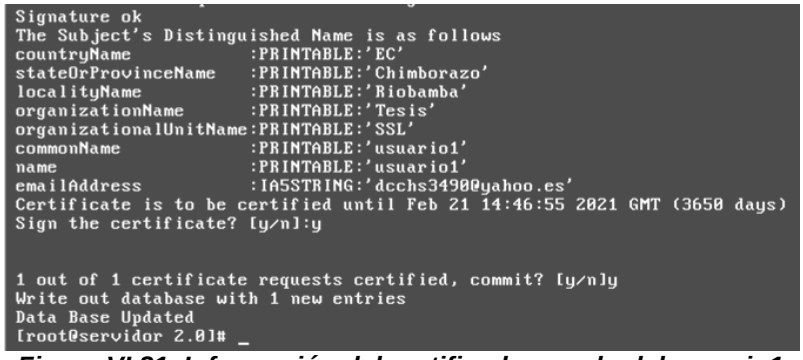


Figura VI.21. Información del certificado creado del usuario1

sh build-key usuario2

Ingrese la información para generar el certificado

```
[root@servidor 2.0]# sh build-key usuario2
Generating a 1024 bit RSA private key
...++++++
.....................++++++
writing new private key to 'usuario2.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:EC
State or Province Name (full name) [CA]:Chimborazo
Locality Name (eg, city) [SanFrancisco]:Riobamba
Organization Name (eg, company) [Fort-Funston]:Tesis
Organizational Unit Name (eg, section) []:SSL
Common Name (eg, your name or your server's hostname) [usuario2]:usuario2
Name []:usuario2
Email Address [me@myhost.mydomain]:dcchs3490@yahoo.es_
```

Figura VI.22. Generar el certificado del usuario 2

Una vez ingresada la información para generar el certificado aprece la pantalla con el detalle del certificado, presione y para guardarlo.

```
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'EC'
stateOrProvinceName   :PRINTABLE:'Chimborazo'
localityName          :PRINTABLE:'Riobamba'
organizationName      :PRINTABLE:'Tesis'
organizationalUnitName:PRINTABLE:'SSL'
commonName            :PRINTABLE:'usuario2'
name                  :PRINTABLE:'usuario2'
emailAddress          :IA5STRING:'dcchs3490@yahoo.es'
Certificate is to be certified until Feb 21 14:49:27 2021 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@servidor 2.0]# _
```

Figura VI.23. Información del certificado creado del usuario2

7. **Generar el parámetro Diffie-Hellman. D**iffie-**H**ellman permite el intercambio secreto de claves entre dos partes que sin que éstas hayan tenido contacto previo, utilizando un canal inseguro, y de manera anónima (sin autenticar). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión, como es el caso de una conexión VPN.

sh build-dh

```
[root@servidor 2.0]# sh build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
..+.....................................................................+.....
..+.....................................................+.....+.....+.....
.........+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
```

Figura VI.24. Parametro Diffie-Hellman

8. Copiar los archivos ca.crt ca.key server.crt server.key dh1024.pem del servidor al directorio /etc/openvpn

Para la conexión de los usuarios con el servidor

```
[root@servidor 2.0]# cd keys
[root@servidor keys]# cp ca.crt ca.key server.crt server.key dh1024.pem /etc/ope
nvpn
[root@servidor keys]# cd .
[root@servidor keys]# cd ..
[root@servidor 2.0]# cd ..
[root@servidor easy-rsa]# cd ..
[root@servidor openvpn]# ls
ca.crt  ca.key  dh1024.pem  easy-rsa  server.crt  server.key
```

Figura VI.25. Copia de archivos

9. Copiar los archivos ca.crt clientex.crt y clientex.key a cada uno de los clientes. (x es el número del cliente)

10. Configurar el servidor

vi /etc/openvpn/server.conf

port 1194

proto tcp

dev tun

ca ca.crt

cert server.crt

key server.key

dh dh1024.pem

#Direcciones que se asignarán a los clientes

server 192.168.37.0 255.255.255.0

ifconfig-pool-persist ipp.txt

keepalive 10 120

comp-lzo

user nobody

group nobody

persist-key

persist-tun

status openvpn-status.log

verb 4

Presionar ESC : wq para guardar los cambios

Descripción:

Port: Especifica el puerto que será utilizado para que los clientes vpn puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en a conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.

ca: Especifica la ubicación exacta del fichero de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del fichero [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor openvpn.

dh: Ruta exacta del fichero [.pem] el cual contiene el formato de Diffie Hellman (requirerido para **–tls-server** solamente).

server: Se asigna el rango IP virtual que se utilizará en la red del túnel VPN.

Ifconfig-pool-persist: Fichero en donde quedarán registrado las direcciones IP de los clientes que se encuentran conectados al servidor OpenVPN.

Keepalive 10 120 : Envía los paquetes que se manejan por la red una vez cada 10 segundos; y asuma que el acoplamiento es abajo si ninguna respuesta ocurre por 120 segundos.

comp-lzo: Especifica los datos que recorren el túnel vpn será compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

status: fichero donde se almacenará los eventos y datos sobre la conexión del servidor [.log]

verb: Nivel de información (default=1). Cada nivel demuestra todo el Info de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.
0 –No muestra una salida excepto errores fatales. **1 to 4 –**Rango de uso normal. **5 –** Salida **R**y **W**caracteres en la consola par los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP.

11. Crear reglas para el iptables

Las reglas nos permitirán que el servidor acepte el tráfico de la OPENVPN

12. Levantar la vpn

```
[root@servidor /]# /etc/init.d/openvpn start
Iniciando openvpn:RTNETLINK answers: File exists
                                                           [  OK  ]
[root@servidor /]# _
```

Figura VI.26. Levantar la vpn

13. Comprobar que el túnel vpn este ejecutándose con el comando ifconfig

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:192.168.37.1  P-t-P:192.168.37.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:553 (553.0 b)
```

Figura VI.27. Comprobación del túnel

14. Instalar el cliente vpn

El cliente que se usará para hacer uso del túnel es el cliente OpenVPN-2.0.9-gui

1. Empiece la instalación del cliente openvpn presionando doble clic sobre el icono de instalación

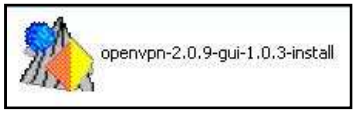


Figura VI.28. Instalador del cliente vpn

2. Iniciando el instalador de OpenVPN GUI

Figura VI.29. Inicio de la instalación

3. A continuación tendremos la licencia acepte

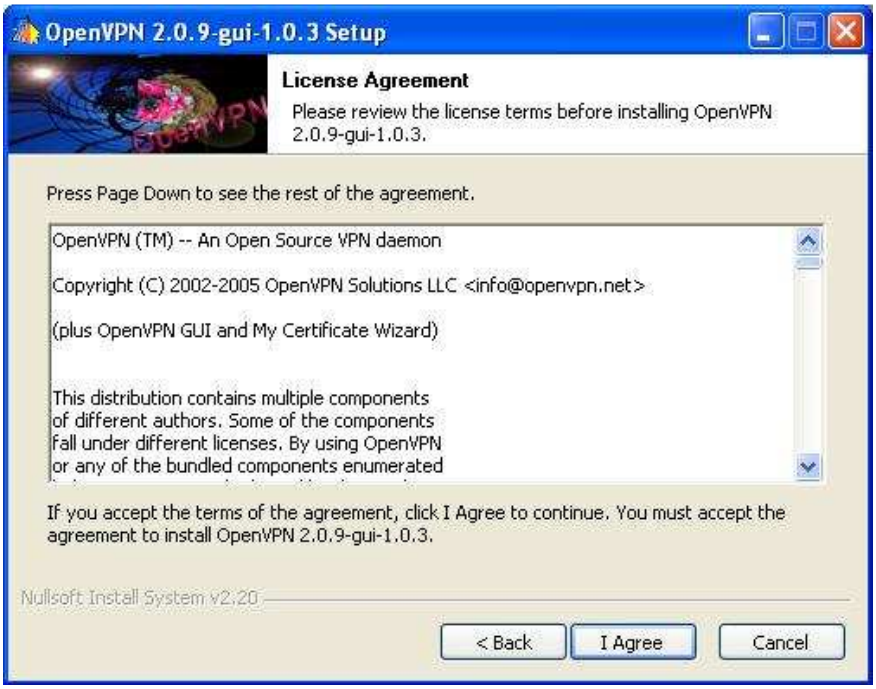


Figura VI.30. Licencia OpenVPN GUI

4. Seleccione los componentes a instalar, se puede dejar las **opciones por defecto**

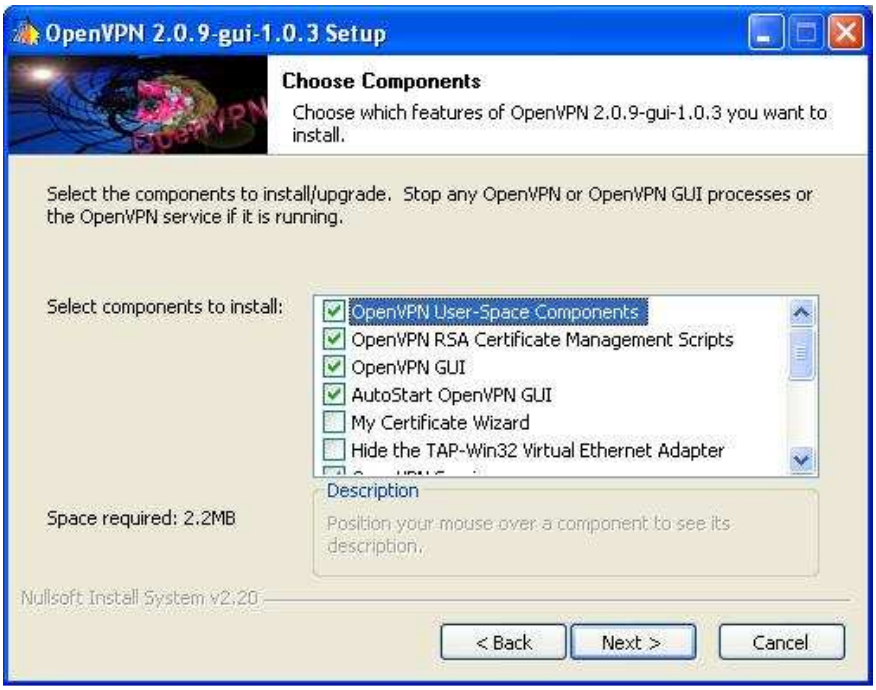


Figura VI.31. Componentes a instalar

5. Seleccione el punto de instalación de **OpenVPN GUI**

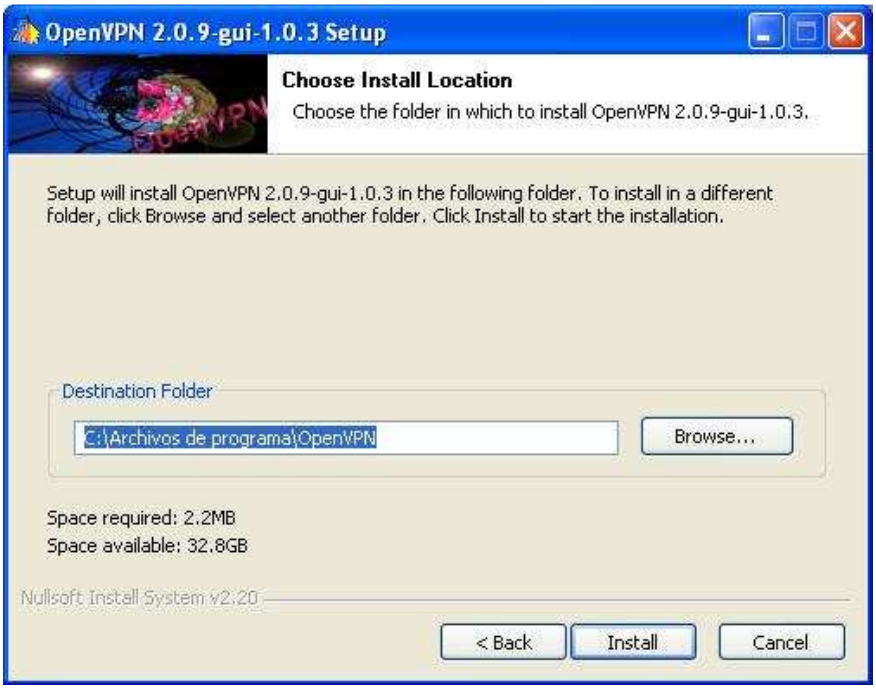


Figura VI.32. Punto de instalación de OpenVPN GUI

6. A continuación se instalará el programa

Figura VI.33. Instalación en proceso

7. Instalación de hardware TAP-Win32 Adapter V8

Figura VI.34. Instalación de TAP-Win32

8. La instalación del cliente vpn se completo satisfactoriamente

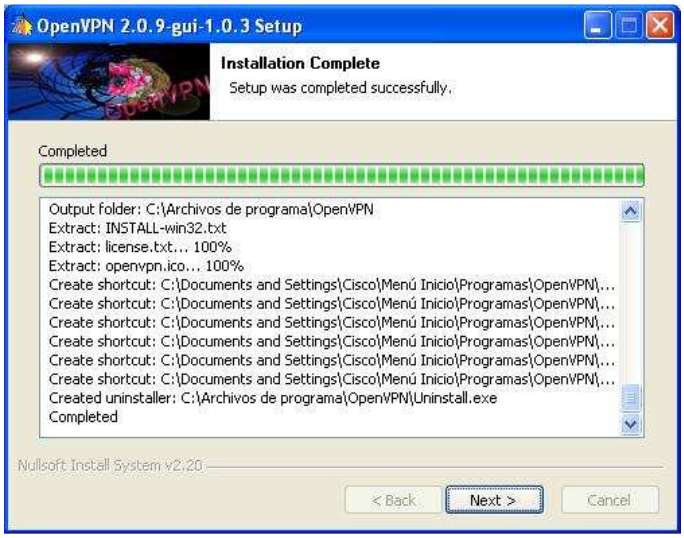


Figura VI.35. Instalación completa

9. Finaliza el proceso de instalación

Figura VI.35. OpenVPN GUI acabado de instalar

10. A continuación se debe **configurar OpenVPN GUI**, debe abrir el directorio **C:\Archivos de programa\OpenVPN**

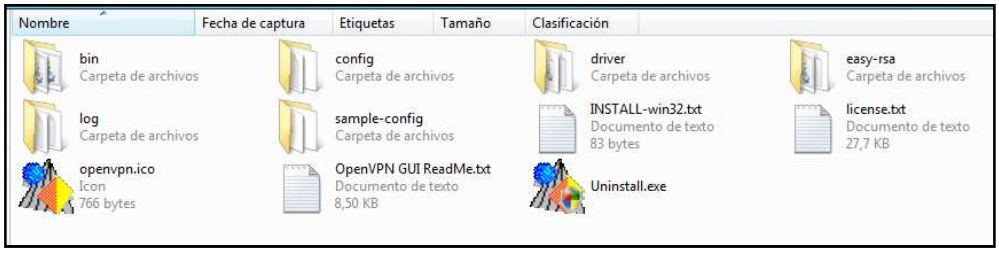


Figura VI.36. Directorio de OpenVPN GUI

11. Dentro del **directorio config** se debe añadir los ficheros que se generó en la instalación del servidor OpenVPN:

- **ca.crt**: Certificado de la autoridad certificadora
- **usuario1.crt**: Certificado del cliente
- **usuario1.key**: Parte privada del certificado del cliente (clave)

12. Se debe crear un fichero de configuración llamado **nombre_usuario.ovpn** con los datos del servidor:

client
dev tun
proto udp
remote 192.168.10.2 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert usuario1.crt
key usuario1.key
comp-lzo
verb 3

En dicha configuración se debe ajustar adecuadamente las siguientes opciones:

- **remote**: Indicamos el **servidor** al que conectar y el **puerto** que sea, por defecto el **1194**
- **cert**: Indicamos el certificado del cliente
- **key**: Indicamos la clave privada del cliente

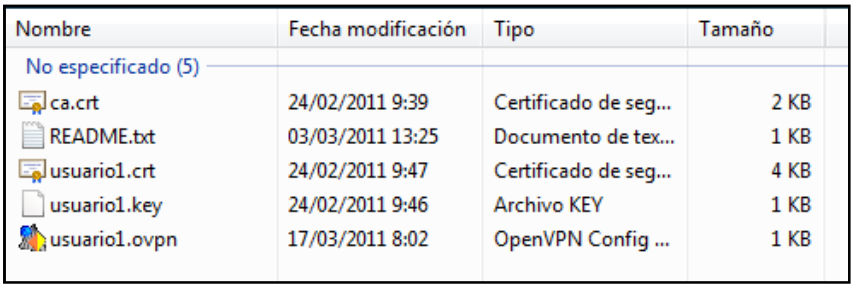


Figura VI.37. Ficheros de configuración de OpenVPN GUI

Descripción:

client: Especifica el tipo de configuración, en este caso tipo cliente OpenVPN. Y que algunas configuraciones las tomará del servidor

Port: Especifica el puerto que será utilizado para que los clientes VPN puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en a conexión a través de VPN
dev: Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.

remote: Host remoto o dirección IP en el cliente, el cual especifica al servidor OpenVPN.
El cliente OpenVPN puede tratar de conectar al servidor con **host:port**en el orden especificado de las opciones de la opción **–remote**.

float: Este le dice a OpenVPN aceptar los paquetes autenticados de cualquier dirección, no solamente la dirección cuál fue especificado en la opción **–remote**.

resolv-retry: Si la resolución del hostname falla para **– remote**, la resolución antes de fallar hace una re-comprobación de n segundos.

nobind: No agrega bind a la dirección local y al puerto. Que actúa solo como cliente no como servidor

ca: Especifica la ubicación exacta del fichero de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del fichero [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor OpenVPN.

remote: Especifica el dominio o IP del servidor así como el puerto que escuchara las peticiones para servicio VPN.

comp-lzo: Especifica los datos que recorren el túnel VPN será compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

verb: Nivel de información (default=1). Cada nivel demuestra toda la Información de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

0 –No muestra una salida excepto errores fatales. **1 to 4 –**Rango de uso normal. **5 –** Salida **R**y **W**caracteres en la consola par los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es usada para paquetes TUN/TAP.

Nota: los archivos cert y key deben ser únicas para cada cliente

13. Se debe arrancar el cliente. Para hacerlo en el system tray debemos tener este icono

Figura VI.38. Icono de cliente vpn

(Si no está presente arrancamos el programa desde Inicio/programas/OpenVPN/OpenVPN GUI)

14. A continuación con el **OpenVPN GUI** ya arrancado en la barra de tareas con el botón derecho podemos hacer el **Connect**:

Figura VI.39. Conectar al servidor OpenVPN

15. A continuación se realizará la **conexión con el servidor OpenVPN**:

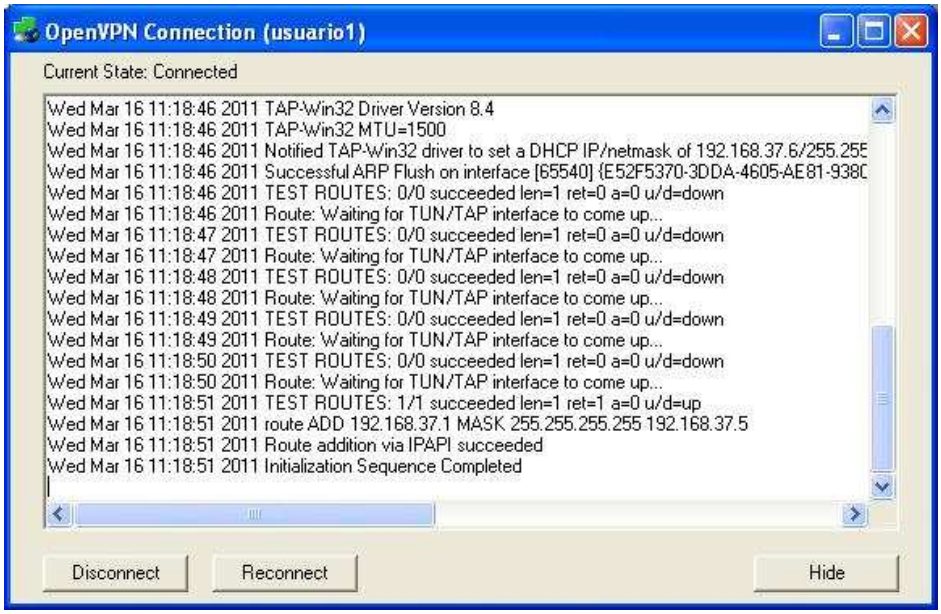


Figura VI.40. Conectando con el servidor OpenVPN

16. Finalmente cuando se marque en verde tendremos la conexión establecida:

Figura VI.41. Conexión establecida

En el servidor se registra

