Universidad Tecnológica Nacional

Proyecto Final

Central de telefonía IP
Migración a las nuevas tecnologías de redes

Autor:

- Oviedo, Julián Ariel

Director:

Proyecto final presentado para cumplimentar los requisitos académicos para acceder al título de Ingeniero electrónico

en la

Facultad Regional Paraná

Fecha

Noviembre de 2017

Declaración de autoría:

Yo declaro que el Proyecto Final “Central de telefonía IP, Migración a las nuevas tecnologías de redes” y el trabajo realizado es propio.
Declaro/s:

- Este trabajo fue realizado en su totalidad, o principalmente, para acceder al título de grado de Ingeniero electrónico, en la Universidad Tecnológica Nacional, Regional Paraná.
- Se establece claramente que el desarrollo realizado y el informe que lo acompaña no han sido previamente utilizados para acceder a otro título de grado o pre-grado.
- Siempre que se ha utilizado trabajo de otros autores, el mismo ha sido correctamente citado. El resto del trabajo es de autoría propia.
- Se ha indicado y agradecido correctamente a todos aquellos que han colaborado con el presente trabajo.
- Cuando el trabajo forma parte de un trabajo de mayores dimensiones donde han participado otras personas, se ha indicado claramente el alcance del trabajo realizado.

Firma:

Fecha:

Agradecimientos:

A mis padres, a su esfuerzo que me ha permitido desarrollarme personalmente y académicamente.

A mi hermano, abuelos, tíos, primos que siempre me han apoyado.

A la Universidad Tecnológica Nacional, institución pública, gratuita y de nivel en la República Argentina.

Universidad Tecnológica Nacional

Abstract

Facultad Regional Paraná

Ingeniero en Electrónica

Título

Oviedo, Julián Ariel

Abstract:

In order to implement a solution in the field of business communications on the region and following the changes and advances in telephony systems applied to packet networks. It was decided to develop and implement an IP PBX which provides support for voice and video communications, considering the security, encryption and authentication of the user's information on the service. Taking advance of the network infrastructure for the general internet use, a telephony data packages prioritization is required for it. Besides, a migration to IPv6 network protocol and interconnection to switched telephone network (PSTN) completes the network system develop.

To achieve the stipulated above, it was decided to use the Asterisk's framework to implement all the IP PBX modules and services. A Mikrotik RB2011 router is selected as the main network equipment. IPsec is the protocol chosen to implement a virtual private network, a VPN. Regarding IPv6 network support, the selected providers are Hurricane Electric and NetAssist; this upgrade is done with a 6to4 tunnel through the internet public network. To extends the IP PBX coverage a trunk connection is implemented with Netelip which is a VoIP provider and gives to possibility to get virtual telephone numbers for it. The migration of IP network technology is achieved by making a connection to the PSTN network through Grandstream's HT503 voice gateway.

The result is a complete IP-PBX system which it is able to provide all the services mentioned before in a reliable, inexpensive and robust manner.

Keywords*: IPv6, IPv4, Internet, GNU Linux, Debian, Asterisk, PBX, Mikrotik, QoS, PSTN, VPN, IPsec, Voice gateway, Tunnel Broker, DID.*

Resumen:

Con el fin de implementar una solución en el ámbito de las comunicaciones empresariales y de instituciones en la región, siguiendo los cambios y avances en los sistemas de telefonía aplicados a redes de paquetes. Se decidió desarrollar e implementar una central de telefonía IP que brinde soporte para comunicaciones de voz y video, considerando la seguridad, encriptación y autenticación de la información de los usuarios que utilicen el servicio; así como también el aprovechamiento de la infraestructura de la red para el uso general de internet, priorizando los paquetes de telefonía. Se considera al mismo tiempo la migración al protocolo de red IPv6 y la interconexión a la red telefónica conmutada, PSTN, para la transmisión de voz.

Con el fin de lograr lo especificado anteriormente se optó por utilizar el framework Asterisk para implementar todos los módulos y servicios de la central de telefonía IP y un router Mikrotik RB2011 como equipo principal de red. IPsec es el protocolo elegido para implementar una red privada virtual (VPN). Con respecto al soporte de red IPv6, los proveedores seleccionados son Hurricane Electric y NetAssist; dicha actualización se alcanza mediante un túnel 6to4 en la red pública de internet. Para extender la cobertura de la central de telefonía IP a nivel mundial, se implementa una conexión troncal con el proveedor VoIP Netelip mediante la compra de números telefónicos virtuales y una conexión troncal SIP entre ambas centrales. La migración a las tecnologías de redes IP se completa realizando la priorización del tráfico de voz sobre los demás servicios y una conexión con la red PSTN mediante el voice gateway HT503 de Grandstream.

El resultado es una central de telefonía IP capaz de brindar todos los servicios anteriormente mencionados de manera confiable, económica y robusta.

Palabras Clave: *IPv6, IPv4, Internet, GNU Linux, Debian, Asterisk, PBX, Mikrotik, QoS, PSTN, VPN, IPsec, Voice gateway, Tunnel Broker, DID.*

Reconocimientos:

A todos los docentes y compañeros que me acompañaron en la carrera.

Índice

Capítulo 1: Introducción 1
Objetivos del proyecto 2
Elementos involucrados en el proyecto 2
Estudio de mercado 3
Pruebas de concepto. ¿Es un producto útil? 9
Capítulo 2: Desarrollo 12
Plataforma 12
Framework Asterisk 13
Comenzando con Asterisk 15
Servidor SSMTP 16
Configuración de los parámetros y funcionalidades de Asterisk 17
sip.conf 18
extensions.conf 21
voicemail.conf 25
confbridge.conf 26
IVR – Respuesta de voz interactiva 28
Red de área local (LAN) 29
Capa de enlace 29
Modo switch 30
Implementación de la capa de enlace en el router Mikrotik RB2011 32
Implementación de IPv6 33
Enrutamiento, prefijo y tipo de identificación de direcciones en IPv6 34
Direcciones implementadas – Unicast 35
Link local address y Global address 35
Configurando RouterOS para IPv6 36
El inconveniente de implementar IPv6 con telefonía IP 37
Pila doble (dual stack) 37
Diagrama de red con pila doble 40
La red pública – internet 40
Network Address Traslation (NAT) 41
6to4 tunnel – Tunnel Broker 43
Hurricane electric 45
NetAssist tunnel broker 48
Firewall 49
Red Privada Virtual (VPN) 50
Protocolo de tunelamiento a utilizar 53
Modos de funcionamiento 54
Protocolos - Encabezados 54
Elección de modo de funcionamiento y protocolo 55

Nivel de encriptación 55
Autenticación e integridad 56
Código a implementar en RouterOS 56
Tipos de conexiones 58
Problemas - NAT 59
Clientes VPN 61
Calidad de Servicio - QoS 62
Calidad de servicio en RouterOS 62
Mangle 66
Arboles de colas 67
Conexión a red PSTN 67
Interfaces FXO/FXS 68
Voice Gateway Grandstream HT503 69
Configuración 70
SIP trunking - Proveedor de telefonía. 76
Configurando nuestra central Asterisk con SIP trunking 79
Capítulo 3: Resultados 81
Capítulo 4: Análisis de Costos 90
Capítulo 5: Discusión y Conclusión 91
Capítulo 6: Literatura Citada 93

Lista de Figuras:

Ilustración 1 - Central IP PBX Grandstream....4
Ilustración 2 - Central IP PBX Grandstream....4
Ilustración 3 - Central IP Panasonic....4
Ilustración 4 - Central IP Yeastar....5
Ilustración 5 - Logos de frameworks de telefonía sobre IP....6
Ilustración 6 - Plataformas de softphones....7
Ilustración 7 - Voice gateway Grandstream....8
Ilustración 8 - Voice gateway Sangoma....8
Ilustración 9 - Voice gateway Digium PCI....8
Ilustración 10 - Diagrama de bloque general....12
Ilustración 11 - Menu select....15
Ilustración 12 - Diagrama de extensiones....17
Ilustración 13 - Diagrama de red LAN....29
Ilustración 14 - Diagrama de puertos....32
Ilustración 15 - Diagrama de puertos....32
Ilustración 16 - Mikrotik RB2011 y switch Atheros 8327....33
Ilustración 17 - Notación IPv6....34
Ilustración 18 - Direcciones Unicast....35
Ilustración 19 - Diagrama de red LAN y direcciones IPv6....37
Ilustración 20 - Direcciones de host conectado a la red LAN....39
Ilustración 21 - Protocolos en pila doble....39
Ilustración 22 - Encabezados de red....39
Ilustración 23 - Diagrama de red y pila doble....40
Ilustración 24 - Diagrama de red y NAT....41
Ilustración 25 - Diagrama de red y NAT....42
Ilustración 26 - Estructura de paquete RTP....43
Ilustración 27 - Encapsulamiento paquete IPv6....44
Ilustración 28 - Encapsulamiento paquete IPv6....44
Ilustración 29 - Diagrama de red túnel 6to4....44
Ilustración 30 - Hurricane network....45
Ilustración 31 - Parámetros de Hurricane tunel broker....46
Ilustración 32 - Diagrama general de túnel broker....48
Ilustración 33 - Diagrama de túnel broker generalizado....48
Ilustración 34 - NetAssit Tunel Broker....49
Ilustración 35 - Tunelamiento....51
Ilustración 36 - Tunelamiento L2TP....52
Ilustración 37 - Tunelamiento GRE....52
Ilustración 38 - Tunelamiento L2TP/IPsec....52
Ilustración 39 - PPTP inseguro....53
Ilustración 40 - Modos y protocolos IPsec....55
Ilustración 41 - IPsec túnel red a red....58
Ilustración 42 - IPsec túnel red a host....59
Ilustración 43 - IPsec túnel híbrido....59
Ilustración 44 - IPsec ESP túnel....60
Ilustración 45 - Cliente Shrew....61
Ilustración 46 - Cliente Shrew....62
Ilustración 47 - Flujo de paquetes RouterOS....63
Ilustración 48 - Flujo de paquetes entre puertos RouterOS....63
Ilustración 49 - Flujo de paquetes IPsec(encriptación)....64
Ilustración 50 - Referencia en flujo de paquetes RouterOS....65

Ilustración 51 - Flujos de paquetes RouterOS v6 65
Ilustración 52 - Flujos de paquetes y arboles de colas RouterOS v.6 65
Ilustración 53 - Referencias - RouterOS 66
Ilustración 54 - CIR y MIR RouterOS 67
Ilustración 55 - Puertos línea telefónica analógica 69
Ilustración 56 - Características Grandstream HT503 69
Ilustración 57 - Grandstream HT503 70
Ilustración 58 - HT503 configuración por Browser 71
Ilustración 59 - HT503 configuración por Browser 72
Ilustración 60 - HT503 configuración por Browser 72
Ilustración 61 - HT503 configuración por Browser 72
Ilustración 62 - HT503 configuración por Browser 72
Ilustración 63 - HT503 configuración por Browser 73
Ilustración 64 - HT503 configuración por Browser 73
Ilustración 65 - HT503 configuración por Browser 74
Ilustración 66 - HT503 configuración por Browser 74
Ilustración 67 - HT503 configuración por Browser 75
Ilustración 68 - HT503 configuración por Browser 75
Ilustración 69 - HT503 configuración por Browser 76
Ilustración 70 - HT503 configuración por Browser 76
Ilustración 71 - Servicio de telefonía IP 77
Ilustración 72 - Plataformas 77
Ilustración 73 - Troncal SIP 77
Ilustración 74 - Características de SIP trunking 78
Ilustración 75 - Troncal SIP 78
Ilustración 76 - Números virtuales adquiridos 78
Ilustración 77 - Tarifas nacionales 80
Ilustración 78 - Tarifas internacionales 80
Ilustración 79 - Ancho de banda 81
Ilustración 80 - Ancho de banda 82
Ilustración 81 - Ancho de banda videollamada 83
Ilustración 82 - Streaming de video 83
Ilustración 83 - Buzón de voz 84
Ilustración 84 - Buzón de voz 84
Ilustración 85 - IPs asignadas 84
Ilustración 86 - Firewall 85
Ilustración 87 - IPs asignadas a host en red 85
Ilustración 88 - IPv6 implementado con éxito 86
Ilustración 89 - Comprobación de conexión IPv6 86
Ilustración 90 - Ping a DNS de Google IPv6 87
Ilustración 91 - Ping a DNS de Google IPv4 87
Ilustración 92 - Usuarios conectados a la VPN 88
Ilustración 93 - Usuarios conectados a la VPN 88
Ilustración 94 - Marcado de paquetes 88
Ilustración 95 - Priorización y colas 89
Ilustración 96 - Llamada realizada a número celular desde interno 89
Ilustración 97 - Llamada realizada a número virtual 89

Lista de Abreviaciones

GPL – General Public License

ASIC – Application specific integrated circuit

Codec – Codificador, decodificador

OSI – Open System Interconnection

MAC – Media Access Control

CLI – Command Line Interface

IPv4 – IP versión 4

IPv6 – IP versión 6

LAN – Local Area Network

WAN – Wide Area Network

VLAN – Virtual LAN

WLAN – Wireless LAN

SMTP – Simple mail transfer protocol

DNS – Domain name system

QoS – Quality of services

VPN – Vitual private network

ISP – Internet service proveider

SIP – Session Initiation Protocol

NAT – Network address traslation

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

RTP – Real-time Transport Protocol

IVR – Interactive Voice Response

PBX – Private Branch Exchange

IPsec – Internet Protocol security

MTU – Maximum Transmission Unit

NSA – National Security Agency

PSTN – Public switched telephone network

PDH – Plesiochronous Digital Hierarchy

SDH – Synchronous Digital Hierarchy

VoIP – Voice over IP

FXS – Foreing Exchange Station

FXO – Foreign Exchange Office

SSH – Secure Shell

Dedicado a:

Mi familia.

Capítulo 1: Introducción

Muchos servicios están migrando de redes desarrolladas e implementadas por y para estos a redes de paquetes con soporte en el protocolo de red IP. Una de las principales razones es que este protocolo de red está basado en la transmisión y enrutamiento de paquetes en forma asíncrona, abstrayéndose tanto de la capa física como del acceso al medio constituido por la capa de enlace.

Podemos nombrar la migración de las señales de broadcast de radio y televisión (tanto analógicas como digital) a servidores en internet, denominados portales que ofrecen la misma señal.
A su vez los servicios OTT (Over The Top) permiten a proveedores vender streaming de audio y video a través de redes IP, como Netflix en cuanto a video o Spotify en cuanto a audio.
Por último, no podemos dejar de nombrar los servicios de mensajería de texto, correos electrónicos y redes sociales que han transformado la forma de comunicación interpersonal.

Todos estos contenidos pueden ser accedidos por diferentes dispositivos electrónicos, como PCs, laptops, celulares, Tablets, SmartTVs, etc. Y esto solo es posible gracias al concepto de paquete de información, los cuales pueden ser encapsulados en diferentes protocolos de acceso al medio físico. De esta forma la misma información puede ser accedida a través de señales satelitales por DVB-S2 o enlaces terrestres DVB-T; redes de telefonía móvil 3G, LTE 4G o 5G; redes de fibra óptica como FTTH; redes de cable coaxial por HFC; redes de par de cobre como ADSL, ADSL2, ADSL2++ o VDSL, etc.

La telefonía también está implementando una migración a estas redes asíncronas de paquetes, desde las tradicionales redes síncronas PDH y SDH. Pero con una diferencia sustancial con respecto a los demás servicios anteriormente mencionados y es que las llamadas de voz o videollamadas deben implementarse en tiempo real. A diferencia de un streaming de video donde los usuarios esperan un tiempo necesario mientras el buffer tiene la suficiente información correcta y ordenada para reproducir el contenido. Esto no es posible en telefonía ya que no permitiría una comunicación fluida y entendible entre las partes.

La transmisión de paquetes en redes de información implica que el enrutamiento y la capacidad de transmisión, dependan de la red en el momento específico, es así que la llegada al destino de los paquetes puede no ser ordenada y son los equipos receptores los encargados de agrupar la información según el orden correspondiente, generar las partes faltantes o corruptas si poseen FEC o en caso contrario pedir una retransmisión. De la misma forma puede producirse pérdidas o retrasos considerables.

Existen 3 problemas que pueden degradar una comunicación de voz o video en tiempo real. Estos son el tiempo de retraso en la transmisión, delay; la pérdida de paquetes de información, packet loss; y la variación en el tiempo de retraso de transmisión, jitter.

En la actualidad la mayoría de las personas han realizado una llamada a través de internet ya sea mediante un servicio VoIP, o servidores y aplicaciones como Skype, Whatsapp, etc. Y se han encontrado con la diferencia de calidad en comparación a una llamada realizada a través de una red tradicional. Notando retrasos en la transmisión o perdidas de información.
Por lo tanto, no solo hay beneficios en cuanto a costo económico y facilidad, flexibilidad de implementación de estos canales, sino que es necesario un desarrollo de ingeniería en redes para brindar calidad de servicio, confiabilidad y robustez. Sin dejar de considerar que internet es una red mundial por lo que es necesario confidencialidad que solamente la encriptación y autenticación del

mensaje entre las partes puede brindar, sumándoles un correcto manejo del acceso al sistema y asignación de credenciales.

Es este el motivo de la elección del tema en el trabajo final de la carrera ingeniería electrónica. La migración de las redes de telefonía se está llevando a cabo a nivel mundial en la fecha, año 2017. Muchas empresas e instituciones que poseen centrales de telefonía tradicional comienzan a utilizar centrales IP y aquellas que no poseen se posicionan frente a estas últimas por el costo económico de la red, la cual a su vez permite el flujo y transporte de otros servicios simultáneamente y posee un alcance mundial.
De la misma forma las empresas de servicio de telefonía comienzan a utilizar la tecnología VoIP sobre los diferentes tipos de redes de última milla.

Para el desarrollo es necesario poseer conocimiento de telefonía tradicional, networking, calidad de servicio, seguridad de información, encriptación y programación.

Objetivos del proyecto

El objetivo de este proyecto es el desarrollo e implementación de una central de telefonía IP completa con todos los elementos involucrados que se detallarán a continuación; de manera tal de obtener una solución económica, confiable y robusta la cual será base y modelo de presentación para desarrollos futuros.

Elementos involucrados en el proyecto

- Servidor.
- Framework de desarrollo.
- Router
- Switch
- Voice gateway
- Softphone
- Infraestructura de red.
- Protocolos de red (enrutamiento, seguridad y calidad de servicio)

Servidor: es el equipo físico sobre el cual se ejecutará la central de telefonía IP.

Framework de desarrollo: entorno de trabajo; módulos concretos de software que sirven de base para la implementación mediante la programación y la comunicación de las diferentes partes para brindar servicios en capa de aplicación. Incluye programas, funciones, bibliotecas y lenguaje interpretado para desarrollar y unir los diferentes módulos y componentes.

Router: equipo electrónico que desempeña sus funciones en la capa de red, capa 3 del modelo OSI; agregando funciones de capa superior.

Switch: equipo electrónico que desempeña sus funciones en la capa de enlace, capa 2 del modelo OSI.

Voice gateway: equipo electrónico que se desempeña como intermediario en la transmisión y recepción de mensajes de telefonía entre una red IP y una red PSTN o entre red IP y red de telefonía móvil 4G, 5G.

Softphone: aplicación o equipo físico que permite la comunicación de paquetes de señalización y datos entre usuarios.

Infraestructura de red: Conjunto de protocolos y medios físicos que permiten la comunicación entre los diferentes equipos o dispositivos electrónicos.

Protocolos de red (enrutamiento, seguridad y calidad de servicio): Conjunto de protocolos para el envío, transmisión y encaminamiento de los paquetes. Direccionamiento y traslación de direcciones. Seguridad y filtrado de paquetes. Priorización de paquetes según el servicio.

Estudio de mercado

Si bien cada uno de los elementos anteriormente mencionados se encuentran en el mercado, por lo que no se desarrollará nada nuevo con respecto a cada componente en específico. Hay que resaltar que no existe una solución para una central de telefonía IP final y completa ya que es necesario todos y cada uno de estas piezas en conjunto, considerando la compatibilidad y programación.

A su vez es una tarea multidisciplinaria en una empresa o institución que involucra diferentes departamentos y áreas.

Al departamento de IT (tecnología informática) para la asignación, gerencia y administración de las cuentas de telefonía, manejo de los números internos asignando a cada usuario las credenciales según su tarea y de esta manera configurar el voicemail, grupos de timbrado, IVR, según sea el caso. Instalación, mantenimiento y configuración de softphones.

Involucra al departamento de Networking para la asignación de direcciones y subredes, configuración y planeamiento de la red con respecto al enrutamiento, configuración de las reglas de firewall y NAT, configuración de VPN y sus credenciales, priorización de tráfico y la calidad del servicio.

Involucra al departamento de ingeniería de campo con respecto a la planificación de la estructura cableada y/o inalámbrica de la red LAN. Armado de Rack y condiciones térmicas para el funcionamiento de los equipos de redes, Routers, Switches y Voice Gateway.

Involucra a su vez al departamento de ventas y finanzas con respecto a la contratación del ancho de banda requerido a los proveedores de internet ISP y diferentes proveedores de servicios de telefonía como SIP Station, SIP Trunking y números de telefonía de red PSTN.

Una empresa que brinde la solución de telefonía IP debe por lo tanto involucrarse en todas las áreas anteriores. Teniendo un conocimiento teórico de los protocolos involucrados, de los elementos o componentes en el mercado y planificación para brindar soluciones correspondientes a cada empresa o institución.

En el mercado nos encontramos con soluciones con respecto a elementos o componentes aislados. Ejemplo, empresas como Grandstream, Panasonic, Yeastar, etc. Nos ofrecen la solución del servidor y el framework, como podemos ver en las siguientes imágenes obtenidas de un portales de venta en internet.

Ilustración 1 - Central IP PBX Grandstream
www.mercadolibre.com.ar

Ilustración 2 - Central IP PBX Grandstream
www.mercadolibre.com.ar

Ilustración 3 - Central IP Panasonic
www.mercadolibre.com.ar

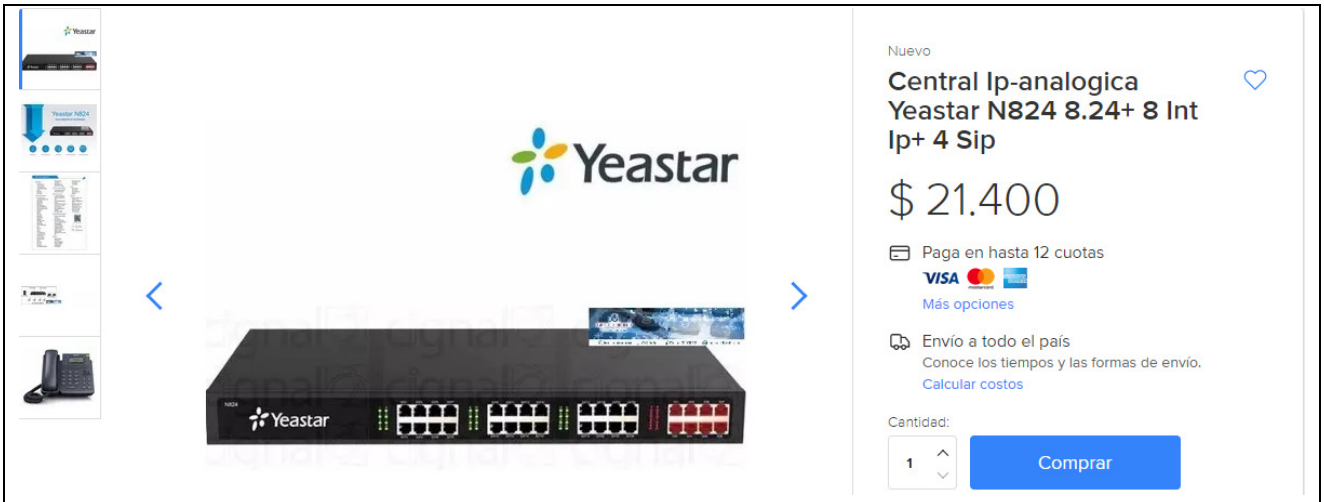


Ilustración 4 - Central IP Yeastar
www.mercadolibre.com.ar

Estas soluciones en el mercado solamente implican el Servidor y el Framework sin configuración previa. Los demás elementos involucrados necesarios para que dicha central de telefonía opere deben todavía desarrollarse e implementarse.

Con respecto al framework de telefonía podemos nombrar

- Asterisk
- FreeSwitch
- 3CX
- Kamailio
- RTPengine.
- OpenSIPS

Hay diferencias entre estos en cuanto a que Asterisk, FreeSwitch, Kamailio y 3CX son frameworks completos para la telefonía implementando servidor SIP, SIP Proxy y Media Server. RTPengine es un Servidor Proxy y un Media Server y OpenSIPS es un SIP Proxy.

Servidor SIP: es un servidor cuya función es el registro, localización de usuarios y credenciales. Generar y dar respuesta a peticiones.

SIP Proxy: es un servidor cuya función es el enrutamiento de paquetes de señalización.

Media Server: es un servidor cuya función es el control y gestión de contenido multimedia como voicemail, envío de correos electrónicos, IVR, etc.

RTP Proxy: es un servidor cuya función es el enrutamiento de paquetes de información (RTP); generalmente están constituidos por routers tradicionales cuyas reglas de enrutamiento, filtrado y calidad de servicio están orientadas a los paquetes RTP de información de telefonía.

Sin lugar a dudas la solución que se debe implementar debe poseer estos 4 tipos de servicios. Es posible a su vez la utilización complementaria de diferentes frameworks, explotando sus características más resaltantes en el caso de que el flujo de información sea importante, nombrando los grandes servidores de telefonía IP mundial. Un ejemplo de esto sería la utilización de la característica de Asterisk en cuanto a utilizarlo como servidor SIP y a Kamailio como SIP proxy.

3CX es la solución más práctica pero no es Open Source y el uso free es muy limitado.

Ilustración 5 - Logos de frameworks de telefonía sobre IP

Con respecto a los elementos denominados Softphones podemos nombrar a los teléfonos IP y a las aplicaciones.

Con respecto a los teléfonos IP existen una gran variedad de marcas en el mercado con diferentes características y precios. Cisco, Grandstream, Yeastar, Escene, Digium, etc.

De la misma manera en las aplicaciones no encontramos con diferentes características que pueden ser desde gratuitos a pagos y la compatibilidad, portabilidad bajo ciertos sistemas operativos. Zoiper, 3CX, SIPDroid, XLite etc.

Las características que pueden presentarse son:

- Números y tipos de cuentas (SIP, IAX2, PJSIP)
- Codificación (A-law, G723, G729, etc.)
- Tipo de conexión de red.
- Retención de llamadas
- Llamada en espera
- Desvío de llamadas
- Llamada de retorno
- Transferencia de llamadas
- Identificador de llamadas

- Rellamada
- Video
- Silencio
- DND
- Respuesta automática
- Cantidad de salas de conferencia
- Marcación rápida, SMS, correo de voz
- Esquema de Tono
- Control de volumen de llamadas IP directa
- Selección del tono de llamada
- Historial de llamadas: realizadas / recibidas / perdidas
- Teclas de función programables,
- Multi-idioma: chino, Inglés, Francés, Ruso, Italiano, Español, Portugués, etc.

Ilustración 6 - Plataformas de softphones
www.simplebusinessphones.com

En cuanto a Voice gateway podemos nombrar marcas como Cisco, Grandstream, Yeastar, Sangoma, Digium, etc. Que brindan la conversión en el transporte de redes. Podemos diferenciar entre equipos

que realizan la conversión de paquetes IP a señalización y envío analógico hacia central PSTN y equipos que realizan la conversión de paquetes IP a transporte PDH en tramas primarias E1/T1.

Ilustración 7 - Voice gateway Grandstream
www.mercadolibre.com.ar

Ilustración 8 - Voice gateway Sangoma
www.mercadolibre.com.ar

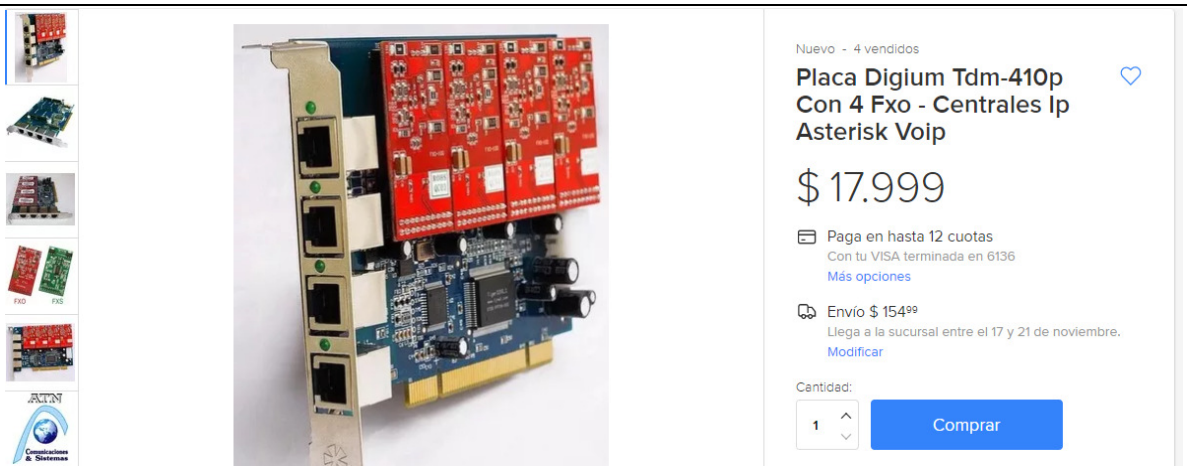


Ilustración 9 - Voice gateway Digium PCI
www.mercadolibre.com.ar

Por último, la variedad de equipos de redes IP como routers, switches e infraestructura de red no se detallará por la gran variedad de estos en el mercado.

Pruebas de concepto. ¿Es un producto útil?

La mayoría de las empresas ya son conscientes de que la telefonía tradicional bajo una red TDM síncrona tienen los días contados. El futuro pasa por Internet, también el de la telefonía, con la tecnología VoIP. Sin embargo, muchas organizaciones no saben muy bien por dónde empezar a la hora de implementar esta tecnología y poner en marcha la telefonía IP, tanto en sus centrales telefónicas como en sus comunicaciones móviles.

Un sistema de comunicación potente y bien gestionado es una máxima para cualquier empresa. Tanto pequeños negocios como grandes empresas se ven obligados a estar operativos en todo momento. Por otro lado, un equipo de trabajo de cualquier empresa necesita estar en constante comunicación para desarrollar su trabajo de una manera óptima. Por ejemplo, el departamento de ventas tiene que poseer una comunicación directa, fluida, confiable con el departamento de IT. En este punto, en el de las llamadas telefónicas, es en el que entra la tecnología VOIP y las centrales telefónicas IP.

La tecnología VOIP permite transmitir voz y datos a través de Internet y las centrales IP utilizan esta tecnología por lo que, para empezar, en lugar de utilizar líneas analógicas, vamos a realizar nuestras llamadas a través de la red y el coste de las facturas de teléfono se va a reducir considerablemente.

Veamos ahora los beneficios:

Ahorro de costes: Al utilizar la conexión a Internet, podemos prescindir de líneas adicionales, que tienen un coste mensual elevado. Además, el sistema permite utilizar aquel operador de Voz sobre IP que más nos interese en cada momento, logrando ahorros de hasta el 90% en el consumo telefónico.

Integración con el Sistema Informático: Es posible realizar y recibir llamadas desde los ordenadores y también se puede utilizar un teléfono IP similar a tu teléfono actual, pero que está comunicado con el ordenador, permitiendo marcar desde el navegador web, el programa de contactos o la aplicación de gestión. Al recibir una llamada, el ordenador puede abrir de forma automática la ficha de la persona que está efectuando la llamada.

Eficiencia en la localización de personas: La solución permite saber si una persona está en su puesto, localizable en su smartphone o no quiere ser molestada. Si una empresa tiene varias oficinas o delegaciones, cualquier persona de una de ellas puede llamar directamente a cualquier persona de la otra.

Facilita el teletrabajo: Cualquier empleado puede tener un teléfono IP en su casa, conectado a su banda ancha. Para el sistema será una extensión más, que tendrá las mismas posibilidades que las extensiones ubicadas en la propia empresa.
Libertad en la elección de Equipos: A diferencia de las centrales basadas en hardware, no obliga a utilizar teléfonos ni aparatos de una marca concreta, teniendo así una gama mucho más amplia de opciones.

Aprovechamiento del equipamiento existente: Si es necesario o conveniente, se pueden aprovechar los teléfonos existentes, aunque no tendrán las mismas prestaciones que los teléfonos IP.

Posibilidad de grabación de llamadas: Siempre que informemos de ello es posible grabar todas las llamadas. Podemos así analizar la forma en que se atiende a los clientes, cómo se cierra una venta o aclarar un malentendido.

Operadora virtual: Facilita a tus interlocutores hablar con la persona correcta. La operadora virtual es capaz de atender varias las llamadas entrantes al mismo tiempo.

Fácil Multiconferencia: No existen complicadas secuencias en el teclado para establecer multiconferencias. Arrastra en pantalla para crear una comunicación entre todos los usuarios que quieras.

Rutas por uso, fechas y horas: Configura fácilmente cómo se enrutan las llamadas, desviar llamadas de unos teléfonos a otros (o incluso de una delegación a otra) si la extensión está en uso, no contesta o está de fiesta. Configura también diferentes normas en función de la hora del día, ajustándose al horario de cada departamento u oficina.

Mejora en la atención al Cliente: Evita a clientes tener que esperar a ser atendidos oyendo molestas melodías. Puedes configurar la solución para que si, pasados unos segundos, nadie ha atendido la llamada, se ofrezca a quien nos llama la posibilidad de colgar y ser llamado en cuanto su interlocutor quede disponible.

Información para la toma de decisiones: Podrás conocer el tiempo medio de espera de tus clientes y cuantas llamadas recibes, permitiéndote así tomar decisiones en el tamaño de tu equipo de atención al cliente.

Recepción de Faxes por email: Con una central IP se pueden recibir los faxes como fichero PDF en la dirección electrónica que se indique. Si es necesario se pueden imprimir o reenviar por correo electrónico a la persona que corresponda.

Recepción de mensajes de voz por email: Si no es posible establecer comunicación con una persona, es posible dejar un mensaje que llegará por e-mail como fichero adjunto de audio.