```
servidor*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
100/100                    192.168.37.6     D   N   A  5060     OK (1 ms)
101                        (Unspecified)    D   N   A  5060     UNKNOWN
102/102                    192.168.10.6     D   N   A  5060     OK (6 ms)
103/103                    (Unspecified)    D   N   A  0        UNKNOWN
4 sip peers [Monitored: 2 online, 2 offline Unmonitored: 0 online, 0 offline]
servidor*CLI>
```

Figura VI.42. Registro del cliente de la vpn

TLS

La implementación de TLS se realizará por medio de Openssl

El primer paso es crear un certificado autofirmado, necesario para la autenticación de los dispositivos.

1. Se selecciona la localización del certificado.

cd /etc/asterisk

2. Con openssl se crea una clave privada

openssl genrsa 1024 > host.key

3. Luego se debe crear un certificado firmado con la clave privada recién creada con la siguiente línea de comandos:

openssl req -new -x509 -nodes -sha1 -days 365 -key host.key > host.cert

4. Luego de ejecutar la línea de comandos se debe completar la información necesaria para el certificado

La parte más importante del certificado es el Common Name donde se debe indicar el dominio o IP que luego se usará para conectar los terminales SIP.

5. Una vez que se tiene los dos archivos se debe crear un nuevo archivo que contenga los dos:

cat host.cert host.key > asterisk.pem

Configuración de Asterisk

Primero se configura el archivo sip_general_custom.conf y se añaden las siguientes líneas:

tlsenable=yes
tlsbindaddr=192.168.10.2
tlscertfile=/etc/asterisk/asterisk.pem

Con la primera línea se activa el soporte TLS. La segunda línea define la dirección IP que Asterisk usará para aceptar las conexiones (si no se define el puerto, el predefinido será el 5061). La tercera línea define la carpeta y nombre del archivo que contiene el certificado.

Para cada extensión que usará el protocolo TLS para conectarse a Asterisk, se añade la línea **transport=tls**

Se guardan los cambios y se deben reiniciar los servicios

Entre en la consola de asterisk con el siguiente comando
asterisk –rvvvvvvvvvvvvvvvvvvv

Actualice la configuración SIP
CLI>**sip reload**

Aparece entre las distintas líneas que el certificado SSL fue creado
SSL certificate ok

Ahora se debe instalar el certificado en el computador donde está instalado el softphone. Para hacer esto se debe copiar el certificado y la clave creada en el servidor.

4.2.2. Realizar pruebas

Las pruebas se realizaron en el escenario implementado en el Laboratorio de la academia Local de Redes Cisco-ESPOCH y con la ayuda del sniffer Wireshark para la captura de los paquetes transmitidos durante la comunicación.

Además se configuro SPAN para habilitar a todos los puertos del switch.

Después de haber realizado las diferentes pruebas y haber observado su desempeño en función de la confidencialidad y la integridad de la comunicación se obtuvieron los siguientes resultados.

Resultados sin implementar ninguna de las técnicas de seguridad

Con la capturadel tráfico durante la transmisión de datos con el sniffer Wireshark como lo muestra la Figura.IV.43 se puede observar con claridad que se captura los paquetes SIP,los mismos que permiten establecer la comunicación entre los usuarios de la central PBX sin ninguna seguridad, se observa de que extensión se realizó la llamada, la dirección IP, el puerto por el cual se transmite la comunicación.

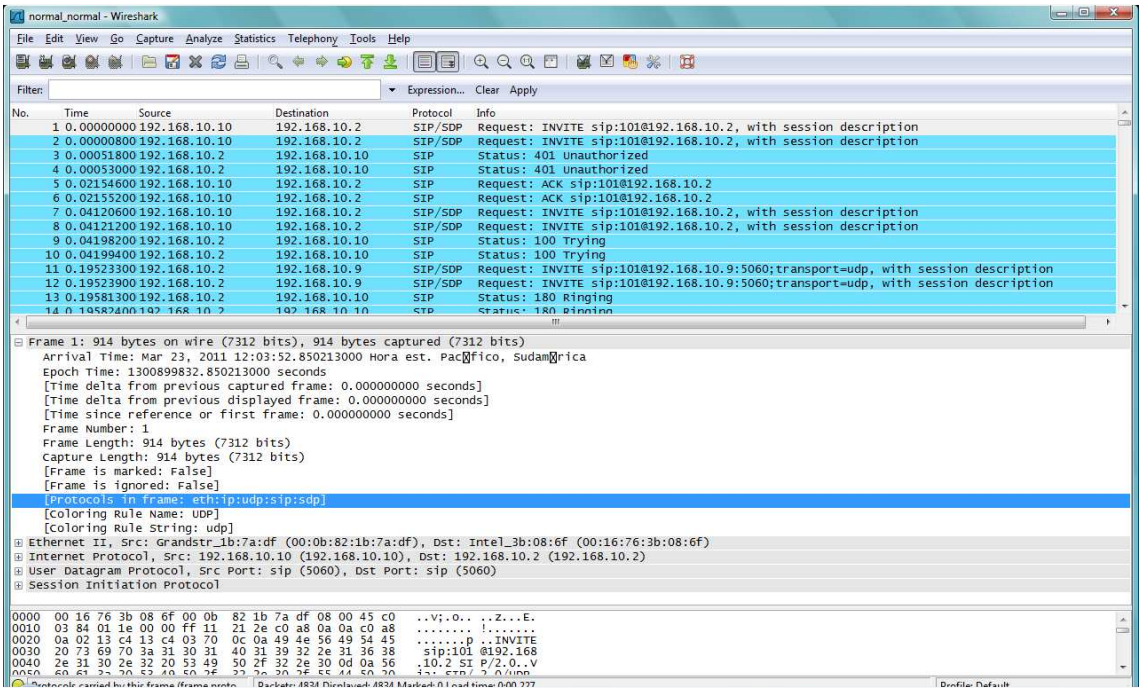


Figura IV.43. Captura de paquetes

Seleccione la opción Telephony y luego VoIP Calls para verificar si la llamada fue capturada.

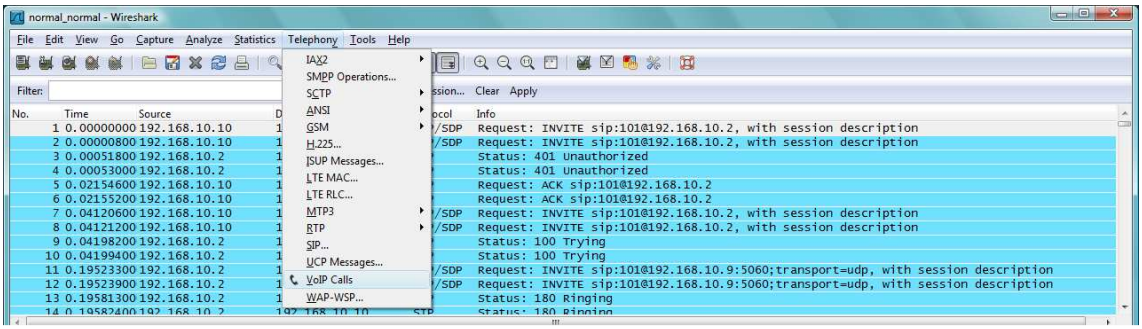


Figura IV.44. Opciones para comprobar si la llamada fue capturada

Aparece la siguiente pantalla en la que muestra que la llamada fue capturada

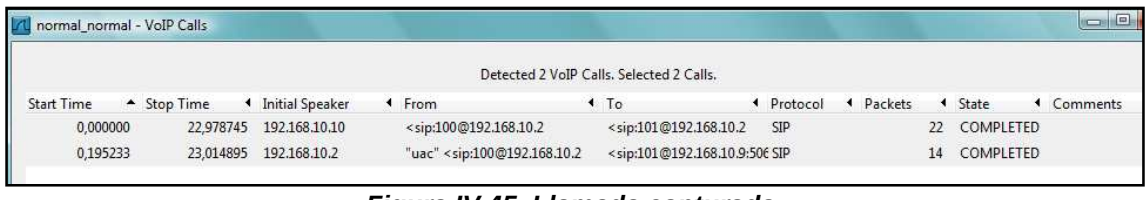


Figura IV.45. Llamada capturada

Para reproducir la llamada capturada se presiona Select All y luego presione Player aparecerá una pantalla en la que se debe presionar la opción Decode. Aparecerá la siguiente pantalla en la que selecciona la conversación que se desea escuchar para

ello presione Play y la conversación se reproduce sin ninguna dificultad y se escucha claramente.

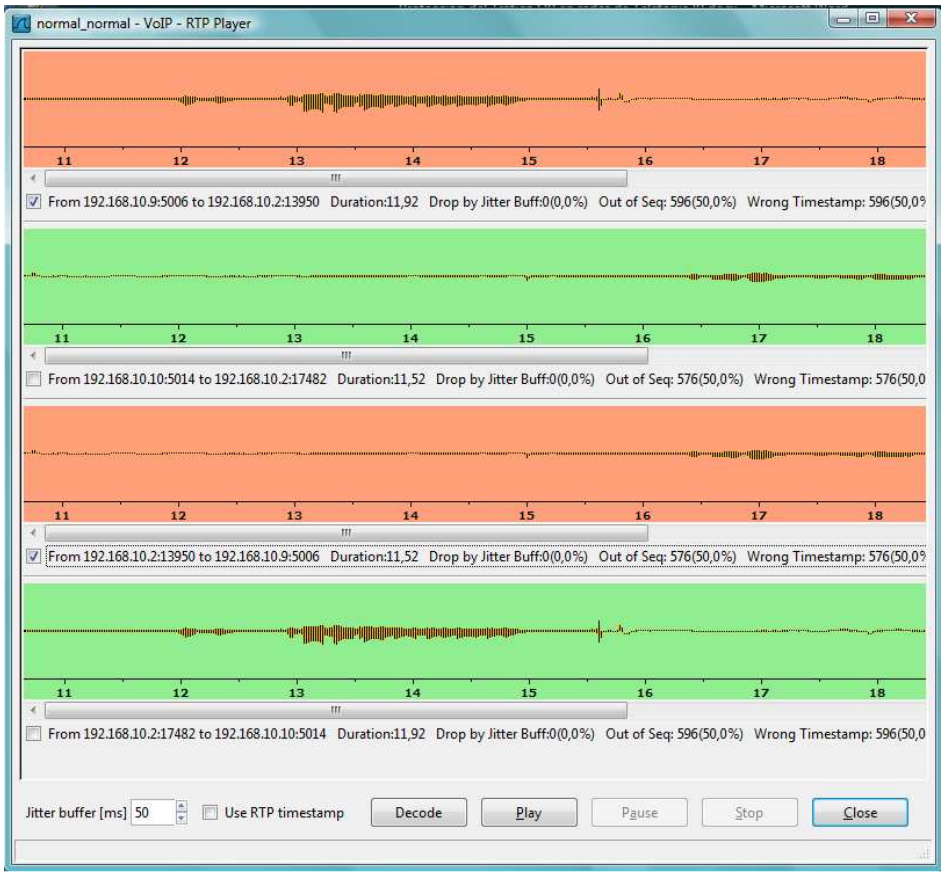


Figura VI.46. Escucha de la llamada

Resultados en escenarios con técnicas de seguridad

Los resultados que se presentan a continuación indican la implementación de cada una de las técnicas de seguridad en el escenario de prueba implementado en la Academia de Redes Locales Cisco-ESPOCH.

Implementado IPsec

La capturada del tráfico con la ayuda del sniffer Wireshark muestra que la comunicación establecida entre dos usuarios de la central Elastix se da a través del protocolo ESP como lo muestra la figura VI.47 indicando que fue implementado IPsec y que usa las direcciones IP de la vpn que se establece al implementarlo y no muestra la dirección física del usuario.

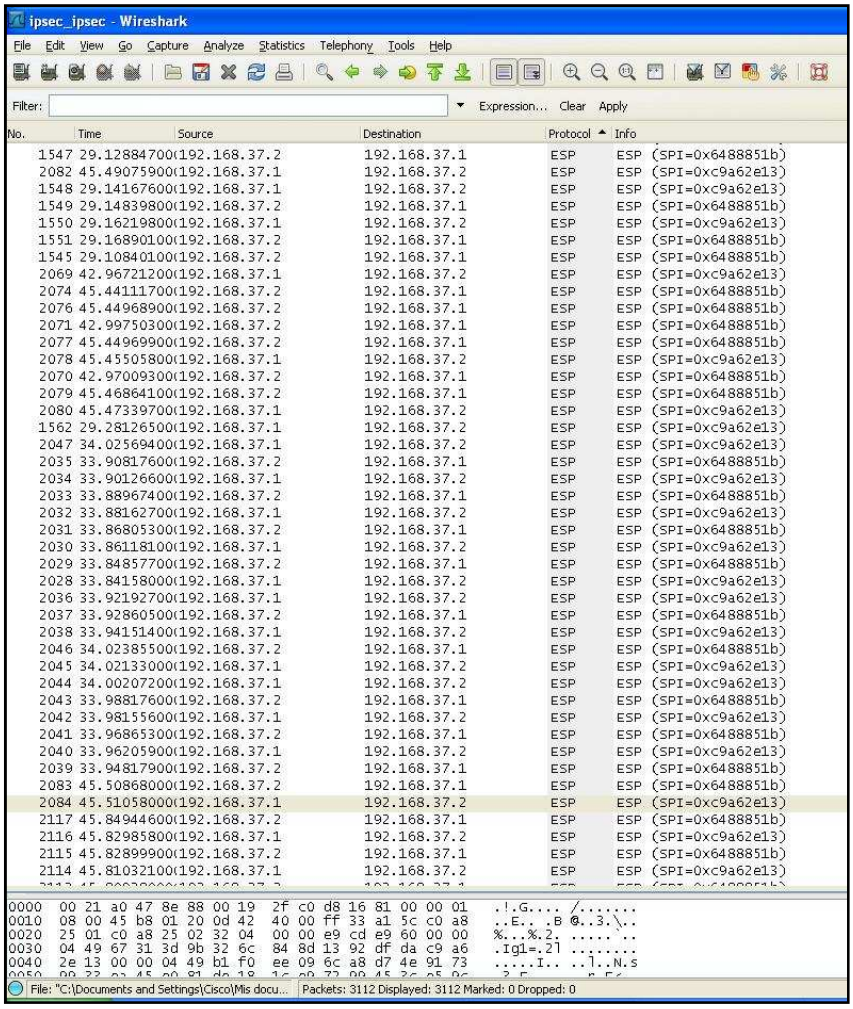


Figura VI. 47. Captura de la comunicación con el protocolo ESP

Seleccione la opción Telephony luego la opción VoIP Calls para verificar que la llamada no fue capturada ya que usa el protocolo ESP.

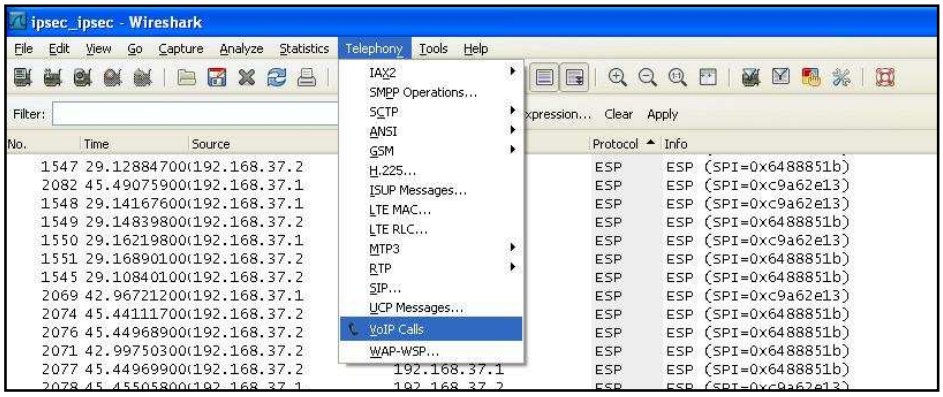


Figura VI.48. Verificar llamadas capturadas

Esta pantalla muestra claramente que la llamada no fue capturada.

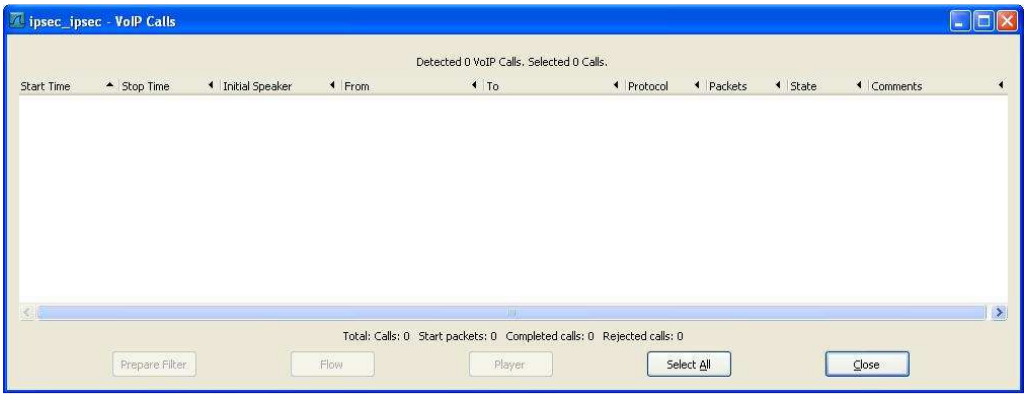


Figura VI.49. La llamada no fue capturada

De esta manera se puede verificar que la integridad y la confidencialidad de la comunicación de voz no es afectada, ya que no permite que la llamada sea capturada y utilizada con fines maliciosos.

Implementado SSL

La información capturada en el sniffer muestra que la comunicación está establecida en la VPN

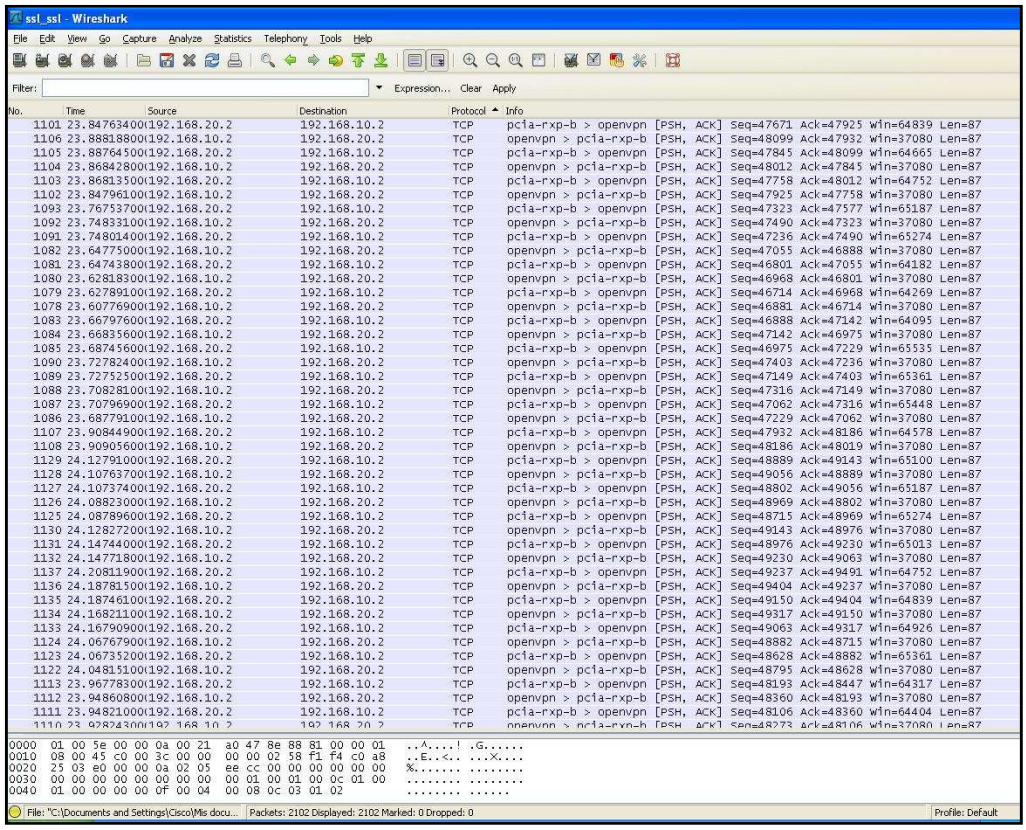


Figura VI.50. Captura de la llamada con VPN

Seleccione la opción Telephony luego la opción VoIP Calls para verificar que la llamada no fue capturada ya que está usando la VPN

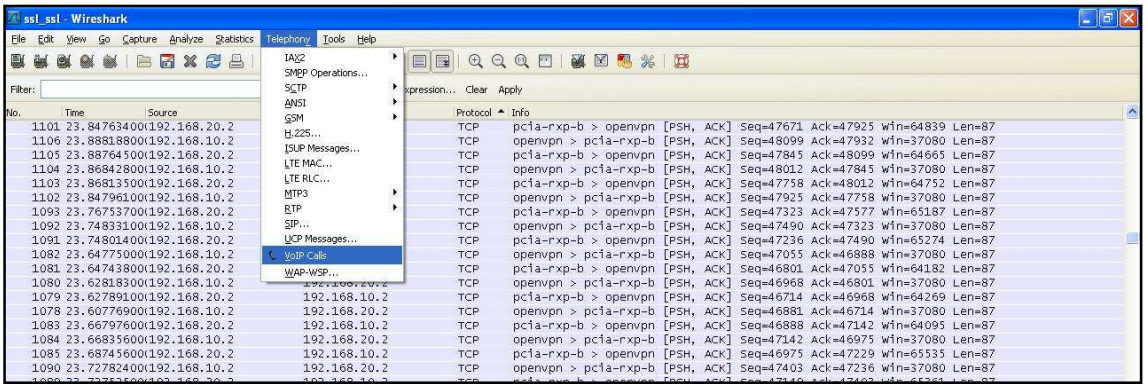


Figura VI.51. Captura del tráfico

Esta pantalla muestra claramente que la llamada no fue capturada.

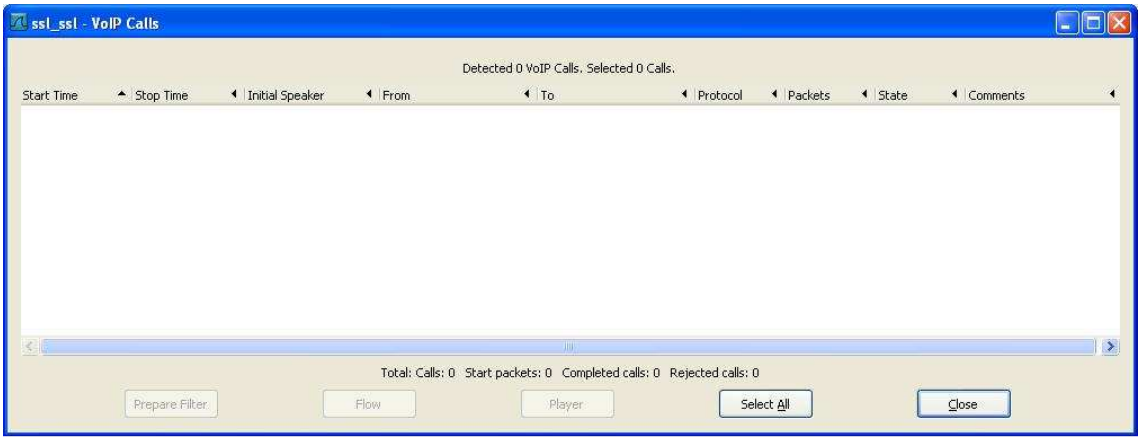


Figura VI.52. La llamada no fue capturada

Al utilizar una red virtual se puede evitar que la llamada sea capturada y la integridad y confidencialidad de la comunicación se vea afectada.

Implementado TLS

La información capturada con el sniffer Wiresharkmuestra que la comunicación está establecida entre dos usuarios de la central Elastix se da a través del protocolo TLS como lo indica la figura IV.53

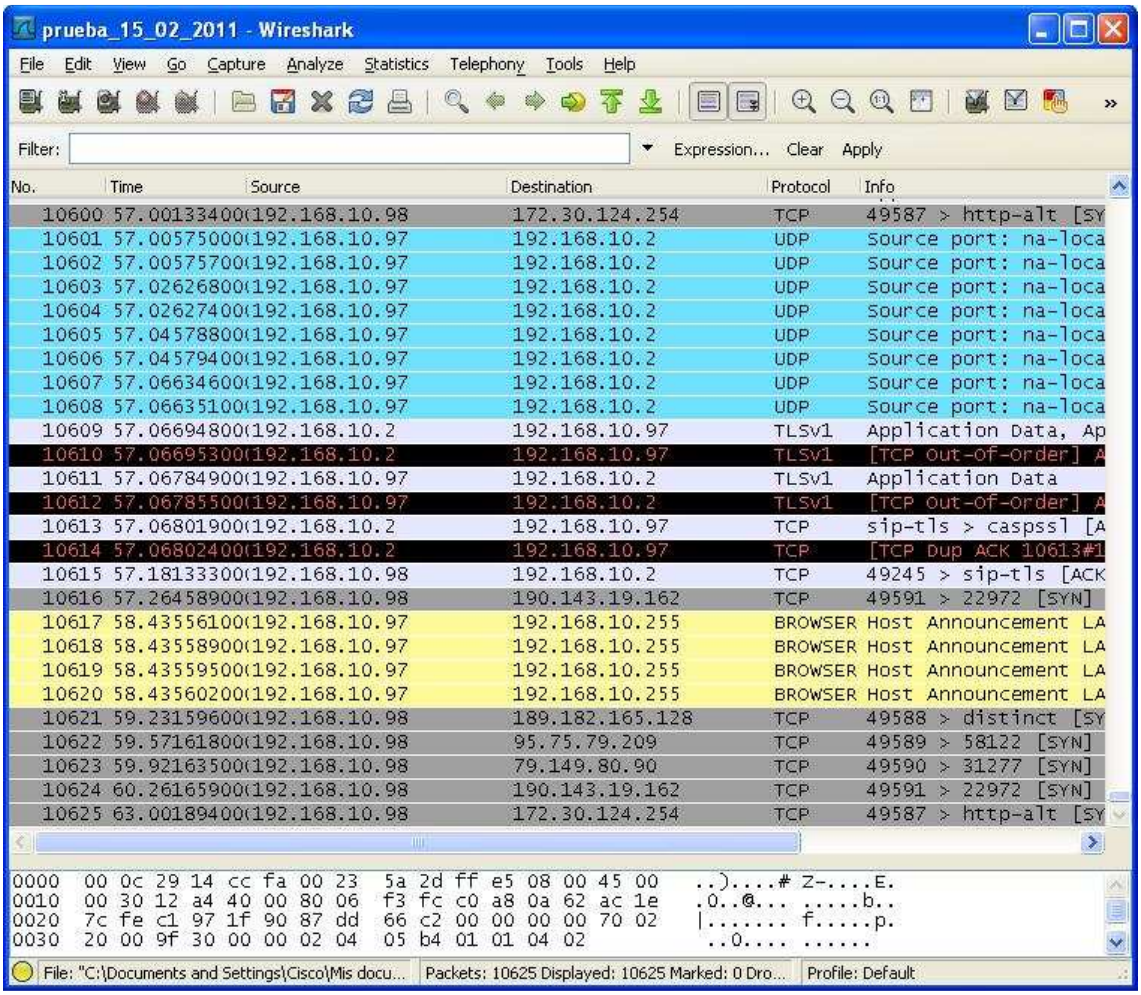


Figura IV.53. Captura del protocolo TLS

Seleccione la opción Telephony luego la opción VoIP Calls para verificar que la llamada no fue capturada ya que usa el protocolo TLS

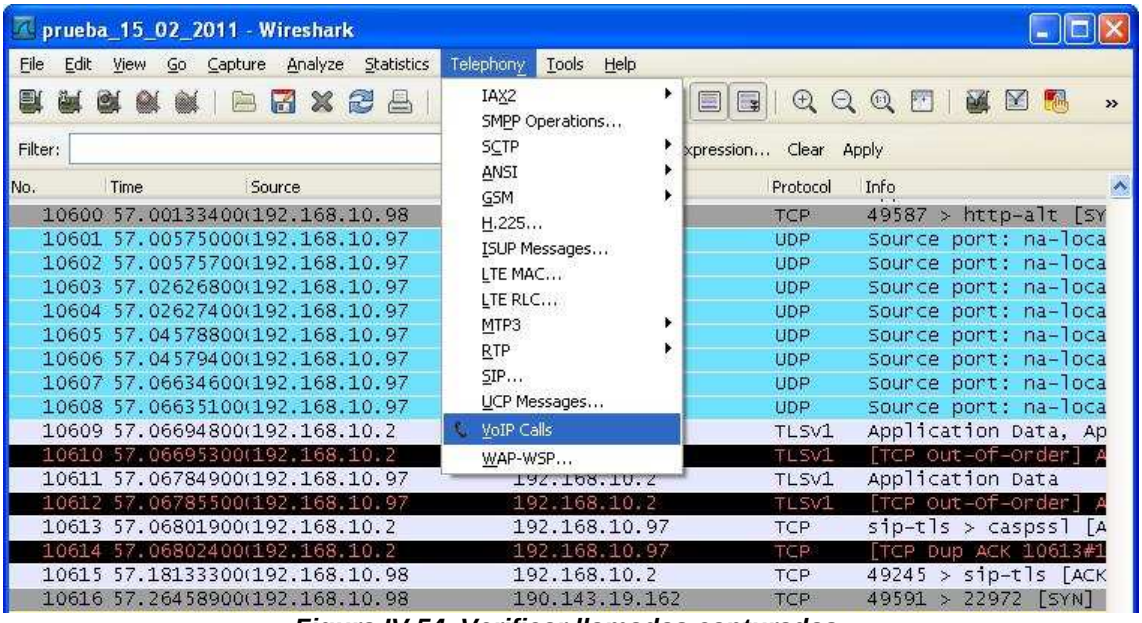


Figura IV.54. Verificar llamadas capturadas

Esta pantalla muestra claramente que la llamada no fue capturada.

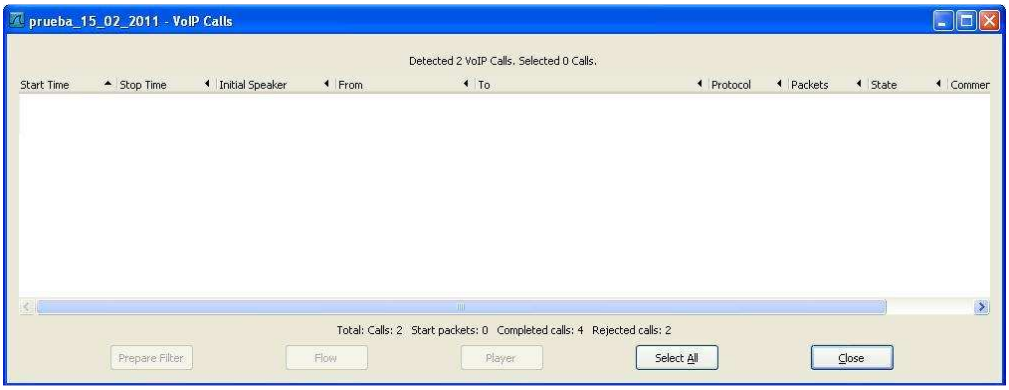


Figura IV.55. La llamada no fue capturada

Al utilizar TLS para realizar la llamada,ésta no será capturada evitando que la integridad y la confidencialidad de la comunicación se vea afectada y utilizada con fines maliciosos.

b) Fase II: Variables a Evaluar

A continuación se detalla las variables a evaluar en base a las cuales se realiza la comparación.

1 Capa en la que operan
2 Estándar
3 Arquitectura
4 Interoperabilidad
5 Protocolo de transporte que usa para establecer la conexión
6 Implementación
7 Encriptación
8 Servicios
9 Integridad
10 Confidencialidad

Capa en la que opera: El modelo OSI es una arquitectura que divide la comunicación en 7 capas, cada capa especifica las funciones que deben implementar un determinado protocolo o dispositivo.Cada una deellas utiliza los servicios del nivel o capa inmediatamente superior, y a su vez ofrece servicios a la capa inmediatamente inferior.

Estándar: El Estándar sirve como tipo, modelo, norma, patrón o referencia,es la herramienta base de la interoperabilidad informática, ha permitido definir cómo interactuaran los miles o millones de componentes informáticos que existen, además permite garantizarfuncionalidades y capacidades de interoperabilidad técnica distintas.

Arquitectura: Es el desarrollo de modelos arquitectónicos de implementación de metadatos, haciendo especial hincapié en los mecanismos de almacenaje y transporte de metadatos en sistemas distribuidos.

Interoperabilidad: La interoperabilidad es la condición mediante la cual sistemas heterogéneos pueden intercambiar procesos o datos. Es la capacidad que tiene un producto o un sistema, cuyas interfaces son totalmente conocidas, para funcionar con otros productos o sistemas existentes o futuros y eso sin restricción de acceso o de implementación.

Protocolo de transporte que usa para establecer la conexión: Para que se establezca la comunicación entre dos aplicaciones, es necesario que haya un protocolo de transporte, ya sea este orientado o no a la conexión.

Implementación: Es el conjunto de procedimientos para llevar a cabo algo con el fin de suplir las necesidades del medio.

Encriptación: Es el conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada. Se puede hablar de dos sistemas de cifrado: sistemas simétricos, en los que se utiliza la misma clave para cifrar y descifrar el mensaje, y sistemas asimétricos, en los que se utiliza una clave para cifrar el mensaje y otra distinta para descifrarlo.

Servicios: Es un conjunto de actividades que buscan responder a las necesidades de un cliente, un servicio no puede verse, probarse antes de ser implementado.

Integridad: Parámetro por medio de la cual una entidad puede asegurarse de que los datos recibidos no han sido modificados en ninguna forma durante el proceso de su transferencia. Es posible, mediante ese servicio, eliminar el riesgo de la corrupción de los datos como resultado de una manipulación deliberada y malintencionada.

Confidencialidad: Mediante la cual se protege una llamada entre dos corresponsales contra laescucha ilegal de terceros no autorizados o malintencionados.

c) Fase III: Responsable

Egresada: Diana Carolina Chapalbay Santillán

d) Fase IV: Características Generales de las Técnicas de Seguridad del protocolo SIP

Las características que poseen las técnicas que brindan seguridad al protocolo SIP son:

Tabla IV. VII. Características generales de las técnicas de seguridad del protocolo SIP

CARACTERÍSTICAS	**TÉCNICAS**		
	IPsec	**SSL**	**TLS**
Capa en la que opera	Capa de red	Capa adicional sobre la de transporte	Capa de transporte
Estándar	Estándar RFC-4301	Utilizado en los navegadores web	Estándar RFC-4279
Arquitectura	Cliente / Servidor	Cliente / Servidor	Cliente / Servidor
Interoperabilidad	Con IPv4 e IPv6	Con IPv4 e IPv6	Con IPv4 e IPv6
Protocolo de transporte que usa para establecer la conexión	Usa los protocolos TCP o UDP para establecer la conexión	Usa TCP para establecer la conexión	Se basa en TCP para establecer la conexión
Implementación	Muy compleja	Compleja	Sencilla
Encriptación	IKE DES y 3 DES AES MD5 para el HMAC RSA	AES DES RC4 MD5 RSA	Certificados X.509 SHA HMAC RSA
Servicios	• Cifra datos y	• Cifrado de	• Cifrado de

	cabeceras • Integridad de datos. • Autentificación de los datos de origen. • No repetición. • Confiabilidad de datos.	datos. • Integridad de datos. • Autenticación de servidores. • No proporciona no repetición • Confiabilidad de datos.	datos • Integridad de datos. • Autenticación de servidores y clientes • No proporciona no repetición • Confiabilidad de datos.
Integridad	El que recibe los paquetes puede autentificar al que envía y asegurarse que el paquete no haya sido modificado.	Para transmitir la información debe establecerse la conexión cifrada.	Para transmitir información es necesario que se establezca un canal seguro.
Confidencialidad	Protege los paquetes IP mediante enlaces seguros extremo a extremo en las comunicaciones. Añaden cabeceras al paquete Ip original y Cifra su contenido para garantizar la confidencialidad.	Crea un canal seguro para la comunicación por lo cual hace posible la confidencialidad en la transmisión de datos.	Trabaja con certificados de clave pública, los mismos que permite que la comunicación se establezca entre los usuarios que posee el certificado.

e) Fase V: Cuantificación de Resultados

Para la realización de la evaluación se ha decidido utilizar una escala cuantitativa ya que las calificaciones que se van a poner están en el rango de 0 a10 para evaluar cada una de las técnicas.

A este rango lo vamos a subdividir para representar las diferentes calificaciones que vamos a dar según se vaya realizando la evaluación, los resultados finales se presentaran numérica y gráficamente.

La calificación de **Regular** recibirá la Técnica que no cumpla con los parámetros establecidos dentro de la variable citada en la comparación, **Eficaz** será la Técnica que maneja bien la variable especificada pero que no se comportaría cien por ciento efectivo el momento de la transmisión, mientras que la calificación **Excelente** será denominada a la Técnica que cumpla con la variable definida y se acople cien por ciento.

El rango de calificación es el siguiente:

Tabla IV.VIII. Rango de calificación

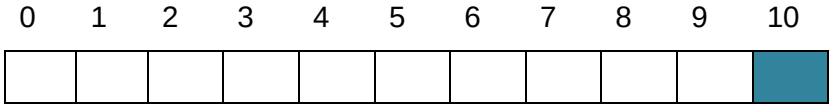
Numeración	0-5	6-8	9-10
Equivalente	Regular	Eficaz	Excelente

f) Fase VI: Evaluación de las Variables

1. Capa en la que operan

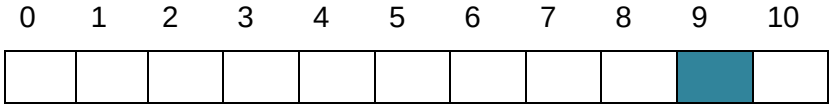
IPsec

IPsec opera en la capa de red, la capa 3 del modelo OSI. Esto hace que IPsec sea tranparente al usuario y a las aplicaciones que este utilice, por tanto las aplicaciones no tienen que ser modificadas para hacer compatible el uso de IPsec, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP. IPsec está orientado a proteger todo el tráfico que circula por la red.



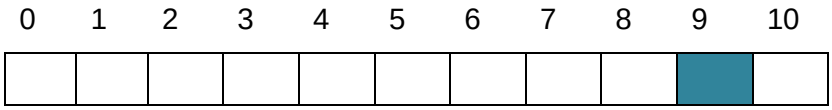
SSL

Opera en la capa de transporte, capa 4 del Modelo OSI, pero actúa como una capa adicional que permite garantizar la seguridad de los datos. De esta forma, SSL es transparente para el usuario.



TLS

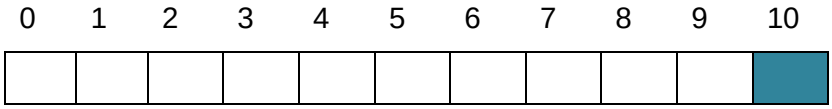
Opera en la capa de transporte, TLS permite a los clientes autenticar servidores y, opcionalmente, a los servidores autenticar clientes. También proporciona un canal seguro ya que cifra las comunicaciones.



2. Estándar

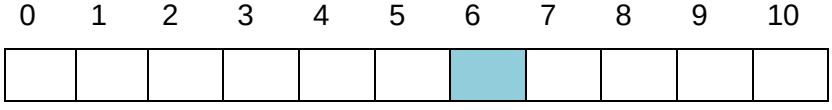