Fácil crecimiento: Al ser un programa, no es necesario comprar tarjetas de líneas ni extensiones. No existe límite al crecimiento del sistema telefónico.

No queda Obsoleta: La solución recibe frecuentes actualizaciones, incorporando nuevas prestaciones por sugerencias de los clientes.

Soporte remoto: Podemos realizar cualquier cambio en la configuración de forma remota y rápida, sin necesidad de pagar desplazamientos de un técnico.

Capítulo 2: Desarrollo

El diagrama de bloques del proyecto es el siguiente.

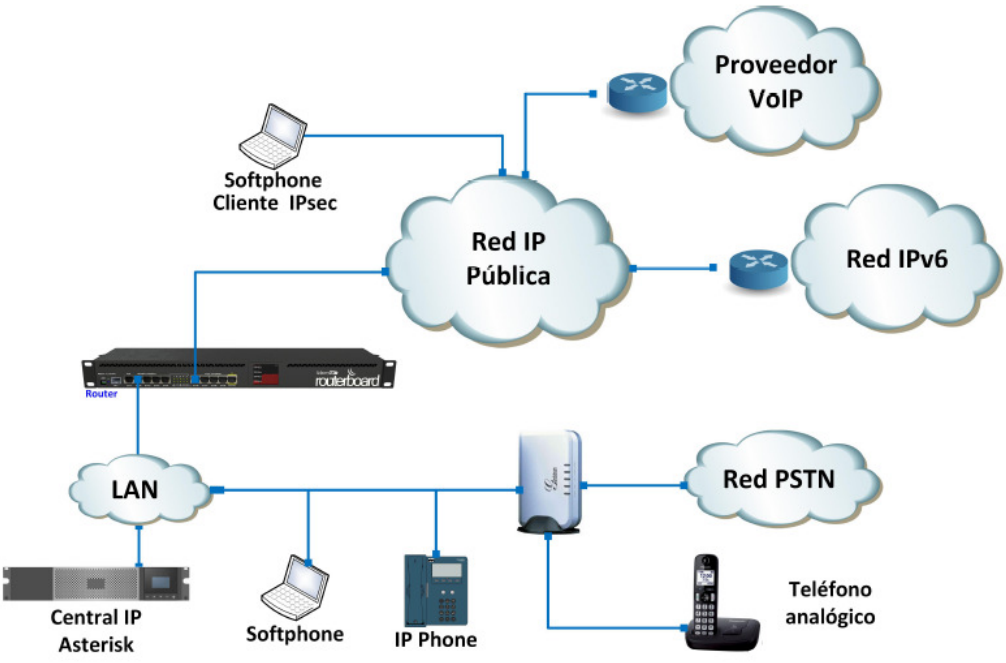


Ilustración 10 - Diagrama de bloque general

Plataforma

Se procedió a instalar Debian Jessi versión 9 en una máquina virtual, utilizando el hypervisor VMware Workstation 12.

Para esto se configuró el hypervisor que simulará una arquitectura x86_64, con configuración de red tipo Bridge por lo que la máquina virtual formará parte de nuestra red física y de esta manera permitir el acceso a recursos en forma directa, es decir, la máquina virtual poseerá su propia dirección MAC y dirección IP.

¿Por qué la virtualización?

"La mayoría de los servidores funcionan a menos del 15 % de su capacidad, lo que causa la expansión de servidores y aumenta la complejidad. Gracias a la virtualización de servidor, se abordan estas ineficiencias mediante la ejecución de varios sistemas operativos como máquinas virtuales en un único servidor físico. Cada una de las máquinas virtuales tiene acceso a los recursos de procesamiento del servidor subyacente. El paso siguiente es agregar un clúster de servidores a un recurso único y consolidado, gracias a lo cual se aumenta la eficiencia general y se reducen los costos. La virtualización de servidor también permite una implementación de cargas de trabajo más rápida, un aumento del rendimiento de las aplicaciones y una disponibilidad superior."
Documentación VMware (https://www.vmware.com/ar/solutions/virtualization.html)

Como las características y consumo de recursos de la central Asterisk no es demasiado para un sistema PC de escritorio actual y mucho menos para un servidor; la mejor opción es la ejecución del sistema sobre un hypervisor de manera tal de ejecutar más de un sistema operativo y por lo tanto

ahorrar recursos, lo que conlleva un ahorro económico. Otra opción es la implementación de la central en un sistema con arquitectura ARM, en un sistema embebido.

Características de la máquina virtual

La máquina virtual está conformada por:
Memoria RAM: 4GB
Números de procesadores: 1 – Intel core i7
Número de cores por procesador: 1
Hard disk: 60 GB Preallocated, tipo SCSI (small computer system interface)
Adaptador de red: Tipo Bridge

La virtualización (virtualization engine), que es la técnica de virtualización de instrucciones y uso de los recursos del sistema. Está configurada en modo automático en VMware Workstation para este proyecto.

Framework Asterisk

Se procedió a instalar las dependencias necesarias para Asterisk en Debían v9.

```
#! /bin/bash
apt-get install bison
apt-get install openssl
apt-get install libssl-dev
apt-get install libasound2-dev
apt-get install libc6-dev
apt-get install libnewt-dev
apt-get install libncurses5-dev
apt-get install zlib1g-dev
apt-get install gcc
apt-get install g++
apt-get install doxygen
apt-get install make
apt-get install mysql-server
apt-get install perl-modules
apt-get install libxml2-dev
```

wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz

contrib/scripts/install_prereq install

Una vez hecho esto, procederemos con la instalación de DAHDI y libpri.

- Dahdi: Se trata de una serie de librerías y utilidades para integrar Asterisk con tarjetas de comunicaciones de diferentes tecnologías. De Dahdi estaremos descargando un paquete llamado Dahdi-linux-complete, que incluye Dahdi Linux (módulos necesarios para las tarjetas) y Dahdi-Tools (utilidades para gestionar Dahdi).

- Libpri: Librerías necesarias para conectar Asterisk con líneas primarias (PRI).

Tanto las utilidades de DAHDI, libpri y Asterisk propiamente dicho son descargados de la página oficial de Asterisk.

http://www.asterisk.org/downloads

Para instalar Dahdi simplemente ejecutamos el siguiente commando.

```
sudo apt-get install asterisk-dahdi
```

Procedemos a instalar libpri, previamente descargado, descomprimiendo y ejecutando:

```
Make
Make install
```

Para la instalación de Asterisk procedemos a descomprimir el fichero descargado y ejecutar:

```
./configure
```

Luego ejecutaremos un make menuselect donde tendremos la posibilidad de instalar solo los módulos que queramos.

```
make menuselect
```

Mostrándonos un menú como el siguiente:

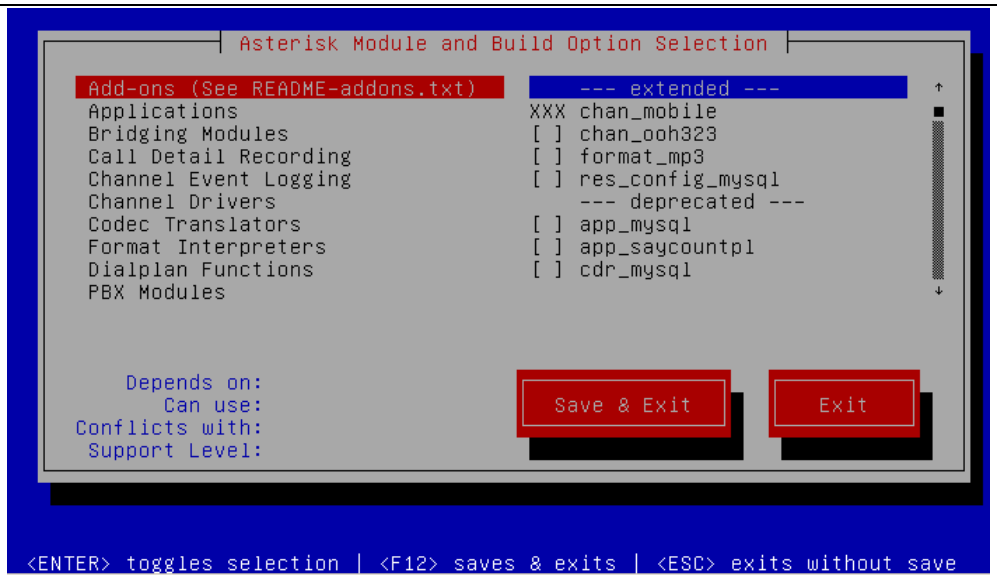


Ilustración 11 - Menu select

Y por últimos instalamos:

make install

Luego Podemos instalar las siguientes características.

make samples

make progdocs

make config

Comenzando con Asterisk

Una vez instalado Asterisk, podemos iniciarlo ejecutando la siguiente instrucción:

service dahdi start

/etc/init.d/asterisk start

Para conectarnos a la consola de Asterisk (CLI – Command Line Interface) tan sólo tendremos que ejecutar desde nuestra terminal el comando "asterisk" seguido de las opciones con las que queramos abrir la consola:

- Opción -c : (Console) - Nos permite abrir la consola. La particularidad de este comando es que si el servicio de Asterisk no se estaba ejecutando, intentará lanzarlo.
- Opción -d : (Debug) - Permite indicar el nivel de debug que queremos para los mensajes que nos aporta el CLI. Si queremos un alto nivel de debug tendremos que pasarle al comando asterisk tantas veces "d" como nivel queramos. Por ejemplo: "dddddd".
- Opción -h : (Help) - Muestra todas las opciones posibles.

- Opción -r : (Running) - Conectamos con un servicio de Asterisk que se está ejecutando en segundo plano.
- Opción -T : (Time) - Para que se muestren marcas de tiempo en cada mensaje de la consola.
- Opción -v : (Verbose) - Permite indicar el nivel de verbose que queremos para los mensajes que nos aporta el CLI. Si queremos un alto nivel de verbose, tendremos que pasarle al comando asterisk tantas veces "v" como nivel queramos. Por ejemplo: "vvvvvv".
- Opción -V : (Version) - Para ver la versión de Asterisk.
- Opción -x : (Execute) - Para ejecutar un comando en concreto. Se utiliza para no tener que entrar en la interfaz, ejecutar el comando y salir. Directamente pasamos inline el comando que queremos que se ejecute. Por ejemplo: asterisk -rx "core restart when convenient".

Para detener la central en el CLI de Asterisk:

CLI> core stop now

Y para programar su arranque cada vez que se reinicie el sistema operativo

chkconfig dahdi on
chkconfig asterisk on

Servidor SSMTP

Para que nuestra central Asterisk envíe correos electrónicos con la grabación del buzón de voz se procedió a instalar: ssmtp y mailutils

apt-get install mailutils ssmtp

Se creó una nueva dirección de correo electrónico de Gmail de manera tal de poder utilizar el servidor SMTP de Gmail. La cuenta es *servidor.smtp@gmail.com*

Luego se procedió a configurar /etc/ssmtp/ssmtp.conf

vim /etc/ssmtp/ssmtp.conf
ssmtp config for gmail or google apps account
Root = yourmail@gmail.com
Mailhub=smtp.gmail.com:587
Hostname=Asterisk

FromLineOverride=yes

UseSTARTTLS=yes

AuthUser=yourmail

AuthPass=Enter-Password

NOTA: Sin espacio antes y después del =

Luego se probó que funcionara el daemon ssmtp con el comando:

ssmtp servidor.ssmtp@gmail.com

subcject:xxxxxxxx

cuerpo:xxxxxxx

Ctrl + D

Configuración de los parámetros y funcionalidades de Asterisk

Para poder implementar las funcionalidades de la central Asterisk, los archivos de configuración, al igual que todo framework en Linux, se encuentran en el siguiente directorio:

/etc/Asterisk

Se procedió a configurar los siguientes archivos:

sip.conf
extensions.conf
voicemail.conf
confbridge.conf

Se desarrolló un conjunto de extensiones para realizar la presentación. Estas son las que se muestran en la siguiente imagen (La extensión de la red PSTN y del teléfono analógico se detallarán en sección posterior).

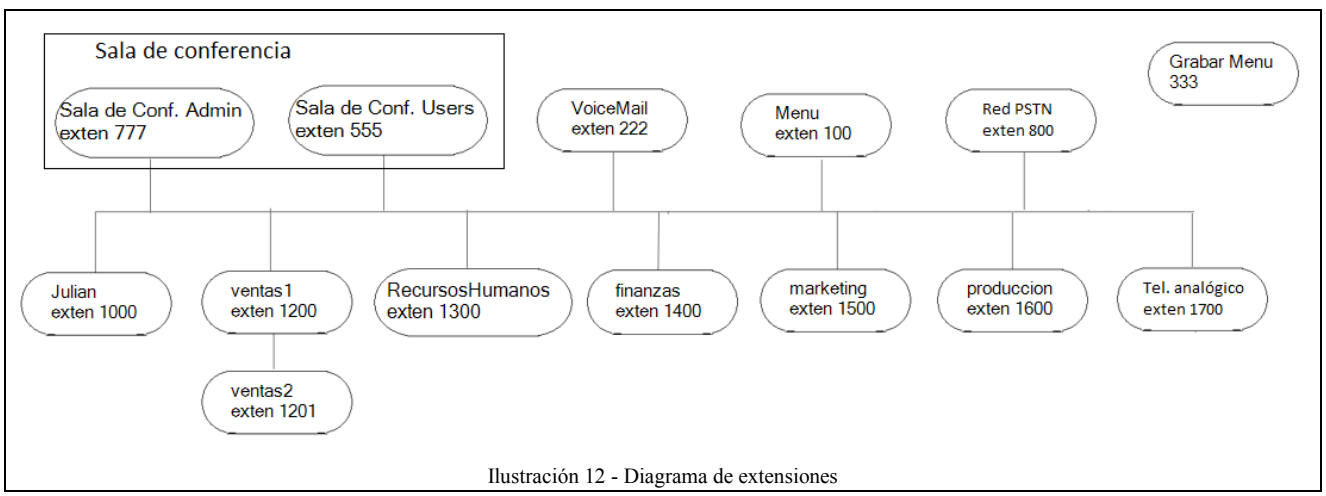


Ilustración 12 - Diagrama de extensiones

En cuanto a la central Asterisk se configuró las siguientes características:

- Funciones de llamada y videollamadas entre extensiones.
- Buzón de Voz para las cuentas Julián, Ventas1 y Ventas2. La grabación del buzón de voz luego es enviada al correo electrónico de cada extensión de manera de comunicar en tiempo real que se realizó una llamada y cuál es el motivo. Para esto se integra Asterisk con el daemon de linux ssmtp.
- Al marcar una extensión que está ausente y no posee buzón de voz, el agente de Asterisk comunicará que la extensión no está disponible. De la misma manera el agente comunicará si la persona está en estado ocupado (busy).
- Extensión propia para grabación de voz interactiva (IVR), la cual brindará un menú con las extensiones existentes en la central y da la posibilidad de llamar a las mismas. Esta extensión está pensada para ser el enlace a las llamadas entrantes a la central, de manera tal que dicho menú guiará a la persona que realizó el llamado para dirigirlo al interno que corresponda.
- Grupos de timbrado. Esto ha sido configurado para el departamento de ventas a razón de realizar la presentación. Si una extensión realiza una llamada a ventas1 y esté no está disponible o se encuentra en estado ocupado (busy) se llamará automáticamente a ventas2 o viceversa, si se llama a ventas2 y este no está disponible se llamará automáticamente a ventas1. Si ambos no están disponibles, se entra al buzón de voz y luego el mensaje es enviado a sus respectivos correos.
- Sala de conferencias. Esta función permite realizar conferencias entre extensiones, habiendo una extensión administrador y extensiones de usuarios (con otros privilegios). Solamente se ha configurado una sola sala de conferencia a modo de presentación.

SIP es la señalización elegida para este proyecto. Esto es debido a su estandarización en la mayoría de softphones, teléfonos IPs y proveedores de telefonía IP. La señalización SIP está definida en la documentación RFC 3261.

La siguiente configuración de los módulos de Asterisk corresponde a la base del sistema. Se anexará nuevas configuraciones en secciones posteriores, las cuales no se agregan a continuación de manera tal de mantener un hilo en el documento.

sip.conf

```
[general]
context=default     ;contexto por defecto para las llamadas entrantes
bindport=5060       ; puerto por defecto
bindaddr=0.0.0.0    ; aceptamos cualquier dirección IP
srvlookup=yes       ;aceptamos búsquedas DNS a nuestro servidor
disallow=all    ;deshabilitamos todos los códec para luego habilitar los correspondientes
allow=ulaw
allow=alaw
```

```
allow=gsm
allow=h263   ;habilitamos codec de video
allow=h263p
allow=h264
language=es-es    ;lenguaje de agente de asterisk, español
videosupport=yes   ;habilitamos video.

[julian]
type=friend      ;la extensión recibirá y podrá realizar llamadas
host=dynamic    ; no le establecemos una ip predeterminada
secret=123456   ;contraseña para el registro del usuario al asterisk
context=users   ;contexto del usuario
qualify=yes    ;la central se asegurará cada 2ms que el usuario está online en llamada
nat=force_rport     ; Se fuerza a trabajar según la RFC3581
dtmfmode=rfc2833       ;señalización inband
voicemail=1000@default    ; agregamos cuenta de voicemail

[ventas1]
type=friend
host=dynamic
secret=123456
context=users
qualify=yes
nat=force_rport
dtmfmode=rfc2833
voicemail=1200@default

[ventas2]
type=friend
host=dynamic
secret=123456
context=users
qualify=yes
nat=force_rport
```

dtmfmode=rfc2833
voicemail=1201@default

[RecursosHumanos]
type=friend
host=dynamic
secret=123456
context=users
qualify=yes
nat=force_rport
dtmfmode=rfc2833
voicemail=1300@default

[finanzas]
type=friend
host=dynamic
secret=123456
context=users
qualify=yes
nat=force_rport
dtmfmode=rfc2833
voicemail=1400@default

[marketing]
type=friend
host=dynamic
secret=123456
context=users
qualify=yes
nat=force_rport
dtmfmode=rfc2833
voicemail=1500@default

[produccion]

type=friend

host=dynamic

secret=123456

context=users

qualify=yes

nat=force_rport

dtmfmode=rfc2833

voicemail=1600@default

extensions.conf

[general]

static=yes

writeprotect=no

autofallthrough=yes ;si un usuario en llamada entra en estado offline se desconecta la llamada

clearglobalvars=no ;no se borran las variables cuando la central se reinicia

priorityjumping=yes ;permitimos el salto en prioridades

[globals]

[users]

exten => 1000,1,GotoIf($[${DEVICE_STATE(SIP/julian)}=UNAVAILABLE]?skip_dial) ;Device not registered

same => n,Dial(SIP/julian,30)

same => n,GotoIf($["${DIALSTATUS}"="BUSY" | "${DIALSTATUS}"="DONTCALL"]?dialed_busy)

same => n, VoiceMail(1000@default)

same => n,Hangup

same => n(skip_dial),Playback(extension&is-curntly-unavail)

same => n, VoiceMail(1000@default)

same => n,Hangup

same => n(dialed_busy),Playback(extension&is-curntly-busy)

same => n, VoiceMail(1000@default)

same => n,Hangup(17) ; generate busy signal

```
exten => 1200,1,Dial(SIP/ventas2,30)
same => n,GotoIf($[${DEVICE_STATE(SIP/ventas1&SIP/ventas2)}=UNAVAILABLE]?skip_dial)
same => n, Dial(SIP/ventas1,30)
same => n(skip_dial),Playback(extension&is-curntly-unavail)
same => n, VoiceMail(1200@default&1201@default)
same => n,Hangup

exten => 1201,1,Dial(SIP/ventas2,30)
same => n,GotoIf($[${DEVICE_STATE(SIP/ventas1&SIP/ventas2)}=UNAVAILABLE]?skip_dial)
same => n, Dial(SIP/ventas1,30)
same => n(skip_dial),Playback(extension&is-curntly-unavail)
same => n, VoiceMail(1200@default&1201@default)
same => n,Hangup

exten => 1300,1,GotoIf($[${DEVICE_STATE(SIP/RecursosHumanos)}=UNAVAILABLE]?skip_dial)
;Device not registered
same => n,Dial(SIP/RecursosHumanos,30)
same => n,GotoIf($["${DIALSTATUS}"="BUSY" | "${DIALSTATUS}"="DONTCALL"]?dialed_busy)
same => n,NoOp(Do More Stuff here, like dial another extension, whatever) ;no answer
same => n,Hangup
same => n(skip_dial),Playback(extension&is-curntly-unavail&please-try-again-later&goodbye)
same => n,Hangup
same => n(dialed_busy),Playback(extension&is-curntly-busy)
same => n,Hangup(17) ; generate busy signal

exten => 1400,1,GotoIf($[${DEVICE_STATE(SIP/finanzas)}=UNAVAILABLE]?skip_dial) ;Device not
registered
same => n,Dial(SIP/finanzas,30)
same => n,GotoIf($["${DIALSTATUS}"="BUSY" | "${DIALSTATUS}"="DONTCALL"]?dialed_busy)
same => n,NoOp(Do More Stuff here, like dial another extension, whatever) ;no answer
same => n,Hangup
same => n(skip_dial),Playback(extension&is-curntly-unavail&please-try-again-later&goodbye)
same => n,Hangup
same => n(dialed_busy),Playback(extension&is-curntly-busy)
```

```
same => n,Hangup(17) ; generate busy signal

exten => 1500,1,GotoIf($[${DEVICE_STATE(SIP/marketin)}=UNAVAILABLE]?skip_dial) ;Device not
registered
same => n,Dial(SIP/marketing,30)
same => n,GotoIf($["${DIALSTATUS}"="BUSY" | "${DIALSTATUS}"="DONTCALL"]?dialed_busy)
same => n,NoOp(Do More Stuff here, like dial another extension, whatever) ;no answer
same => n,Hangup
same => n(skip_dial),Playback(extension&is-curntly-unavail&please-try-again-later&goodbye)
same => n,Hangup
same => n(dialed_busy),Playback(extension&is-curntly-busy)
same => n,Hangup(17) ; generate busy signal

exten => 1600,1,GotoIf($[${DEVICE_STATE(SIP/produccion)}=UNAVAILABLE]?skip_dial) ;Device
not registered
same => n,Dial(SIP/produccion,30)
same => n,GotoIf($["${DIALSTATUS}"="BUSY" | "${DIALSTATUS}"="DONTCALL"]?dialed_busy)
same => n,NoOp(Do More Stuff here, like dial another extension, whatever) ;no answer
same => n,Hangup
same => n(skip_dial),Playback(extension&is-curntly-unavail&please-try-again-later&goodbye)
same => n,Hangup
same => n(dialed_busy),Playback(extension&is-curntly-busy)
same => n,Hangup(17) ; generate busy signal

exten => 1700,1,GotoIf($[${DEVICE_STATE(SIP/telefonoanalogico)}=UNAVAILABLE]?skip_dial)
same => n,Dial(SIP/telefonoanalogico,30)
same => n,GotoIf($["${DIALSTATUS}"="BUSY" | "${DIALSTATUS}"="DONTCALL"]?dialed_busy)
same => n,NoOp(Do More Stuff here, like dial another extension, whatever) ;no answer
same => n,Hangup
same => n(skip_dial),Playback(extension&is-curntly-unavail&please-try-again-later&goodbye)
same => n,Hangup
same => n(dialed_busy),Playback(extension&is-curntly-busy)
same => n,Hangup(17) ; generate busy signal
```

```
;/////////////////////////////////////////////////////////////////////////////////////
; Buzón de Voz
;/////////////////////////////////////////////////////////////////////////////////////
exten => 222,1,Answer()       ; extensión para casilla de voz
exten => 222,n,VoiceMailMain(@default)

;/////////////////////////////////////////////////////////////////////////////////////
;Conferencia
;/////////////////////////////////////////////////////////////////////////////////////

;Conferencia, invitado, usuarios
exten => 555,1,Progress()
exten => 555,2,Wait(1)
exten => 555,3,ConfBridge(1,default_bridge,default_user, menu-conferencia-usuario)

;Conferencia administrador
exten => 777,1,Progress()
exten => 777,2,Wait(1)
exten => 777,3,ConfBridge(1,default_bridge, admin_user , menu-conferencia-usuario)

;/////////////////////////////////////////////////////////////////////////////////////
; extension para llamar y escuchar el menu
;/////////////////////////////////////////////////////////////////////////////////////

exten => 100,1,Goto(menu-inicio,s,1)

; para grabar el menu
exten => 333,1, Answer()
exten => 333,n, Wait(0.5)
exten => 333,n, Record(menu-inicio.gsm)
exten => 333,n, Wait(1)
exten => 333,n, Playback(menu-inicio)
exten => 333,n,Handup()
```

```
[menu-inicio]
exten => s,1, Answer()
exten => s,2, Wait(0.5)
exten => s,3, Background(menu-inicio)
exten => s,4, WaitExten(5)

exten => 1,1, Goto(users,1000,1)
exten => 2,1, Goto(users,1200,1)
exten => 3,1, Goto(users,1300,1)
exten => 4,1, Goto(users,1400,1)
exten => 5,1, Goto(users,1500,1)
exten => 6,1, Goto(users,1600,1)

exten => *,1,Goto(s,1)
exten => t,1, Playback(goodbye)      ;el time out
exten => t,2, Hangup()

exten => i,1,Playback(pbx-invalid)     ;si el usuario presiona una tecla no valida
exten => i,2,Goto(s,1)
```

voicemail.conf

```
[general]

format = wav ; se grabará en formato wav
attach = yes ; se incluirá en el envío del email como adjunto
maxmsg = 1000 ; numero máximo de mensajes posibles
envelope = yes ; nos dará la el dia la hora y quien ha dejado el msg
maxsilence = 10 ; tras 10 segundos de silencio se cortará la llamada y se enviará el mail
silencethreshold = 128 ; este numero representa el nivel de audio y  sirve para definir que se
considera silencio. Más bajo el numero, más sensible al ruido
maxlogins = 3 ; numero máximo de intento de logings
mailcmd=/usr/sbin/ssmtp -t ; aplicación usada para el envio del email
fromstring=Buzon de Voz - PBX ; el nombre que aparecerá en el remitente del envio
```

[default]

1000 => 123456, Julian Oviedo,julianov403@gmail.com
1200 => 123456, ventas1,julianov403@outlook.com
1201 => 123456, ventas2,julian_403@hotmail.com

confbridge.conf

[general]

[admin_user]
type=user
pin=123456
marked=yes
admin=yes
music_on_hold_when_empty=yes
announce_user_count=yes

[default_user]
type=user
pin=123456
wait_marked=yes
end_marked=yes
music_on_hold_when_empty=yes
announce_user_count=yes

[default_bridge]
type=bridge
max_members=10
video_mode=follow_talker

[menu-conferencia-usuario]
type=menu
*=playback_and_continue(grabacion-conferencia-usuario)
*1=toggle_mute

```
1=toggle_mute
*2=leave_conference
2=leave_conference
*3=decrease_listening_volume
3=decrease_listening_volume
*4=increase_listening_volume
4=increase_listening_volume
*5=reset_listening_volume
5=reset_listening_volume
*6=decrease_talking_volume
6=decrease_talking_volume
*7=increase_talking_volume
7=increase_talking_volume
*8=reset_talking_volume
8=reset_talking_volume
*0=no_op
0=no_op

[menu-conferencia-admin]
type=menu
*=playback_and_continue(grabacion-conferencia-admin)
*1=toggle_mute
1=toggle_mute
*2=admin_toggle_conference_lock ; only applied to admin users
2=admin_toggle_conference_lock  ; only applied to admin users
*3=admin_kick_last       ; only applied to admin users
3=admin_kick_last        ; only applied to admin users
*4=decrease_listening_volume
4=decrease_listening_volume
*5=increase_listening_volume
5=increase_listening_volume
*6=decrease_talking_volume
6=decrease_talking_volume
*7=increase_talking_volume
```

7=increase_talking_volume

*8=no_op

8=no_op

Al presionar el asterisco dentro de la conferencia, el usuario escuchará un mensaje indicándole todas las opciones del menú. Dichas opciones han sido grabadas por mí. NOTA: la grabación debe ser formato .sln y encontrarse en el path /var/lib/asterisk/sounds

IVR – Respuesta de voz interactiva

Creación de IVR, respuesta de voz interactiva (Interactive Voice Response)

Para la grabación del menú que se ejecutará cuando se marque la extensión 100. Se procede a marcar la extensión 333 y luego a grabar el audio. Se puede observar en sip.conf como se implementó dichas extensiones.

El menú que se desplegará al marcar la extensión 100 es el siguiente:

1 - Transferir a supervisor
2 - Transferir a Ventas
3 - Transferir a Recursos Humanos
4 - Transferir a finanzas
5 - Transferir a marketing
6 - Transferir a producción
* (Asterisco) – Repetir el mensaje

Si el usuario marca otro número se le notificará y se le repetirá el menú.

Red de área local (LAN)

El siguiente diagrama de red brinda una visión desde el punto de vista de la red LAN. Red de área local.

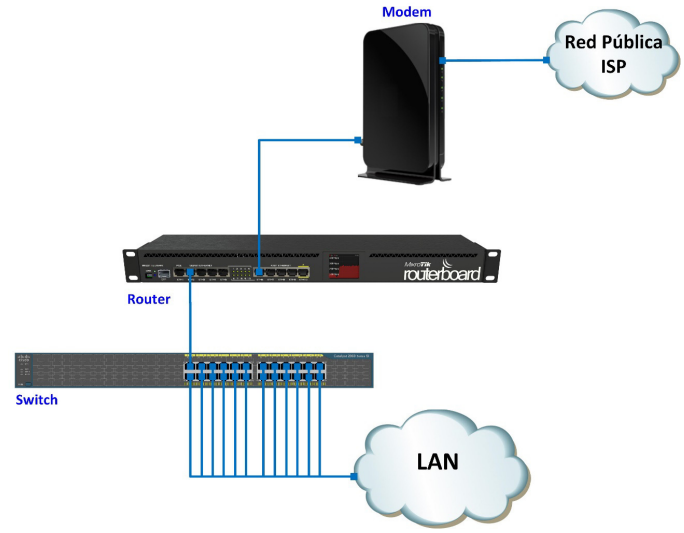


Ilustración 13 - Diagrama de red LAN

El acceso a la red pública desplegado por el ISP está dado por una red última milla cuya interfaz física puede ser par de cobre, cable coaxial, fibra óptica o enlace de microondas. No se utiliza un enlace local con la red pública (siguiendo los protocolos de capa 1 y 2) ethernet (IEEE 802.3x) o wifi (IEEE 802.11x), los cuales son implementados solamente en la red LAN. Esto es debido a las características del medio y el número de usuarios en comparación con el número de clientes en la red desplegada por el proveedor de internet. Dichos medios de acceso implican un proceso de acondicionamiento de la señal tanto en frecuencia como en estados modulativos e intensidades de señales electromagnéticas, por lo que necesariamente se requiere un modem.

Los modem actuales no solamente actúan sobre la capa 1 del modelo OSI, sino que son sistemas que actúan a su vez en capa 2 y 3.

Capa de enlace

Mikrotik da la posibilidad de implementar una conexión entre puertos en modo switch o mediante un bridge. Este último término es la definición genérica para sistemas que trabajan en capa 2.

Bridge: Interconecta segmentos de red (o divide una red en segmentos) haciendo la transferencia de datos de una red hacia otra con base en la dirección física de destino de cada paquete.

El término bridge, formalmente, responde a un dispositivo que se comporta de acuerdo al estándar IEEE 802.1D.

En definitiva, un bridge conecta segmentos de red formando una sola subred (permite conexión entre equipos sin necesidad de routers). Funciona a través de una tabla de direcciones MAC, las cuales son detectadas en cada segmento al que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo de otro segmento, el bridge copia la trama para la otra subred, teniendo la capacidad de desechar la trama (filtrado) en caso de no tener dicha subred como destino. Para conocer por dónde enviar cada trama que le llega

(encaminamiento) incluye un mecanismo de aprendizaje automático, por lo que no necesitan configuración manual.

Podemos diferenciar 2 tipos según la interfaz.

- Puentes homogéneos

Interconecta LAN con el mismo protocolo MAC (el nivel físico puede diferir), es decir, no hay conversión de protocolos a nivel 2, simplemente almacenamiento y reenvío de tramas. Un ejemplo de dispositivo homogéneo es un Switch Ethernet.

- Puentes heterogéneos

El puente dispone de una entidad superior encargada de la transformación de cabeceras entre distintos tipos de interfaces. Recibe tramas por una interfaz (por ejemplo: Wi-Fi) para enviarlas por otra diferente (por ejemplo: Ethernet). Un ejemplo de este tipo de dispositivo es un punto de acceso en una red Wifi.

Ambas configuraciones son sistemas que trabajan en capa 2 y la primera diferencia entre un bridge y un switch es debido al marketing, si bien la verdadera distinción está dada en un bridge heterogéneo y un bridge homogéneos (conocidos estos últimos normalmente como switch). La mayor diferencia en RouterOS es que el modo bridge trabaja a nivel de software y un switch realiza las tareas sobre un hardware dedicado. Por lo tanto, el modo bridge consume más recursos de CPU.

Podemos hacer referencia a la documentación brindada por Mikrotik:

"Ethernet-like networks (Ethernet, Ethernet over IP, IEEE802.11 in ap-bridge or bridge mode, WDS, VLAN) can be connected together using MAC bridges. The bridge feature allows the interconnection of hosts connected to separate LANs (using EoIP, geographically distributed networks can be bridged as well if any kind of IP network interconnection exists between them) as if they were attached to a single LAN. As bridges are transparent, they do not appear in traceroute list, and no utility can make a distinction between a host working in one LAN and a host working in another LAN if these LANs are bridged (depending on the way the LANs are interconnected, latency and data rate between hosts may vary)."
Documentación de Mikrotik (https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge)- (pág. 1)

Debido a que el modo switch consume menos recursos del CPU y que en la red LAN se conectarán más de 2 host, se implementará este modo, dejando de lado el modo bridge.

Modo switch

Haciendo referencia a la documentación brindada por Mikrotik:

"There are several types of switch chips on Routerboards and they have a different set of features. Most of them (from now on "Other") have only basic "Port Switching" feature, but there are few with more features." https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features

Las diferentes variantes de routerboards implementan diferentes tipos de chipset, "switch" con diferentes funcionalidades.