IPsec

IPsec está definido en el Estándar RFC-4301, es un conjunto de estándares del IETF para incorporar servicios de seguridad enIP y que responde a la necesidad creciente de garantizar un nivel de seguridadimprescindible para las comunicaciones entre empresas y comercio electrónico.



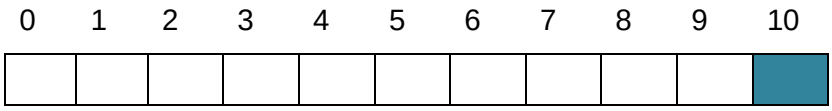
SSL

SSL trabaja a nivel de socket por lo que permite ser usado tanto para proteger documentos de hipertexto como también servicios como FTP, SMTP, TELNET. Además es usado en la mayoría de navegadores.



TLS

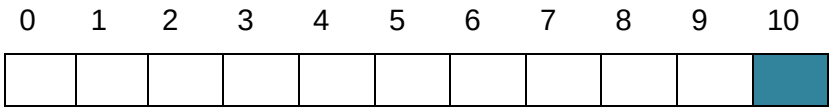
Estándar RFC-4279, TLS es un protocolo estándar que se usa para proporcionar comunicaciones Web seguras en Internet o en intranets, usando un modelo de autenticación y privacidad de la información entre extremos.



3. Arquitectura

IPsec

IPsec se halla constituido por dos protocolos de seguridad de tráfico: IP Authentication Header **(AH)** que proporciona integridad, IP Encapsulating Security Payload **(ESP)** que proporciona confidencialidad, con la implementación de IPsec modo túnel en el escenario de prueba el protocolo utilizado para establecer la comunicación segura es ESP, muestra en detalle cada una de las partes que lo integran permitiendo garantizar la confidencialidad y la integridad de la comunicación de voz.



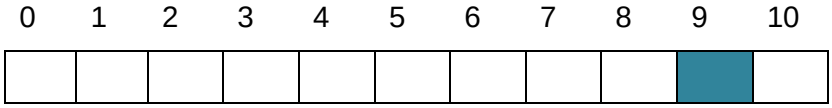
SSL

SSL se introduce como una especie de nivel o capa adicional, situada entre la capa de Aplicación y la capa de Transporte, sustituyendo los sockets del sistema operativo, lo que hace que sea independiente de la aplicación que lo utilice.

El protocolo de registro se encarga de encapsular el trabajo delos elementos de la capa superior, construyendo un canal seguro de comunicaciones entre losdos extremos objeto de la comunicación.

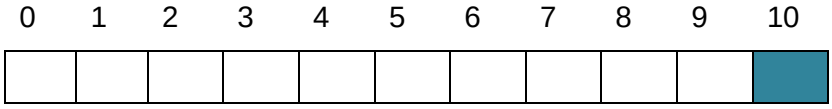
Al realizar las pruebas en el escenario este indica que se estableció la comunicación a través del protocolo TCP indicando con esto que la llamada llega a su destino; indica además el puerto de destino establecido para la VPN; este puerto es configurado

tanto en el servidor como en cada uno de los clientes para redireccionar el tráfico con esto garantiza la confidencialidad de la comunicación de voz.



TLS

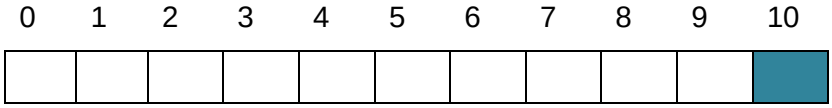
Con la implementación de TLS como técnica de seguridad para garantizar la integridad y confidencialidad de la comunicación de voz en el escenario de prueba, este indica que la comunicación se estableció por el puerto 5061 con el protocolo de transporte TCP y el protocolo de seguridad TLS el mismo que no permite que la comunicación sea interceptada.



4. Interoperabilidad

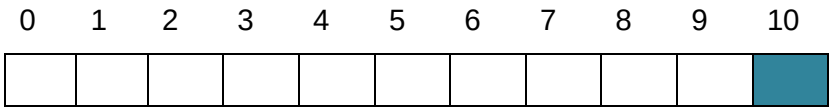
IPsec

IPsec es una parte obligatoria de IPv6, y su uso es opcional con IPv4. Aunque el estándar está diseñado para ser indiferente a las versiones de IP.



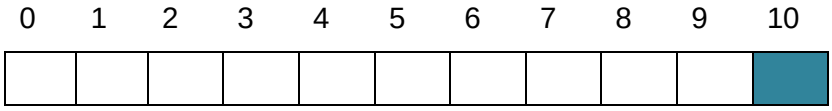
SSL

SSL es interoperable tanto en IPv4 como en IPv6, la gran mayoría de transacciones comerciales que se realizan hoy en día en la red se protegen mediante SSL.



TLS

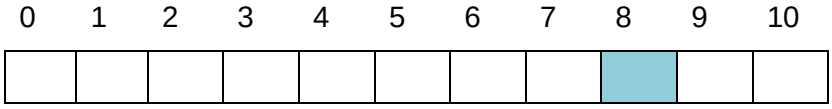
Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través del protocolo IPv4 o IPv6.



5. Protocolo de transporte sobre el cual funciona

IPsec

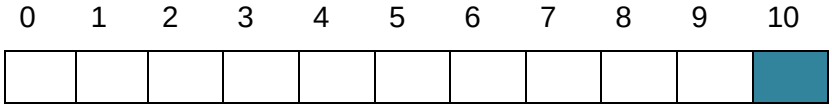
IPsec provee seguridad a protocolos de capas superiores UDP y TCP los protocolos de transporte más usados, al trabajar con UDP es posible que la comunicación no llegue a su destino.



SSL

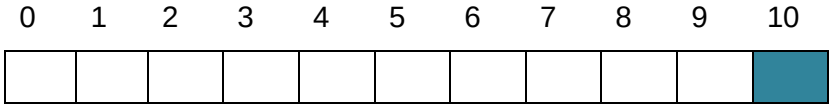
SSL es capaz de trabajar de forma transparente con todos los protocolos que trabajan sobre TCP, es decir protocolos orientados a la conexión lo que garantiza que la comunicación llegará a su destino.

Opera entre la capa de transporte y la de sesión del modelo OSI (o entre lacapa de transporte y la de aplicación del modelo TCP)



TLS

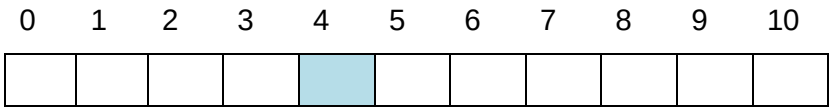
Usado para proteger protocolos orientados a la conexión como TCP, esta característica permitirá que la información llegue a su destino.



6. Implementación

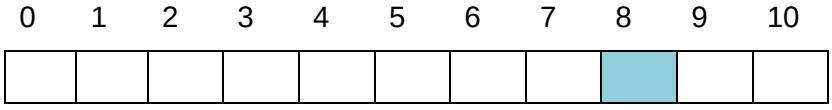
IPsec

La implementación de IPsec es sumamente complejo pues para hacerlo primero se debe corroborar que los equipos a utilizar posean soporte para la implementación del mismo, además de ello se debe seguir un conjunto de pasos en forma secuencial sin olvidarlos para obtener una correcta implementación. IPSec ha sido postulado en ocasiones como sucesor o competidor de SSL. Sin embargo su mayor complejidad en cuanto a implantación y mantenimiento reducen su ámbito de actuación



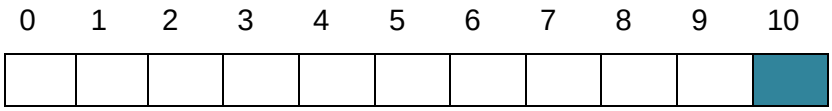
SSL

La gran difusión del protocolo, y su implantación por parte de administradores de sistemas para la seguridad de la información y la transparencia para el usuario que, en la mayoría de los casos ni siquiera se entera de que lo está usando lo ha convertido en el protocolo dominante. Sin embargo la implementación de SSL resulta un tanto tediosa ya que se debe crear certificados tanto para el servidor como para cada uno de los clientes que se desee que se conecte por este medio para establecer la comunicación, sin olvidar que además se debe copiar en cada cliente el certificado del servidor al cual se va a conectar y el certificado del cliente con su respectiva clave.



TLS

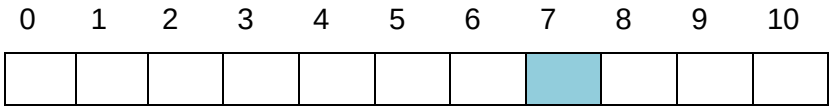
La facilidad de implantación lo ha convertido en una solución sumamente aceptada en la seguridad de la información ya que la mayoría de las aplicaciones TLS basan su implementación en certificados X.509, los cuales proveen un estándar y son utilizados ampliamente en diferentes aplicaciones. Además no es necesario crear certificados para el cliente que se va a conectar es suficiente con la instalación del certificado del servidor en el equipo que será cliente.



7. Encriptación

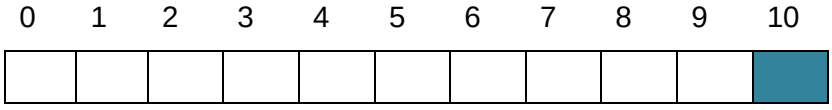
IPsec

IPsec utiliza principalmente el protocolo IKE para generar las claves, es más flexible pero necesita más esfuerzo para su configuración tanto software como hardware.Se ha implementado IPSec utilizando el algoritmo de encriptación aes 256, el hash sha y claves pre-compartidas esto hace que sea vulnerable a intrusos que puedan conocer la clave.



SSL

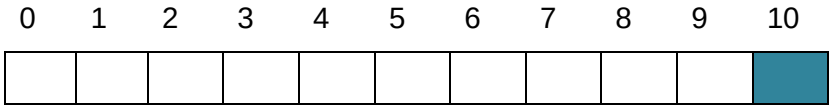
Utiliza clave pública para cifrar la comunicación, es flexible no requiere de mucho esfuerzo para su configuración.Durante la transmisión de datos los mensajes son fragmentados y comprimidos por el protocolo de registro antes de su envío y descomprimidos y reconstruidos por el mismo protocolo al otro extremo de la comunicación. Utiliza para generar las claves el algoritmo RSA 1024, el parámetro Diffie-Hellman para el intercambio de claves entre las dos partes sin que estas hayan tenido contacto previo, de esta manera se garantiza que se establece un canal seguro para realizar la comunicación.



TLS

TLS se basa en algoritmos que permiten establecer una conexión segura entre un cliente y un servidor.La autenticación de usuarios de basa en el uso de certificados digitales para establecer la comunicación. Se creó el certificado autofirmado necesario para la autenticación de los dispositivos, para ello se generó la clave con el algoritmo rsa 1024 y luego el certificado firmado con la clave creada anteriormente con la ayuda

de certificado x.509, esto posibilita que se establezca un canal seguro de comunicación evitando que intrusos puedan interceptar la llamada.



8. Servicios

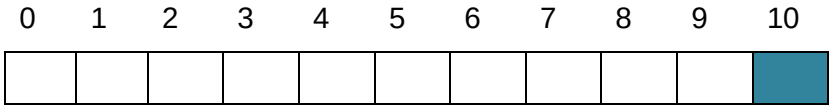
IPsec

Confiabilidad de datos.- Los paquetes enviados son cifrados antes de ser enviados a través de la red.

Integridad de datos.- El que recibe los paquetes puede autentificar al que envía y asegurarse que el paquete no haya sido modificado.

Autentificación de los datos de origen.- El que recibe los datos puede autentificar el origen de los paquetes IPsec enviados.

No repetición.- El que recibe los paquetes IPsec puede detectar y rechazar paquetes retransmitidos.



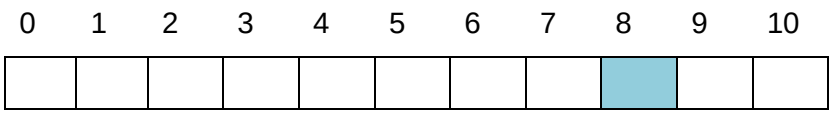
SSL

Confiabilidad de datos.-la fase operativa de intercambio de datos se realiza mediante encriptación y des-encriptación de clave privada.

Integridad de datos.- La integridad de los datos se ve reflejada ya que se utiliza claves secretas para cada función

Autenticación de los datos de origen.- Se utilizan certificados X.509 para la autenticación. Los certificados de servidores son obligatorios, mientras que los de cliente son opcionales.

No repetición.- No posee esta característica



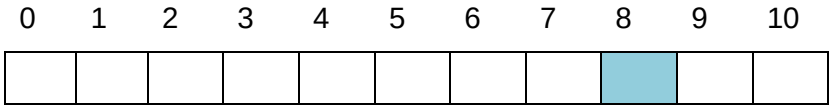
TLS

Confiabilidad de datos. Esta característica se basa en que para que los datos se transmita se debe establecer un conexión segura.

Integridad de datos. La integridad de los datos en TLS se basa en un proceso de cifrado de clave pública que garantiza la seguridad de los datos que se envían.

Autenticación de los datos de origen Cada paquete enviado en una conexión TLS, va cifrado,

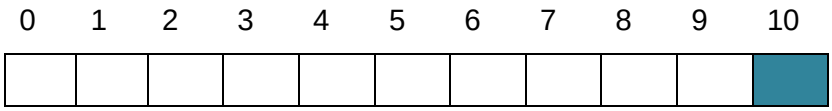
No repetición. No goza de esta característica



9. Integridad

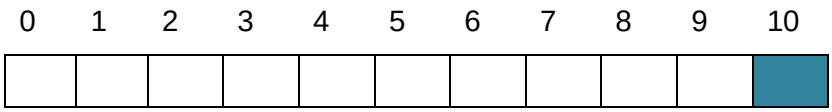
IPsec

La integridad de datos garantiza que no se han modificado los paquetes durante el trayecto para ello IPsec crea túneles para establecer la comunicación haciendo posible que los intrusos no sean capaces de interceptar la comunicación y puedan alterar su contenido.



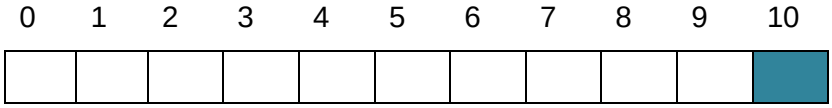
SSL

SSL proporciona servicios de seguridad a la pila de protocolos, encriptando los datos salientes de la capa de Aplicación antes de que estos sean segmentados en la capa de Transporte y encapsulados y enviados por las capas inferiores, proporciona integridad ya que utiliza en conjunción certificados digitales en ambos extremos.



TLS

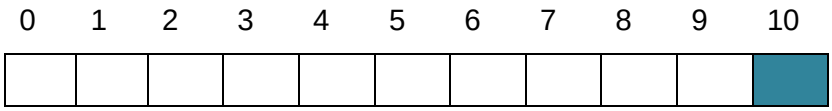
Utiliza certificados digitales en los dos extremos de la comunicación además de cifrar los datos que se van a transmitir proporcionado integridad a los mismos.



10. Confidencialidad

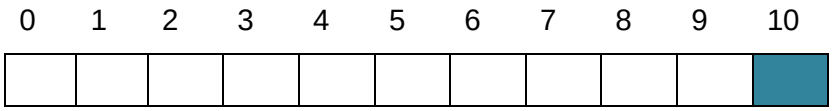
IPsec

En donde la confidencialidad de datos protege a los paquetes de suplantación, para ello IPsec emplea cifrado.IPSec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP. IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.



SSL

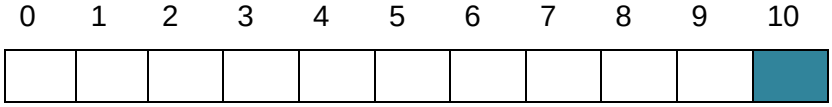
Crear un canal de comunicaciones seguro entre un cliente y un servidor independiente del sistema operativo usado por ambos y que se beneficiara de forma dinámica y flexible de los nuevos adelantos en materia de cifrado a medida de que estos esten disponibles.



TLS

La confidencialidad consiste en intercambiar paquetes con datos cifrados mediante claves simétricas. Al inicio de cada sesión, cliente y servidor se ponen de acuerdo en que claves utilizarán para cifrar los datos. Siempre se utilizan dos claves distintas: una para los paquetes enviados del cliente al servidor, y la otra para los paquetes enviados en sentido contrario.

Se establece la conexión, y antes de la autenticación del usuario, queda establecido un canal cifrado seguro.



Resultados

A continuación la tabla muestra los resultados obtenidos del análisis realizado a las técnicas de seguridad basándose en las variables.

Tabla IV.IX. Resultado del Análisis Comparativo

VARIABLES	TECNICAS		
	IPsec	SSL	TLS
Capa en la que opera	10	9	9
Estándar	10	6	10
Arquitectura	10	9	10
Interoperabilidad	10	10	10
Protocolo de transporte sobre el cual funciona	8	10	10
Implementación	4	8	10
Encriptación	7	10	10
Servicios	10	8	8
Integridad	10	10	10
Confidencialidad	10	10	10
PARCIAL	89	90	97
# MUESTRAS	10	10	10
TOTAL	8.9	9.0	9.7

La principal diferencia que se da entre las técnicas radica en el grado de dificultad en su implementación pues IPsec es bastante compleja, la implementación de SSL se

basa en VPNpor ende resulta compleja mientras que la implementación de TLS es sumamentesimple haciéndolo ampliamente aceptable.

4.3. Análisis de Resultados.

Frente a esto se obtiene resultados óptimos de seguridad, puesto que ya no es posible que la comunicación sea interceptada y utilizada con fines maliciosos que comprometan la integridad y la confidencialidad de la misma.

Las tres técnicas implementadas obtuvieron una calificación de excelente pues se ubicaron en el rango de 9-10, ya que cada una de ellas cumple el propósito de la mantener la integridad y la confidencialidad de la comunicación, pero la técnica que más se adapta es TLS por su facilidad al momento de la implementación.

Las calificaciones obtenidas por cada una de las técnicas en porcentaje se definen así:

10 es el 100%

IPsec

10 100

8.9 X= $\frac{8.9 \times 100}{10}$ = 89 %

SSL

10 100

9.0 X= $\frac{9.0 \times 100}{10}$ = 90 %

TLS

10 100

9.7 X= $\frac{9.7 \times 100}{10}$ = 97 %

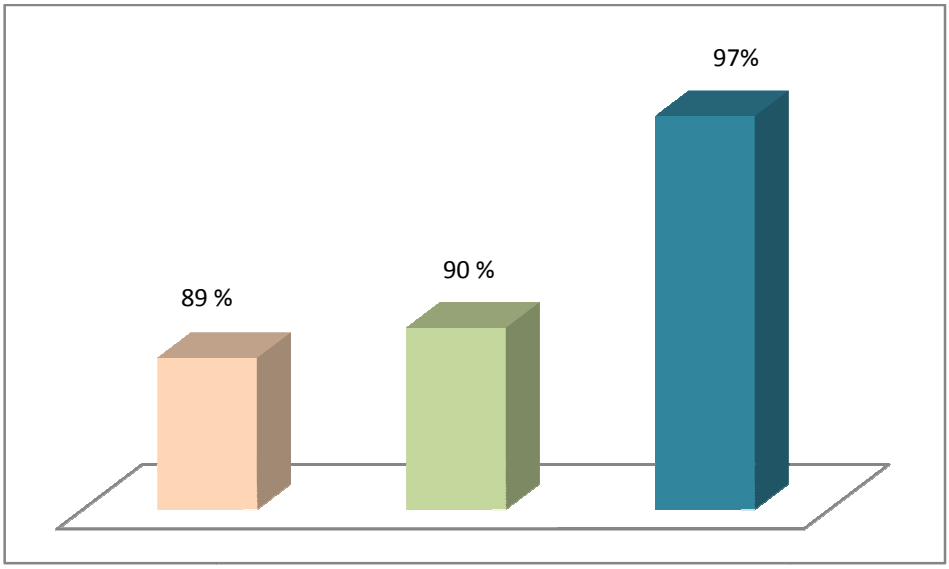


Figura.IV.56. Resultado Análisis Comparativo

4.4. Comprobación de la Hipótesis

Para la comprobación de la Hipótesis planteada para el desarrollo de la Tesis se utiliza una Encuesta, la misma que permite conocer el desempeño de la técnica escogida como la más adecuada para mantener la integridad y confidencialidad en la comunicación de voz en Telefonía IP.

Las preguntas serán evaluadas mediante una escala de 0 y 1 definida de la siguiente manera:

Tabla VI.X. Valoración de Preguntas

Numeración	0	1
Equivalente	No	Si

4.4.1. Hipótesis

La protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas conseguirá confidencialidad e integridad en la comunicación de voz.

4.4.2. Tipo de Hipótesis

Hipótesis de Investigación

4.4.3. Población y Muestra

La encuesta (***Ver Anexo 2***) se aplicó a los estudiantes que ingresan y personal que se encuentra a cargo del Laboratorio de la Academia Local de Redes Cisco ESPOCH, siendo realizadas 10 encuestas en su totalidad.

4.4.4. Operacionalización de variables

Variable Independiente

Protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas

Variable Dependiente

Confidencialidad e integridad en la comunicación de voz.

4.4.5. Operacionalización conceptual

Tabla IV.XI. Operacionalización Conceptual

Variable	Tipo	Concepto
Protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas	Independiente	Analizar diferentes técnicas de seguridad que permite proteger el tráfico en telefonía IP con la utilización del protocolo SIP para establecer la comunicación.