Mikrotik RB2011 posee un chipset Atheros-8327 (puerto Gigabit Ethernet ether1-ether5) y Atheros-8227 (puertos Fast Ethernet ether6-ether10), los cuales son integrados ASIC y están diseñado para realizar tareas de network switching cumpliendo con las siguientes características:

"The AR8327 is the latest in high performance small network switching. It is ultra-low power, has extensive routing and data management functions and includes hardware NAT functionality (AR8327N).

The AR8327/AR8327N is a highly integrated seven-port Gigabit Ethernet switch with a fully non-blocking switch fabric, a high-performance lookup unit supporting 2048 MAC addresses, and a four-traffic class Quality of Service (QoS) engine.

The AR8327 has the flexibility to support various networking applications. The AR8327/AR8327N is designed for cost-sensitive switch applications in wireless AP routers, home gateways, and xDSL/cable modem platforms. The AR8327/AR8327N complies with 10Base-T, 100Base-T and 1000Base-T specifications, including the MAC control, pause frame, and auto-negotiation, providing compatibility with all industry-standard Fast Ethernet and Gigabit Ethernet networks."
Atheros datasheet (pág. 1 – general description).

La funcionalidad de switching permite la circulación de tráfico de alta velocidad en un grupo de puertos, permitiendo que los mismos tengan la funcionalidad de un switch ethernet convencional.
Es posible configurar esta función seleccionando un puerto como master-port.
El master-port será el puerto en el cual RouterOS se comunicará con los demás puertos del grupo.
La interfaz que ha sido configurada como master-port quedará inactiva.

Por ejemplo, dada las 5 interfaces Gigabit Ethernet del Atheros-8327

```
[admin@MikroTik] > interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME      MTU   MAC-ADDRESS       ARP        MASTER-PORT      SWITCH
 0 R  ether1    1500  00:0C:42:3E:5D:BB enabled
 1    ether2    1500  00:0C:42:3E:5D:BC enabled    none             switch1
 2    ether3    1500  00:0C:42:3E:5D:BD enabled    none             switch1
 3    ether4    1500  00:0C:42:3E:5D:BE enabled    none             switch1
 4 R  ether5    1500  00:0C:42:3E:5D:BF enabled    none             switch1
```

Si configuramos los puertos ether4 y ether5 con el puerto ether3 como master-port

```
[admin@MikroTik] /interface ethernet> set ether4,ether5 master-port=ether3
[admin@MikroTik] /interface ethernet> print
Flags: X - disabled, R - running, S - slave
 #    NAME      MTU   MAC-ADDRESS       ARP        MASTER-PORT      SWITCH
 0 R  ether1    1500  00:0C:42:3E:5D:BB enabled
 1    ether2    1500  00:0C:42:3E:5D:BC enabled    none             switch1
 2 R  ether3    1500  00:0C:42:3E:5D:BD enabled    none             switch1
 3  S ether4    1500  00:0C:42:3E:5D:BE enabled    ether3           switch1
 4 RS ether5    1500  00:0C:42:3E:5D:BF enabled    ether3           switch1
```

El diagrama de puertos será el siguiente:

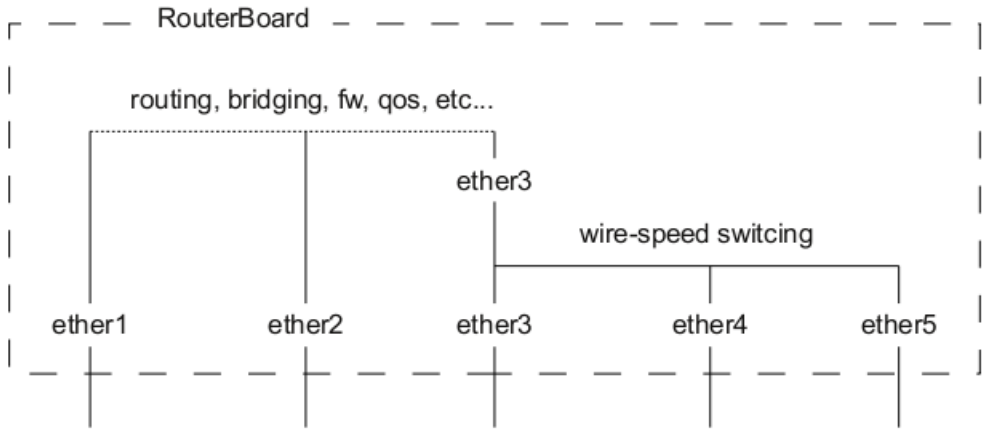


Ilustración 14 - Diagrama de puertos
https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features

Desde el punto de vista del router, será equivalente a tener un router con 3 puertos ethernet y en el puerto ethernet 3, tener conectado un ethernet switch de 3 puertos.

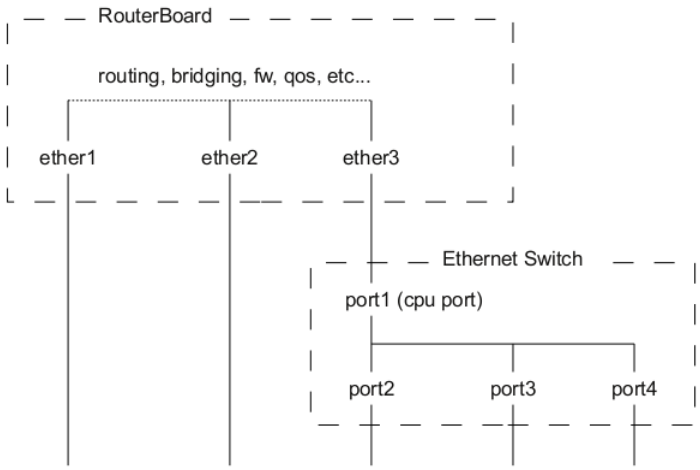


Ilustración 15 - Diagrama de puertos
https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features

Es decir, si sobre el puerto ether4 se recibe una trama ethernet cuya dirección MAC coincide con la de la tabla de switcheo que está relacionada con el puerto ether5, el circuito dedicado del switch decidirá hacer la transmisión directa a este puerto. Ahora bien, si la dirección MAC de destino que presenta la trama que ha sido recibida en el puerto ether4 coincide con la dirección del puerto ether3 (master-port), la cual debe ser configurada con una dirección IP que será el Gateway de la LAN, el circuito dedicado del switch enviará la trama al CPU del router para ser procesada en la capa 3.

Implementación de la capa de enlace en el router Mikrotik RB2011

La siguiente es la configuración que se aplicará al router para este proyecto.

El puerto ether2 es denominado LAN y es el master-port del puerto ether1, ether3, ether4 y ether5.

El puerto ether6 es denominado puerto WAN y es el puerto que conecta con la red externa.

```
/interface ethernet
set [ find default-name=ether2 ] name=LAN
set [ find default-name=ether6 ] name=WAN
set [ find default-name=ether1 ] master-port=LAN
set [ find default-name=ether3 ] master-port=LAN
set [ find default-name=ether4 ] master-port=LAN
set [ find default-name=ether5 ] master-port=LAN
```

De esta manera, el diagrama esquemático primero, el cual presenta un switch físico es equivalente al siguiente:

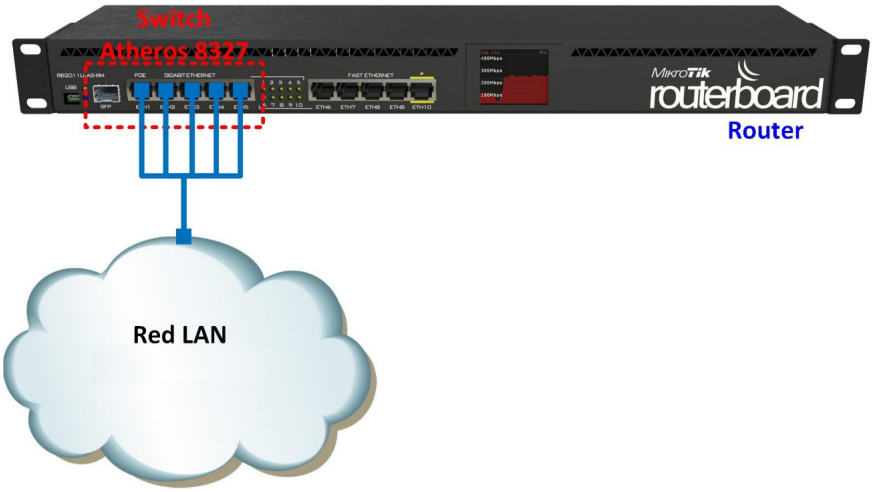


Ilustración 16 - Mikrotik RB2011 y switch Atheros 8327

Aunque se seguirá haciendo referencia al switch físico en los siguientes diagramas de red, para diferenciar la capa de enlace de la capa de red, es decir, del router propiamente dicho.

Implementación de IPv6

Un requerimiento de la cátedra es la implementación de IPv6 en la red LAN. Siguiendo la documentación RFC 3513 se menciona que hay 3 tipos de direcciones: unicast, anycast y multicast.

En IPv6 no se define la dirección de broadcast, la cual ha sido sustituido por las direcciones de multicast, ni tampoco se define una dirección que identifique a la red ya que todas las direcciones hacen referencia a interfaces y no nodos.

En la documentación RFC se hace referencia a una interface como sinónimo de host. Por lo que utilizaré ambos términos.

Una sola interface puede tener más de una dirección IPv6, a diferencia de IPv4. La distinción en estos 3 grupos es la siguiente:

Unicast: es una dirección que identifica a una sola interface. Un paquete enviado a una dirección unicast se direcciona a la interface con dicha dirección IP.

Anycast: es una dirección que identifica a un grupo de interfaces. Un paquete enviado a una dirección anycast es enviado solamente a una interface de dicho grupo, la más cercana según la distancia de ruteo.
Multicast: es una dirección que identifica a un grupo de interfaces. Un paquete enviado a una dirección multicast es enviado a todas las interfaces de dicho grupo.

Por lo tanto, siguiendo lo mencionado anteriormente implementaré solamente direcciones unicast en la red LAN, de manera tal de que no existan grupos de interfaces comunes, ya que en la red no existirán diferentes equipos que brinden los mismos servicios. Generalmente las direcciones anycast se implementan en servidores DNS, ya que, una misma dirección engloba diferentes servidores físicos que brindan el mismo servicio en capas superiores. Según la tabla de enrutamiento se direccionaría al servidor físico más cercano desde el punto de vista de la red, disminuyendo la congestión del tráfico que generaría un único servidor con una sola dirección IP.

Ahora bien, ante la posibilidad de que una institución u organización que posea diferentes departamentos en lugares geográficos distantes y la cual implementa una intranet y una VPN que virtualmente "una" las redes físicas de cada lugar mediante un túnel en la red pública. Es posible implementar una central de telefonía en cada red LAN, con la misma dirección IPv6, la cual sea definida como una interface de anycast. Por lo tanto, cuando un softphone realice una llamada, la señalización se enrutaría hacia la central de telefonía más cercana según la tabla de ruteo. Lamentablemente la telefonía IP con soporte IPv6 no ha sido desarrollada completamente hasta la fecha.

Cabe resaltar que una interface puede tener asignada una dirección unicast, anycast o multicast al mismo tiempo. Y a su vez tener asignadas los diferentes tipos de direcciones unicast.

Enrutamiento, prefijo y tipo de identificación de direcciones en IPv6

Las direcciones IPv6 tienen una longitud de 128-bits y se escriben en formato Hexadecimal. Están compuestas por 32 dígitos agrupados en lo que se suele denominar como "Hexteto" (4 dígitos hexadecimales), es decir, en 8 hextetos separados por dos puntos (:).

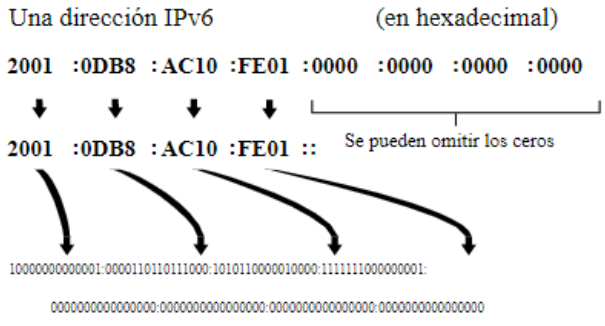


Ilustración 17 - Notación IPv6

Los campos que están más a la izquierda de una dirección IPv6 contienen el prefijo, que se emplea para enrutar paquetes. Debido a la extensión de una dirección IPv6, no se tiene una máscara de subred en formato de dirección IPv6, es por ello que solamente se emplea la longitud o duración de prefijo para delimitar la porción de red y de hosts en este tipo de direcciones. La longitud de prefijo pude ir desde /0 hasta /128, siendo la longitud de prefijo típica en un host /64.

El tipo de dirección IPv6 es identificado por los bits de mayor orden, según lo siguiente:

Address type	Binary prefix	IPv6 notation	Section
Unspecified	00...0 (128 bits)	::/128	2.5.2
Loopback	00...1 (128 bits)	::1/128	2.5.3
Multicast	11111111	FF00::/8	2.7
Link-local unicast	1111111010	FE80::/10	2.5.6
Site-local unicast	1111111011	FEC0::/10	2.5.6
Global unicast	(everything else)		

Las direcciones de Anycast son tomadas del espacio de direcciones unicast y no son distinguibles sintácticamente de unas de otras. Cuando se configura más de una interface con la misma dirección unicast, se estable por lo tanto una dirección anycast.
Las interfaces que han sido asignadas con una dirección anycast deben configurarse para tal fin. Es decir, la capa de aplicación debe conocer este funcionamiento.

Direcciones implementadas – Unicast

En las direcciones unicast los primeros 64bits identifican el prefijo de red, y son usados para encaminamiento; los últimos 64bits identifican el interface de red del host.

bits	48 (o más)	16 (o menos)	64
campo	*routing prefix*	*subnet id*	*interface identifier*

Ilustración 18 - Direcciones Unicast

El prefijo de red (network prefix) (prefijo de encaminamiento o (routing prefix) junto con el identificador de subred o (subnet id) está situado en los 64 bits más significativos de la dirección IPv6. El tamaño del routing prefix puede variar; un prefijo de mayor tamaño significa un tamaño menor para subnet id. El subnet id permite a los administradores de red definir subredes dentro de la red disponible.

Los 64 bits de identificador del interface (interface identifier) son generados automáticamente con la dirección MAC de la interface y el algoritmo EUI-64 modificado.

Por lo tanto, solamente los equipos de capa 3 pueden leer y diferenciar los prefijos y el network subnet id para el enrutamiento. En cuanto a routers de redes WAN, es decir, de proveedores de internet, solamente enrutaran siguiendo los 64 primeros bits. En cuanto a routers de redes LAN si podrán diferenciar subnet id del router prefix. Esto brinda una mejora en rendimiento de CPU de los routers.

Link local address y Global address

Cada host en la red LAN implementada tiene 2 tipos de direcciones unicast, una de enlace local y otra global. A continuación, realizaré una breve descripción de los tipos de direcciones unicast.

Hay 3 tipos básicos de direcciones unicast IPv6.

Link local address (de enlace local): que es la dirección que se asigna automáticamente al iniciar un dispositivo y es una dirección única que tiene un prefijo FE80::/10 y no son enrutadas externamente. Es el propio sistema operativo del host el que asigna esa dirección de manera

autónoma, utilizando el prefijo seguido de la dirección MAC del mismo, implementando el algoritmo EUI-64 modificado.
Una dirección de enlace-local es una dirección IP creada únicamente para comunicaciones dentro de una subred local. Los routers no enrutan paquetes con direcciones de enlace local. La dirección de enlace-local es necesaria para operaciones de subcapa IPv6 dentro del Neighbor Discovery Protocol el cual sustituye el protocolo ARP y utilizando el protocolo ICMPv6 los host descubren a sus vecinos.

Global address (dirección global): es la dirección que identifica al host en la red pública mundial y es una dirección que es dada por el ISP. Son direcciones que pueden ser enrutadas hacia la red pública y tienen el prefijo 2000::/3.

Unique local address (única dirección local): internamente ruteables y es lo que se conoce como una dirección privada. Dichas direcciones no deben ser enrutadas a la red pública. El prefijo es FC00::/7.

Configurando RouterOS para IPv6

Todo host en la red que soporta IPv6 tiene configurada una dirección de enlace local, la cual es asignada automáticamente al iniciar el sistema operativo. Por lo tanto, solamente hay que configurar una dirección global que identifique a cada host en la red pública mundial. Para esto se debe implementar un servidor DHCPv6.

```
/ipv6 address
add address=2001:470:5:550:4e5e:cff:fe1e:8b48 eui-64=yes interface=LAN
/ipv6 pool
add name=poolIPv6 prefix=2001:470:5:550: :/64 prefix-length=64
/ipv6 dhcp-server
add address-pool=poolIPv6 interface=LAN name=dhcp-IPv6
/ipv6 settings
set forward=yes
set accept-router-advertisements=yes
/ipv6 nd
set [ find default=yes ] advertise-dns=yes advertise-mac-address=yes
```

En la primera línea se define la dirección global de la interface LAN que físicamente corresponde al puerto ether2 del router. Cabe resaltar que dicha dirección debe definirse dentro del rango de direcciones que pertenecen al prefijo del pool de IPs que implementará el servidor DHCP. El campo de interface identifier (identificador de interfaz) es completado por la dirección MAC del puerto del router.

En la segunda línea configuramos el pool de IPs que el servidor DHCP utilizará para la asignación de las mismas a los host correspondientes de la red. Como se puede observar dicho pool está dentro del rango del prefijo que corresponde a las IPs unicast globales.

En la tercera línea se define el servidor DHCP para que utilice el pool de IPs definido anteriormente y el cual fue llamado “poolIPv6”. Este está referenciado a la interface LAN, que es el puerto ether2 que tiene conexión lógica con el switch Atheros.

En la cuarta línea se habilita el envío de paquetes IPv6 de la LAN a la WAN y el router advertise el cual habilita el router a descubrir la información de la red para el enrutamiento a través de la lectura de los prefijos de los paquetes entrantes.

En la quinta línea se habilita el network discovery, detección de red, que en este caso se define con las características por default, pero haciendo explícito la distribución de DNS y el descubrimiento de los enlaces locales además de los globales, es por esto la sentencia advertise-mac-address. Para completar la interface id en la dirección IP.

La detección de red es un conjunto de mensajes y procesos que determinan la relación entre los nodos vecinos. Este protocolo reemplaza el protocolo ARP y es utilizados por los hosts para descubrir routers en la red, así como demás direcciones, prefijos y otros parámetros de configuración. Es usado por los routers para advertir la presencia de host, routers, el mejor camino para enviar paquetes siguiendo los protocolos dinámicos de enrutamiento, etc.

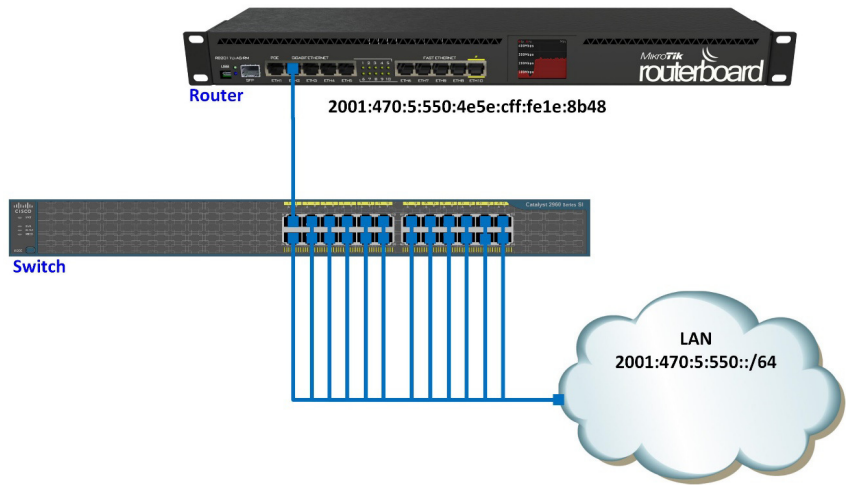


Ilustración 19 - Diagrama de red LAN y direcciones IPv6

El inconveniente de implementar IPv6 con telefonía IP

Me he encontrado con un problema cuando implementé efectivamente una red con IPv6 y es que ningún softphone con soporte para Windows trabaja con IPv6 (año 2017), tenemos si actualmente implementaciones de softphones con soporte IPv6 para IOx.

Por lo tanto, no es posible utilizar una red LAN con IPv6 puro, ya que la capa de aplicación actual para voice, es decir, para las comunicaciones de voz y video en tiempo real no soporta dicha actualización en la capa de red.

Pila doble (dual stack)

Por lo tanto, la solución es implementar un mecanismo de Pila doble y coexistir direcciones IPv6 con IPv4. Esto es un método de migración a IPv6 muy utilizado actualmente.

El denominado "mecanismo de pila doble” que se describe en el documento RFC 2893.

Para implementar un mecanismo de pila doble, ya habiéndose configurado el soporte para IPv6, se debe proceder a implementar el soporte IPv4.

```
/ip pool
add name=poolIPv4 ranges=100.64.0.3-100.64.0.254
/ip dhcp-server
add add-arp=yes address-pool=poolIPv4 disabled=no interface=LAN name=dhcp-IPv4
/ip address
add address=100.64.0.1/24 interface=LAN network=100.64.0.0
/ip arp
add address=100.64.0.2 interface=LAN mac-address=00:50:56:38:24:50
/ip dhcp-server network
add address=100.64.0.0/24 dns-server=8.8.8.8 gateway=100.64.0.1
```

En la primera línea se define el pool de IPv4 que utilizará el servidor DHCP. El rango de IPs comienza en 100.64.0.3 debido a que la dirección 100.64.0.1 está reservada como gateway, por lo que será la dirección de la interface LAN del router, es decir, la dirección del puerto físico ether2. La dirección 100.64.0.2 está reservada para la central de telefonía Asterisk, la cual posee una dirección IP fija ya que será el destino de los paquetes SIP de señalización, los cuales son enviados por los teléfonos IPs y softphones.

En la segunda línea se define el servidor DHCP que utilizará el pool de IP anteriormente definido, el cual posee el nombre “poolIPv4” y está ligado a la interface LAN.

En la tercera línea se define la dirección IP de la interface LAN, con la IP 100.64.0.1 que será el gateway de la LAN.

En la cuarta línea se define como estática la dirección IP 100.64.0.2 la cual está ligada a la MAC 00:50:56:38:24:50 que es la interface de la máquina virtual donde corre la central de telefonía IP basada en Asterisk.

En la quinta línea se define las características del servidor DHCP, a que red pertenece, su gateway y la dirección IP del servidor DNS.

Una vez configurado el router podemos ver en la siguiente imagen las direcciones IPs de una PC conectada a la red.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:470:5:550:a8f2:c617:6b1:e770
   Temporary IPv6 Address. . . . . . : 2001:470:5:550:6410:fe04:4c3:c058
   Link-local IPv6 Address . . . . . : fe80::a8f2:c617:6b1:e770%18
   IPv4 Address. . . . . . . . . . . : 100.64.0.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::4e5e:cff:fe1e:8b48%18
                                       100.64.0.1
```

Ilustración 20 - Direcciones de host conectado a la red LAN

De esta manera el host se convierte en un host "híbrido" y dependiendo de la resolución de nombres será el protocolo que usará para cada requerimiento en particular. De acuerdo a lo mostrado en el gráfico siguiente.

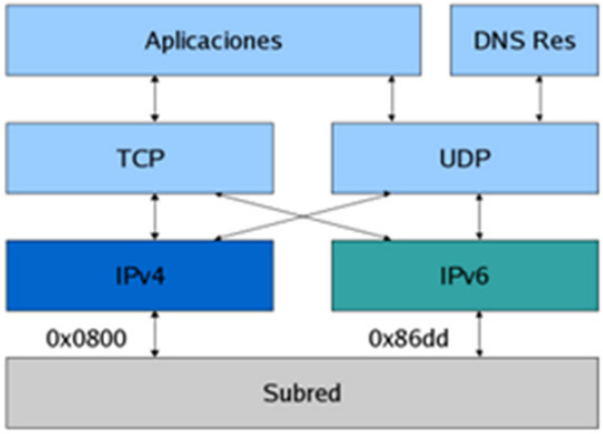


Ilustración 21 - Protocolos en pila doble

Un backbone se dice que es de pila doble si todos los routers y switches de capa 3 pueden manejar tanto IPv4 como IPv6.
Como las cabeceras (headers) son diferentes, no hay problemas en diferenciar el tráfico desde el punto de vista del router.

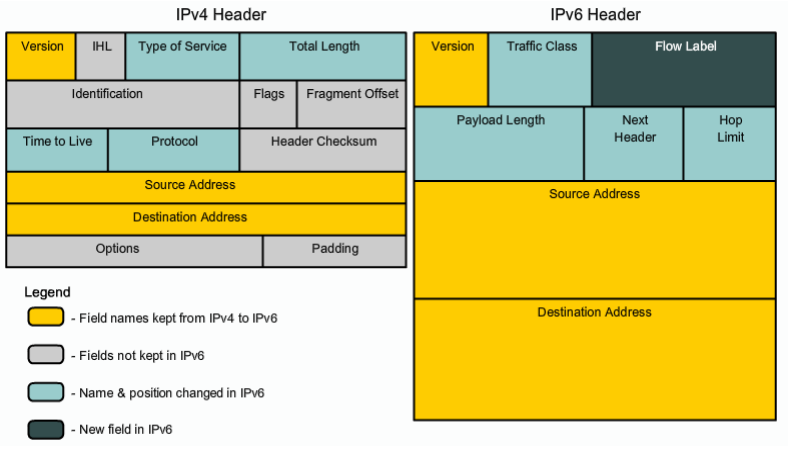


Ilustración 22 - Encabezados de red

Diagrama de red con pila doble

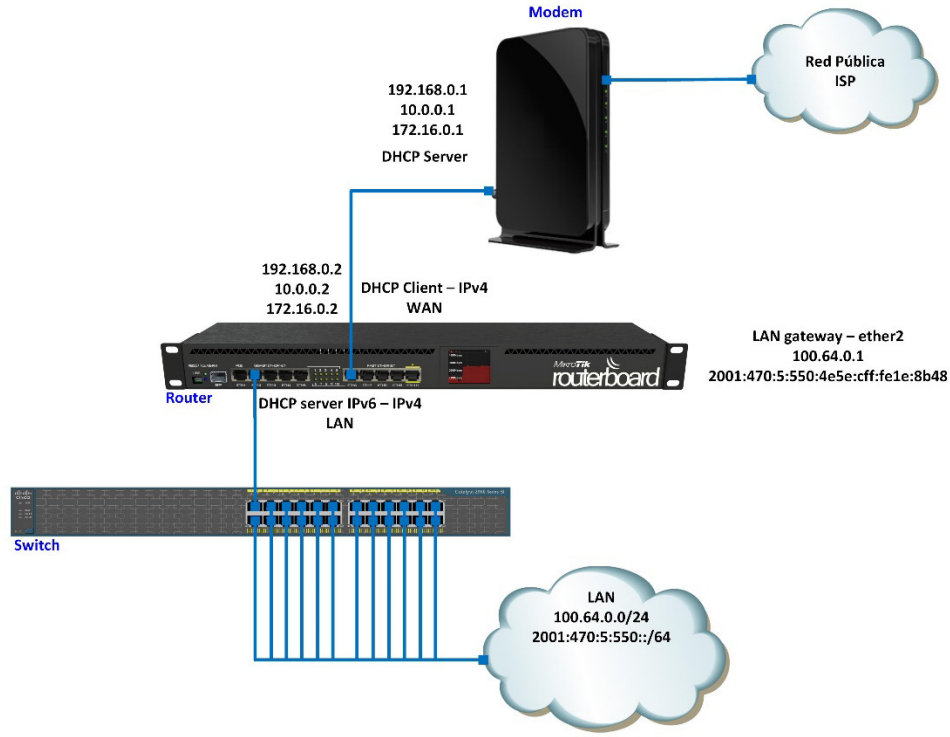


Ilustración 23 - Diagrama de red y pila doble

La red pública – internet

Hasta el momento solamente se ha configurado la red LAN, sin considerar la conexión a la red pública.

Como el objetivo del proyecto es implementar una central de telefonía IP para instituciones, organizaciones, empresas, etc. Las cuales poseen oficinas, departamentos en diferentes lugares geográficos con su propia red LAN física, donde las mismas deberán ser interconectadas a través de la red pública, de manera de tal de establecer conexión con la central de telefonía y entre softphones. Y a su vez hay que considerar que dichas redes LAN no solamente brindarán servicio de telefonía, sino también otros servicios, requiriendo conexión a internet.

Es por lo tanto necesario configurar la conexión con la red pública, también denominada comúnmente como internet. Constituyendo una intranet extendida a través de una VPN.

En cuanto al uso de IPv4 en la red LAN, las cuales son utilizadas por la central de telefonía y softphones para la comunicación, es necesario implementar un mecanismo de traslación de direcciones, NAT. Esto es debido a que los proveedores de internet brindan un numero limitados de direcciones públicas por carencia de estas a nivel mundial. Generalmente se asocia una única dirección IP pública a usuarios residenciales. Aunque es posible comprar más de una dirección pública según las capacidades de la empresa, ejemplo un /29. En todo caso el número de direcciones es muy limitado y no puede cubrir en ningún caso el número de host totales en la red privada o intranet.

Hasta la fecha, año 2017, los proveedores de servicio de internet (ISP) a nivel mundial utilizan solamente soporte IPv4. Por lo tanto, no es posible enrutar paquetes con cabecera IPv6 a la red pública.

Para implementar una conexión entre redes con soporte IPv6 a través de una red con soporte IPv4, como lo es la red pública dada por los proveedores de internet, es necesario implementar un mecanismo de transporte o tunelamiento.

Debido al gran número disponibles de direcciones IPv6 a nivel mundial no se define un mecanismo de NAT, ya que los proveedores de internet brindan un prefijo de IPv6 para la asignación de direcciones a los hosts. Un ISP que admita IPv6 puede brindar a las empresas prefijos de sitio de IPv6 de hasta 48 bits.

Network Address Traslation (NAT)

Dado el diagrama de red que se presentó anteriormente. Debe considerarse que el proveedor de internet brinda una única IP pública. El modem es el equipo encargado del acondicionamiento de los niveles de tensión u ópticas, así como de la traslación en frecuencia correspondiente y la codificación para la transmisión de la señal en el medio de la última milla.

A su vez dichos equipos implementan servicios de capa 3, como implementar un network address traslation NAT y un servidor DHCP, el cual brinda direcciones IPv4 privadas.

En cuanto a la asignación de IPv4 privadas, los pools de uso privados asignados por IANA son:

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
169.254.0.0/16

Como la red a la que estamos tratando en este trabajo final es concebida para que el usuario final no deba configurar las IPs de manera de no preocuparse por el solapamiento de las mismas y considerando que se desconoce el tipo de modem o equipo intermedio que se utiliza. Esto no debe ser una característica que limite la implementación de la red a un modem o dispositivo intermedio en particular. Se optó por implementar en la red LAN un pool de IPs que ha sido reservada por la IANA para escenarios de Carrier Grade NAT, según lo definido en el documento RFC 6598.

Este pool de IPs es el siguiente: 100.64.0.0/10

Si lo observamos desde la visión de la capa de red, es decir, desde la capa 3 del modelo OSI. Podemos ver el diagrama en la siguiente imagen.

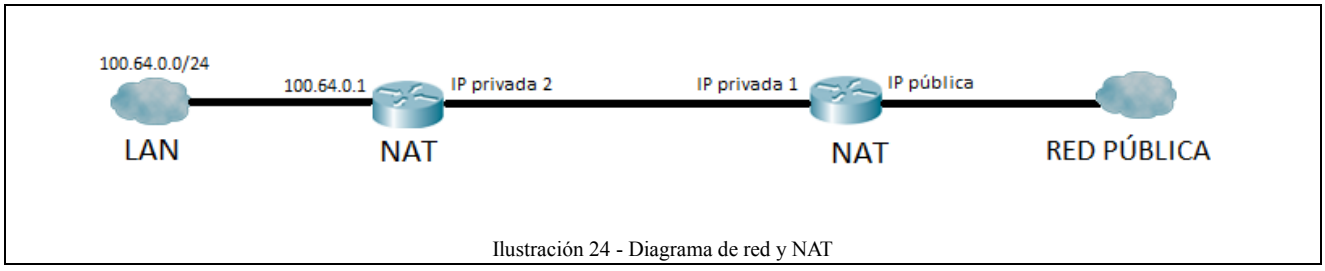


Ilustración 24 - Diagrama de red y NAT

En cambio, si el modem no es de capa 3, es decir, se implementa un modo bridge puro.

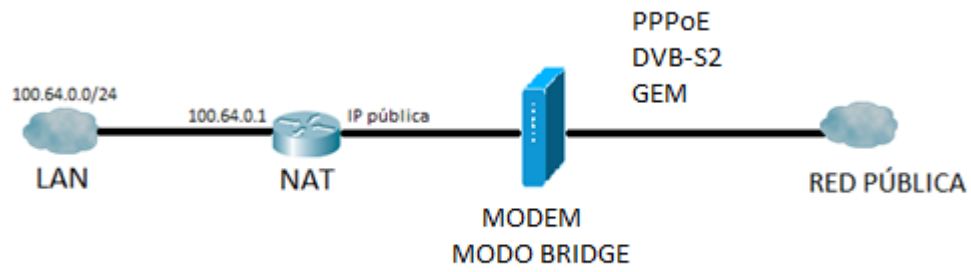


Ilustración 25 - Diagrama de red y NAT

Por ejemplo, si el acceso al medio es par de cobre, configurándose los parámetros de la cuenta PPPoE (point to point over ethernet) o PPPoA (pint to point over ATM) según sea el caso, en el modem, este puede actuar en modo bridge. Un ejemplo comercial de un modem con esta característica es el DSL 320B de D-Link.

Para la configuración del router Mikrotik, agregamos las siguientes líneas de código:

```
/ip dhcp-client
add default-route-distance=0 dhcp-options=clientid disabled=no interface=WAN use-peer-ntp=no
```

En la línea anterior se agrega un cliente DHCP en la interface WAN que corresponde al Puerto físico ether6 del router. De manera tal que tome la dirección IP privada dada por el servidor DHCP del modem o equipo intermedio.

Luego se configura el NAT.

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=WAN
add action=dst-nat chain=dstnat dst-port=5060 protocol=udp to-addresses=100.64.0.2 to-
ports=5060
add action=accept chain=dstnat dst-port=20000-40000 protocol=udp src-port=20000-40000 to-
ports=20000-40000
```

La acción masquerade relacionada con la interface WAN es necesaria ya que se desconoce la dirección IP que será asignada a la interface WAN y a la que será trasladadas las direcciones de la red LAN. La cadena es source nat ya que es la dirección de origen la que es modificada mientras que la dirección de destino se mantiene intacta.