Confidencialidad e integridad en la comunicación de voz.	Dependiente	Garantizar que la comunicación no sea interceptada por un intruso y utilizada con fines maliciosos.

4.4.6. Operacionalización metodológica

Tabla IV.XII. Operacionalización Metodológica

Variable	Categoría	Indicadores	Técnicas	Fuentes de Verificación
Protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas	Actividad Investigación	Análisis de diferentes técnicas de seguridad	Revisión de documentos	Internet
Confidencialidad e integridad en la comunicación de voz.	Actividad Investigación	No interceptación de la comunicación No escucha de la comunicación	Observación directa	Laboratorio de la Academia de Redes Locales Cisco-ESPOCH

4.4.7. Comprobación de la hipótesis de la investigación realizada

4.4.7.1. Planteamiento de la hipótesis

Ho. “La protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas no conseguirá confidencialidad e integridad en la comunicación de voz”

Hi. “La protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas conseguirá confidencialidad e integridad en la comunicación de voz”

4.4.7.2. Nivel de significancia

Una vez establecida la hipótesis nula y alternativa, se debe determinar el nivel de significancia, que para el caso del presente análisis se utiliza un nivel de significación estadística de **0.05,** para obtener un nivel de confianza aceptable.

4.4.7.3. Criterio

Para el análisis de los resultados se ha seleccionado la técnica T-Student como estadístico de prueba de la hipótesis planteada. La fórmula es la siguiente:

$$t = \frac{\overline{X1} - \overline{X2}}{\sqrt{\frac{S^2 1}{n1} + \frac{S^2 2}{n2}}}$$

En donde "$\overline{X1}\ y\ \overline{X2}$" son los valores de la mediay $S^2 1\ y\ S^2 2$ son la varianzasmuéstrales.

Se debe determinar el **criterio de decisión**. Entonces se acepta **Ho** cuando:
$t_{tabla} < t_{calculado}$

Donde el valor de t_{tabla} representa el valor proporcionado por la tabla de "distribución t-Student", según el nivel de significación elegido y los grados de libertad.

Para determinar los grados de libertad **(gl)** se debe aplicar la siguiente fórmula:

$$gl = \frac{\left(\frac{S^2 1}{n1} + \frac{S^2 2}{n2}\right)^2}{\frac{\left(\frac{S^2 1}{n1-1}\right)^2}{n1} + \frac{\left(\frac{S^2 2}{n2-1}\right)^2}{n2}} - 2$$

Donde n1 y n2 son el tamaño de la muestra de cada grupo.

4.4.7.4. Cálculos

Los resultados que se presentan a continuación son los que arrojó la investigación realizada.

Tabla IV.XIII. Resultados de la encuesta sobre Confidencialidad

CONFIDENCIALIDAD				
Pregunta	**Con la técnica de seguridad TLS**		**Sin la técnica de seguridad**	
	Garantiza	**No garantiza**	**Garantiza**	**No garantiza**
1	10	0	0	10
2	10	0	0	10
TOTAL	20	0	0	20

Tabla IV.XIV. Resultados de la encuesta sobre Integridad

INTEGRIDAD				
Pregunta	**Con la técnica de seguridad TLS**		**Sin la técnica de seguridad**	
	Garantiza	**No garantiza**	**Garantiza**	**No garantiza**
3	10	0	0	10
4	10	0	0	10
TOTAL	20	0	0	20

Tabla IV.XV. Resultados de la encuesta sobre Calidad

CALIDAD AFECTADA				
Pregunta	**Con la técnica de seguridad TLS**		**Sin la técnica de seguridad**	
	Garantiza	**No garantiza**	**Garantiza**	**No garantiza**
5	7	3	10	0
6	7	3	10	0
TOTAL	14	6	20	0

Tabla para obtener el valor de la distribución t-Student para la comprobación de la hipótesis.

Tabla IV.XVI. Resultados Generales

Preguntas	Con técnica de Seguridad	Sin técnica de seguridad	$X1-\overline{X1}$	$X2-\overline{X2}$	$(X1-\overline{X1})^2$	$(X2-\overline{X2})^2$
1	10	0	1	-3	1	9
2	10	0	1	-3	1	9
3	10	0	1	-3	1	9
4	10	0	1	-3	1	9
5	7	10	-2	7	4	49
6	7	10	-2	7	4	49
	$\overline{X1}$=9	$\overline{X2}$=3			12	137

Valor de las varianzas:

$$S^2 1 = \frac{12}{9} = 1.33$$

$$S^2 2 = \frac{137}{9} = 15.22$$

Aplicando t-Student

$$t = \frac{9 - 3}{\sqrt{\frac{1.33}{10} + \frac{15.22}{10}}} = 4.69$$

Valor de grados de libertad

$$gl = \frac{\left(\frac{1.33}{10} + \frac{15.22}{10}\right)^2}{\frac{\left(\frac{1.33}{9}\right)^2}{10} + \frac{\left(\frac{15.22}{9}\right)^2}{10}} - 2 = 8$$

De acuerdo a la tabla estadística de distribución t-Student, con un nivel de significancia 0,05 a 8 grado de libertad, genera un valor de **t_{tabla} = 0.815 (*Ver Anexo 5*)**

4.4.7.5. Decisión

Como:

$t_{calculado}$ = 4,69 y t_{tabla}= 0.815

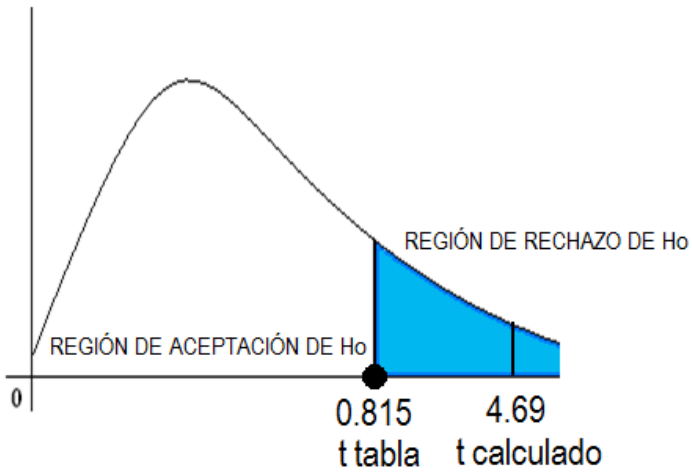


Figura VI.57. Demostración de la Hipótesis

Entonces:

$$t_{calculado} < t_{tabla}$$

Se concluye que se rechaza la hipótesis nula por encontrarse fuera del área de aceptación y se acepta la hipótesis alternativa de la investigación:

“La protección de tráfico SIP en redes de Telefonía IP a través del análisis de técnicas de seguridad en Redes Corporativas conseguirá confidencialidad e integridad en la comunicación de voz”

4.4. Propuesta metodológica

Se basa en los aspectos necesarios paraimplementar seguridad en Redes de Telefonía IP que garanticen la confidencialidad e integridad de la comunicación de voz.

Alcance

Brindar seguridad en la comunicación de voz en telefonía IP en redes Corporativas garantizando la integridad y la confidencialidad de la misma para evitar que la información sea utilizada con fines maliciosos. Todos los pasos necesarios para este fin están detallados en el Manual de Usuario ***(Ver Anexo 4).***

Caracterización

Implementar TLS

- Instalar Openssl
- Crear certificado
- Configurar el cliente para que use TLS

Con el fin de garantizar la integridad y la confidencialidad de la comunicación de voz en redes de Telefonía IP.

Política

Implementar TLS en la central telefónica PBX Elastix.

- Instalación de la central PBX Elastix 2.0.3 en un computador.
- Crear usuarios en la central Elastix.

La misma que permite crear usuarios que hagan uso de la telefonía IP para establecer las llamadas de forma segura, a la vez que permita reducir los costos para las empresas que lo implementen.

Para los usuarios que utilicen TLS es necesario que los mismos soporten este protocolo; por lo cual los usuarios serán creados en computadoras con la ayuda del softphone phonerlite.

- Instalación del Softphone PhonerLite
- Configuración de los usuarios en el softphone.

TLS permite que se establezca la comunicación cuando existe un canal seguro entre los nodos, por ello es indispensable que los dos extremos se encuentren configurados con este protocolo para poder establecer el canal seguro y así realizar la llamada sin tener la dificultad de que la comunicación sea interceptada por un intruso.

Seguridad

Para la implementación de TLS es necesario hacer uso de OpenSSL para poder crear los certificados a través de X.509, los mismos que serán utilizados por los usuarios creados con la ayuda del softphone.

De esta manera serán autentificados los usuarios que posean el certificado para evitar que usuarios que se configuren con la misma extensión que se halla configurado para que utilice TLS pueda conectarse a la central sin ninguna dificultad.

Los recursos que se utilizan para implementar TLS es principalmente un servidor asterisk, instalar el software OpenSSL y configurar TLS en las extensiones que se desee que utilicen este protocolo para la comunicación.

- Configurar el archivo sip_general_custom.conf
- Configurar el archivo sip_general_custom.conf

Auditorio

Esta metodología está dirigida en primer lugar a aquellas personas que están responsabilizadas para implementar seguridad en redes de telefonía IP, a los administradores de PBX, especialistas en informática, debido a los conocimientos técnicos que poseen y los profesionales de la seguridad y protección, por su experiencia y conocimientos generales de esta especialidad.

Localización

Esta implementado en un escenario de prueba en la Academia de Redes Locales Cisco-ESPOCH, en el cual se realizó las pruebas para determinar que la implementación de TLS en Telefonía IP en redes Corporativas conseguirá la confidencialidad y la integridad de la comunicación.

CONCLUSIONES

- La gran ventaja del protocolo SIP es su sencillez pero se ve limitado en establecer comunicación segura ya que no posee mecanismos de seguridad y esta se puede ver alterada y sustraída con fines maliciosos.

- Es indispensable tomar medidas de seguridad al implementar un sistema VoIP, las técnicas analizadas en esta investigación son eficaces para cumplir las funciones para lo cual fueron implementados.

- Al implementar el escenario de prueba en el Laboratorio de la Academia de Redes Locales Cisco con cada una de las técnicas que brinda seguridad en Telefonía IP, y al realizar el análisis de las características y evaluar sus resultados se llegó a la conclusión que la técnica más adecuada para establecer una comunicación segura y garantizar la integridad y confidencialidad de la comunicación de voz en redes Corporativas es TLS ya que alcanzó el 97%, frente a IPsec que alcanzó el 89% y SSL alcanzó el 90% , la principal diferencia que existe entre las tres técnicas es su implementación pues TLS es sumamente simple.

- La propuesta metodológica está enfocada a la implementación de TLS para establecer una comunicación segura en Telefonía IP en Redes Corporativas y mantener la integridad y confidencialidad de la comunicación. Para ello se propone el uso de software OpenSSL para generar el certificado que ayuda a la autenticación de los dispositivos yel uso del softphone phonerlite para la configuración de los usuarios TLS.

RECOMENDACIONES

- Se recomienda que la implementación de IPsec se realice como un servidor con la ayuda del software Openswan o Freeswanpara garantizar la confidencialidad de la comunicación de voz.

- Que la implementación de TLS se realice en la red de Telefonía IP de la Escuela Superior Politécnica de Chimborazo para garantizar la integridad y confidencialidad de la comunicación de voz.

- Para tener una buena recepción y transmisión de audio aprovechando el potencial que ofrece TLS se recomienda utilizar equipos que soporten este protocolo.

RESUMEN

La investigación realizada está orientada al análisis comparativo de Técnicas de Seguridad en Telefonía IP en Redes Corporativas, para seleccionar la más adecuada y aplicarla con la finalidad de garantizar la confidencialidad y la integridad de la comunicación de voz.

Para la presente investigación se utilizó los métodos Inductivo-Deductivo, Científico, Experimental y Comparativo. De acuerdo a la implementación de cada una de las técnicas que proporcionan seguridad en telefonía IP en un escenario de prueba en la Academia de Redes Locales Cisco-ESPOCHy al análisis comparativo realizado mediante los parámetros: Capa en la que operan, Estándar, Arquitectura, Interoperabilidad, Protocolo de transporte que usa para establecer la conexión, Implementación, Encriptación, Servicios, Integridad y Confidencialidad, se pudo concluir que TLS con el 97% es la mejor opción para cumplir con los objetivos de la investigación y por su sencillez en el momento de implementarla con OpenSSL en Asterisk 2.0.3 PBX.

La implantación de esta técnica, garantiza la confidencialidad e integridad de la comunicación de voz, además permite tener una calidad adecuada para realizar las llamadas entre los usuarios de la central.

En la actualidad es necesario implementartécnicas de seguridad en telefonía IP, para evitar que la comunicación establecida entre dos usuarios de la central sea interceptada y usada con fines maliciosos que afecten la integridad de la misma.

SUMMARY

The carried out investigation is guided to the comparative analysis of Technical of Security in Telephony IP in Corporate Network, to select the most appropriate and to apply it with the purpose of guaranteeing the confidentiality and the integrity of the voice communication.

For the present investigation it was used the Inductive-deductive, Scientific, Experimental and Comparative methods. According to the implementation of each one of the techniques that provide security in telephony IP in a test scenario in the Local Network Academy Cisco-ESPOCH and to the comparative analysis carried out by means of the parameters: It castrates in the one that operate, Standard, Architecture, Interoperability, Protocol of transport that it uses to establish the connection, Implementation, Encryption, Services, Integrity and Confidentiality, you could conclude that TLS with 97% is the best option to fulfill the objectives of the investigation and for its simplicity in the moment to implement it with OpenSSL in Asterisk 2.0.3 PBX.

The installation of this technique, guarantees the confidentiality and integrity of the voice communication, he/she also allows to have an appropriate quality to carry out the calls among the users of the power station.

At the present time it is necessary to implement technical of security in telephony IP, to avoid that the established communication between two users of the power station are intercepted and used with malicious ends that affect the integrity of the same one.

GLOSARIO

Alternativa: Acción o derecho que tiene cualquier persona o comunidad para ejecutar algo o gozar de ello alternando con otra.

Análisis: Estudio, mediante técnicas informáticas, de los límites, características y posibles soluciones de un problema al que se aplica un tratamiento por ordenador

Autenticación: Asegurar que sólo los individuos autorizados tengan acceso a los recursos, consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite garantizar el acceso a recursos únicamente a las personas autorizadas.

Clave: Una clave es número codificado y encriptado en un archivo que sirve para encriptar/desencriptar los mensajes transmitidos/enviados.

Clave Privada: Criptografía de claves simétricas o también llamada criptografía de clave privada. Este sistema criptográfico requiere que las dos partes que intervienen hayan intercambiado previamente una clave para cifrar y descifrar la información.

Clave Pública: Criptografía de claves asimétricas o también llamada de clave pública. Conocida por sus siglas en ingles PKI. Utiliza dos claves diferentes para cada una de las partes que intervienen en la comunicación. Una clave es pública y la otra privada, la pública se usa para cifrar la información y la privada para descifrarla.

Confidencialidad: Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian, consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación

Entidad: Lo que constituye la esencia o la forma de una cosa

Estándar: Conjunto de especificaciones técnicas utilizadas para unificar el desarrollo de hardware o de software.

Implementar: Poner en funcionamiento, aplicar métodos, medidas, etc., para llevar algo a cabo.

Integrar: Constituir un todo

Integridad: Garantizar que los datos sean los que se supone que son, es decir no hayan sido alterados durante la transmisión

Network Server: Son los encargados de procesar peticiones SIP provenientes de los UA y generar alguna respuesta.

Red Informática: Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros ordenadores.

RTP: Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real.

SA: Las asociaciones de la seguridad (SA) son acuerdos entre los pares de la comunicación.

SDP: El protocolo SDP describe las sesiones multimedia para propósitos de aviso de sesión, invitaciones de sesión, y otras formas de iniciación de sesiones multimedia. El SDP es utilizado por protocolos de señalización

Spoofing: Es el uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

TCP: Permite crear conexiones entre varios programas que usan la red de datos compuesta por computadoras a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

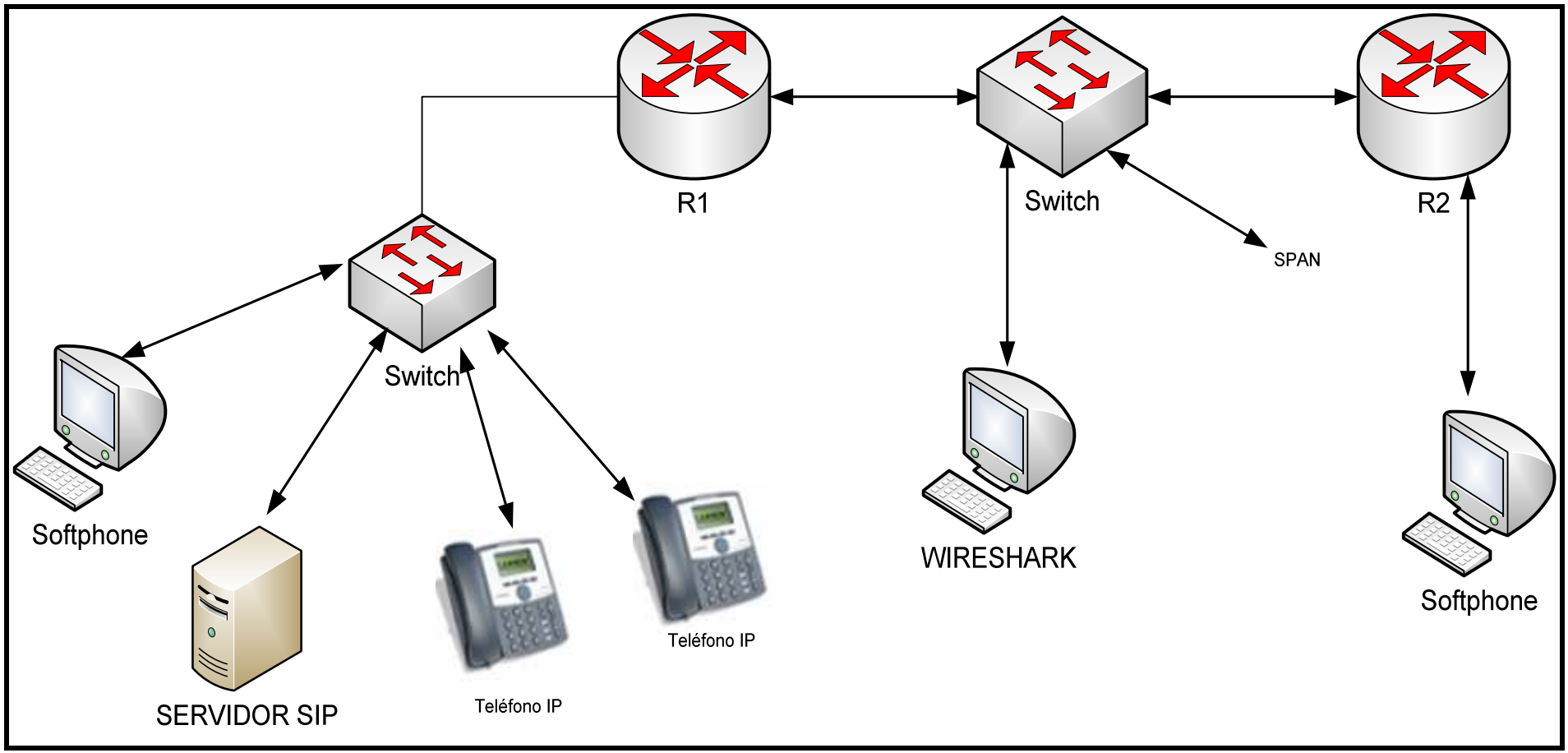
Teléfono IP: Es un teléfono similar a un teléfono tradicional con la diferencia que está adaptado para ser utilizado en entornos IP.

UDP: (User Datagram Protocol) Protocolo abierto, no orientado a la conexión y por lo que no establece un diálogo previo entre las dos partes, ni tampoco mecanismos de detección de errores. Generalmente se emplea en lugar del TCP, cuando no se necesitan fuertes controles en la comunicación de los datos. Brinda mayor velocidad y menos complejidad.

ANEXOS

ANEXO 1

ESQUEMA DE LA RED


R1
Switch
R2
SPAN
Switch
Softphone
WIRESHARK
Softphone
SERVIDOR SIP
Teléfono IP
Teléfono IP

ANEXO 2

ENCUESTA

ENCUESTA

Objetivo: La siguiente encuesta se aplica para comprobar la hipótesis de la tesis titulada, **"PROTECCIÓN DE TRÁFICO SIP EN REDES DE TELEFONÍA IP A TRAVÉS DEL ANÁLISIS DE TÉCNICAS DE SEGURIDAD EN REDES CORPORATIVAS",** implementado en un escenario de prueba en el laboratorio de la Academia de Redes Locales CISCO-ESPOCH

Por favor complete la encuesta cuidadosamente y con la mayor franqueza, señale sus respuestas con una "X".

1. Con la captura de los paquetes con el sniffer Wireshark durante la comunicación establecida entre dos usuarios de la central PBX se da la interceptación de la conversación.

Sin técnica de seguridad		**Con la técnica de seguridad TLS**	
Si	☐	Si	☐
No	☐	No	☐

2. Al reproducir la conversación capturada con la ayuda del sniffer wireshark establecida entre dos usuarios de la PBX, se producela escucha de la conversación.

Sin técnica de seguridad		**Con la técnica de seguridad TLS**	
Si	☐	Si	☐
No	☐	No	☐

3. Considera usted que el nivel de seguridad establecido para realizar llamadas entre 2 usuarios de la central PBX compromete la integridad de la comunicación.

Sin técnica de seguridad		**Con la técnica de seguridad TLS**	
Si	☐	Si	☐
No	☐	No	☐

4. Considera usted que al establecer la comunicación de voz por un canal seguro de transmisión, ésta podría ser manipulada deliberadamente.

Sin técnica de seguridad		**Con la técnica de seguridad TLS**	
Si	☐	Si	☐
No	☐	No	☐

5. Considera usted que al realizar la llamada entre dos usuarios de la central, la calidad de la voz es afectada.

Sin técnica de seguridad		**Con la técnica de seguridad TLS**	
Si	☐	Si	☐
No	☐	No	☐

6. Durante el período de comunicación establecido entre dos usuarios de la central PBX existe ruido:

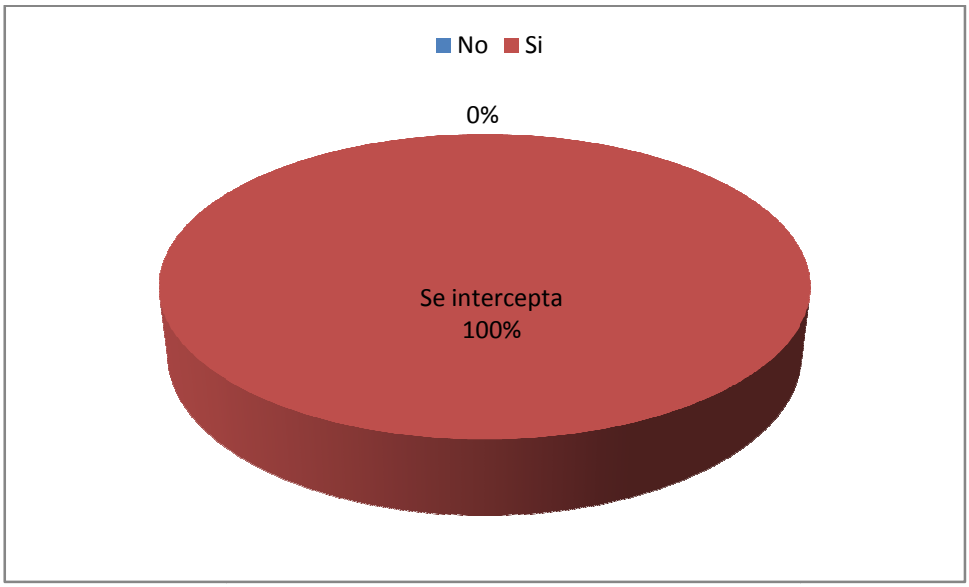
Sin técnica de seguridad		**Con la técnica de seguridad TLS**	
Si	☐	Si	☐
No	☐	No	☐

ANEXO 3

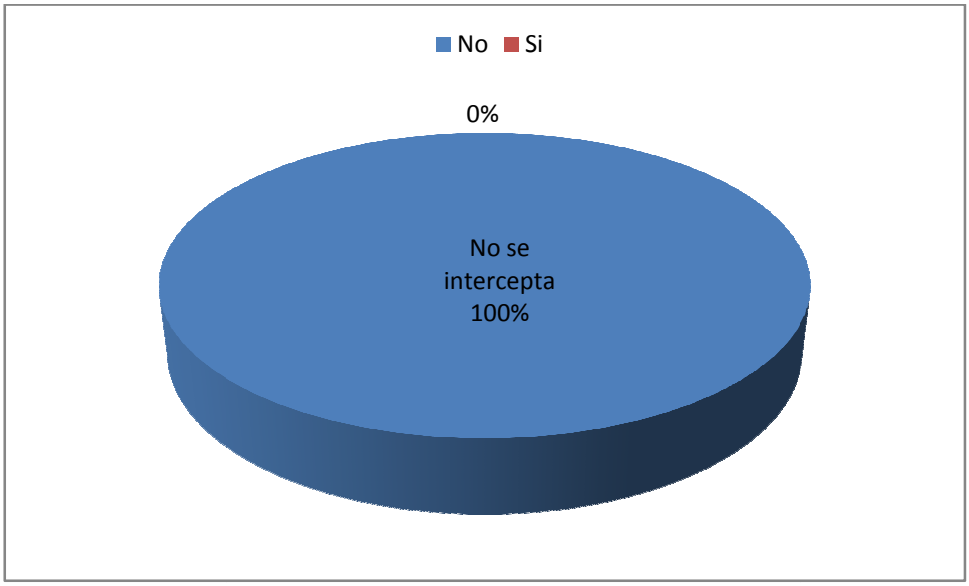
TABULACIÓN DE LA ENCUESTA

1. Con la captura de los paquetes con el sniffer Wireshark durante la comunicación establecida entre dos usuarios de la central PBX se da la interceptación de la conversación.

Sin la Técnica de Seguridad

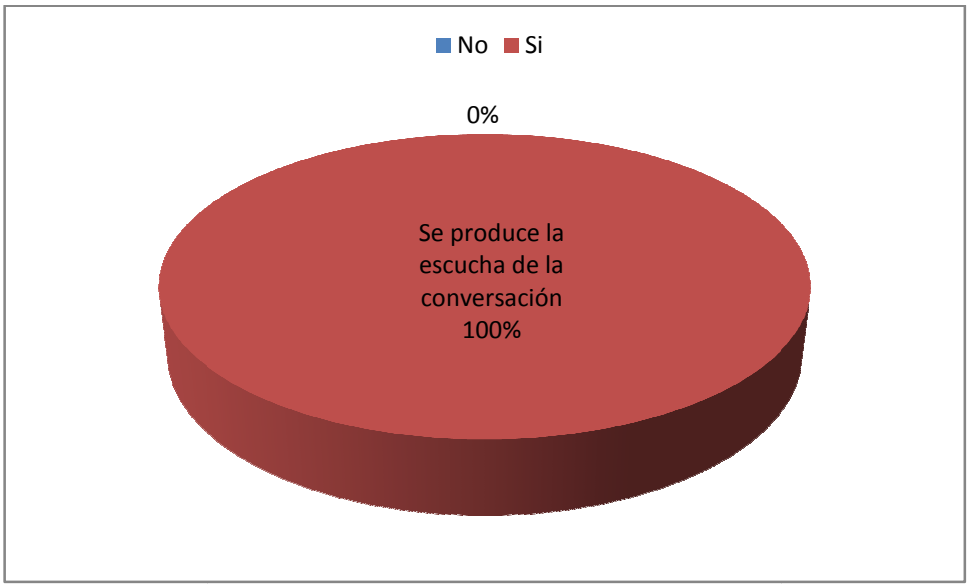


Con la Técnica de Seguridad TLS

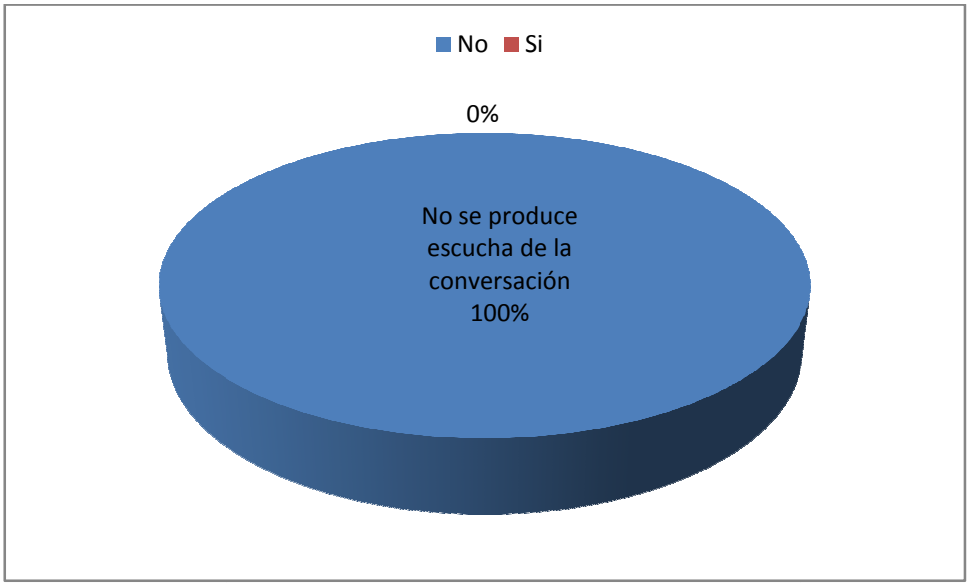


2. Al reproducir la conversación capturada con la ayuda del sniffer wireshark establecida entre dos usuarios de la PBX, se produce la escucha de la conversación.

Sin la Técnica de Seguridad

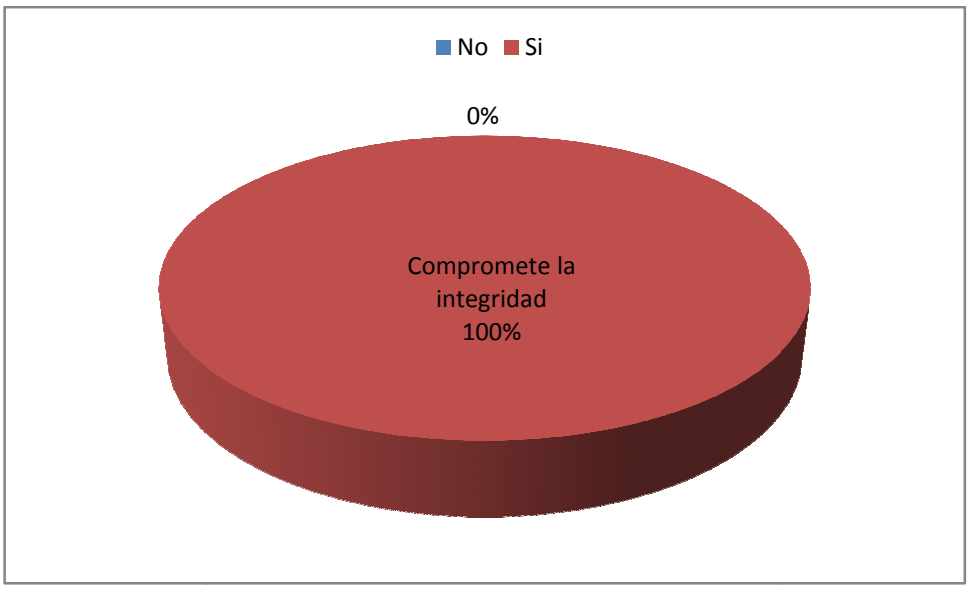


Con la Técnica de Seguridad TLS

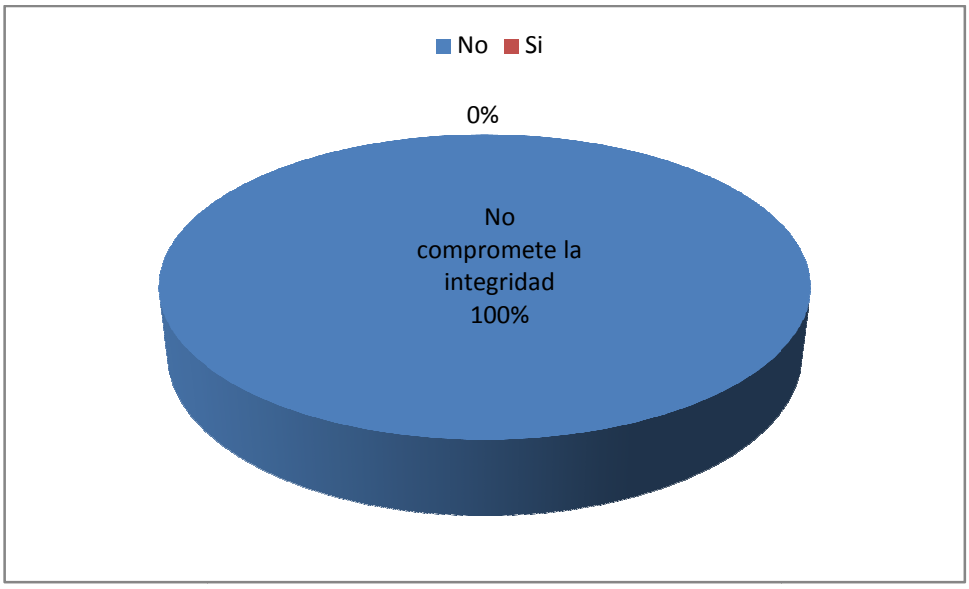


3. Considera usted que el nivel de seguridad establecido para realizar llamadas entre 2 usuarios de la central PBX compromete la integridad de la comunicación.

Sin la Técnica de Seguridad

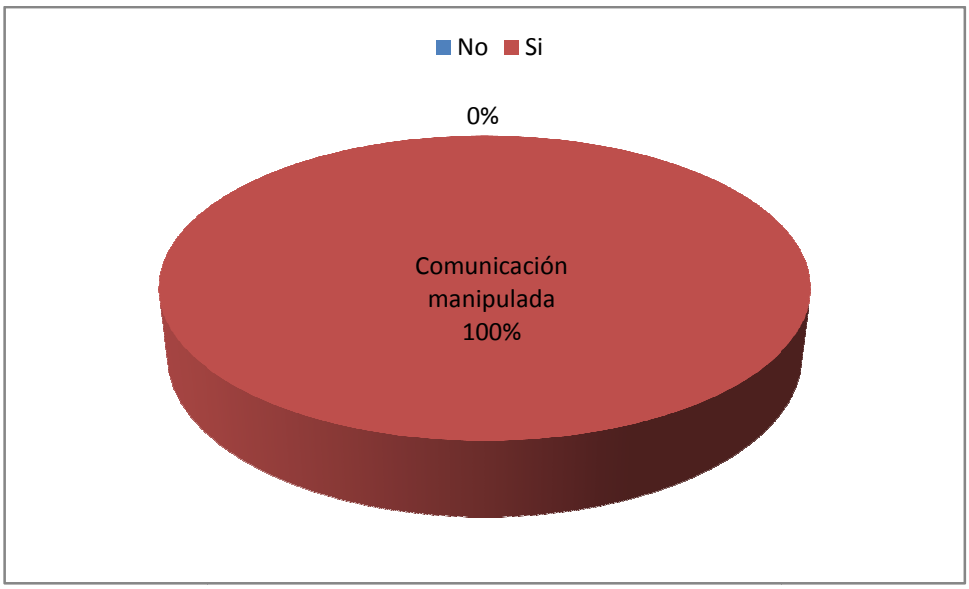


Con la Técnica de Seguridad TLS

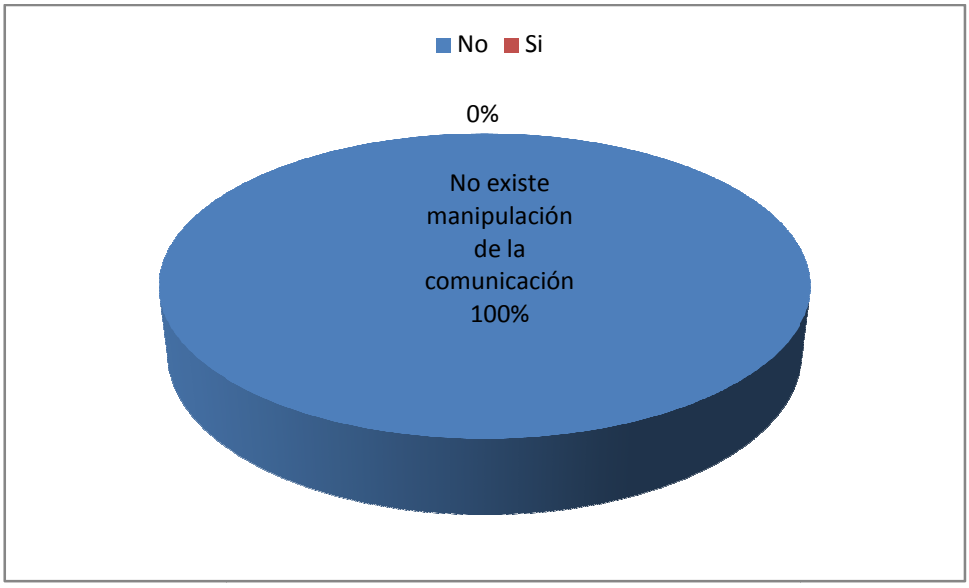


4. Considera usted que al establecer la comunicación de voz por un canal seguro de transmisión, ésta podría ser manipulada deliberadamente.

Sin la Técnica de Seguridad

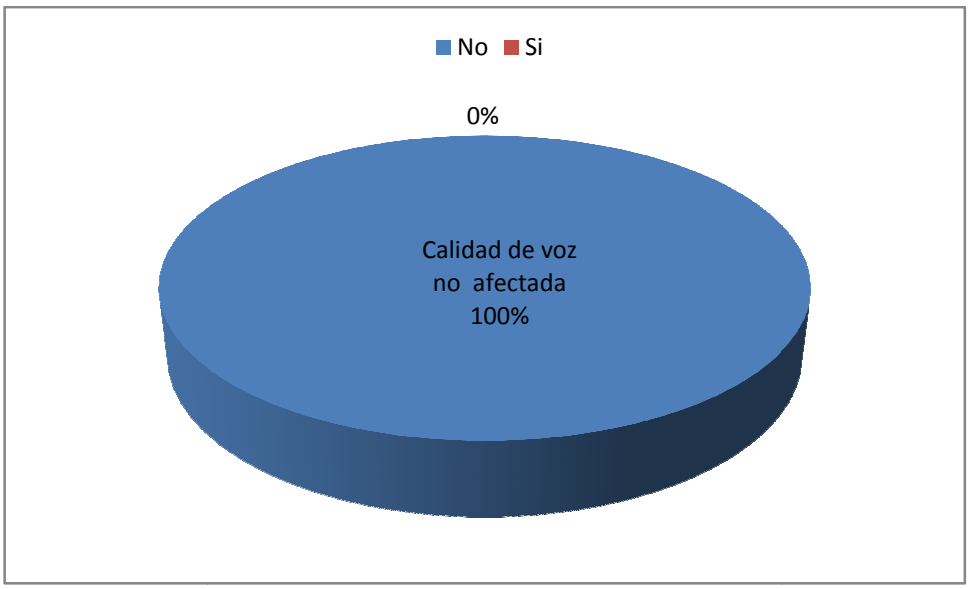


Con la Técnica de Seguridad TLS

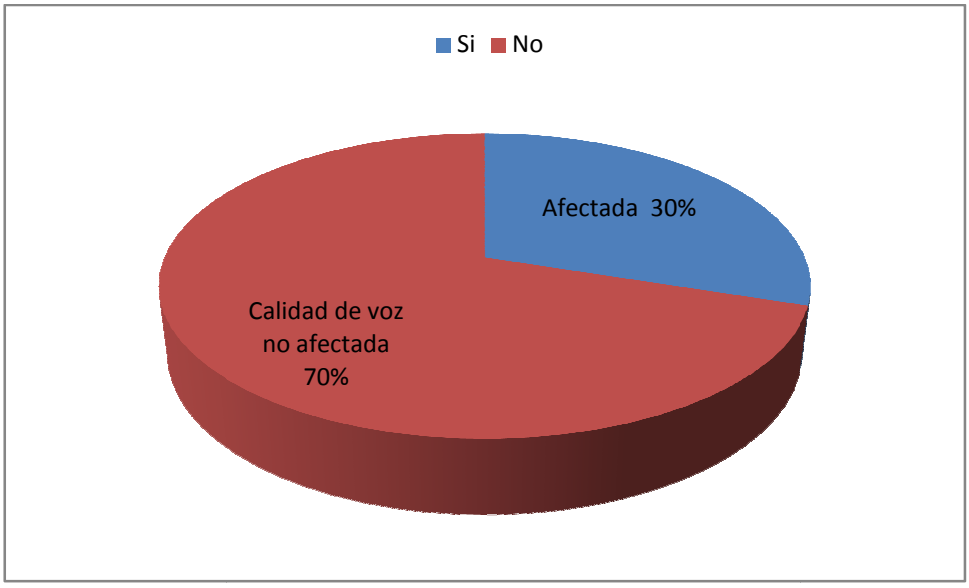


5. Considera usted que al realizar la llamada entre dos usuarios de la central, la calidad de la voz es afectada.

Sin la Técnica de Seguridad

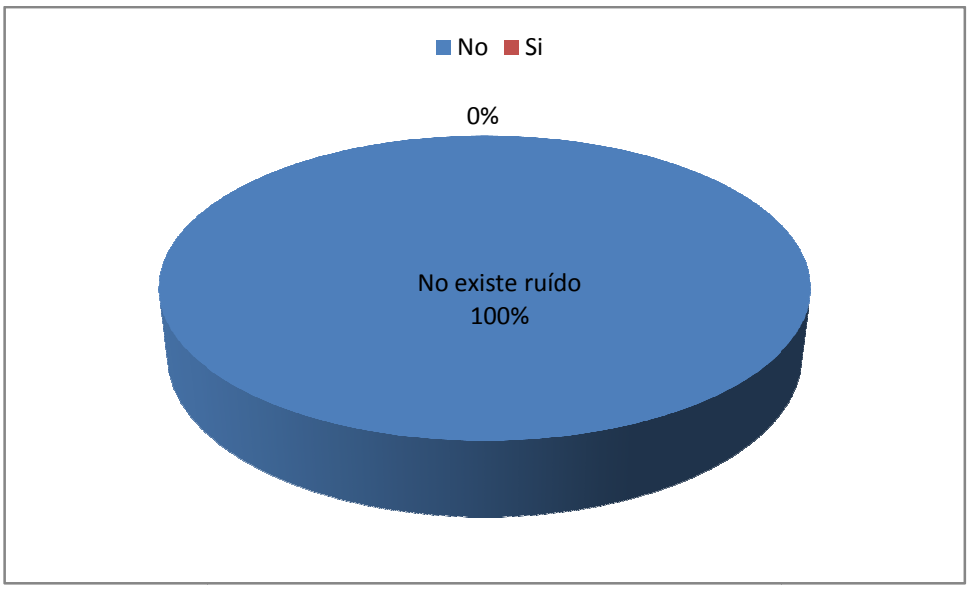


Con la Técnica de Seguridad TLS

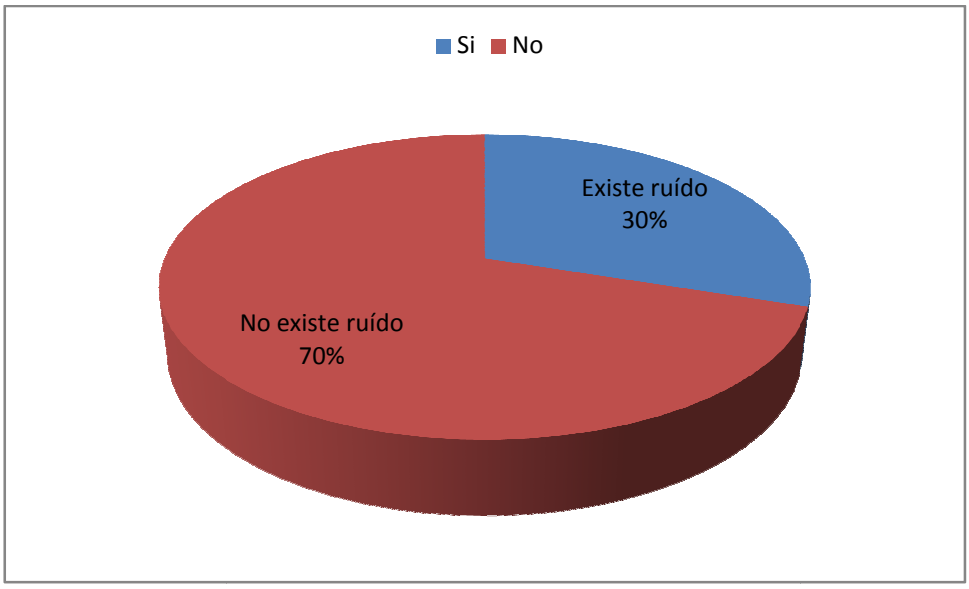


6. Durante el período de comunicación establecido entre dos usuarios de la central PBX existe ruido.

Sin la Técnica de Seguridad



Con la Técnica de Seguridad TLS



ANEXO 4

MANUAL DE USUARIO

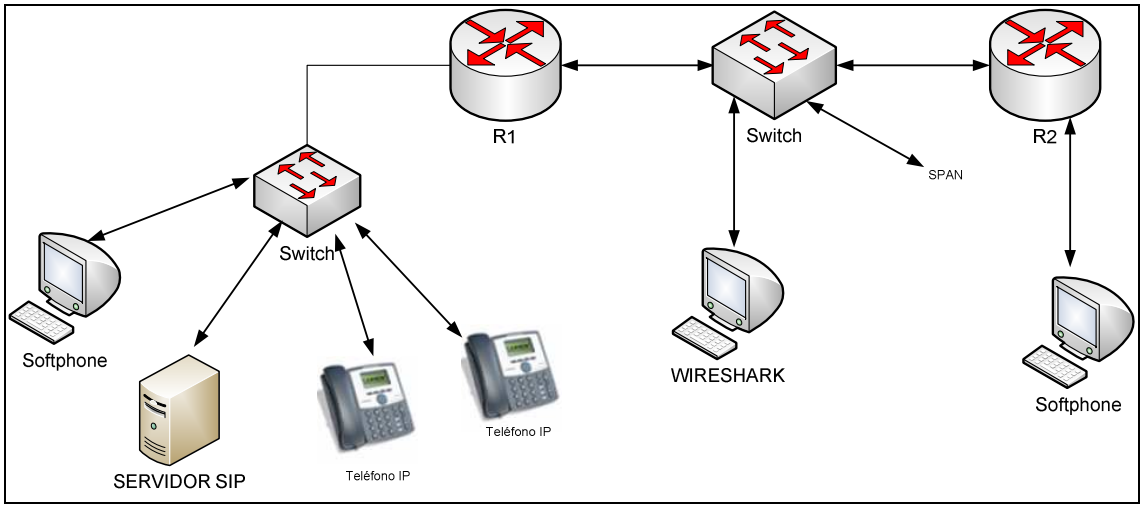
1. Introducción

Este manual está orientado a implementar seguridad en la comunicación de Telefonía IP en redes Corporativas de manera sencilla a través de la implementación de un escenario de prueba se conseguirá este objetivo, el mismo que se desarrollará en el software Elastix 2.0.3 como servidor utilizando el protocolo SIP que es el encargado de manejar el establecimiento, control y terminación de las sesiones de comunicación de VoIP.

Se usará 2 router 2800 series, 2 switch catalyst 2560 para armar la red, en el un switch se configurará SPAN para capturar el tráfico de la red a través del sniffer Wireshark, dos teléfonos IP Grandstream Budgetone-201 como usuarios SIP normales, dos softphone PhonerLite como usuarios SIP que soporta el protocolo TLS, un ordenador con el sniffer Wireshark, todos estos componentes nos ayudarán en la implementación de la técnica que nos ayuden a asegurar las comunicaciones de Telefonía IP.

2. Escenario

El escenario de prueba que nos ayudará a implementar seguridad en comunicaciones de Telefonía IP es:



Escenario de prueba

2.1 Requerimientos de Hardware

- Un switch Cisco Catalyst 3560
- Dos teléfonos IP Grandstream Budgetone-201
- Cinco Computadoras:

  1 Instalar elastix

  2 Instalar el sniffer

  3 Ayudará en la configuración de elastix en forma gráfica al acceder a través de un navegador web a la dirección del servidor elastix

  4 y 5 Instalar los softphone PhonerLite 1.86 y los clientes vpn

2.2 Requerimientos Software

- Sofware Elastix 2.0.3
- Sniffer Wireshark
- Softphone PhonerLite 1.86
- Cliente VPN-GUI
- Openssl

- Openvpn

3. Asterisk

Asterisk fue concebido y desarrollado por Mark Spencer. Es un software de central telefónica con capacidad para voz sobre IP que es distribuido bajo licencia libre.

Asterisk organiza sus archivos en algunos directorios. Entre los más importantes tenemos a los siguientes.

Directorios de Asterisk

Directorio	Descripción
/etc/asterisk/	Aquí residen los archivos de configuración de asterisk
/usr/lib/asterisk/modules/	Este directorio contiene los módulos de Asterisk
/usr/sbin/	Aquí reside el binario de Asterisk
/var/log/asterisk/	Contiene los logs de Asterisk
/var/lib/asterisk/agi-bin/	Directorio donde residen los scripts AGI
/var/lib/asterisk/mohmp3	Carpeta que contiene archivos para música en espera
/var/lib/asterisk/sounds	Sonidos que Asterisk utiliza como prompts de voz
/var/spool/asterisk/	Directorio donde Asterisk guarda archivos que genera producto de su funcionamiento como voicemails y grabaciones de llamadas
/var/run/	Archivos con información de PIDs
/var/log/asterisk/	Aquí residen los archivos de log de Asterisk como el /var/log/asterisk/full o el log de texto de CDRs

Fuente: elastix a Ritmo de Merengue rev 1.3.pdf de Alfio Muñoz

Archivos de configuración

Asterisk se puede configurar a través de algunos archivos de configuración ubicados en la ruta /etc/asterisk. Estos archivos de configuración se encuentran en texto plano para facilitar su modificación desde la línea de comandos utilizando el editor.
Algunos de los más importantes son los siguientes.

Archivos de configuración

Archivo	Descripción
extensions.conf	Aquí reside el plan de marcado. En Elastix este archivo incluye otros más para organizar el plan de marcado de mejor manera. Estos archivos adicionales empiezan con la cadena extensions
sip.conf	Aquí se definen los endpoints SIP
iax.conf	Aquí se definen los endpoints IAX
zapata.conf	Archivo de configuración de los canales tipo ZAP. Aquí se puede troncalizar dichos canales y configurar algunos parámetros

Fuente: elastix a Ritmo de Merengue rev 1.3.pdf de Alfio Muñoz

4. Elastix 2.0.3

Elastix es una distribución de "Software Libre" de código abierto (GPL) de Servidor de Comunicaciones Unificadas que integra en un solo paquete algunas tecnologías claves como:

- VoIP PBX
- Fax
- Mensajería Instantánea
- Email
- Colaboración

Elastix implementa gran parte de su funcionalidad sobre 4 programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix. Estos brindan las funciones de PBX, Fax, Mensajería Instantánea e Email, respectivamente.
La parte de sistema operativo se basa en CentOS 5.5, una popular distribución Linux orientada a servidores.

Es una solución completamente software y corre bajo GNU/Linux. Esta configuración le confiere una robustez innata para desplegar servicios típicos de los sistemas tradicionales, pero aporta mucha más flexibilidad, control, creatividad y a muy bajo costo.

Interacción con cualquier lenguaje de programación para realizar cualquier función que se desee. Todo se hace vía software y de manera transparente, cumpliendo los estándares fijados de manera que pueda interoperar con otros sistemas o tecnologías de manera clara y cercana.

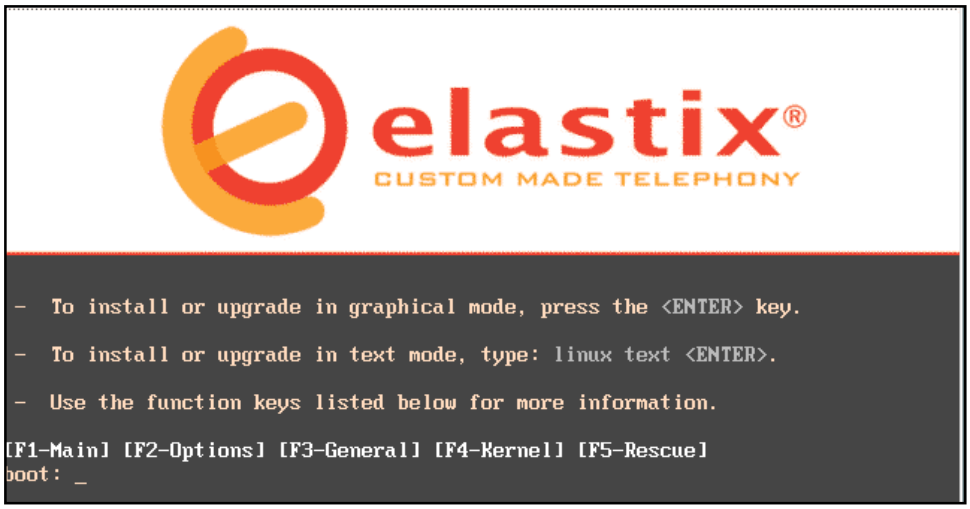
Una centralita o PBX es un dispositivo de telefonía que actúa como un conmutador de llamadas de una red telefónica o de conmutación de circuitos.

Es una solución menos cara que proporciona a cada usuario de la empresa una línea telefónica externa, pueden conectar teléfonos, maquinas de fax y otros dispositivos de comunicación.

4.1 Instalación

Elastix se distribuye como un archivo ISO puede ser quemado a un CD desde cualquier software de grabación de CDs.

Inserte el CD de instalación de Elastix al momento de encender su máquina. Una vez hecho esto aparecerá una pantalla como la siguiente:



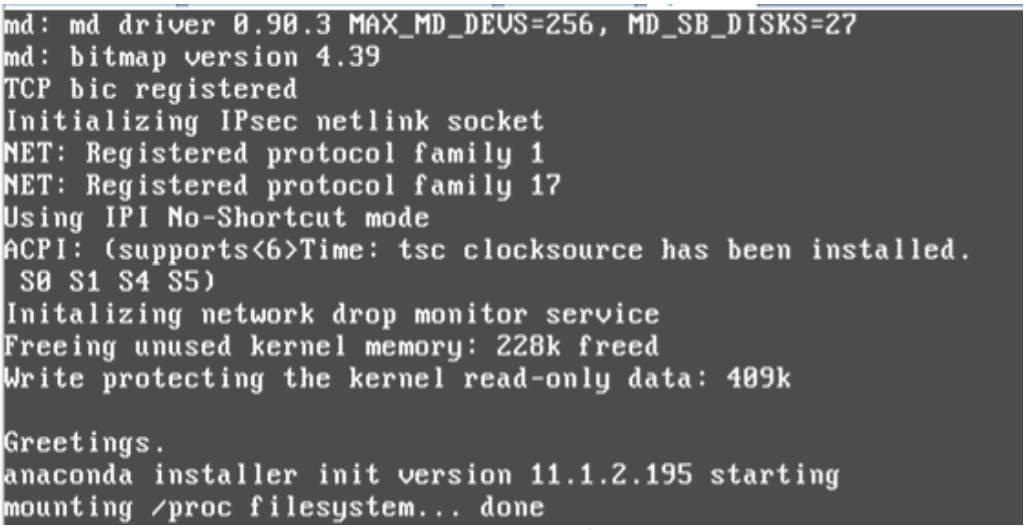
Inicio de la Instalación

El CD de instalación de Elastix formateará TODO el disco duro durante el proceso de instalación así que asegúrese de no tener información que vaya a necesitar en su disco duro.

Si usted es un usuario experto puede ingresar en modo avanzado digitando el comando: advanced

Caso contrario espere, el CD de instalación iniciará la instalación automáticamente ó presione Enter.

El sistema muestra una serie de datos que va cargando



Datos cargando

Proceda a escoger el idioma que le ayudará durante el proceso de instalación, seleccione español y presione la tecla TAB hasta que se coloque sobre el Ok.

Selección del idioma

Proceda a escoger el tipo de teclado de acuerdo al idioma

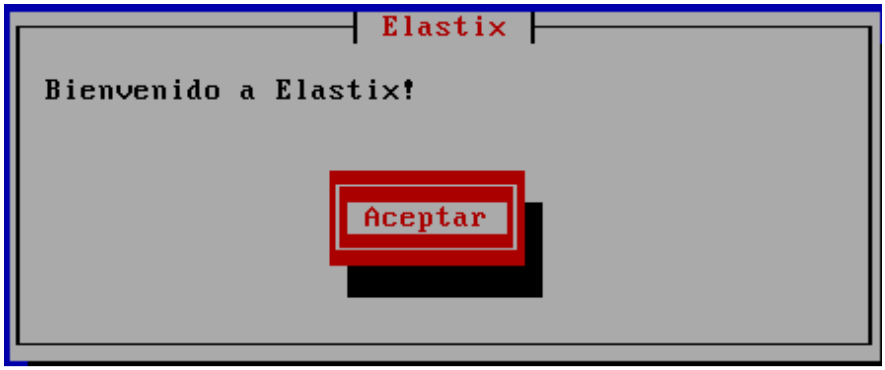
Selección del tipo de teclado

Se escoge es que corresponde al teclado en español.

Instalación de elastix en proceso

Instalación en proceso

Posteriormente, se entra a la pantalla de recibimiento, donde se da la bienvenida a Elastix; hacer click en la opción Aceptar.

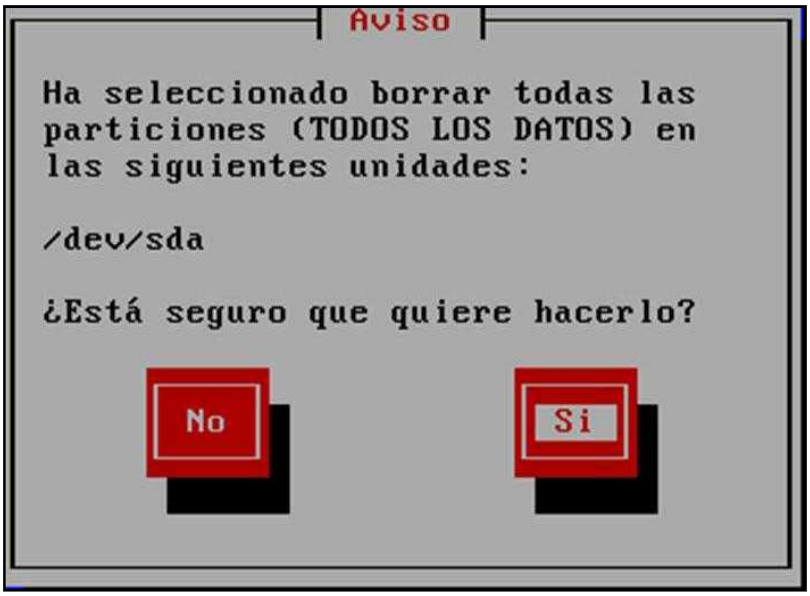


Bienvenida

Seleccione el tipo de partición que desee para instalar Elastix.

Selección del tipo de partición

Seleccione "Aceptar y presione "ENTER", le saldrá un cuadro de aviso donde advierte si esta seguro que quiere borrar toda la información de todas las particiones, a lo que se responde que sí.



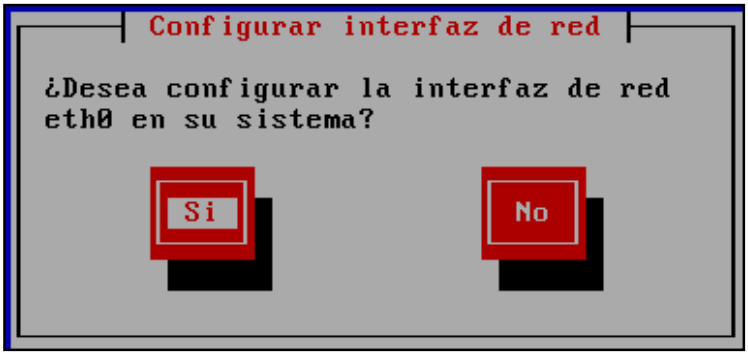
Borrar particiones

NOTA: se borrarán todos los datos de su disco duro.

Finalizado esto, saldrá un mensaje preguntando si quiere revisar como han quedado las tablas de particiones, escoja la opción **No y** presione **Enter**

Revisión de la capa de particiones

Si no posee un servidor DHCP conectado a su equipo se debe configurar la tarjeta de red



Configuración de la tarjeta de red

Seleccione la opción Activar soporte para IPv4 y presione Aceptar

Activación de IPv4

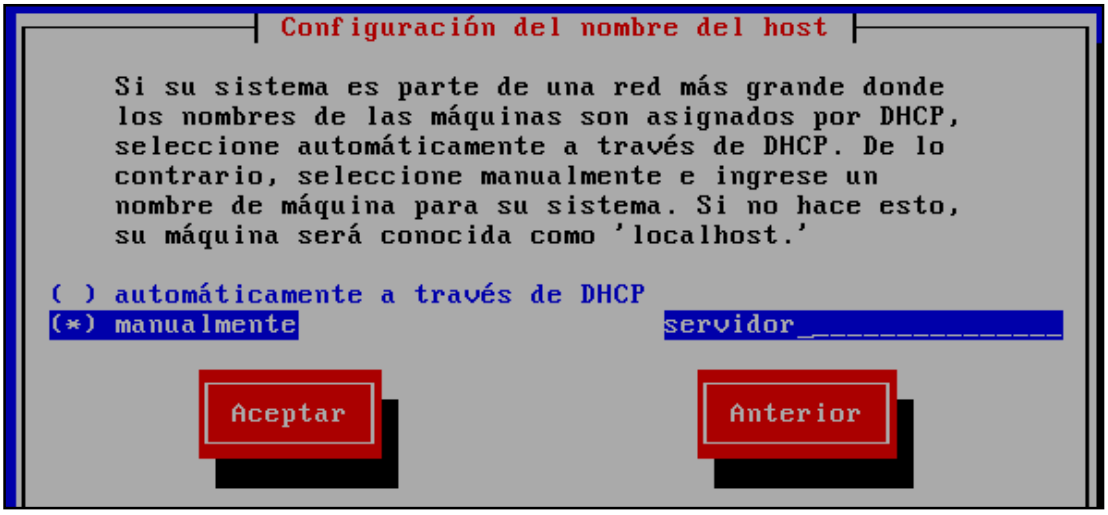
Configure la dirección IP y la Máscara de red

Asignación de la dirección IP y la máscara

Configure la puerta de enlace

Configuración de la puerta de enlace

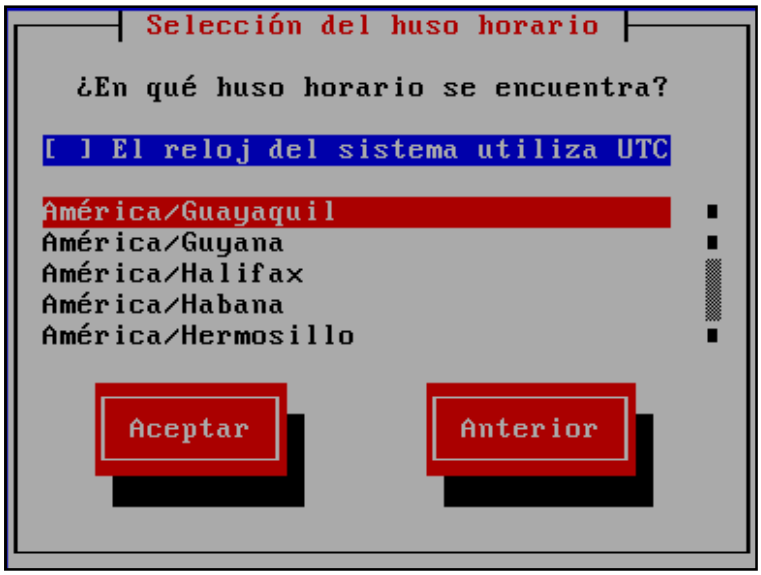
Configure manualmente el nombre del host si no posee un servidor DHCP



Configuración del nombre del host

La siguiente pantalla muestra el gestor de arranque. Por defecto sale en la primera opción que es el GRUB, le damos "TAB" y luego "Aceptar".

Seleccione el huso horario el país correspondiente, se selecciono América/Guayaquil presione TAB y luego Aceptar.

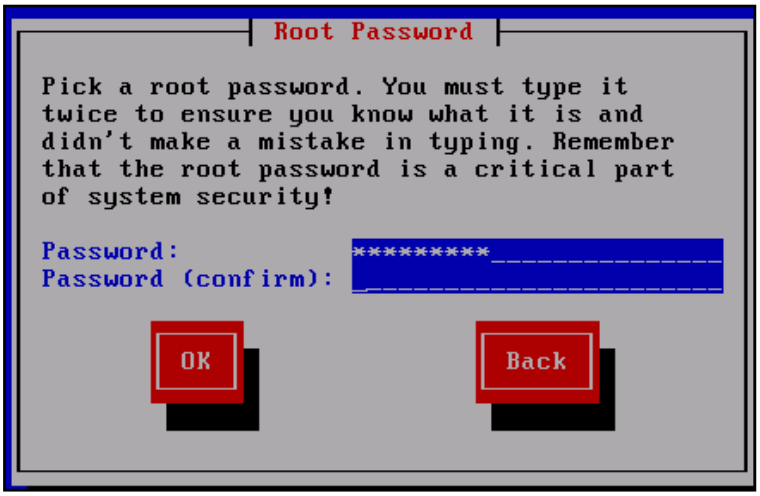


Selección del huso horario

Seleccione los paquetes que desea instalar por defecto se deja las opciones seleccioandas.

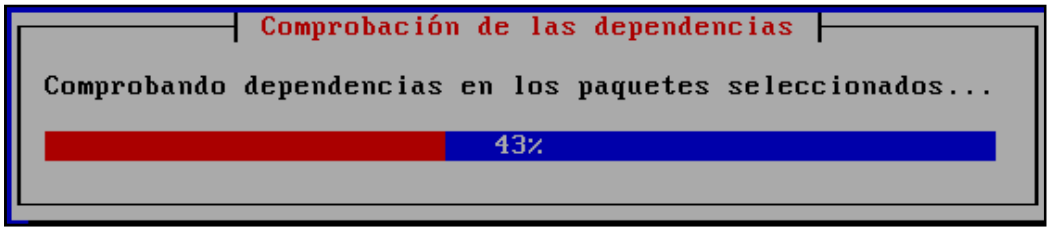
Selección de los paquetes a instalar

Digite la contraseña que será usada por el administrador de Elastix. Recuerde que esta es una parte crítica para la seguridad del sistema. Presione OK



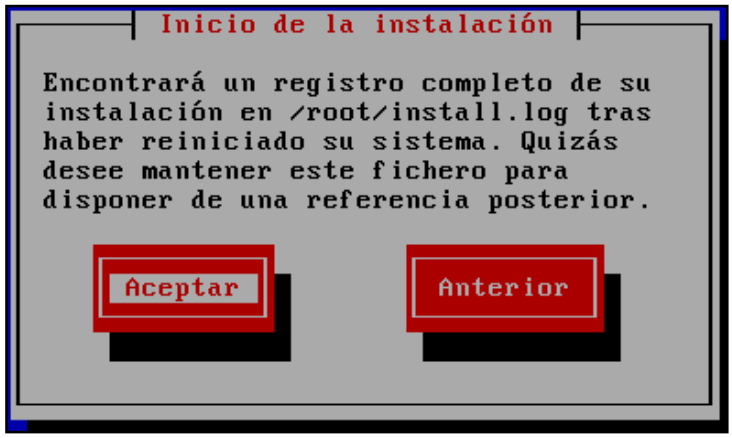
Contraseña

Primero se buscará las dependencias necesarias para la instalación.



Comprobación de dependencias

Cuando esto finalice se mostrará una ventana donde se indica que todas las actividades del proceso de instalación estarán disponibles en un archivo de log cuando el sistema haya arrancado.

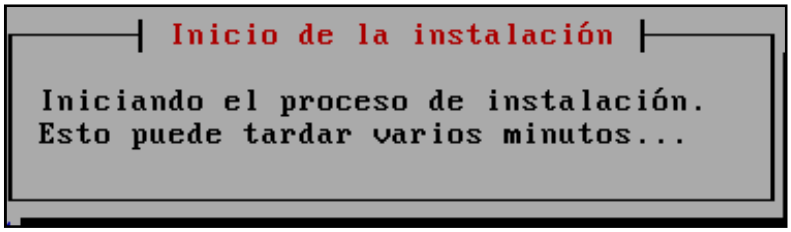


Registro de Instalación

Luego comenzara con el formateo de las particiones ya creadas y los sistemas de archivos.