La segunda acción que corresponde al dest-nat (destination nat) y hace referencia a la traslación IP del destino de un paquete SIP (UDP), señalización entre softphones y la central de telefonía que tiene como destino la dirección IP de la central de telefonía, es por esto la especificación del puerto 5060.

De esta manera un softphone desde la red pública podrá intercambiar información de señalización con la central de telefonía Asterisk. Ya que todo paquete SIP tiene como puerto el 5060 y este debe ser ligado a la dirección 100.64.0.2.

La tercera acción es aceptar la traslación en dirección de un paquete con destino desde la WAN hacia una dirección de la red LAN. Dicha traslación se realiza para paquetes UDP cuyo puerto destino estén en el rango del 20000 al 40000. Estos puertos están libres por defecto y son los utilizados por los paquetes RTP, UDP para la comunicación de voz y video en tiempo real.

Cada comunicación de voz entre softphones utiliza un puerto UDP y una video llamada utiliza 2 puertos. Es por este motivo la definición de un rango.

La siguiente imagen describe el paquete de comunicación:

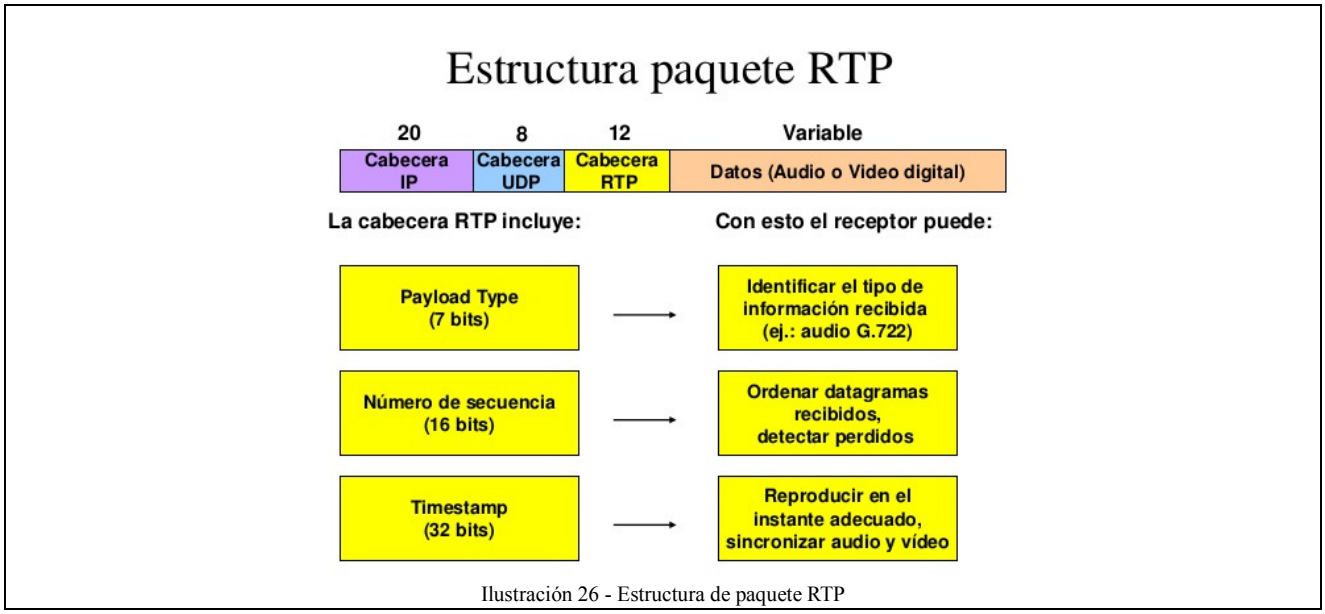


Ilustración 26 - Estructura de paquete RTP

6to4 tunnel – Tunnel Broker

Para la conexión entre redes que implementan IPv6 a través de una red con soporte IPv4 como lo es la del proveedor de internet ISP, se utilizará un túnel 6to4. Según lo especificado en el documento RFC 3056.

La encapsulación de IPv6 consiste en preparar el paquete de datos original más la cabecera IPv6 y sus cabeceras de extensiones (según lo estipulado en el documento RFC 2460) y encapsular dichos datos en el payload de un paquete con cabecera IPv4. El resultado es un paquete con dirección origen y destino IPv4.

El paquete original es procesado, encapsulado y enviado a una dirección IPv4 específica para realizar el túnel. De la misma manera el paquete que deba ser enviado al interior de la red LAN es procesado, decapsulado y enviado al host con la dirección IPv6 de destino.

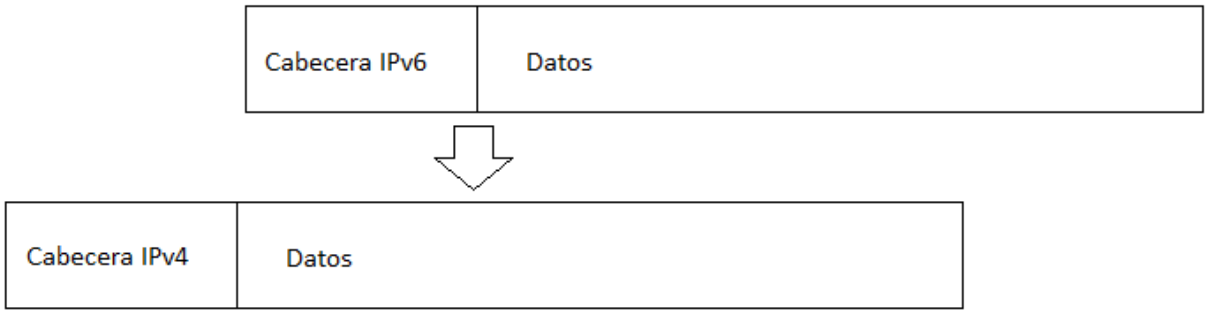


Ilustración 27 - Encapsulamiento paquete IPv6

Es decir que el paquete de red encapsulado en capa de red es:

Ilustración 28 - Encapsulamiento paquete IPv6

Desde el punto de vista del diagrama de red el túnel 6to4 es implementado en la red pública con soporte IPv4.

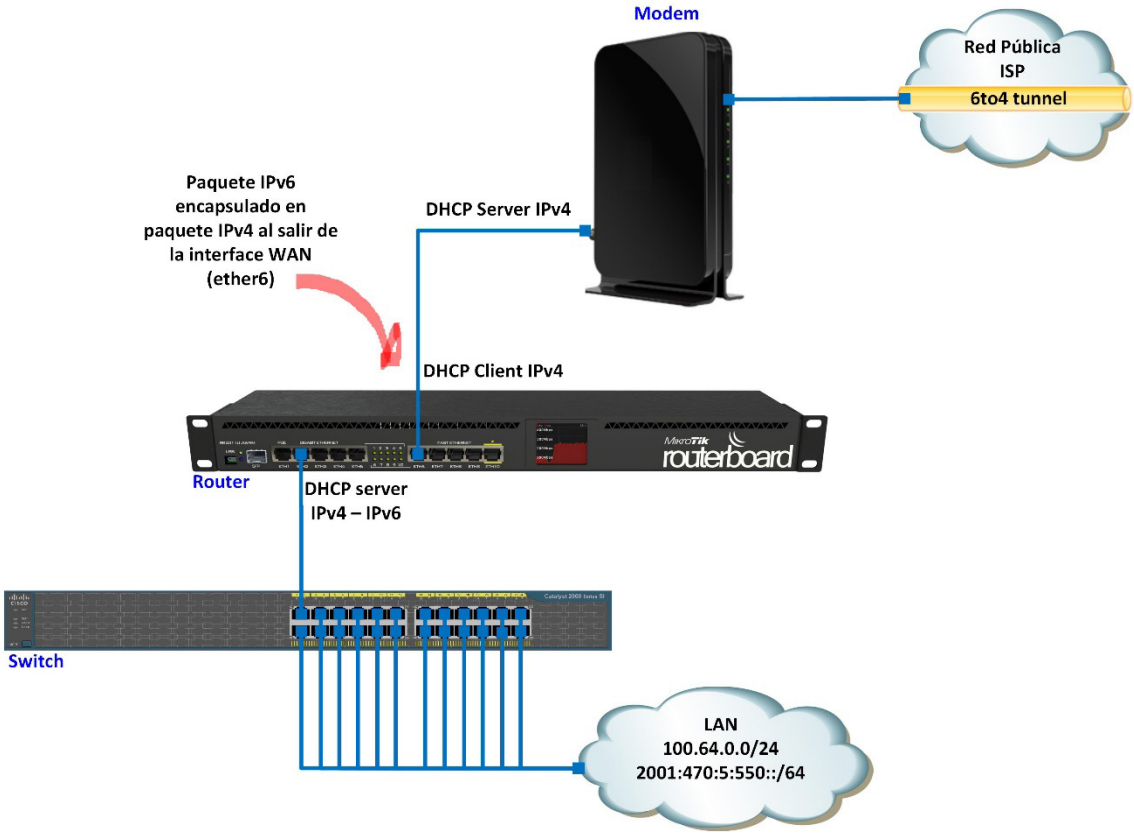


Ilustración 29 - Diagrama de red túnel 6to4

Hurricane electric

Hurricane Electric es un backbone global en Internet (ISP, es decir, un proveedor de servicios de internet) especializado en IPv6. Trabaja desde sus centros de datos en el Área de la Bahía de San Francisco, situados principalmente en Fremont (California).

Hurricane Electric controla varios backbones IPv4/IPv6 en Asia, Norte América y Europa, que están conectados a distintos puntos neutros (conexión con redes IPv4) de todo el mundo. Y opera actualmente el backbone más grande de IPv6 en el mundo, medido por el número de redes conectadas. En octubre de 2010, Hurricane Electric fue la primera en conectar 1000 redes IPv6.

Ofrece servicios gratuitos como un tunnel broker IPv6 que permite configurar túneles estáticos y BGP.

En el contexto de redes, un tunnel broker es un servicio que provee un túnel de red. Estos túneles pueden proveer de conectividad encapsulada mediante la infraestructura existente hacia otra infraestructura.

Los gateway router que trabajan con el protocolo de encapsulamiento y tunelamiento 6to4 son denominados relay router. De esta manera Hurricane Electric constituye un proveedor de internet, ISP, virtual.

La página principal de Hurricane Electric es:

http://he.net/

Por lo tanto, la empresa Hurricane Electric al brindar un tunnel bróker es posible implementar un tunnel 6to4 hacia sus relay routers de manera tal de encapsular el paquete IPv6 en un paquete IPv4, con una dirección destino a un gateway conectado a la red pública (con soporte IPv4) y que realizar el decapsulamiento y el envío de paquete hacia el core (red principal del proveedor de internet) de Hurricane electric, la cual opera bajo IPv6 e interconecta otras redes de IPv6.

A continuación, un mapa de la red IPv6 de Hurricane Electric.

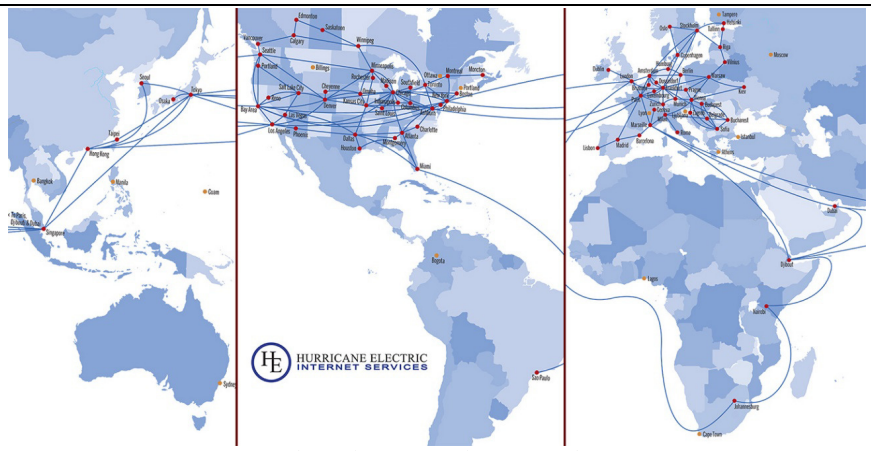


Ilustración 30 - Hurricane network
https://he.net

Es necesario registrarse en la página de Hurricane Electric donde se brinda la opción de configurar el tunnel bróker. Para esto y una vez realizada la cuenta en sus servidores debemos especificar la dirección IPv4 pública la cual constituye uno de los puntos del túnel y se genera un prefijo IPv6 global, el cual debe ser configurado para la asignación de IPv6 a los hosts. En la siguiente imagen se puede observar los datos brindados por Hurricane Electric al momento de realizar la cuenta del túnel.

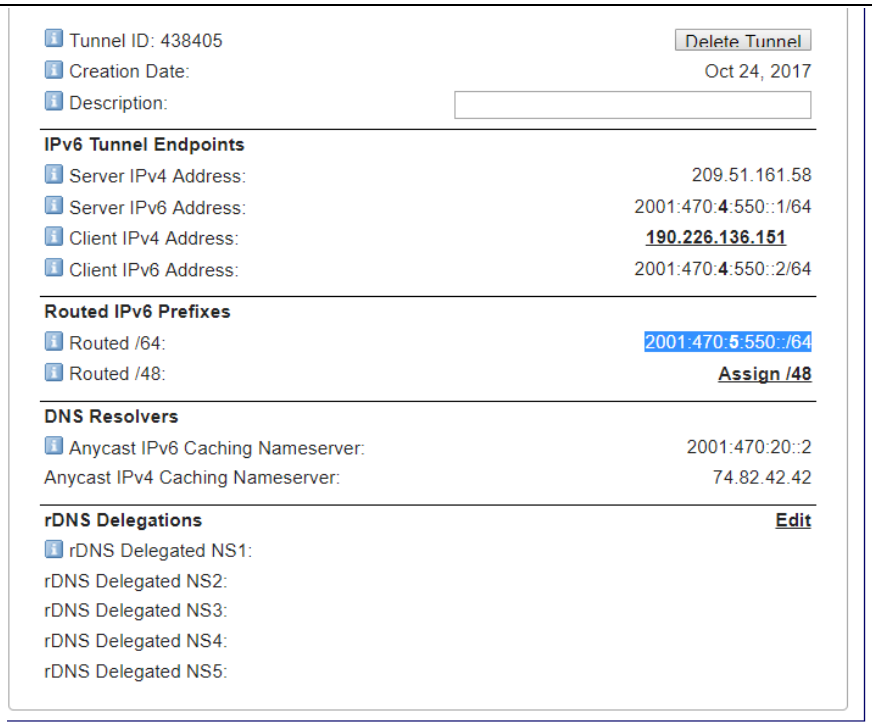


Ilustración 31 - Parámetros de Hurricane tunel broker
https://he.net

Podemos ver que al momento de realizar la configuración del tunnel bróker, mi dirección pública era 190.226.136.151. Las demás direcciones especificadas son las siguientes:

La dirección Server IPv4 Address corresponde a la dirección IPv4 del relay router. Es la dirección de destino del paquete IPv4 que encapsula el paquete original IPv6. Es el punto de entrada al backbone de Hurricane Electric, desde la red con soporte IPv4.

La dirección Server IPv6 corresponde a la dirección IPv6 del relay router, viéndolo desde el puerto que conecta con la red interna de Hurricane Electric con soporte IPv6. La dirección Server IPv4, anteriormente definida, corresponde a la dirección IP del puerto del relay router que conecta con la red IPv4.

La dirección Client IPv6 Address corresponde a la dirección del router Mikrotik utilizado, es decir, el de la LAN. Esta dirección debe ser asignada a la interface virtual sit1, en el router que implementa el túnel. De esta manera dicha interface, virtualmente, conecta a la red de Hurricane electric y todos los paquetes IPv6 salientes de la LAN serán enrutados a esta dirección. Como se configura un ND y un enrutamiento dinámico GBP (border gateway protocol), el router aprenderá las interfaces del backbone de Hurricane Electric y el enrutamiento a través de esta.

El prefijo brindado para la asignación de IPv6 globales de los hosts en la red LAN es la definida en Routed/64.