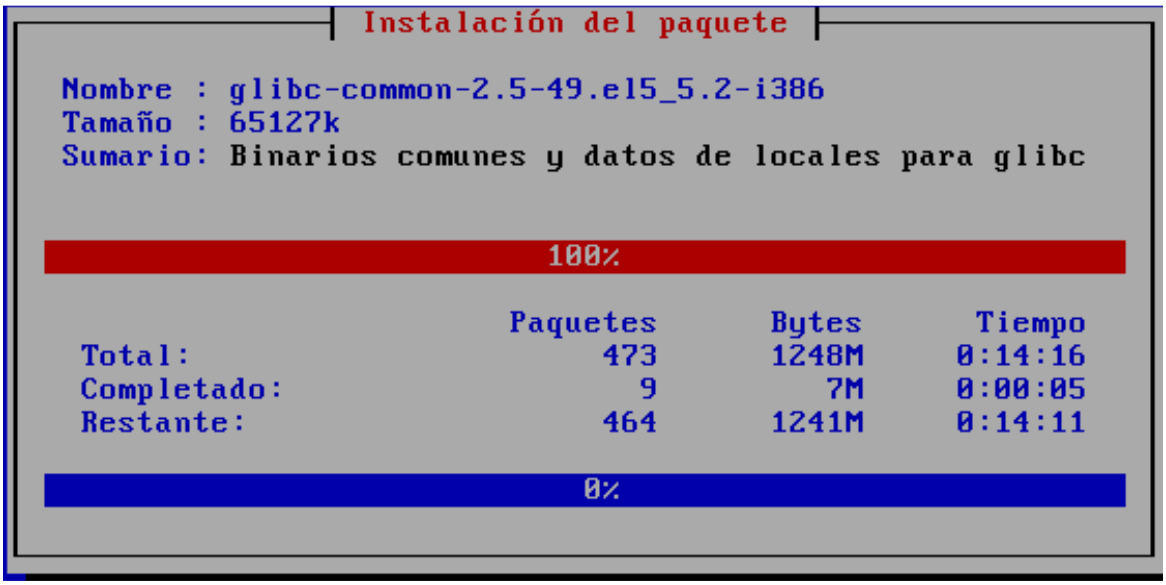
Copia de archivos

Inicia la instalación de los paquetes



Inicio de la Instalación de paquetes

Al término de esto, aparece una pantalla donde se muestra las instalaciones de cada uno de los paquetes que componen a Elastix.

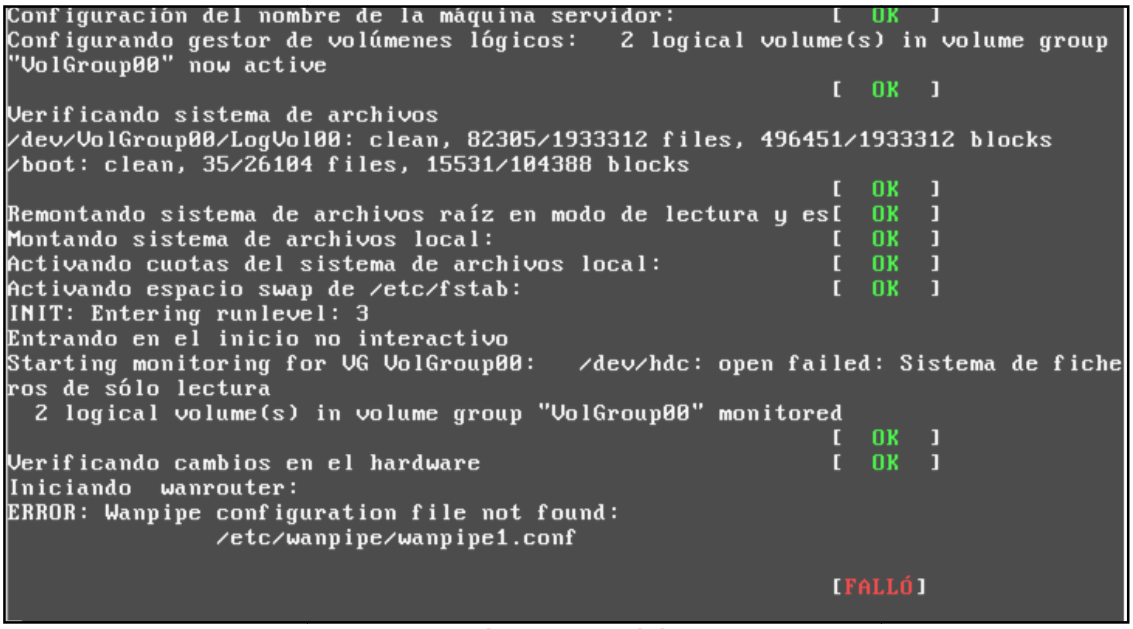


Instalación de paquetes

Cuando la barra de progresión de la parte de abajo llegue al 100%, el sistema estará instalado completamente. El sistema se reiniciara y cuando vuelva a subir se mostrara una pantalla similar a la pantalla inicial.

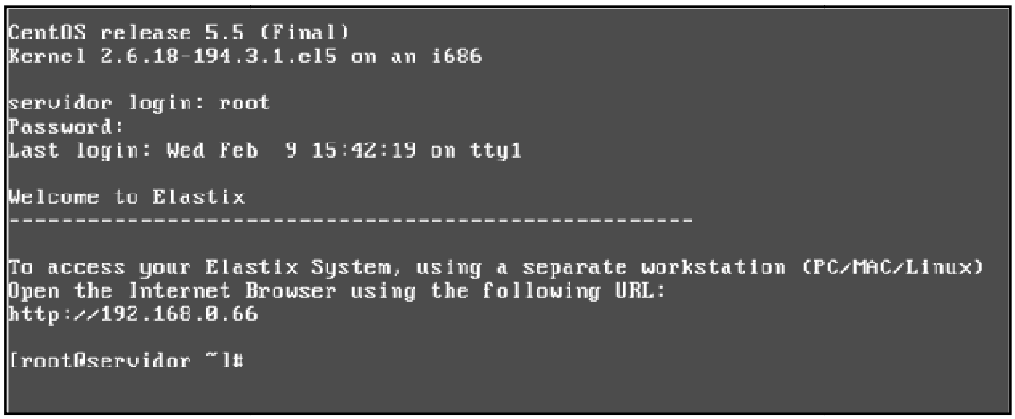
La PBX ejecutara una serie de procesos de arranque y scripts de inicio hasta que finalmente arribe a la pantalla de bienvenida.

No se preocupe si se le aparece la palabra "Fallo" en algunos procesos del momento de arranque, ya que hay servicios y componentes que no se instalan y provocan dicho estatus, como es el caso del Wanpipe, el cual es el driver de las tarjetas Sangoma.



Procesos al momento del arranque

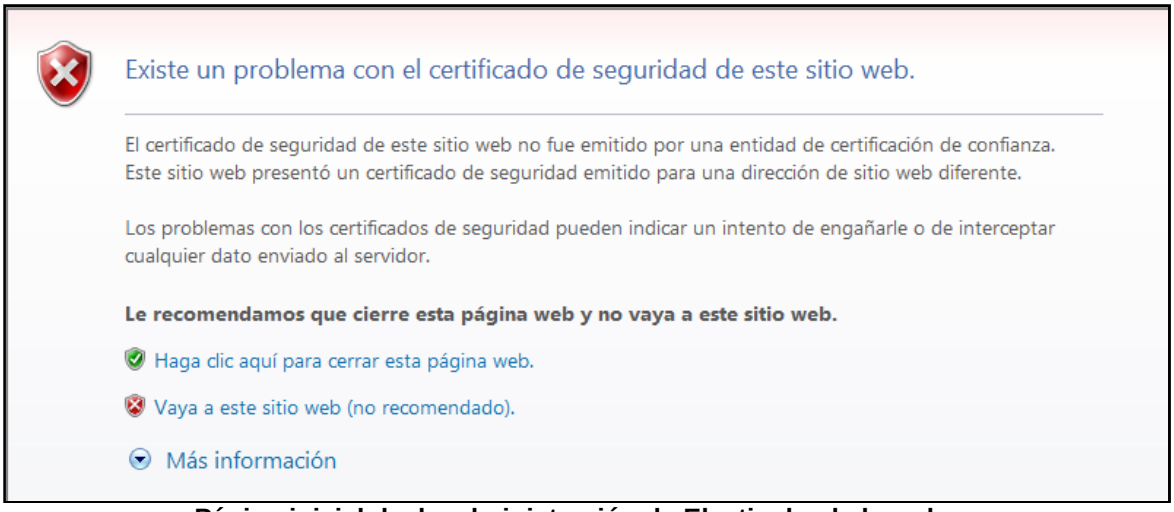
Al finalizar la instalación del Elastix, aparece la ventana de la consola de la pbx, donde pide un usuario (Elastix login:), ahí se coloca "root" y en el password se presiona el que se utilizó en la instalación.



Pantalla de inicio de la PBX

Administrar Elastix mediante la Interfase Web

La interfase Web de Elastix es una aplicación completa de administración del servidor de comunicaciones unificadas, para acceder a esta interfaz en el navegador web poner la dirección IP del servidor elastix y presionar Enter, aparecerá la siguiente pantalla.



Página inicial de la administración de Elastix desde la web

Esta pantalla indica una advertencia de que no conoce esa entidad emisora de certificados (ya que Elastix se comunica por SSL, que es la conexión segura y emite un certificado), para ello seleccione la opción Vaya a este sitio no recomendado, luego de ello aparece la ventana de logeo con Elastix, en la cual debe ingresar el usuario admin y la contraseña que se utilizó en la instalación.

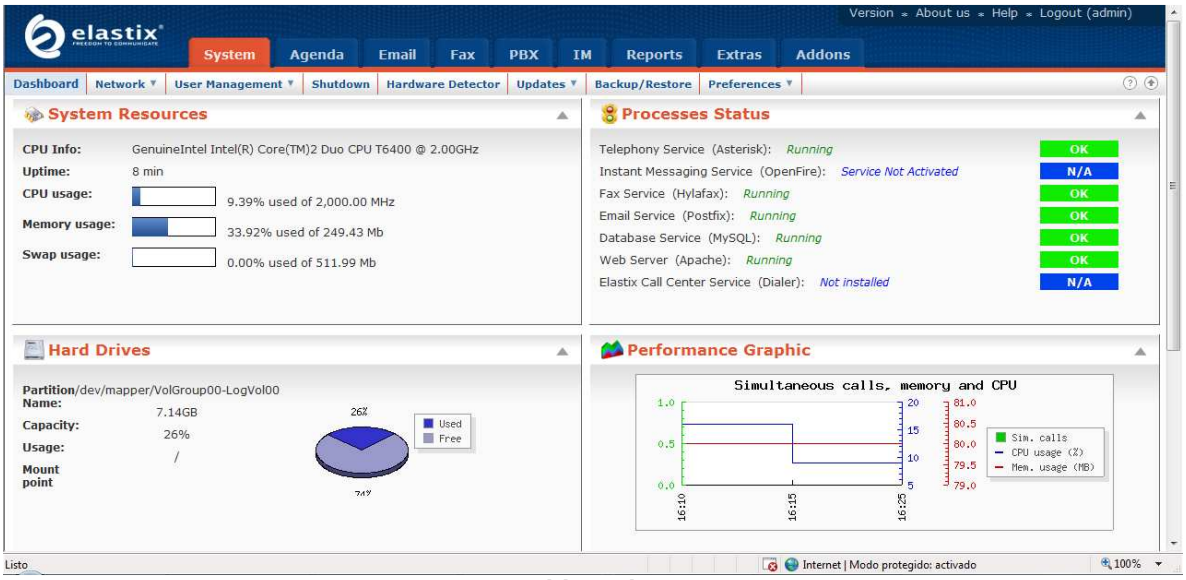
Logeo de la PBX

Las funcionalidades que podemos administrar desde esta interfaz son:

System

Dentro de System encontramos algunas funcionalidades:

1. **Dashboard.** Se encuentra información de los Recursos del sistema, Discos Duros, Estado del los Procesos, Rendimiento, Actividad de las Comunicaciones.



Dashboard

2. Network:

Es el menú de configuración de los parámetros de red. Dentro de esta pestaña se encuentra:

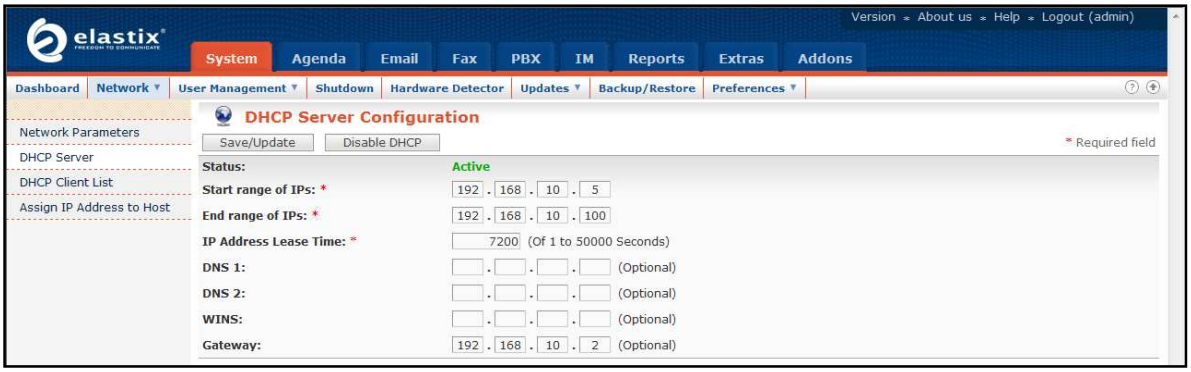
Network parameters. Aquí se pueden configurar parámetros de red como dirección IP y máscara de red, gateway, nombre de host, servidores DNS. Para ello se debe dar click al botón de "Editar parámetros de Red". Para cambiar parámetros como dirección IP y mascara de red, se debe dar click sobre " Ethernet 0 ", el cual esta bajo de "Lista de Interfaces Ethernet".

Network Parameters

Servidor DHCP. Este servicio es de suma importancia si se quiere asignar de forma automática direcciones a los demás equipos de la red como son: Teléfonos IP, ATAs, etc. Solo se debe ver el rango que se desee asignar, el tiempo que desee que los clientes mantengan esas IP antes de hacer una nueva petición al servidor, servidores

DNS externos o de la red local, servidores WINS, y la puerta de enlace predeterminada.

Una vez que se haya llenado todos estos valores, se debe presionar el botón de "Save/Update" y luego “Enable DHCP” para activar el servicio.



Servidor DHCP

3. Administrar Usuarios

Dentro del Menú de administración de usuarios se encuentra.

Menú de administración de usuarios

Grupos. Permite configurar grupos de usuarios

Permisos de Grupo. Aquí se configuran los permisos de accesoa los diferentes módulos para un grupodeterminado

Usuarios. Permite administrar usuarios y asignarlosa grupos. También permite asociar cuentasde email y extensiones telefónicas ausuarios

4. Apagar (Shutdown)

Esta es una forma fácil de apagar y reiniciar el sistema, se debe tener cuidado con esta parte cuando se este trabajando con sistemas en producción.

Menú Apagar

5. Detección de Hardware (Hardware Detector)

Este menú permite detector los dispositivos que se encuentren conectados de la central.

Menú Hardware Detector

6. Actualizaciones (Updates)

Esta parte es muy importante ya que nos presenta todos los paquetes instalados del sistema. Dentro del Menú de actualizaciones se encuentra:

Menú de actualizaciones

Packages. Listado de paquetes con la opción deinstalar o actualizar

Repositories. Se pueden configurar los repositorios enbase a los cuales se realizan lasactualizaciones

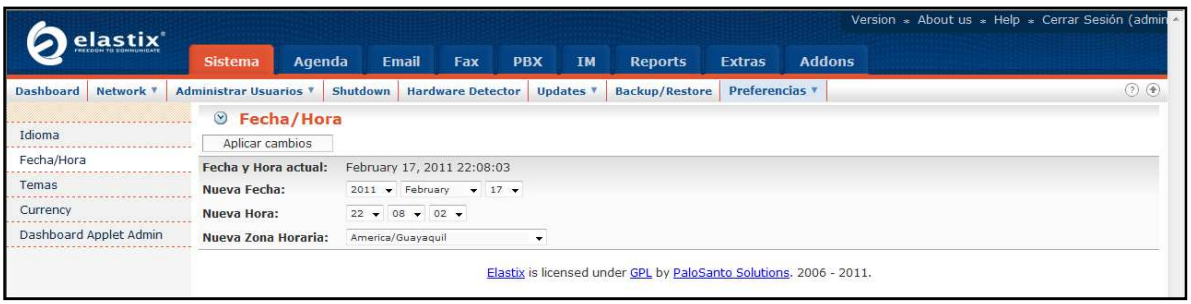
7. Respaldar/Restaurar (Backup/Restore)

Modulo para respaldar el servidor Elastix y también para subir respaldos y restituir información

Backup

8. Preferences

En preferences se puede seleccionar el idioma para la administración de la PBX, la fecha, hora, apariencia del sistema, etc. Dentro de esta pestaña se encuentra:



Preferences

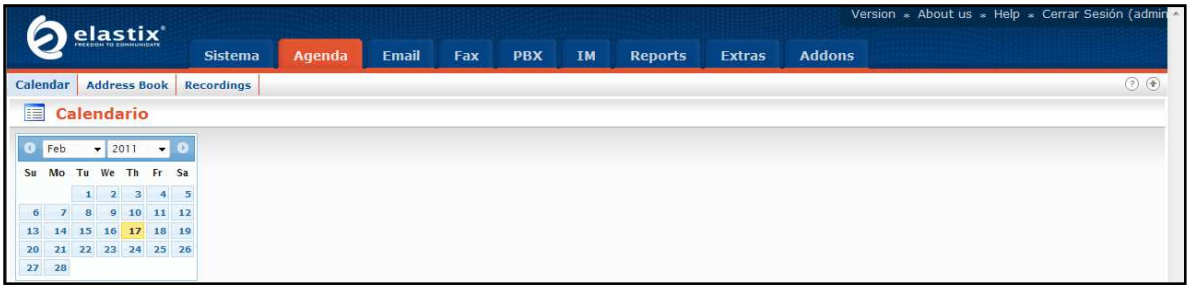
Idioma Cambia el idioma de toda la interfase Web de Elastix

Fecha/Hora Cambia la fecha, hora y zona horaria del servidor

Temas Permite cambiar los temas (skins) para darle a la interfase de Elastix un diferente look

Agenda

Se encuentra el calendario, libreta direcciones y mensajes asociados a módulo calendar.



Agenda

Calendar. Módulo de calendario para agendar eventos que inclusive pueden generar llamadas telefónicas automáticas

Address Book. Libreta de direcciones

Recordings Interfase. para grabar mensajes que se pueden asociar con el módulo Calendar y que se reproducen cuando se genera una llamada automática

Email

En la pestaña email se encuentra:

Email

Domains. Creación de dominios de email. Elastix soporta multidominios.

Accounts. Creación de cuentas de email y asignación de cuotas de espacio en disco duro

Relay. Configuración de relay para permitir a otras redes utilizar a Elastix para enviar su email

Webmail. Interfase de Webmail basada en software

Roundcube. Soporte para "cuotas" configurable desde el Web

Fax

Dentro de esta pestaña se encuentra:

Fax

Virtual Fax List. Listado de extensiones de fax virtuales. Es decir que recibirán faxes en formato PDF en un buzón de email

New Virtual Fax. Este módulo permite crear extensiones de fax nuevas

Fax Master. Permite configurar una dirección email 106que recibirá notificaciones delfuncionamiento del fax

Fax Clients. Configuración de permisos de acceso para aplicaciones clientes de fax

Fax Visor. Visor de faxes que permite visualizar faxes en formato PDF

Template. Email Herramienta de configuración de plantilla de email que se enviará cada vez que arribe un fax

PBX

Dentro de PBX se encuentra:

PBX

PBX Configuration. Aquí se encuentra embebido freePBX.Desde aquí se hacen la mayoría de configuraciones a nivel de central telefónica

Flash Operator. Panel Panel de operador basado en flash, herramienta muy útil para el recepcionista

Voicemails. Listado de voicemails. Se debe haber asociado previamente al usuario con una extensión telefónica para poder ver el listado

Monitoring. Listado de grabaciones telefónicas. Al igual que con el módulo anterior el usuario debe estar asociado con una extensión

Echo Canceller. Actividad del cancelador de eco

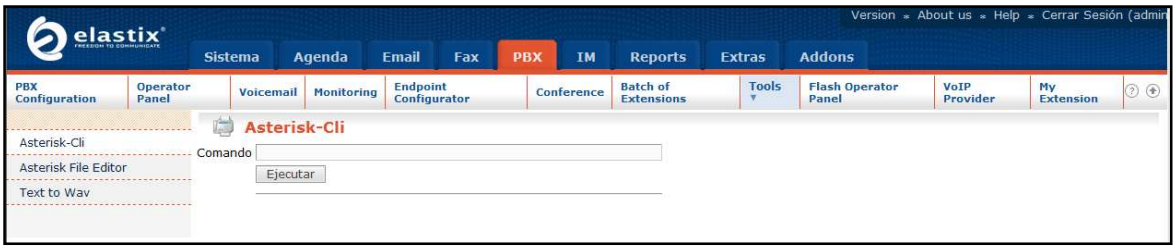
Endpoint Configuration. Herramienta muy útil para provisiona lotes grandes de teléfonos en corto tiempo

Conference. Módulo para agendar conferencias temporales

Extensions Batch. Módulo para crear grandes lotes de extensiones

Tools Menú con herramientas varias

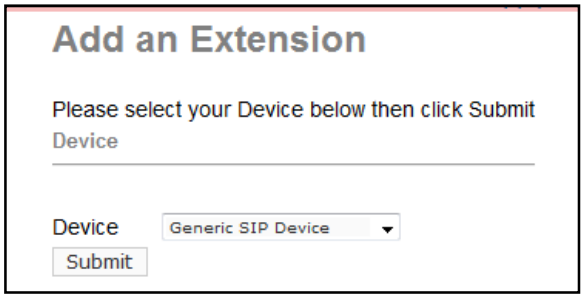
- **Asterisk CLI.** Permite ejecutar comandos del CLI desde el Web
- **File Editor**. Permite editar archivos de texto plano desde el Web



Tools

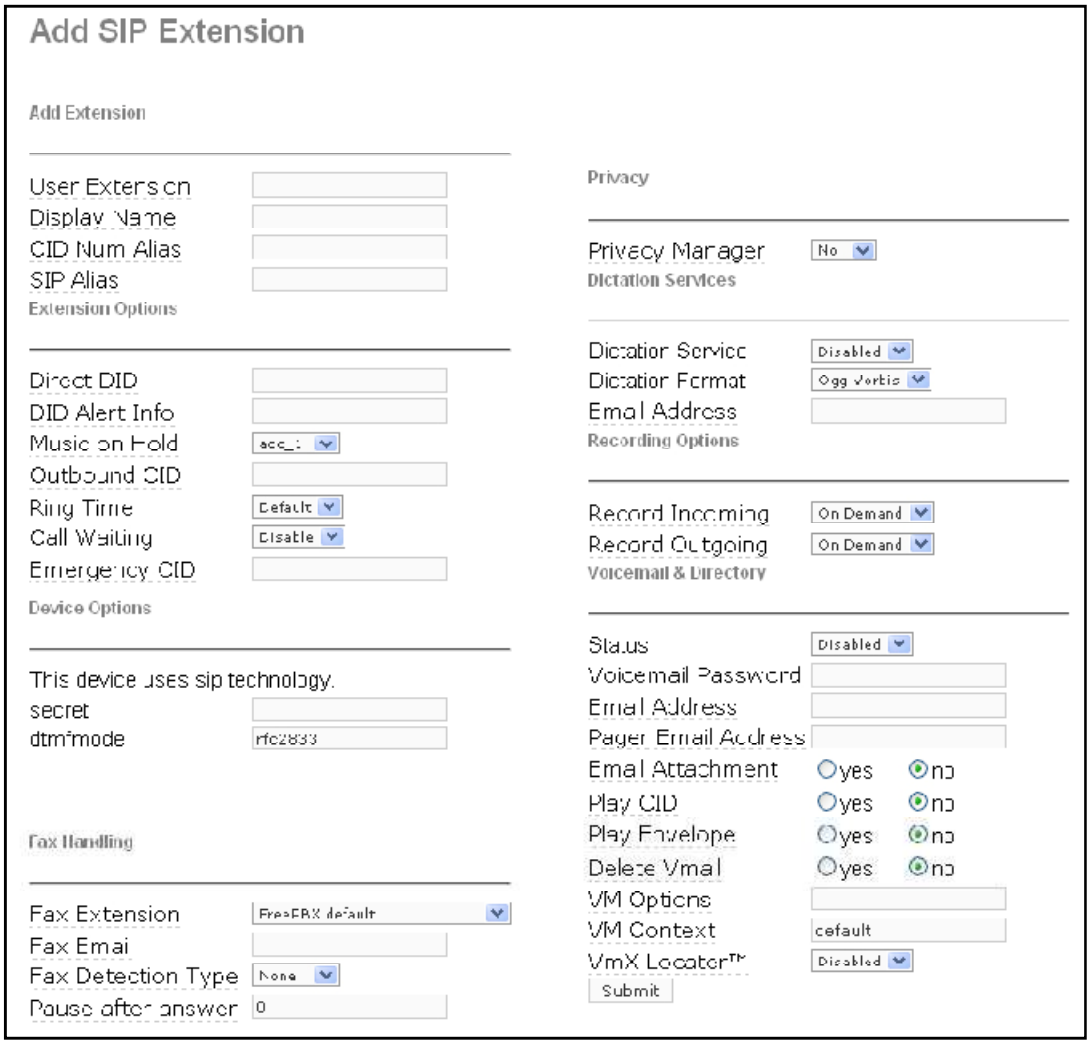
Configurar Extensiones

Lo primero que hay que hacer para recibir llamadas es configurar una extensión para ello en la parte de extensiones aparece la opción de crear "Generic Sip Device", presione el botón "submit".



Crear Extensión SIP

Se presentará el formulario con los campos a ser llenados para crear una extensión.



Formulario para crear una nueva extensión

User Extensions: es el número de la extensión que se va a asignar

Display Name: es el nombre que aparece en una extensión vecina cuando se marca hacia ella.

CID Num Alias: es una máscara para el número que se tiene.

SIP Alias: si usted desea asignar un nombre a una extensión para que otras extensiones SIP puedan marcarle de esta forma, aquí es que debe ser colocado. SIP soporta el marcado por nombre, además de la marcación numérica, es decir, que en vez de SIP/100 se puede utilizar SIP/uas y funciona de la misma manera.

Outbound CID: en este campo se puede colocar un caller-id (identificador de número) diferente al de la central cuando se este marcando fuera de la central. El proveedor debe soportar este procedimiento para que funcione correctamente.

Ring Time: tiempo que debe timbrar una extensión antes de entrar al buzón de voz, por lo general, esta opción no se configura sino que se toma del valor que ya esta expresado en general settings.

Call Waiting: se usa para llamadas en espera. Es de suma importancia que esta opción este habilitada (enable), porque de aquí depende que el teléfono pueda recibir otra llamada cuando la línea está ocupada.

Call Screening: esta función permite que cuando un usuario llama desde fuera a la extensión, se le requiera grabar su nombre para luego la central transferir dicha grabación, dando la opción de aceptar o rechazar la llamada.

Call Screening: con memoria (Memory). Lo que hace es poner al sistema a requerir la grabación del nombre de la persona que llama por primera vez. Ya con su nombre y número registrados, cuando vuelva a marcar desde ese mismo número, la PBX simplemente verificara su caller id y no requerirá que grabe su nombre sino que pondrá la última grabación que se haya hecho desde ese número.

Emergency CID: este es un Caller Id que se utilizara solamente cuando se hace una llamada de emergencia

DID Description: este es un campo solamente descriptivo, se utiliza para hacer una descripción del DID. Direct Inward Dialing es un servicio ofrecido por las compañías telefónicas para ser usado con los sistemas de central telefónica de los clientes, en donde la compañía telefónica asigna un rango de números asociados con una o más líneas telefónicas. Su propósito es permitir a una empresa asignar un número personal a cada empleado, sin requerir una línea telefónica separada por cada empleado. De esta manera, el tráfico telefónico puede ser segmentado y administrado más fácilmente.

Add Inbound DID: este campo sirve para agregar un DID directamente a esta extensión cuando se marque hacia afuera.

Add Inbound CID: se usa en conjunto con "Add Inbound CID".

This device uses sip technology: Se define el tipo de tecnología que se está usando, este es el único campo que cambia cuando se cree otro tipo de extensión.

Secret: esta es la contraseña que se asigna a la extensión que se crea.

Dtmfmode: (Dual Tone Multifrecuency) Multifrecuencia de doble tono. Tonos en diferentes hertz que utilizan una telefonía para marcar números. Cada número u opción del teléfono tiene un tono propio que es identificado en la telefonía.

Este campo puede tener cuatro opciones:inband, rfc2833, info y auto. Es recomendable que se utilice la opción que viene por defecto.

Language Code: con esta opción, si se tiene las voces instaladas en español e inglés al mismo tiempo, especifique "es" y todos los avisos o anuncios se escucharan en español.

Record Incoming: esta opción sirve para grabar todas las conversaciones salientes si se selecciona "always", o no grabar nunca si se selecciona "never". Por defecto viene "OnDemand", es decir, que se puede decidir cuando grabar, inclusive si estamos en medio de una conversación.

Record Outgoing: aplica igual que para Record Incoming, pero esta es para llamadas entrantes.

Status: Esta dentro de Voicemail & Directory, sirve para habilitar el uso de buzón de voz a la extensión, por defecto viene deshabilitado.

Voicemail Password: se trata de la contraseña del buzón de voz, la que el usuario debe utilizar para recoger sus mensajes. Esta clave solo puede ser numérica y el usuario puede cambiarla cuando entra al menú de su buzón de voz.

Email Address: es el correo donde los mensajes de voz serán enviados una vez recibidos, los mensajes son anexados en formato Wav.

Pager Email Address: este correo solo sirve para recibir notificaciones cortas acerca de que tiene un mensaje de voz en su buzón.

Email Attachment: esta es la opción que permite anexar o no el mensaje que se recibe en el buzón de voz.

Play CID: se trata de la opción que anuncia el teléfono o la extensión de la persona que dejo el mensaje de voz.

Play Envelope: Esta opción habilitada permite escuchar la fecha y la hora en la que la persona dejo el mensaje de voz.

Delete Voicemail: si esta opción está habilitada, todos los mensajes de voz serán enviados por correo y después serán automáticamente borrados.

VM Options: sirve para pasar parámetros a las opciones de buzón de voz como cantidadmáxima de mensajes, zona horaria, etc.

VmX Locater™: cuando esta opción es habilitada el usuario tiene control sobre sus mensajes de voz y de su buzón

Voicemail Instructions: cuando no está habilitada, la persona que va a dejar un mensaje de voz solo escuchara un pito (beep). Cuando esta seleccionada utilizamos los avisos o anuncios por defecto que trae el sistema.

Press 0: esta opción se usa cuando la persona que llama, mientras está escuchando el saludo de bienvenida del buzón de voz, pueda presionar el cero y ser redirigida a la recepción.

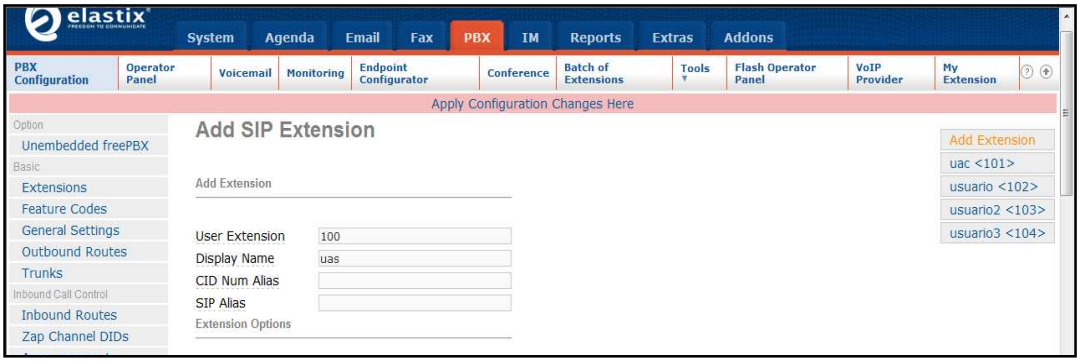
Press 1: hace la misma función, pero por lo general, se coloca un número celular u otro número externo.

Press 2: se refiere a lo mismo que las anteriores opciones.

Procedemos a crear la extensión SIP 100, para esto se debe agregar este número en el campo "User Extensions", luego en el "Display name" se pone uas.

Después de esto, en el campo "secret" se coloca la clave que se desee.

Con estas opciones es suficiente. En la parte del fondo presione "Submit". Luego de esto, aparece en la parte superior de la página una banda de color rosado que dice: "Apply Configuration Changes Here", de click sobre dicha banda para actualizar los cambios y estará creada la extensión exitosamente



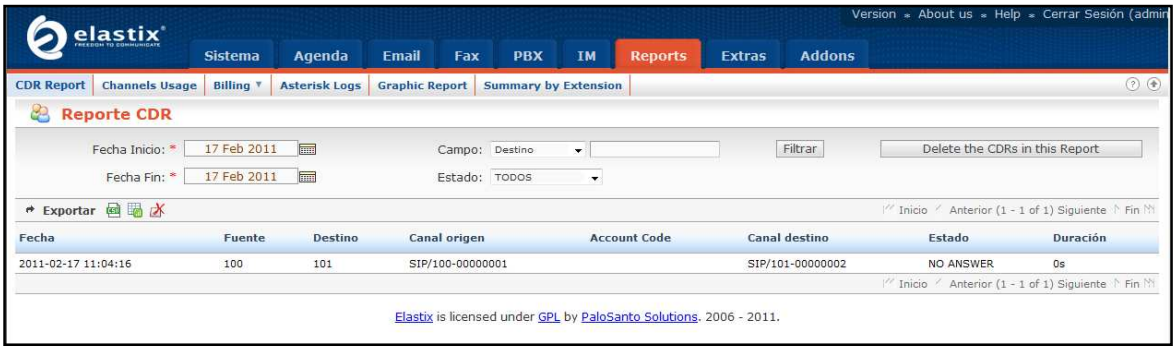
Extensión

IM

OpenFire Interfase embebida para administrar el servidor Openfire

Reports

Dentro del menú Reporta se encuentra:



Menú Reports

CDR Report. Reporte de CDRs con opciones de filtrado por campos y por fechas

Channels Usage. Reporte de uso de canales. Se pueden ver gráficos por diferentes tipos de tecnología como SIP e IAX

Billing. Menú de tarifación

Asterisk Logs Interfase.para ver el log de Asterisk con filtrado por fechas y cadenas de texto

Graphic Report. Permite obtener un reporte en un tiempo determinado.

Summary by Extension. Muestra un resumen de las actividades de las extensiones.

Extras

En el menú Extras se encuentra:

Menú Extras

vTigerCRM. Software de poderoso CRM embebido

Calling Cards. Interface basada en software A2Billing para administrar tarjetas de llamadas

Downloads Menú de descargas

- **Softphones**. Listado de aplicaciones de softphones recomendadas
- **Fax Utilities**. Listado de aplicaciones de fax recomendadas

- **Instant Messaging.** Listado de clientes de IM recomendados

5. Sniffer Wireshark

Es un sniffer, es decir un programa que al ejecutarse comienza a copiar todos los frames que llegan o salen de una PC, es una analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones de datos y protocolos.

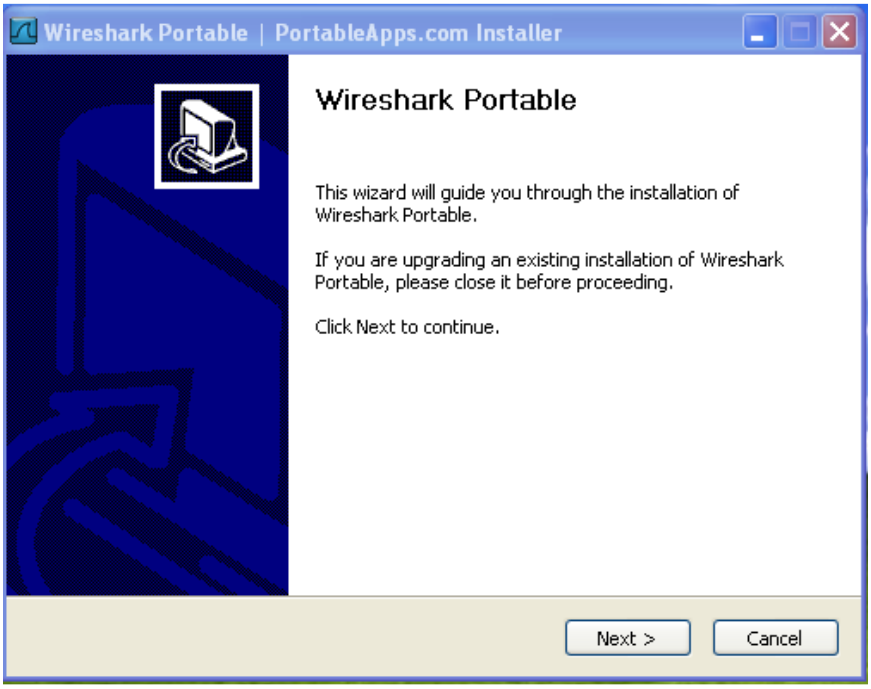
5.1 Instalación

Para instalar el sniffer Wireshark es necesario seguir los siguientes pasos:

1. Doble clic sobre el instalador del sniffer Wireshark

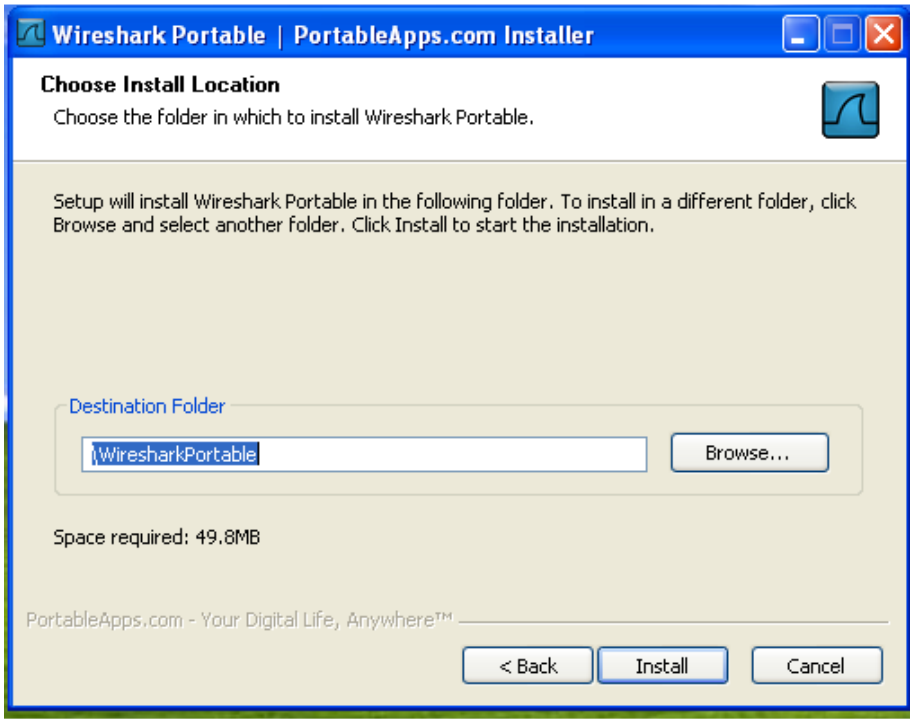
Instalador de Wireshark

2. Aparecerá la siguiente ventana presione Next



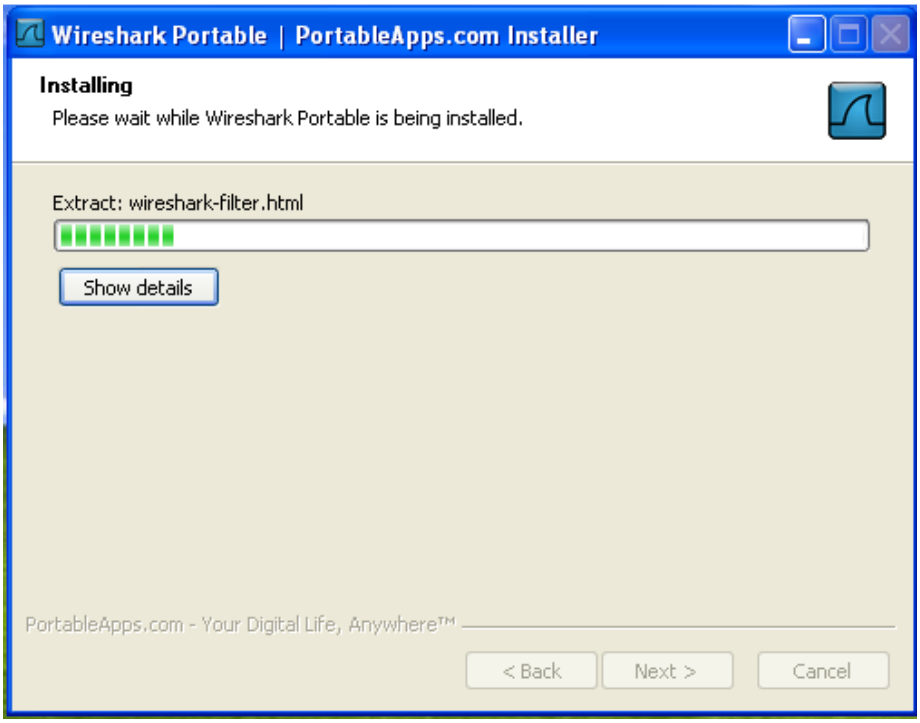
Inicio de la instalación de Wireshark

3. Seleccione la ruta donde desee instalar Wireshark y presione Install



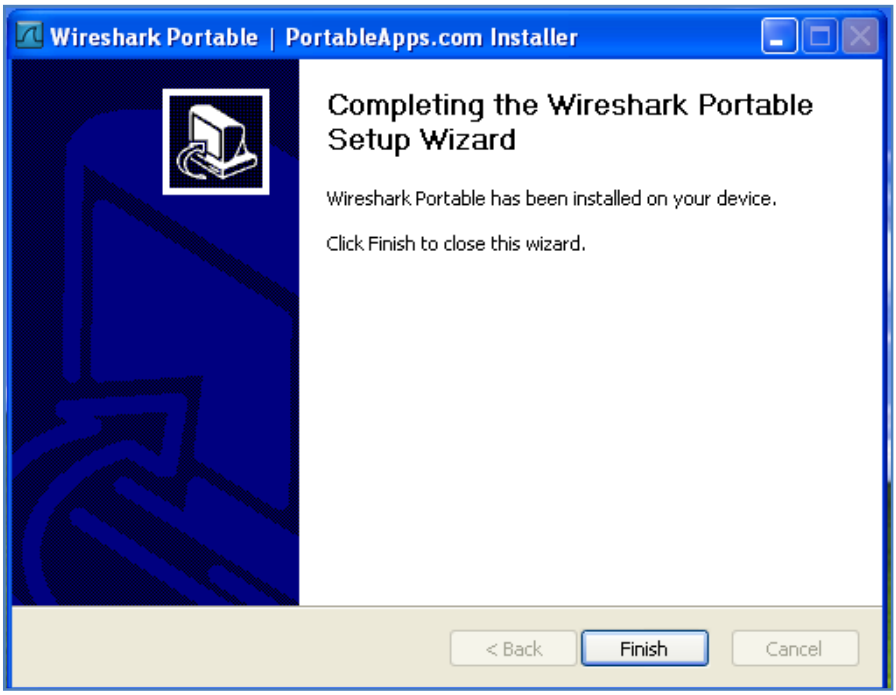
Selección de la ruta

4. Instalación en proceso espere a que la barra se complete



Instalación en proceso

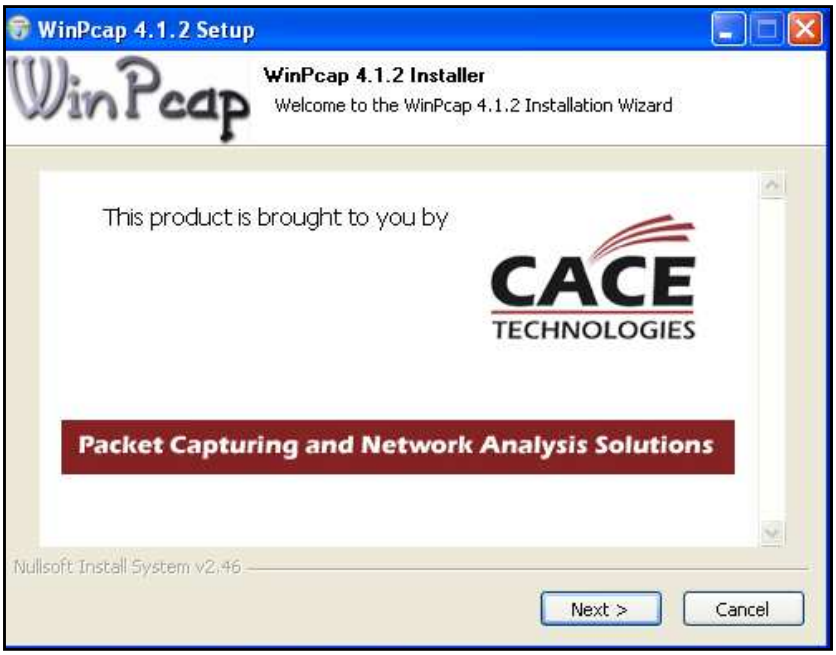
5. La instalación esta completa presione Finish



Instalación completa

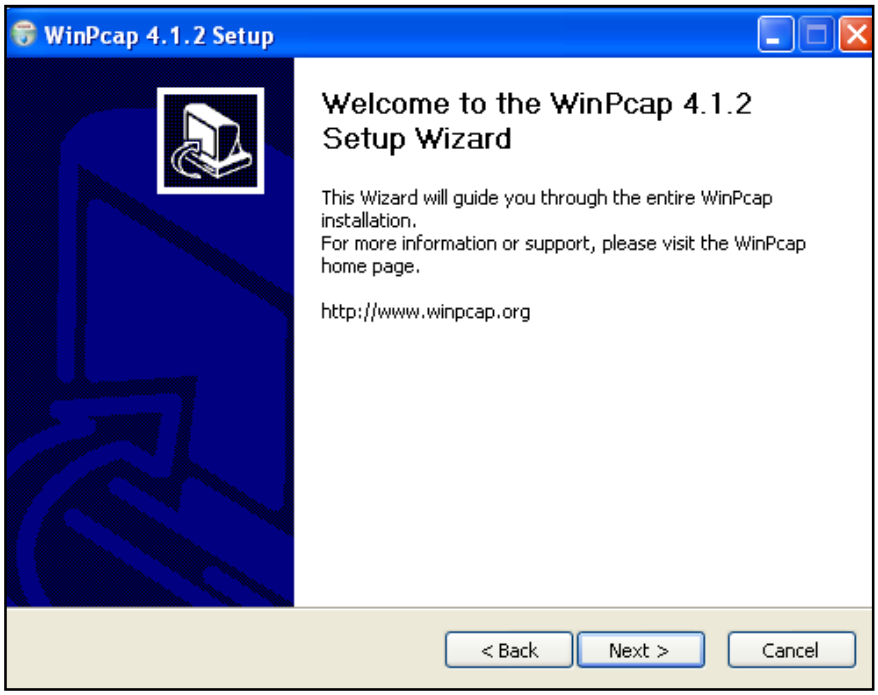
5.2 Configuración de Wireshark

1. Una vez instalado Wireshark de doble clic sobre el icono creado en el escritorio y se aparecerá la siguiente pantalla de inicio de instalación de WinPcap



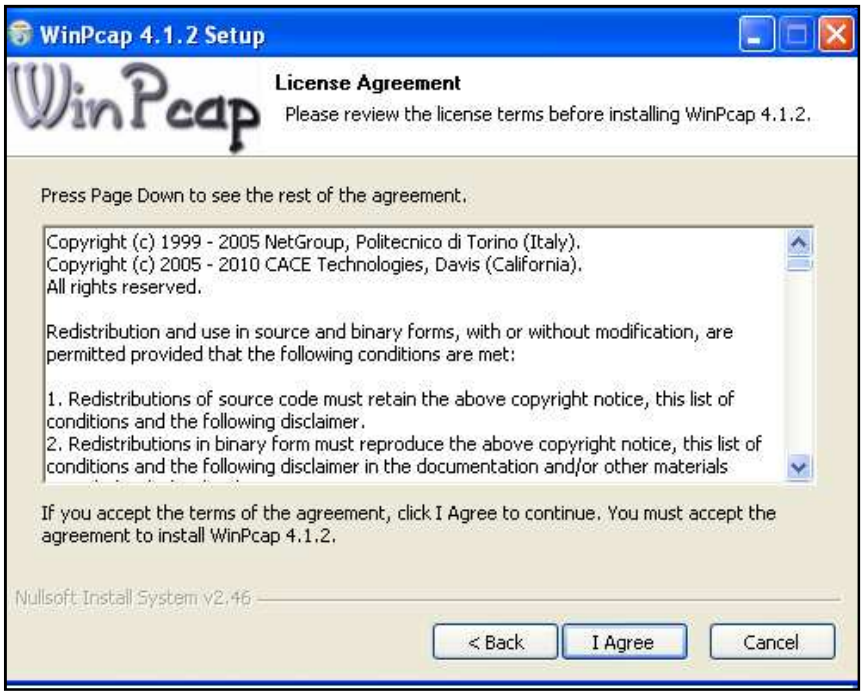
Inicio de Instalación de WinPcap

2. Pagina de Bienvenida de WinPcap presione Next



Bienvenida de WinPcap

3. Acepte la licencia de WinPcap presionando I Agree

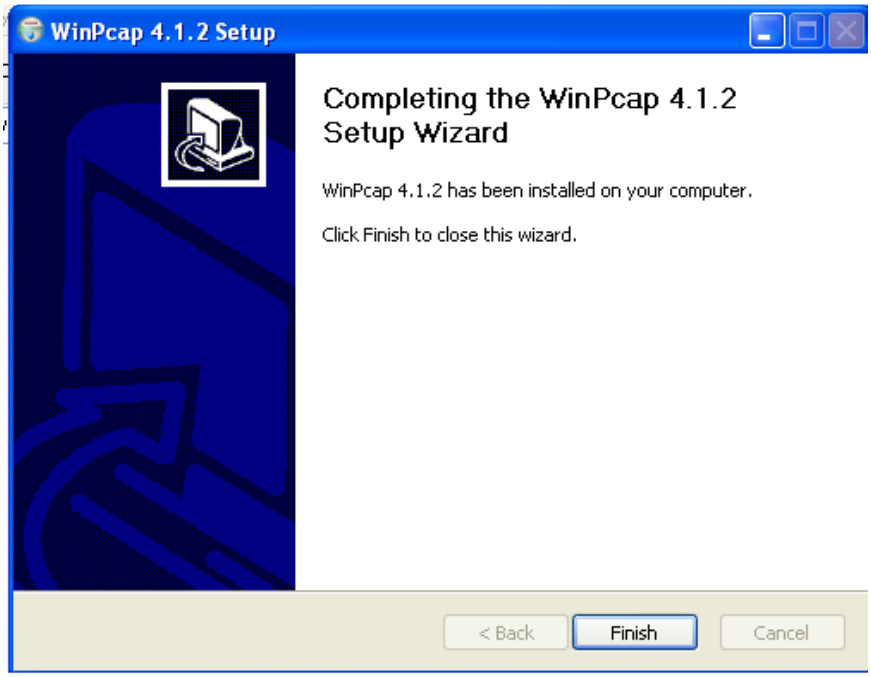


Licencia

4. Instalación de WinPcap

Instalación de WinPcap

5. La instalación de WinPcap se ha completado

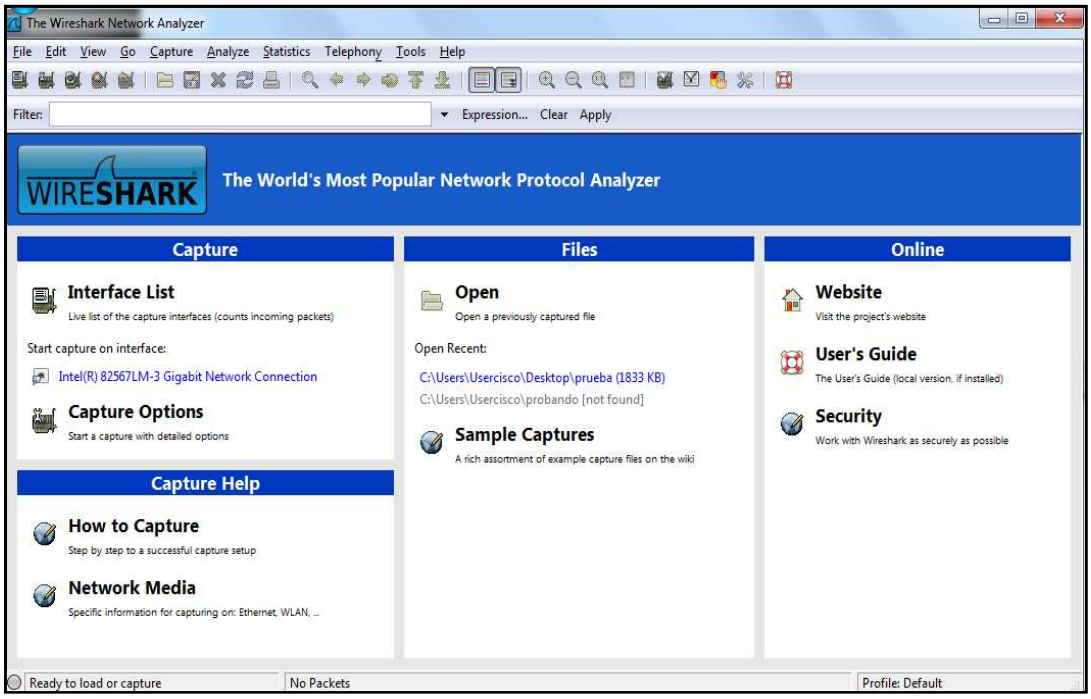


Instalación de WinPcap completa

5.3 Ejecución de Wireshark

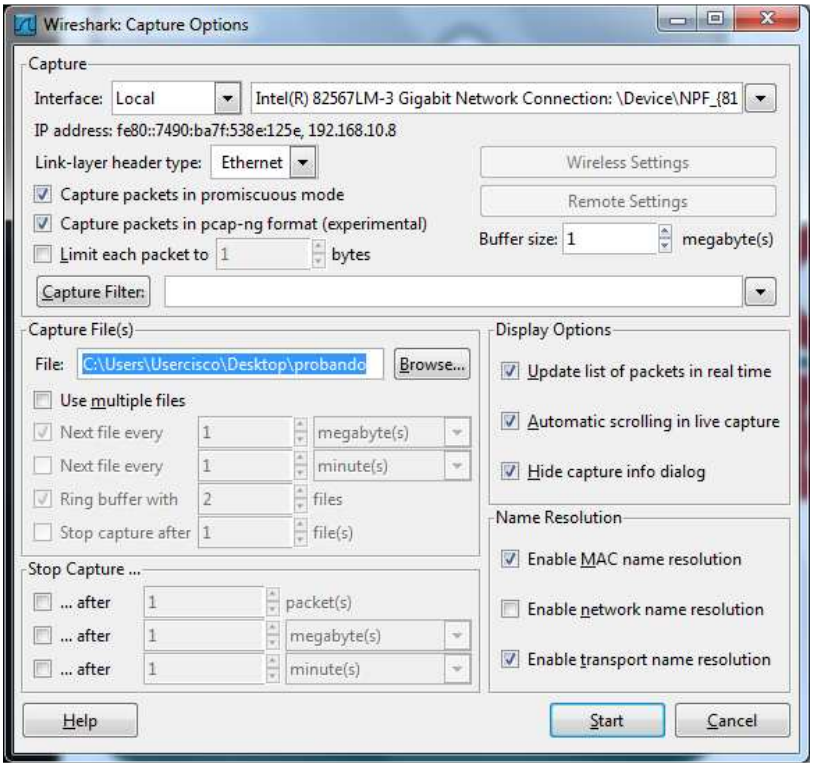
Para realizar la captura el tráfico en la red se debe seguir los siguientes pasos.

1. Una vez configurado WinPcap aparecerá la siguiente pantalla



Pantalla de Inicio de Wireshark

2. Seleccione la opción Capture Options y aparece la siguiente pantalla

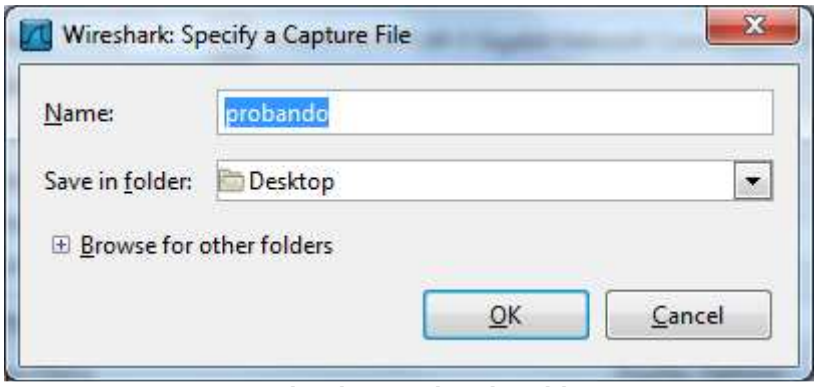


Capture Options

En este pantalla seleccione de la Pestaña Capture las opciones Capture packets in

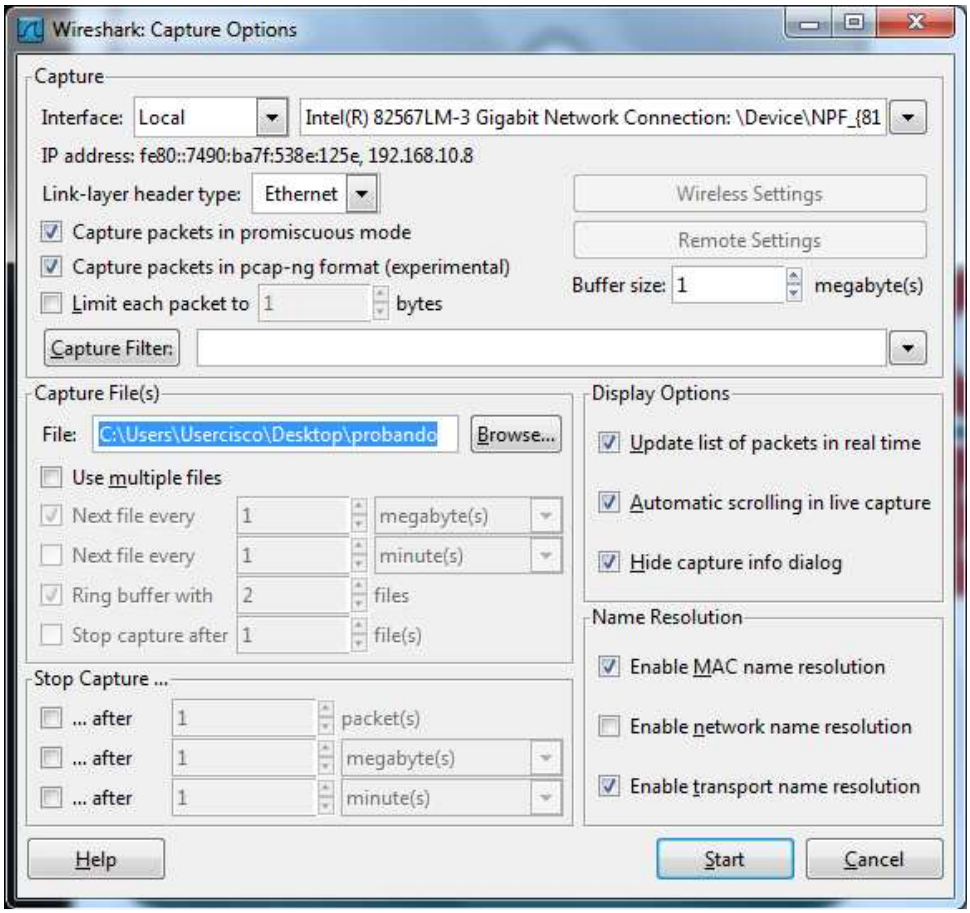
promiscuos mode y Capture packets in pcap-ng format (experimental) y en la pestaña Capture Files(s) seleccione File para escoger donde guardar la captura.

3. Asigne un nombre y la carpeta donde desee guardar y presione OK



Ruta donde guardar el archivo

4. Presione Start y comenzará la captura



Inicio de la captura

6. Switch Cisco Catalyst 2950 24 puertos

Para el correcto funcionamiento del Switch Cisco Catalyst 3560 es necesario:

- PC
- Cable directo categoría 5e

Cable directo

Elementos del switch

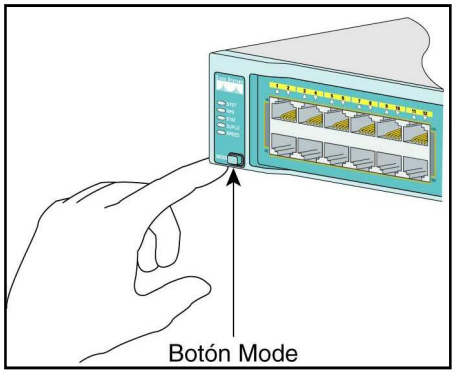
- Switch Catalyst 3560
- Cable de consola
- Cable de poder
- Dos abrazaderas para instalación
- Cuatro tornillos phillips número 12
- Cuatro tornillos phillips número 8 con cabeza phillips
- Cubierta del conector para el sistema de energía redundante
- Dos tornillos número 4 con cabeza redonda
- Cuatro patas de goma para el montaje
- Guía de cable
- Un tornillo Phillips negro para la máquina
- Documentación

Pasos para su uso

Cuando usted configure el switch por primera vez, deberá utilizar el Express Setup para ingresar la información IP inicial. Esto habilitará el switch para conectarse con los routers locales y con Internet. Luego podrá tener acceso al switch a través de la dirección IP para configurarlo con mayor detalle.
Para ejecutar el Express Setup:

- Verifique que no haya ningún dispositivo conectado al switch, porque durante el Express Setup, el switch actúa como servidor DHCP.

- Conecte el cable de alimentación AC al switch y a una toma de corriente alterna con conexión a tierra. La prueba de encendido (POST) comienza. Durante el POST, los LED parpadearán mientras que una serie de pruebas verificará que el switch funcione adecuadamente. El comportamiento de los LED durante el POST es impredecible y podría variar.
- Espere a que el switch termine el POST. Podría tomar varios minutos para que el switch termine esta operación.
- Verifique que el POST haya terminado al confirmar que el LED SYST está en verde y parpadeando rápidamente. Si el switch falla el POST, el LED SYST cambiará a color ámbar.
- Los errores de POST son generalmente fatales. Llame a Cisco Systems inmediatamente si su switch falla el POST.
- Pulse y mantenga presionado el botón Mode por 3 segundos. Cuando todos los LED ubicados sobre el mismo hayan cambiado a color verde, suéltelo. Si los LED ubicados sobre el botón Mode comienzan a parpadear después de que usted haya presionado el botón, suéltelo. Cuando parpadean los LED significa que el switch ya ha sido configurado previamente y no se puede entrar al modo de Express Setup.



Verifica el funcionamiento del switch

- Verifique que el switch esté en el modo Express Setup confirmando que todos los LED ubicados sobre el botón Mode están de color verde. (Los LED del sistema de energía redundante (RPS) y de potencia sobre Ethernet (PoE) permanecen apagados en algunos modelos.
- Conecte un cable directo Ethernet categoría 5e a cualquier puerto Ethernet 10/100 o 10/100/1000 en el panel frontal del switch con el puerto Ethernet de su PC.

Conexión al switch

- Verifique que los LED de ambos puertos Ethernet estén de color verde.
- Espere 30 segundos.

7. Router 2800 Series

Para el tráfico que atraviesa una nube de red, la determinación de la ruta se produce en la capa de red (capa 3). La función de determinación de ruta permite al router evaluar las rutas disponibles hacia un destino y establecer el mejor manejo de un paquete. Los servicios deenrutamiento utilizan la información de topología de red al evaluar las rutas de red. El router determina qué ruta debe utilizar buscando en la **tabla de enrutamiento IP** para enviar paquetes desde la red origen a la red destino. Las entradas de esta tabla de enrutamiento las pueden configurar el administrador de red (mediante rutas estáticas) o se puede rellenar a través de procesos dinámicos ejecutados en la red (protocolos de enrutamiento). Después de que el router determina qué ruta debe utilizar, procede a enviar el paquete. Toma el paquete que aceptó en una interfaz y lo envía hacia otra interfaz o puerto que represente la mejor ruta hacia el destino del paquete.

Funciones

Las funciones del router son:

- **Determinación de ruta**

El router utiliza la porción de red de la dirección destino del paquete IP entrante para realizar la selección de la ruta para transferir el paquete al siguiente router a lo largo de la ruta. Para ello utiliza la **tabla de encaminamient**o. Permite al router seleccionar la interfaz más adecuada para enviar un paquete.

- **Conmutación de paquetes**

Permite que el router acepte un paquete en una interfaz y lo envíe a través de una segunda interfaz. De esta forma podemos describir el procesamiento básico que sufre un paquete IP en un router, en los siguientes pasos:

1. Recepción de una trama de enlace de datos en una interfaz del router.
2. Descarte y eliminación del encabezado de enlace de datos de la trama.
3. Envío del paquete de red resultante al proceso de capa de red adecuado.
4. Examen del encabezado de protocolo de red (dirección IP destino)
5. Consulta de la tabla de enrutamiento por parte del proceso de capa de red.
6. Obtención del interfaz de salto siguiente (de salida) mas adecuado al destino.
7. Encapsulación en una nueva trama de enlace de datos del paquete de red.
8. Envío a la cola de la interfaz de salida seleccionada.
9. Envío de la nueva trama a la red hacia el salto siguiente.

A medida que un paquete se desplaza a través de la red, su dirección MAC se modifica, pero la dirección de red sigue siendo la misma. Este proceso tiene lugar cada vez que el paquete se envía a través de otro router. En el router que se encuentra conectado a la red del host destino, el paquete se encapsula en el tipo de trama de enlace de datos de la LAN destino y se entrega al host destino.

Elementos

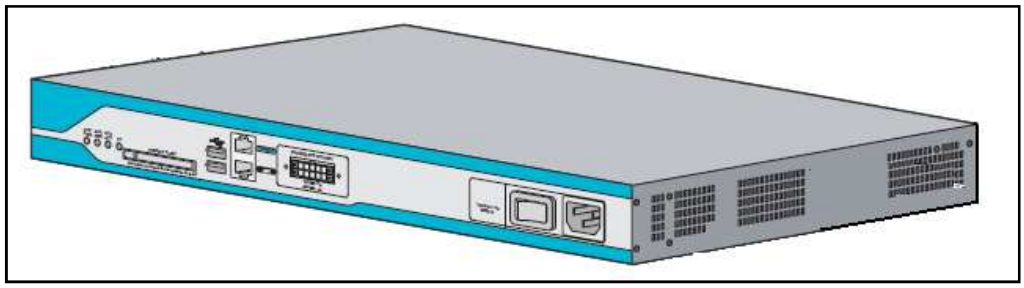
Para el correcto funcionamiento del Router 2800 Series es necesario:

- Un PC que ejecute un software de emulación de terminal
- Cable directo categoría 5e
- Cable de consola
- Cable de alimentación
- Tarjeta de registro de productos Cisco

Pasos para su uso

- Conecte el cable de alimentación, el de consola.

- Verifique que el router este apagado por medio del interruptor que se encuentre en off
- Encienda el router para su configuración.



Router 2800 Series

8. EIGRP

EIGRP es un protocolo de enrutamiento que permite la conexión de redes. Para su configuración se debe seguir los siguientes pasos:

- Entrar al modo de configuración con el comando config
- Configurar las direcciones IP, mascara
- Confirmar la información de los router e interfaces con el comando show running-config
- Una vez configuradas establecer eigrp con el comando router eigrp 1
  R1(config)#**router eigrp 1**
  R1(config-router)# **no auto-summary**
  R1(config-router)# **network 192.168.10.0**
  R1 (config-router)#**network 192.168.37.0**
  R1 (config-router)#**end**
- Probar la conectividad de la red con el comando ping

9. SPAN

El tráfico que entra o sale de los puertos de origen se puede controlar mediante el uso de SPAN.

SPAN no afecta a la conmutación de tráfico de red en los puertos de origen, una copia de los paquetes recibidos o enviados por la fuente de las interfaces se envían a la interfaz de destino. Sin embargo, un exceso de solicitudes de destino SPAN, puede

causar congestión en el interruptor. Los puertos de destino no pueden recibir o reenviar el tráfico, salvo que el requerido para la sesión SPAN.

Una sesión SPAN es una asociación de un puerto de destino con puertos de origen. Usted puede monitorear el tráfico entrante o saliente en una serie o rango de puertos.

9.1 Funcionalidad

En la tarea de administración de redes LAN es de fundamental importancia mantener un atento monitoreo del tráfico y del desempeño de los dispositivos de la infraestructura de red. En este contexto es frecuente que por diferentes motivos (detección de tráfico no deseado, relevamiento de actividad de ciertos protocolos, etc.) el Administrador requiera utilizar un analizador de protocolos para monitorear, decodificar y comprender el tráfico de la red.

Para esta tarea, luego de instalar el analizador de protocolos en una terminal, se ha de conectar la estación de monitoreo a un switch a fin de capturar y revisar el tráfico que está atravesando la red.

Cuando se monta una estación de monitoreo, en principio se busca capturar tanto tráfico como resulte posible para luego filtrarlo y de ese modo quedarse con lo que verdaderamente se está buscando. Sin embargo, si la estación de monitoreo está conectada a una boca de un switch lo único que se puede capturar es el tráfico generado en la misma terminal o que tiene a esa terminal como destino, así como el tráfico de broadcast que esté circulando por ese segmento de red.

9.2 Funcionamiento

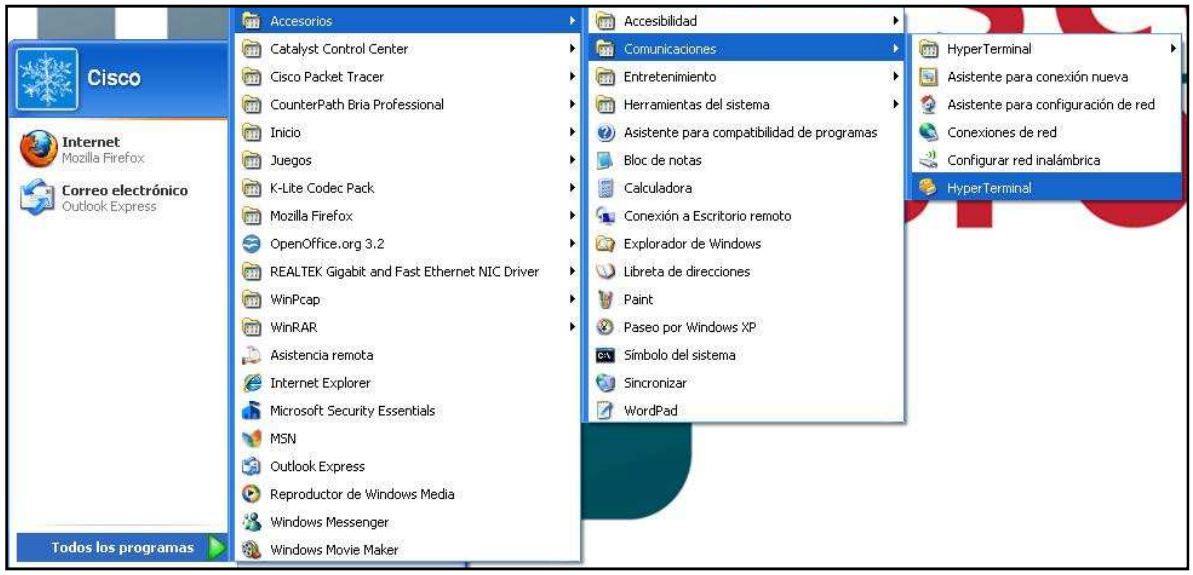
SPAN permite tomar el tráfico que atraviesa por un puerto, grupo de puertos o VLAN completa de un switch y lo copia en el puerto de destino, que es el puerto en el que debemos conectar nuestra estación de monitoreo. Adicionalmente, al configurar esta funcionalidad se especifica no sólo los puertos de origen y destino, sino también si se desea copiar el tráfico que tiene ese puerto como origen, destino o ambos.

9.3 Configuración

La configuración es simple.

Conecte la estación de monitoreo al puerto Fastethernet que desee y monitoree todo el tráfico que pasa a través de los restantes puertos del dispositivo. Indique al dispositivo que envíe copia al puerto Fastethernet que escogió.

1. Ingrese a un terminal para administrar al switch vía comandos



Acceso a una terminal

2. Asigne el nombre a la conexión y escoja el icono y presione Aceptar

Descripción de la conexión

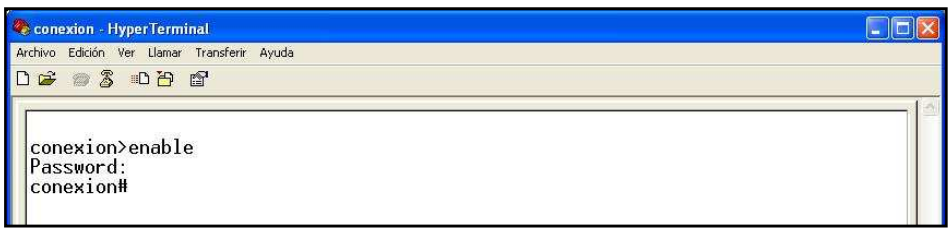
3. Seleccione la forma de conexión COM1y presione Aceptar

Conexión

4. Seleccione las propiedades de la conexión COM1 y presione Aceptar

Propiedades de COM1

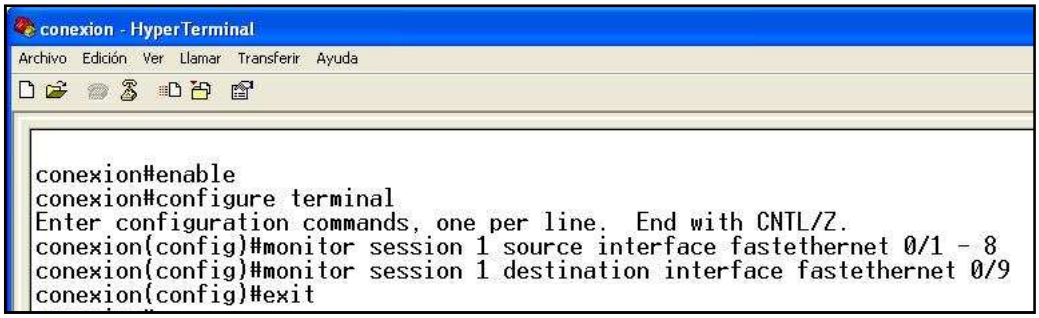
5. Digite enable para entrar al modo de administrador y la contraseña



Conexión establecida

Ejecute los siguientes comandos para configurar SPAN

Switch(config)#monitor session 1 source interface fastethernet 0/1 - 8 both
Switch(config)#monitor session 1 destination interface fastethernet 0/9



Comandos de configuración de SPAN

Se ha definido que todo el tráfico que pase por las interfaces F0/1 - 8 se vea reflejado por la F0/9

Es preciso tener presente que este tipo de operaciones son un requerimiento intensivo para el dispositivo, y que consecuentemente pueden afectar sensiblemente la performance del mismo. Asegúrese de deshabilitar esta función cuando haya terminado la tarea utilizando el comando

Switch(config)#no monitor session 1

Verifique el SPAN con el siguiente comando:

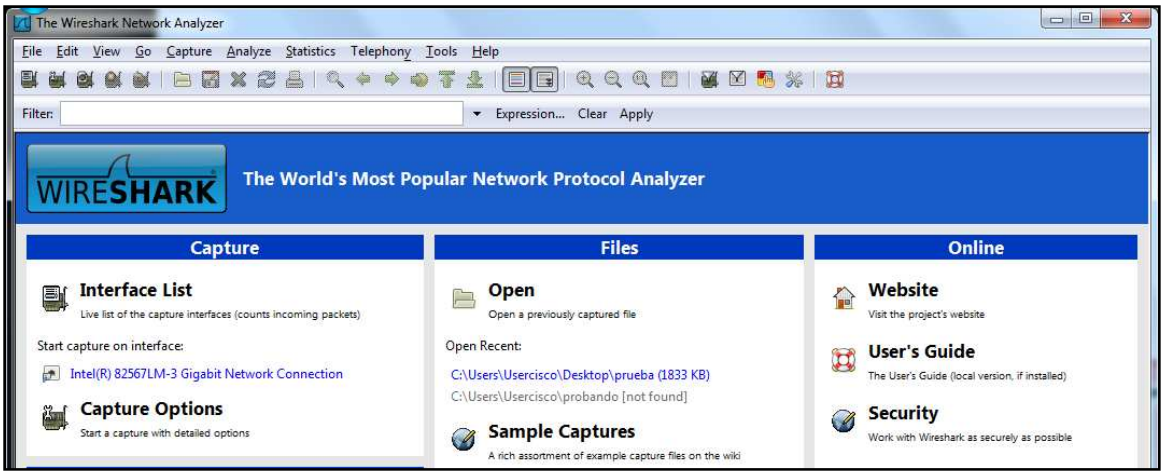
S1# show monitor session 1
Aparece la siguiente información:

```
conexion#show monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/1-8
Destination Ports      : Fa0/9
    Encapsulation      : Native
          Ingress      : Disabled
```

Ejecución de SPAN en el switch

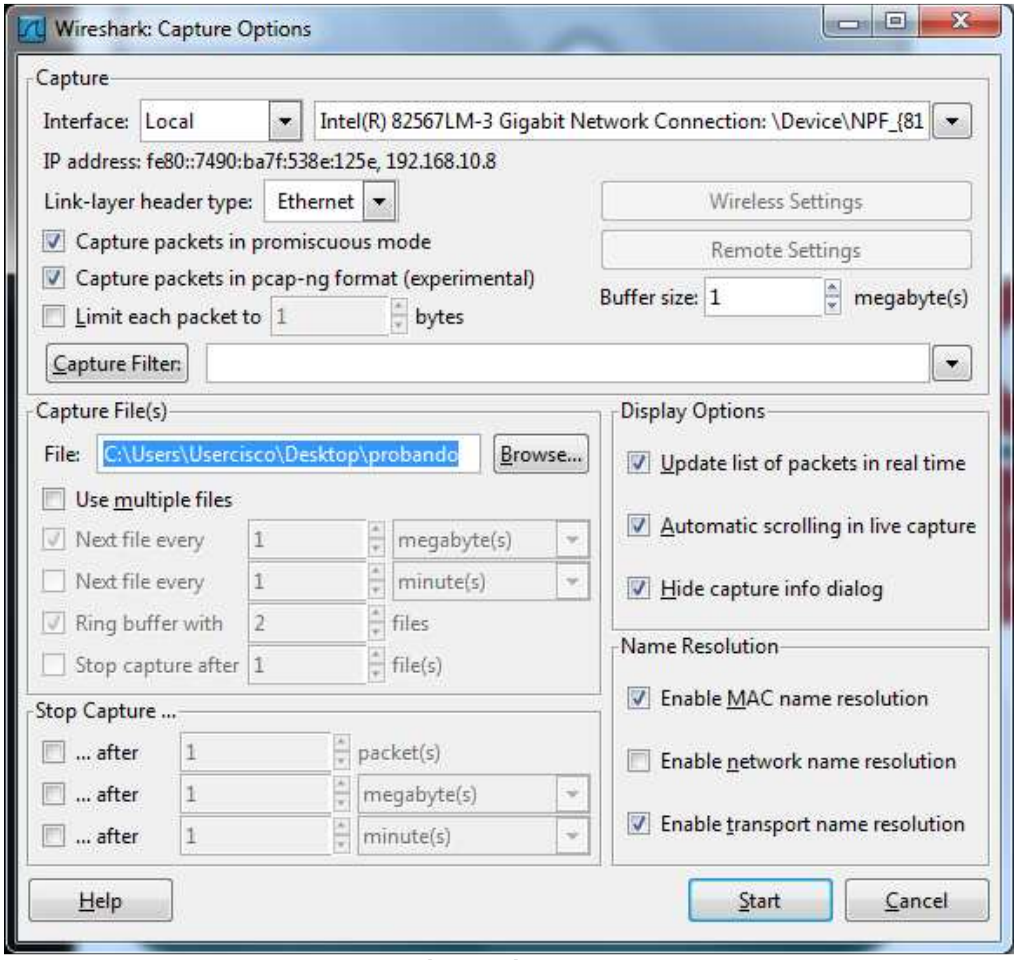
Captura de la voz en el sniffer Wireshark

1. Para la captura de paquetes presione la opción **Capture Options**



Captura de paquetes

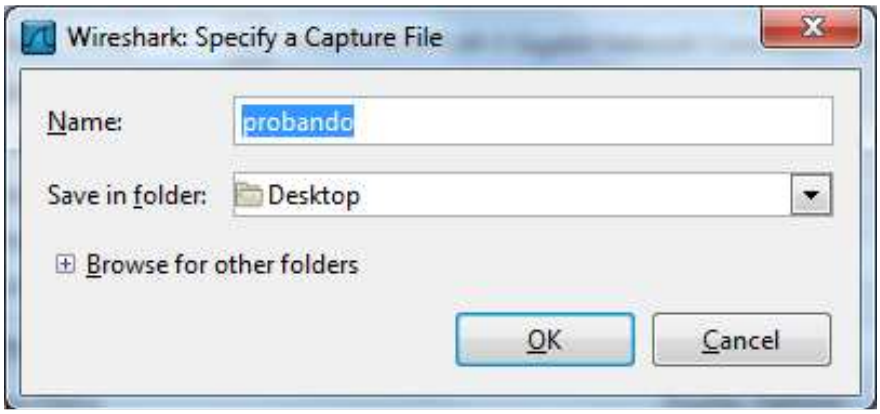
2. Una vez seleccionada la opción Capture Option aparece la siguiente pantalla



Opciones de captura

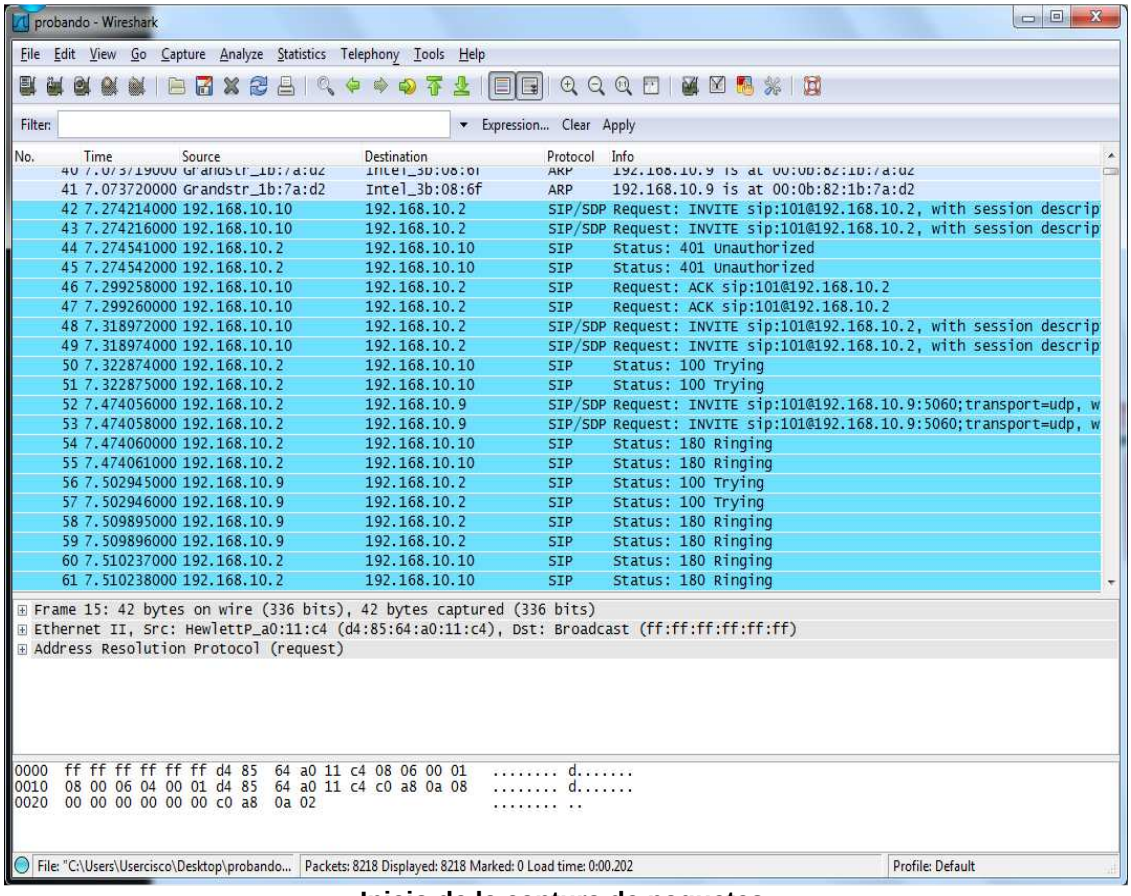
En este pantalla se selecciona las opciones Capture packets in pcap-ng format (experimental) y en Capture Files(s) seleccione File para escoger donde guardar la captura.

3. Se debe asignar un nombre y la carpeta donde se guarda la captura de los paquetes y presione OK



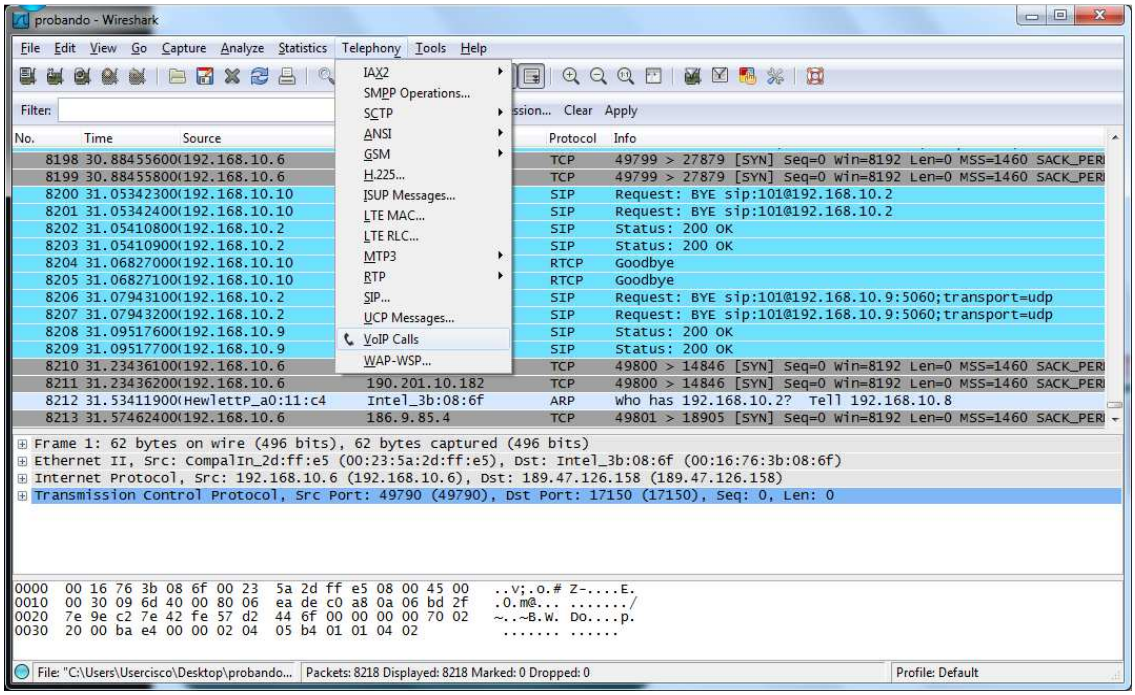
Ruta de la captura

4. Una vez realizado los pasos anteriores presione Start y comenzará la captura



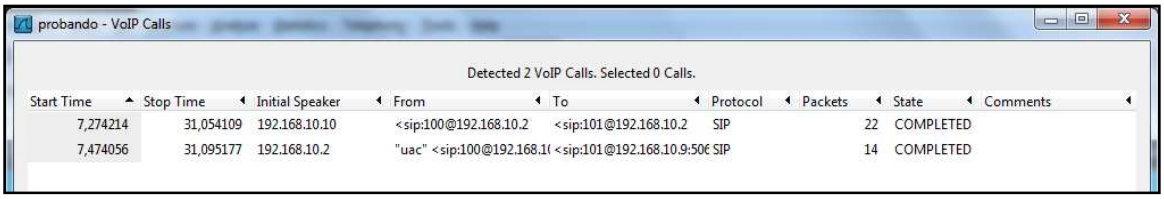
Inicio de la captura de paquetes

5. Al término de la captura seleccione la opción Telehony y escoja la opción VoIP Calls esta opción permite presentar la pantalla en la que indica las llamadas capturadas.



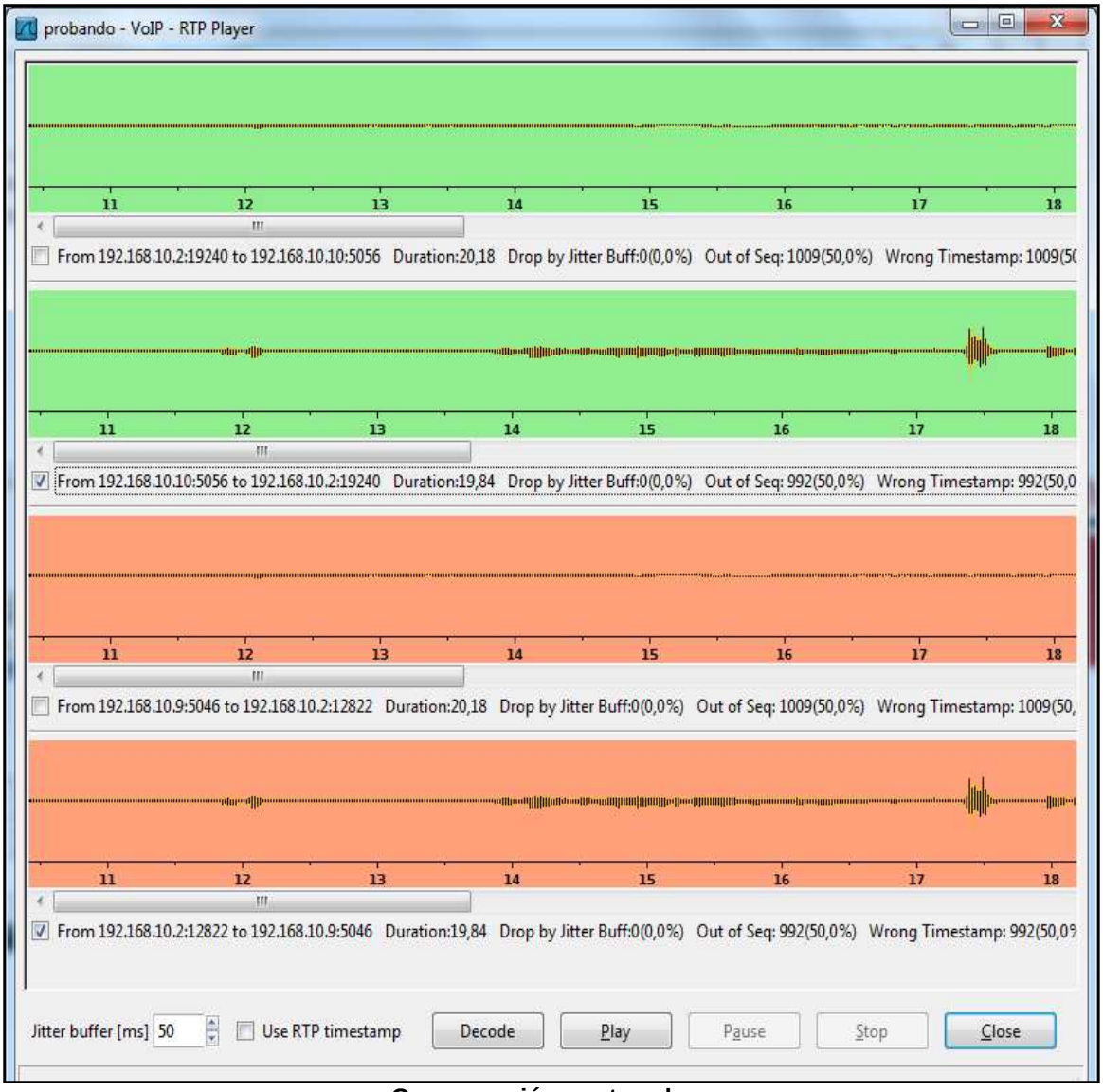
Verificar las llamadas capturadas

6. Se aparece la siguiente pantalla en la que indica los paquetes que han sido transmitidos mediante el protocolo SIP del origen al destino.



Paquetes transmitidos de origen a destino

7. Seleccione la opción Select All luego presione la opción Decode y le aparece la pantalla donde esta guardada la VoIP. Seleccione la opción 2 y 4 y presione play para escuchar la conversación.



Conversación capturada

10. Instalación de Softphone

Para la instalación del softphone que se utilizará para los clientes sip se debe seguir los siguientes pasos:

1. Doble clic sobre el instalador del softphone

Instalador del softphone

2. Seleccione el idioma que le ayudará en el proceso de instalación y presione Aceptar

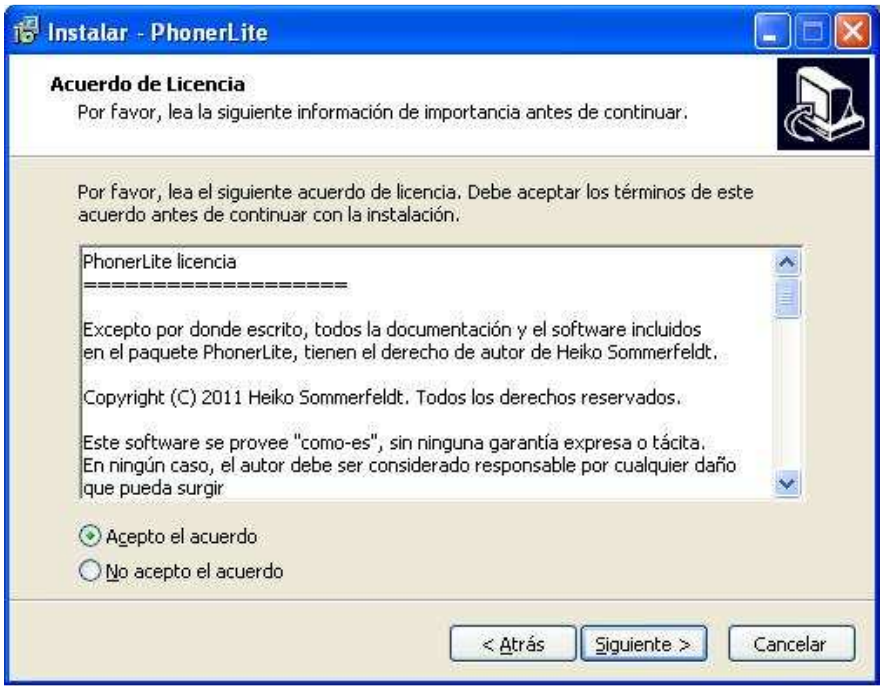
Idioma de la instalación

Escoja español que le guriara para una instalación correcta del softphone PhonerLite

3. Aparece la pantalla de Bienvenidos presione Aceptar para continuar con la instalación

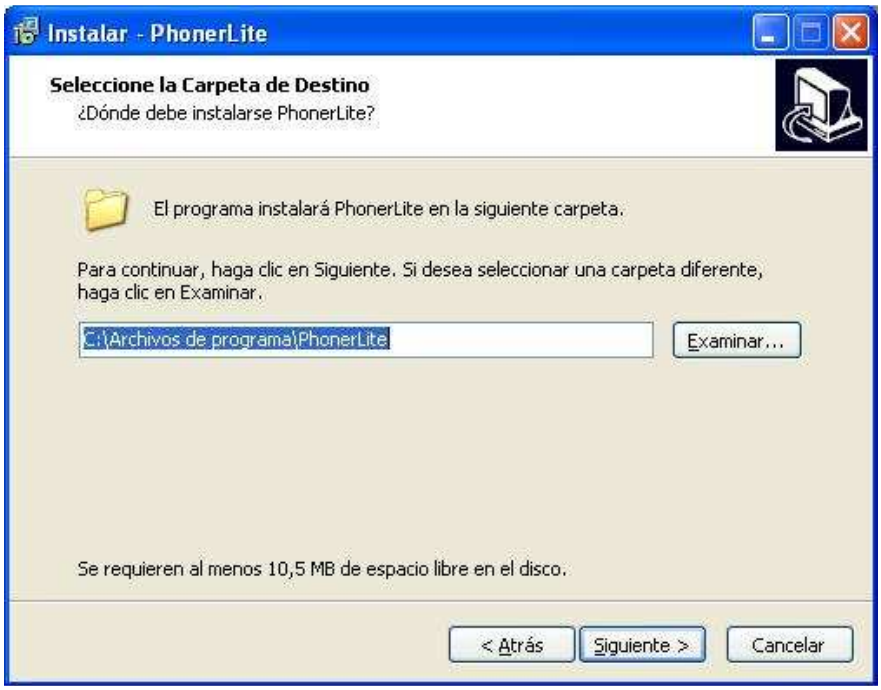
Pantalla de Bienvenida

4. Acepte el acuerdo de licencia y presione Siguiente



Licencia

5. Seleccione la ruta donde se instalará el softphone

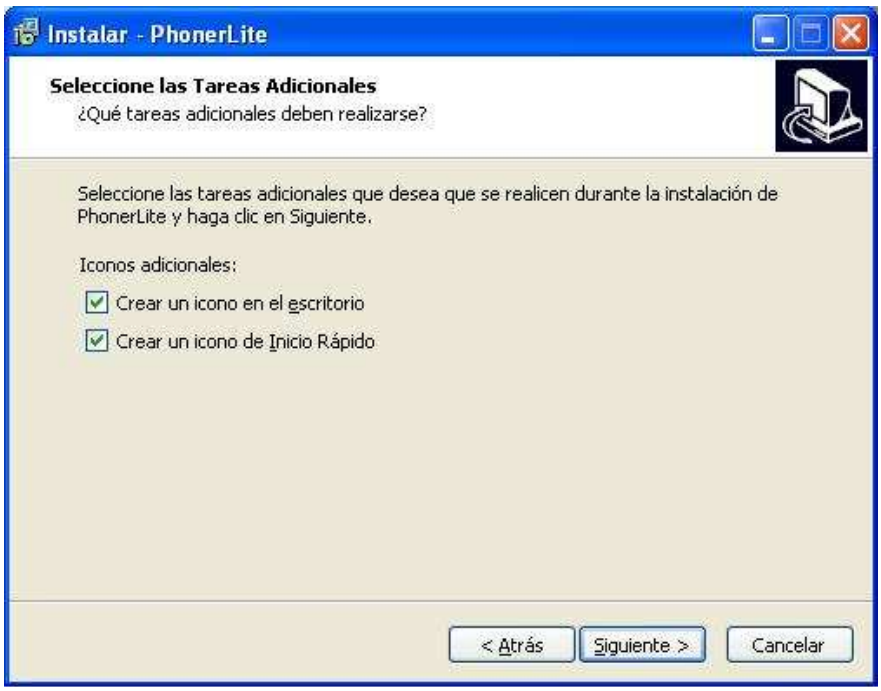


Ruta de instalación

6. Seleccione la carpeta del menú de inicio donde se colocarán los accesos directos del programa y presione Siguiente

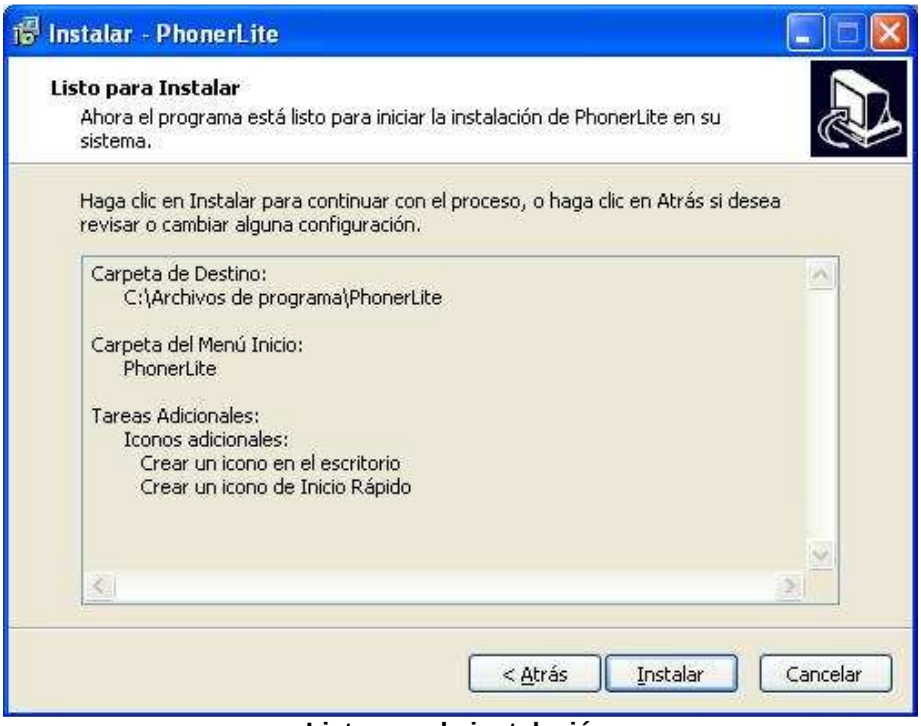
Carpeta de Inicio

7. Seleccione las tareas adicionales que desean que se realice durante la instalación y presione Siguiente



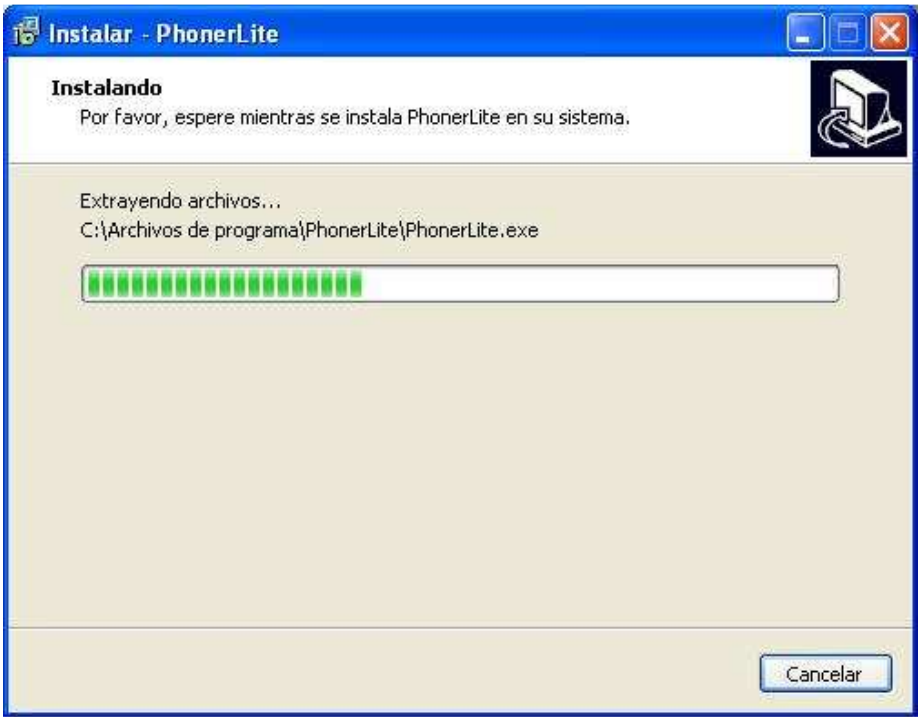
Tareas Adicionales

8. Presione Instalar para empezar el proceso de instalación



Listo para la instalación

9. El proceso de instalación ha empezado espere un momento hasta que finalice



Proceso de instalación en marcha

10. Una vez que se complete la instalación aparece la siguiente pantalla presione Finalizar

Instalación completa

11. Finalizada la instalación se debe configurar el cliente seleccione la opción Configuración Manual y digite la dirección del servidor al cual se van a conectar el cliente

Configuración del cliente

12. Llene los datos conforme a la información del cliente

Datos del cliente

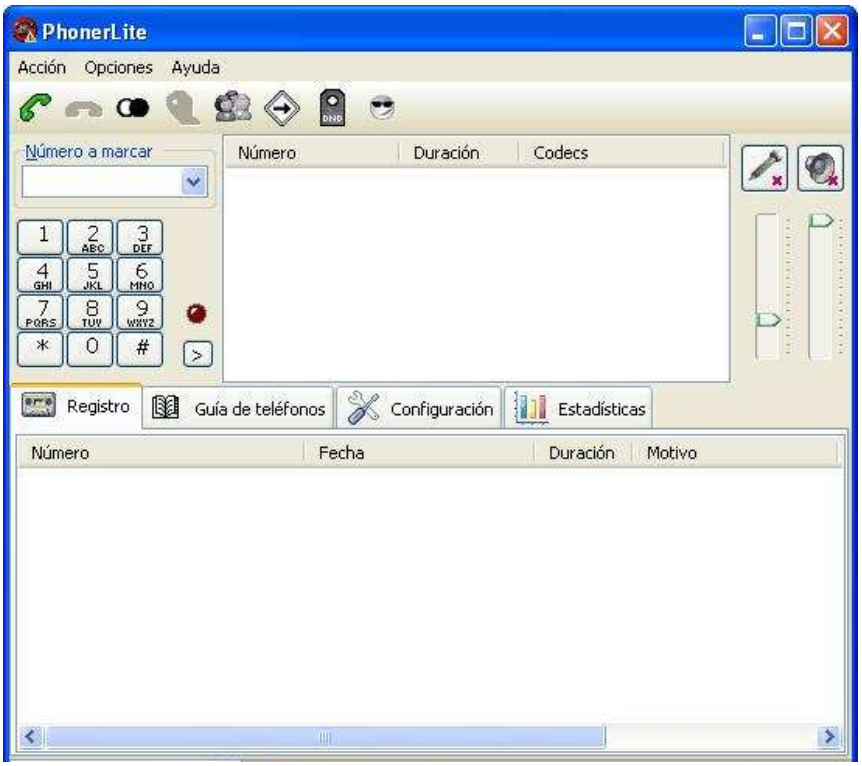
13. Seleccione el medio que se utilizará para el sonido

Sonido

14. Presione el icono  para confirmar la creación de la cuenta de usuario

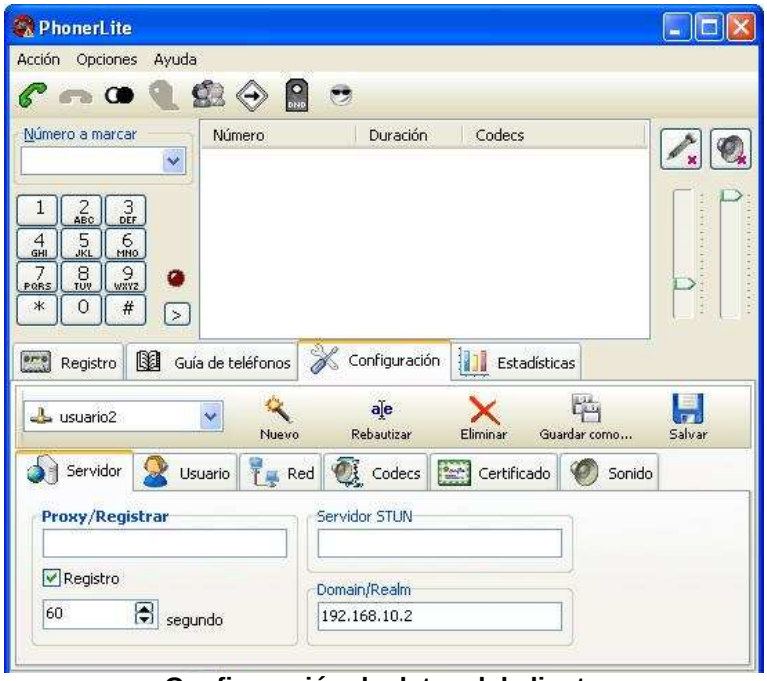
Confirmación de la cuenta del cliente

15. Pantalla de administración de PhonerLite



Administración de PhonerLite

16. Presione Configuración para verificar la información del cliente sea correcta si se debe realizar algún ésta es la pestaña que le ayudará para la administración del cliente



Configuración de datos del cliente

11. Configuración de TLS

Con el protocolo TLS todo el flujo de comunicación queda encriptado y sin posibilidad de ser “interceptado” por personas ajenas a la conversación.

La implementación de TLS se realizará por medio de Openssl para ello en el servidor Elastix instalarlo con el comando yum install Openssl.

El primer paso es crear un certificado autofirmado, necesario para la autenticación de los dispositivos.

Se selecciona la localización del certificado.
cd /etc/asterisk

Con openssl se crea una clave privada:
openssl genrsa 1024 > host.key

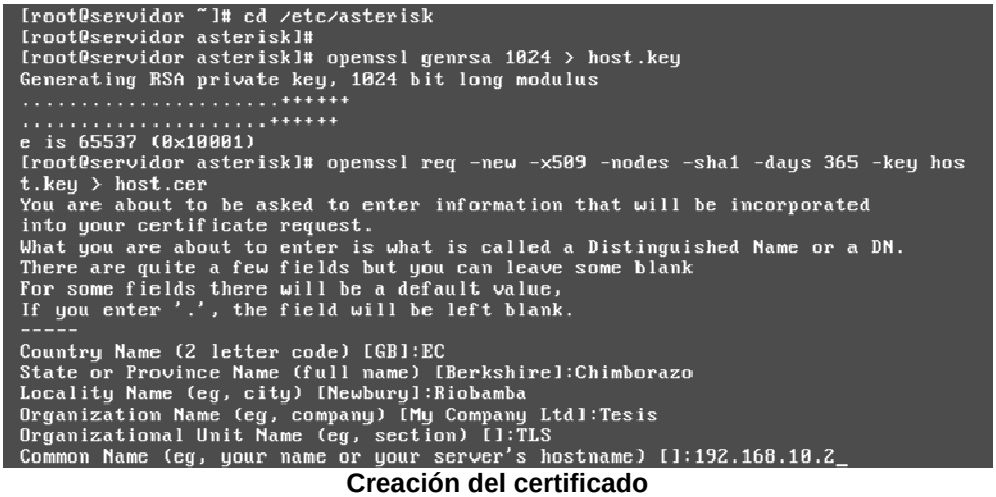
Luego se debe crear un certificado firmado con la clave privada recién creada con la siguiente línea de comandos:

openssl req -new -x509 -nodes -sha1 -days 365 -key host.key > host.cert

Luego de ejecutar la línea de comandos se debe completar la información necesaria para el certificado:

La consola entregará el siguiente mensaje:
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:EC
State or Province Name (full name) [Berkshire]:Chimborazo
Locality Name (eg, city) [Newbury]:Riobamba
Organization Name (eg, company) [My Company Ltd]:Tesis
Organizational Unit Name (eg, section) []:TLS
Common Name (eg, your name or your server's hostname) []:**192.168.10.2**
Email Address []:dcchs3490@yahoo.es



Creación del certificado

La parte más importante del certificado es el Common Name donde se debe indicar el dominio o IP que luego se usará para conectar los terminales SIP.

Una vez que se tiene los dos archivos se debe crear un nuevo archivo que contenga los dos:
cat host.cert host.key > asterisk.pem

Configuración de Asterisk

Primero se configura el archivo sip_general_custom.conf y se añaden las siguientes líneas:
tlsenable=yes
tlsbindaddr=192.168.10.2
tlscertfile=/etc/asterisk/asterisk.pem

Con la primera línea se activa el soporte TLS. La segunda línea define la dirección IP que Asterisk usará para aceptar las conexiones (si no se define el puerto, el predefinido será el 5061). La tercera línea define la carpeta y nombre del archivo que contiene el certificado.

Para cada extensión (usuario) que usará el protocolo TLS para conectarse a Asterisk, se añade la línea en el archivo sip_additional.conf:
transport=tls

Se guardan los cambios y se deben reiniciar los servicios

Entre en la consola de asterisk con el siguiente comando
asterisk –rvvvvvvvvvvvvvvvvvvvv

Actualice la configuración SIP
CLI>**sip reload**

Aparece entre las distintas líneas que el certificado SSL fue creado
SSL certificate ok

Se debe configurar el softphone PonerLite en cada cliente para que utilice el protocolo TLS

PhonerLite

Para hacer esto por medio de la web copiamos el archivo host.cer en ese computador y lo podemos instalar clicando sobre el archivo. Empezará el proceso de instalación del certificado.

Una vez terminado tenemos que asegurarnos que ese certificado esté entre la lista de los certificados en que se confía.

Instalación del certificado

Para la instalación del certificado se debe seguir los siguientes pasos:

1. Doble clic sobre el icono para inciar el proceso de instalación del certificado

Icono de instalación del certificado

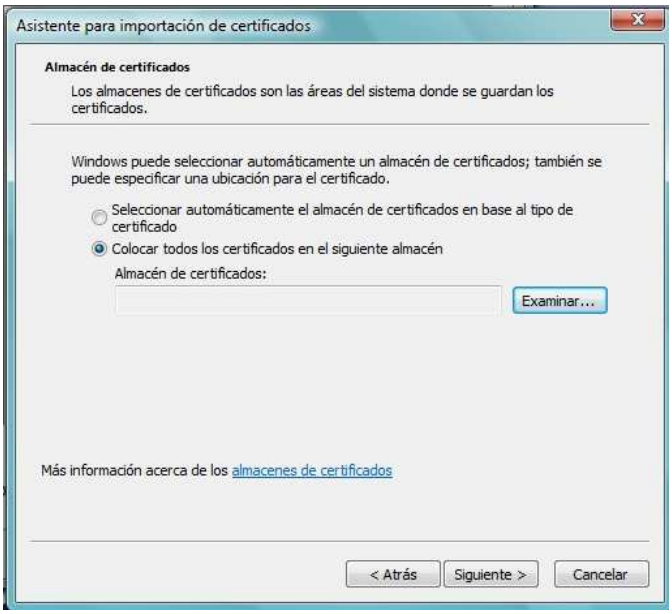
2. Información del certificado que se va a instalar

Información del certificado

3. La siguiente pantalla muestra el asistente para importación de certificados

Asistente de importación de certificados

4. Examine el almacén donde se guardara el certificado



Examine el almacén de certificados

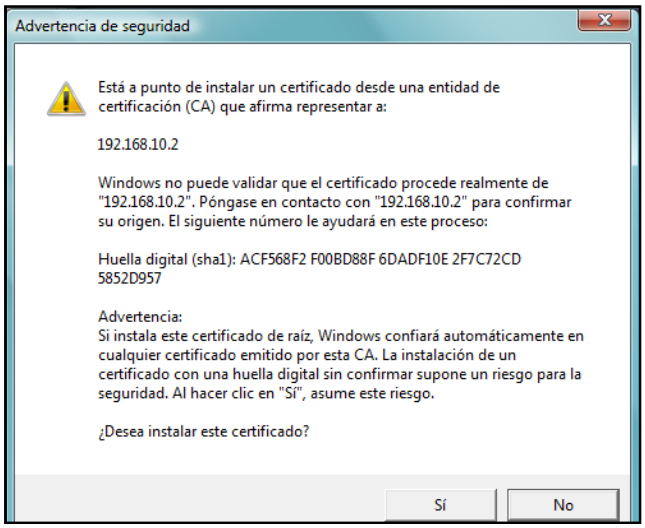
5. Seleccione la carpeta Entidades de certificación raíz de confianza para guardar el certificado

Almacén de certificados

6. Una vez escogida el almacén de certificados presione Siguiente para finalizar la importación del certificado

Incorporación del certificado al almacén raíz

7. Le aparece la pantalla de advertencia de seguridad ya que al instalar el certificado en la carpeta raíz Windows confiará automáticamente en el certificado emitido por esta CA.



Advertencia de seguridad

8. La importación del certificado se completo correctamente

Importación completa

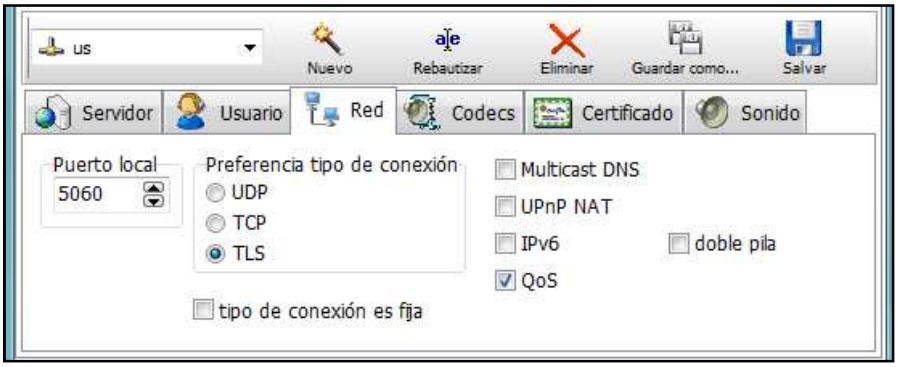
9. Una vez finalizada la importación del certificado se muestra la información del mismo

Información del certificado

10. Detalles del certificado

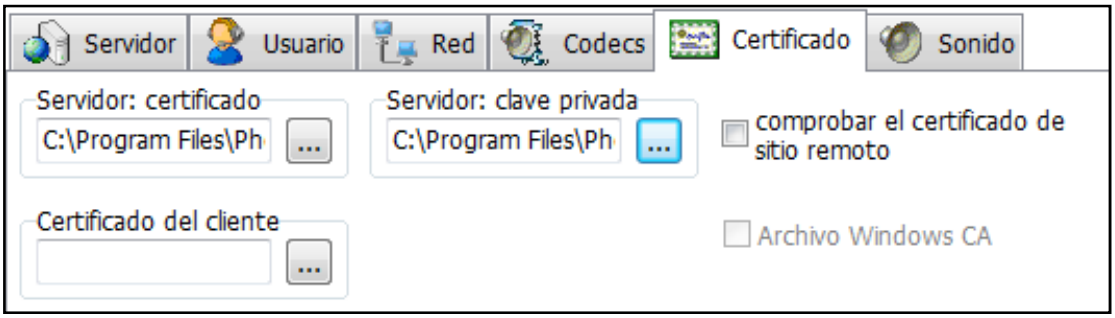
Detalles del certificado

Luego de la instalación del certificado en cada uno de los clientes se debe configurar en el softphone PonerLite cada cliente para que utilice el protocolo TLS



Selección de TLS

En la figura se puede ver las opciones que deben ser seleccionadas para la activación del certificado del servidor y su respectiva clave.



Localización de los certificados.

ANEXO 5

TABLA DE DISTRIBUCIÓN

T-STUDENT

Tabla de Distribución t de Student

x \ n	1	2	4	5	6	7	8	9	10	15	20	25	30	40	50
0,00	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500
0,05	0,516	0,518	0,519	0,519	0,519	0,519	0,519	0,519	0,519	0,520	0,520	0,520	0,520	0,520	0,520
0,10	0,532	0,535	0,537	0,538	0,538	0,538	0,539	0,539	0,539	0,539	0,539	0,539	0,539	0,540	0,540
0,15	0,547	0,553	0,556	0,557	0,557	0,558	0,558	0,558	0,558	0,559	0,559	0,559	0,559	0,559	0,559
0,20	0,563	0,570	0,574	0,575	0,576	0,576	0,577	0,577	0,577	0,578	0,578	0,578	0,579	0,579	0,579
0,25	0,578	0,587	0,593	0,594	0,595	0,595	0,596	0,596	0,596	0,597	0,597	0,598	0,598	0,598	0,598
0,30	0,593	0,604	0,610	0,612	0,613	0,614	0,614	0,615	0,615	0,616	0,616	0,617	0,617	0,617	0,617
0,35	0,607	0,620	0,628	0,630	0,631	0,632	0,632	0,633	0,633	0,634	0,635	0,635	0,636	0,636	0,636
0,40	0,621	0,636	0,645	0,647	0,648	0,649	0,650	0,651	0,651	0,653	0,653	0,654	0,654	0,654	0,655
0,45	0,635	0,652	0,662	0,664	0,666	0,667	0,668	0,668	0,669	0,670	0,671	0,672	0,672	0,672	0,673
0,50	0,648	0,667	0,678	0,681	0,683	0,684	0,685	0,685	0,686	0,688	0,689	0,689	0,690	0,690	0,690
0,55	0,660	0,681	0,694	0,697	0,699	0,700	0,701	0,702	0,703	0,705	0,706	0,706	0,707	0,707	0,708
0,60	0,672	0,695	0,710	0,713	0,715	0,716	0,717	0,718	0,719	0,721	0,722	0,723	0,723	0,724	0,724
0,65	0,683	0,709	0,724	0,728	0,730	0,732	0,733	0,734	0,735	0,737	0,738	0,739	0,740	0,740	0,741
0,70	0,694	0,722	0,739	0,742	0,745	0,747	0,748	0,749	0,750	0,753	0,754	0,755	0,755	0,756	0,756
0,75	0,705	0,734	0,753	0,756	0,759	0,761	0,763	0,764	0,765	0,768	0,769	0,770	0,770	0,771	0,772
0,80	0,715	0,746	0,766	0,770	0,773	0,775	0,777	0,778	0,779	0,782	0,783	0,784	0,785	0,786	0,786
0,85	0,724	0,758	0,778	0,783	0,786	0,788	0,790	0,791	0,792	0,796	0,797	0,798	0,799	0,800	0,800
0,90	0,733	0,768	0,790	0,795	0,799	0,801	0,803	0,804	0,805	0,809	0,811	0,812	0,812	0,813	0,814
0,95	0,742	0,779	0,802	0,807	0,811	0,813	0,815	0,817	0,818	0,821	0,823	0,824	0,825	0,826	0,827
1,00	0,750	0,789	0,813	0,818	0,822	0,825	0,827	0,828	0,830	0,833	0,835	0,837	0,837	0,838	0,839
1,05	0,758	0,798	0,824	0,829	0,833	0,836	0,838	0,839	0,841	0,845	0,847	0,848	0,849	0,850	0,851
1,10	0,765	0,807	0,833	0,839	0,843	0,846	0,848	0,850	0,851	0,856	0,858	0,859	0,860	0,861	0,862
1,15	0,772	0,815	0,843	0,849	0,853	0,856	0,858	0,860	0,862	0,866	0,868	0,869	0,870	0,872	0,872
1,20	0,779	0,823	0,852	0,858	0,862	0,865	0,868	0,870	0,871	0,876	0,878	0,879	0,880	0,881	0,882
1,25	0,785	0,831	0,860	0,867	0,871	0,874	0,877	0,879	0,880	0,885	0,887	0,889	0,890	0,891	0,891
1,30	0,791	0,838	0,868	0,875	0,879	0,883	0,885	0,887	0,889	0,893	0,896	0,897	0,898	0,899	0,900
1,35	0,797	0,845	0,876	0,883	0,887	0,890	0,893	0,895	0,897	0,901	0,904	0,905	0,906	0,908	0,908
1,40	0,803	0,852	0,883	0,890	0,894	0,898	0,900	0,902	0,904	0,909	0,912	0,913	0,914	0,915	0,916
1,45	0,808	0,858	0,890	0,897	0,901	0,905	0,907	0,910	0,911	0,916	0,919	0,920	0,921	0,923	0,923
1,50	0,813	0,864	0,896	0,903	0,908	0,911	0,914	0,916	0,918	0,923	0,925	0,927	0,928	0,929	0,930
1,55	0,818	0,869	0,902	0,909	0,914	0,917	0,920	0,922	0,924	0,929	0,932	0,933	0,934	0,935	0,936
1,60	0,822	0,875	0,908	0,915	0,920	0,923	0,926	0,928	0,930	0,935	0,937	0,939	0,940	0,941	0,942
1,65	0,827	0,880	0,913	0,920	0,925	0,929	0,931	0,933	0,935	0,940	0,943	0,944	0,945	0,947	0,947
1,70	0,831	0,884	0,918	0,925	0,930	0,934	0,936	0,938	0,940	0,945	0,948	0,949	0,950	0,952	0,952
1,75	0,835	0,889	0,922	0,930	0,935	0,938	0,941	0,943	0,945	0,950	0,952	0,954	0,955	0,956	0,957

BIBLIOGRAFÍA

1. **LUCA DE TENA, JUAN IGNACIO**. Sams Teach Yourself Networking in 24 Hours/ Manual Imprescindible de Redes, Madrid, Anaya Multimedia. Grupo Anaya, 2010. pp. 379, 381, 394, 396.

2. **GÓMEZ, JULIO Y GIL, FRANCISCO.** VoIP y Asterisk Redescubriendo la Telefonía, México, Alfaomega, 2009. pp. 245-266

BIBLIOGRAFÍA INTERNET

3. CAPA DE CONEXIÓN SEGURA (SSL)

http://es.kioskea.net/contents/crypto/ssl.php3

2010-10

http://www.tecnologiahechapalabra.com/tecnologia/glosario_tecnico/articulo.asp?i=4397

2011-03

http://andres-seguridad.blogspot.com/2008/05/ssl-secure-sockets-layer.html

2011-03

4. MODELO OSI

http://es.wikipedia.org/wiki/Modelo_OSI

2010-08

http://www.ie.itcr.ac.cr/faustino/Redes/Clase1/1.1ModeloOSI.pdf

2010-08

5. **MODELO TCP/IP**

http://www4.uji.es/~al019803/tcpip/paginas/CapaAplicacion.htm

2010-08

http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet

2010-08

6. **PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)**

http://es.wikipedia.org/wiki/Capa_de_transporte

2010-10

http://www.saulo.net/pub/tcpip/b.htm
2010-10
http://es.wikipedia.org/wiki/Transmission_Control_Protocol
2010-11
http://es.kioskea.net/contents/internet/tcp.php3
2010-11

7. **PROTOCOLO DE CONTROL DE TRANSPORTE DE TIEMPO REAL (RTCP)**

http://es.wikipedia.org/wiki/Real_time_control_protocol
2010-11
http://es.wikipedia.org/wiki/RTP/RTCP
2010-11
http://es.kioskea.net/contents/internet/rtcp.php3
2010-11

8. **PROTOCOLO DE DATAGRAMA DE USUARIO (UDP)**

http://es.wikipedia.org/wiki/User_Datagram_Protocol
2010-10
http://www.masadelante.com/faqs/udp
2010-10
http://es.kioskea.net/contents/internet/udp.php3
2010-11

9. **PROTOCOLO DE ENRUTAMIENTOEIGRP**

http://es.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol
2010-09
http://www.garciagaston.com.ar/verpost.php?id_noticia=204
2010-09
http://www.dsi.uclm.es/asignaturas/42650/PDFs/practica4.pdf
2010-09

10. PROTOCOLO DE INICIO DE SESIONES (SIP)

http://www.quarea.com/tutorial/sip_session_initiation_protocol
2010-09

http://www.quarea.com/tutorial/sip_session_initiation_protocol
2010-09
http://www.telefoniaip.uchile.cl/capacitacion_telefonia.htm
2010-09
https://www.tlm.unavarra.es/investigacion/seminarios/slides/20080516_Juanra_Apuntes_de_Seguridad_en_SIP.pdf
2010-10
http://trajano.us.es/~fornes/RSR/2005/SIP/PresentacionSIP.ppt
2010-10
https://www.tlm.unavarra.es/investigacion/seminarios/slides/20080516_Juanra_Apuntes_de_Seguridad_en_SIP.pdf
2010-10

11. PROTOCOLO DE INTERNET (IP)

http://es.kioskea.net/contents/internet/protip.php3
2010-09
http://www.dte.us.es/tec_inf/itis/sis_dist/Tema_IP.pdf
2010-09

12. PROTOCOLO DE SEGURIDAD DE INTERNET (IPsec)

http://www.dragonjar.org/ipsec-las-redes-del-futuro-cercano.xhtml
2010-09
http://www.networkworld.es/Telefonia-IP-segura-con-Secure-SIP/seccion-/articulo-177105
2010-10
http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/ch10s02.html
2010-10
http://www.cu.ipv6tf.org/pdf/victor_villagra.pdf
2010-11

13. PROTOCOLO DE TRANSPORTE DE TIEMPO REAL (RTP)

http://es.kioskea.net/contents/internet/rtcp.php3
2010-11
http://www.arcesio.net/rtp/rtprtcp3.html
2010-11

http://manuelasanchezdl.blogspot.com/2009/01/protocolo-rtprtcp.html
2010-11

14. ROUTER

http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1616/ccmigration_09186a00802c35a2.pdf
2011-01

15. SEGURIDAD DE LA CAPA DE TRANSPORTE (TLS)

http://seguridadvoip.wordpress.com/2010/10/14/implementacion-del-protocolo-tls-en-asterisk/
2010-11
http://es.wikipedia.org/wiki/Transport_Layer_Security
2010-11
http://www.naguissa.com/universidad/wiki-td/SSL_TLS.html
2010-11
http://es.wikipedia.org/wiki/Transport_Layer_Security
2010-12
http://www.monografias.com/trabajos74/protocolo-tls-transport-layer-security/protocolo-tls-transport-layer-security.shtml
2011-01
http://www.uv.es/sto/cursos/seguridad.java/html/sjava-25.html
2011-02

16. SOLUCIÓN DE CONECTIVIDAD BASADA EN SOFTWARE (Open VPN)

http://www.bellera.cat/josep/pfsense/openvpn_cs.html
2011-02

17. TELEFONÍA IP

http://www.usergioarboleda.edu.co/grupointernet/telefonia.htm
2010-09
http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet
2010-09
http://www.telefoniaip.uchile.cl/capacitacion_telefonia.htm
2010-09

18. VULNERABILIDADES SIP

http://www.gestiopolis.com/administracion-estrategia/vulnerabilidades-en-la-convergencia-ip.htm
2010-09
http://bibdigital.epn.edu.ec/bitstream/15000/2186/1/CD-2938.pdf
2010-09
http://bibdigital.epn.edu.ec/bitstream/15000/81/1/CD-0052.pdf
2010-10
http://www.javirodriguez.com.es/?tag=sip
2010-10
http://www.socinfo.es/contenido/seminarios/vasco2/justicia.pdf
2010-10