Por lo tanto, la configuración del router Mikrotik es la siguiente:

```
/interface 6to4
add comment="Hurricane Electric IPv6 Tunnel Broker" !keepalive local-address=100.64.0.1
mtu=1280 name=sit1 remote-address=209.51.161.58
/ip neighbor discovery
set sit1 comment="Hurricane Electric IPv6 Tunnel Broker"
/ipv6 dhcp-server
add address-pool=poolIPv6 interface=LAN name=dhcp-IPv6
/ipv6 pool
add name=poolIPv6 prefix=2001:470:5:550::/64 prefix-length=64
/ipv6 address
add address=2001:470:4:550::2 advertise=no interface=sit1
add address=2001:470:5:550:4e5e:cff:fe1e:8b48 eui-64=yes interface=LAN
/ipv6 nd
set [ find default=yes ] advertise-dns=yes
/ipv6 route
add !bgp-as-path !bgp-atomic-aggregate !bgp-communities !bgp-local-pref !bgp-med !bgp-origin
!bgp-prepend !check-gateway distance=1 gateway=2001:470:4:550::1 !route-tag
add !bgp-as-path !bgp-atomic-aggregate !bgp-communities !bgp-local-pref !bgp-med !bgp-origin
!bgp-prepend !check-gateway distance=1 gateway=2001:470:4:550::1 !route-tag
add !bgp-as-path !bgp-atomic-aggregate !bgp-communities !bgp-local-pref !bgp-med !bgp-origin
!bgp-prepend !check-gateway distance=1 gateway=2001:470:4:550::1 !route-tag
add !bgp-as-path !bgp-atomic-aggregate !bgp-communities !bgp-local-pref !bgp-med !bgp-origin
!bgp-prepend !check-gateway distance=1 dst-address=2000::/3 gateway=\
   2001:470:4:550::1 !route-tag
add !bgp-as-path !bgp-atomic-aggregate !bgp-communities !bgp-local-pref !bgp-med !bgp-origin
!bgp-prepend !check-gateway distance=1 dst-address=2000::/3 gateway=\
   2001:470:4:550::1 !route-tag
add !bgp-as-path !bgp-atomic-aggregate !bgp-communities !bgp-local-pref !bgp-med !bgp-origin
!bgp-prepend !check-gateway distance=1 dst-address=2000::/3 gateway=\
   2001:470:4:550::1 !route-tag
add !bgp-as-path !bgp-atomic-aggregate !bgp-communities !bgp-local-pref !bgp-med !bgp-origin
!bgp-prepend !check-gateway distance=1 dst-address=2000::/3 gateway=\
```

2001:470:4:550::1 !route-tag

El siguiente es un diagrama esquemático de la conexión entre las redes.

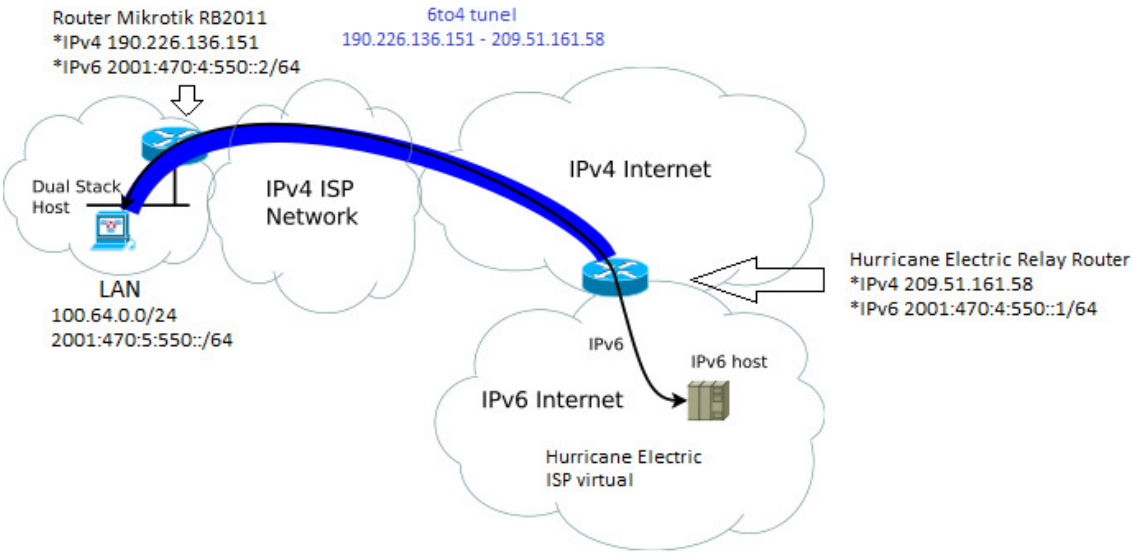


Ilustración 32 - Diagrama general de túnel broker

Virtualmente existe una conexión directa entre la red LAN y la red IPv6 de Hurricane Electric.

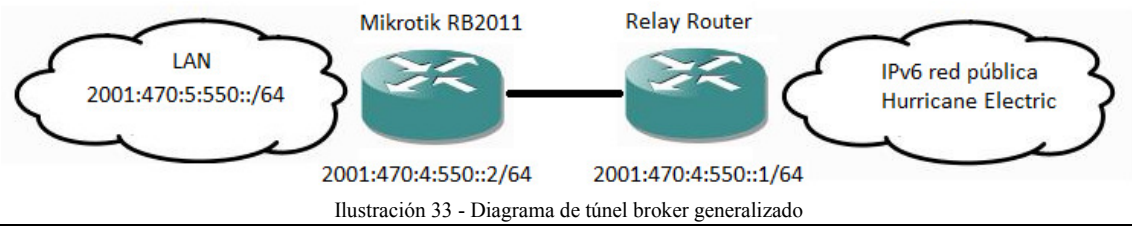


Ilustración 33 - Diagrama de túnel broker generalizado

NetAssist tunnel broker

El inconveniente que ha surgido al implementar el túnel 6to4 con la red Hurricane Electric es que sus servidores requieren una respuesta ICMP de nuestra red, es decir, de la interface WAN del router para poder establecer el enlace. Este requerimiento, es a manera de confirmación de que la persona que registró la dirección IP del punto final del túnel sea correcta.

Esto puede ocasionar un problema ya que es posible que el proveedor de internet filtre los paquetes ICMP hacia nuestra red, los paquetes con destino, no las respuestas. En caso contrario sería necesario informarles y realizar el pedido de la habilitación del ICMP hacia nuestro equipo.

Otra posibilidad es que muchas empresas o instituciones realizan un filtrado de los paquetes ICMP hacia sus equipos con el objetivo de no hacer visible su red LAN o intranet a IP finders.
Por lo tanto, la solución más conveniente es un proveedor de túnel bróker que no requiera una respuesta ICMP y que al mismo tiempo presente un backbone IPv6 importante. El proveedor elegido es NetAssist.

El registro y la configuración es análogo a Hurricane Electric, como se puede ver en la siguiente imagen.

You are logged in as "**julianov403@gmail.com**" [Logout].

Your NetAssist IPv6 Tunnel Broker details:

Server IPv4 address	62.205.132.12
Client IPv4 address	181.111.67.38
Server IPv6 address	2a01:d0:ffff:6348::1/64
Client IPv6 address	2a01:d0:ffff:6348::2/64
Routed /48 IPv6 network	2a01:d0:e348::/48
IPv6 DNS server	2a01:d0::1
Your e-mail (login)	julianov403@gmail.com
Change	

Set reverse (backresolve) DNS:

2a01:d0:ffff:6348::2	IN PTR	
8.4.3.e.0.d.0.0.1.0.a.2.ip6.arpa	IN NS	
8.4.3.e.0.d.0.0.1.0.a.2.ip6.arpa	IN NS	
Change		

Ilustración 34 - NetAssit Tunel Broker
http://tb.netassist.ua

La configuración del router Mikrotik es:

```
/interface 6to4 add comment="NetAssist IPv6 Tunnel Broker" disabled=no local-
address=181.111.67.38 mtu=1280 name=sit1 remote-address=62.205.132.12

/ipv6 route add comment="" disabled=no distance=1 dst-address=2000::/3
gateway=2a01:d0:ffff:6348::1 scope=30 target-scope=10

/ipv6 address add address=2a01:d0:ffff:6348::2/64 advertise=yes disabled=no eui-64=no
interface=sit1
```

Firewall

Una vez configurada la Red es necesario configurar el firewall. La configuración del firewall es estándar.

- Reglas generales

Escritura de firewall: siempre conviene empezar con las reglas de estado, para ahorrar procesamiento y acelerar las conexiones ya establecidas y las relativas.

```
ip firewall filter add connection-state=established action=accept chain=input
ip firewall filter add connection-state=related action=accept chain=input
add action=accept chain=forward connection-nat-state=srcnat,dstnat
ip firewall filter add connection-state=invalid action=drop  chain=input
```

Esto es debido a que una vez establecida una conexión o una negación, el firewall guarda los estados de esta y luego son aceptadas o negadas en estas primeras reglas sin necesidad de seguir las siguientes reglas.

- Fuerza bruta

Para impedir que, por ejemplo, nos descubran la password del SSH utilizando fuerza bruta podemos implementar un mecanismo que habilite sólo tres intentos de acceso y luego bloquee la IP por 10 días:

```
ip firewall filter add chain=input connection-state=new protocol=tcp dst-port=22 action=add-src-to-address-list address-list=ssh-blacklist address-list-timeout=10d src-address-list=ssh3
ip firewall filter add chain=input connection-state=new protocol=tcp dst-port=22 action=add-src-to-address-list address-list=ssh3 address-list-timeout=1m src-address-list=ssh2
ip firewall filter add chain=input connection-state=new protocol=tcp dst-port=22 action=add-src-to-address-list address-list=ssh2 address-list-timeout=1m src-address-list=ssh1
ip firewall filter add chain=input connection-state=new protocol=tcp dst-port=22 action=add-src-to-address-list address-list=ssh1 address-list-timeout=1m
ip firewall filter add chain=input protocol=tcp dst-port=22 action=drop address-list=ssh-blacklist
```

- DoS

Los ataques de DoS se llevan a cabo consumiendo y agotando los recursos del equipo/red atacado. Existen algunas formas de mitigarlos.

Una estrategia es utilizar tarpit. Esto baja la ventana TCP a 0, impidiendo que haya transferencia de datos, pero dejando que se generen las conexiones.

```
ip firewall filter add chain=input dst-address=100.64.0.1 protocol=tcp dst-port=22-8291
action=tarpit connection-limit=1,32
```

Red Privada Virtual (VPN)

Ante la necesidad de conectar equipos y la imposibilidad de realizar una conexión, ya sea cableada o inalámbrica, dedicada solamente estos debido a las distancias geográficas y el costo que conllevaría un enlace propio; es posible, sin embargo, realizar una conexión lógica a través de la red pública desplegada por los proveedores de internet. Un túnel es una herramienta útil para esta tarea.

Se conoce como túnel o tunneling a la técnica que consiste en encapsular un protocolo de red sobre otro. Por ejemplo, un paquete IP transportando otro paquete IP o un paquete IP transportando una

trama ethernet son ejemplos de túneles. Mientras que un paquete IP transportando un paquete TCP es una conexión de red normal.

Los túneles proveen un mecanismo de transporte de protocolos. Existen diferentes razones para implementarlos:

- La infraestructura de la red no soporta el protocolo a utilizar. La red pública no posee protocolos propios de encriptación, y es lo que debemos implementar en este proyecto.
- La infraestructura de la red no soporta el enrutamiento de paquetes debido a la falta de información o tipos de direcciones. No se puede enrutar y manejar en la red pública direcciones de red privada, que es lo que necesitamos en este proyecto.
- La infraestructura de red no posee soporte para el tipo de tráfico. Que es lo que implementamos en este proyecto al utilizar un túnel 6to4, ya que la red pública no posee infraestructura para paquetes IPv6.

Un túnel consiste en 4 partes principales, el encabezado de red para el túnel, el encabezado propio del túnel, el encabezado de red del paquete original (cabecera de red PDU) y los datos (PDU payload).

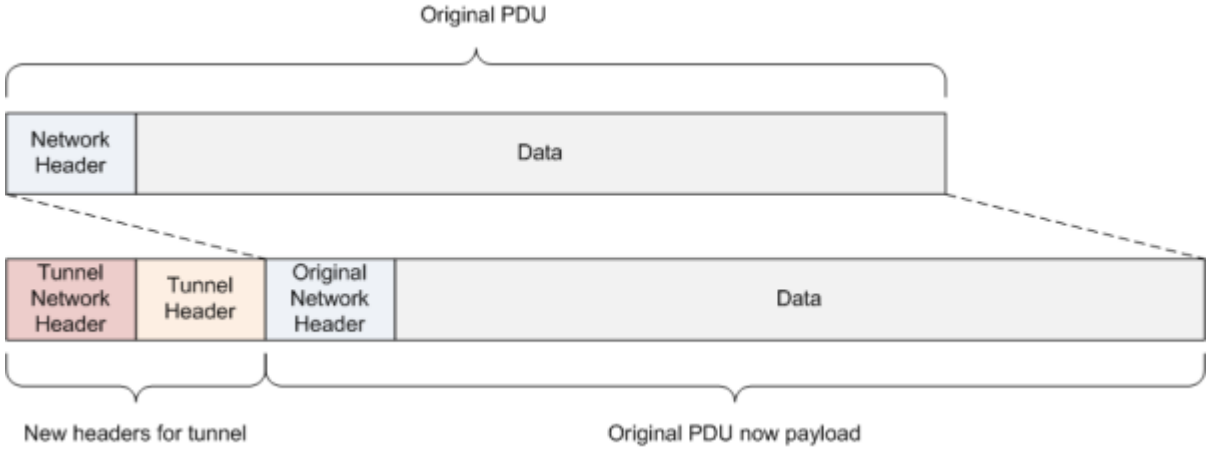


Ilustración 35 - Tunelamiento
https://infrastructureadventures.wordpress.com/tag/vpn

Tunnel Network Header: Esta cabecera contiene las direcciones de fuente y destino de los puntos finales del túnel. Puede contener cabeceras de una sola capa o de múltiples capas del modelo OSI. Por ejemplo, un túnel GRE solo consiste de una cabecera IP (capa 3), mientras que el túnel L2TP consiste en una cabecera IP y UDP (capa 3 y capa 4).

Tunnel Header: es el encabezado específico del protocolo de túnel, por lo que GRE, IPSec, L2TP, PPTP, etc. tienen su propio formato de encabezado. Los puntos finales del túnel pueden tener múltiples túneles entre ellos y, entre otras cosas, los encabezados del túnel permiten que los puntos finales identifiquen el tráfico de un túnel u otro.

Original Network Header: es el encabezado de red del paquete original que está encapsulada en el túnel. El encabezado de red original generalmente no es examinado por los dispositivos de red ya que es parte de la carga útil del túnel, al igual que cualquier otro dato de carga útil.

Hay diferentes formatos, algunos solamente encapsulan la capa de red, otros encapsulan la capa de red y de transporte, otros encapsulan a su vez la capa de enlace. Existe la posibilidad de utilizar más de un encapsulamiento según las necesidades.

Tipos de túneles que encapsulan la capa de enlace: L2TP, EoIP, VPLS.
Tipos de túneles que encapsula la capa de red: IPsec, GRE, PPTP.
Como ejemplo podemos visualizar en la siguiente imagen el frame o paquete del protocolo L2TP.

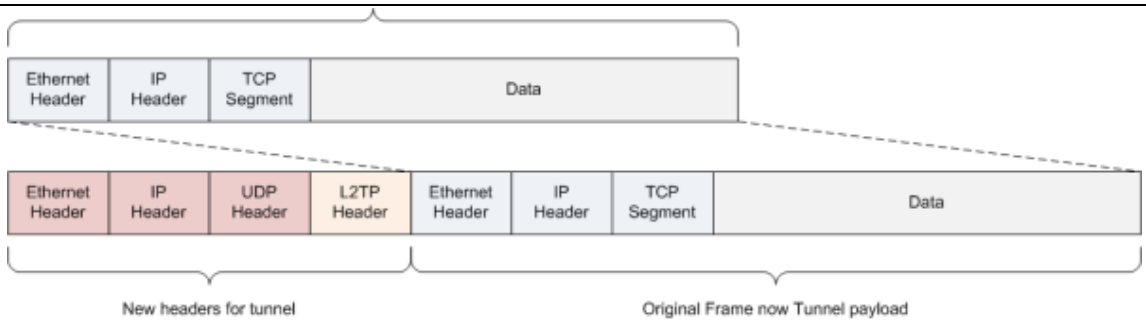


Ilustración 36 - Tunelamiento L2TP
https://infrastructureadventures.wordpress.com/tag/vpn/

Donde se observa que los encabezados definidos en New headers for tunnel corresponden a las cabeceras del paquete enviado con un paquete UDP en la capa de transporte y cuya información corresponde a la trama completa de la LAN (capa 2 del modelo OSI), extendiendo así la red y de esta manera al compartir la capa de enlace es posible comunicar los protocolos propios de esta como lo es el protocolo ARP, el VLAN TAG, etc.

Un ejemplo de un tunnel de capa de red es el GRE, donde podemos observar el frame en la siguiente imagen.

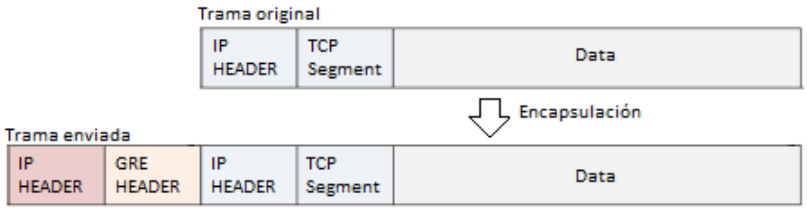


Ilustración 37 - Tunelamiento GRE

En el caso anterior estamos encapsulando la trama de red solamente.

De la misma manera se pueden implementar el encapsulado de más de un protocolo. Por ejemplo, el siguiente frame corresponde a una encapsulación L2TP la cual es encapsulada siguiendo el protocolo IPsec. Esto es conocido como L2TP/IPsec, que implementa Windows nativamente.

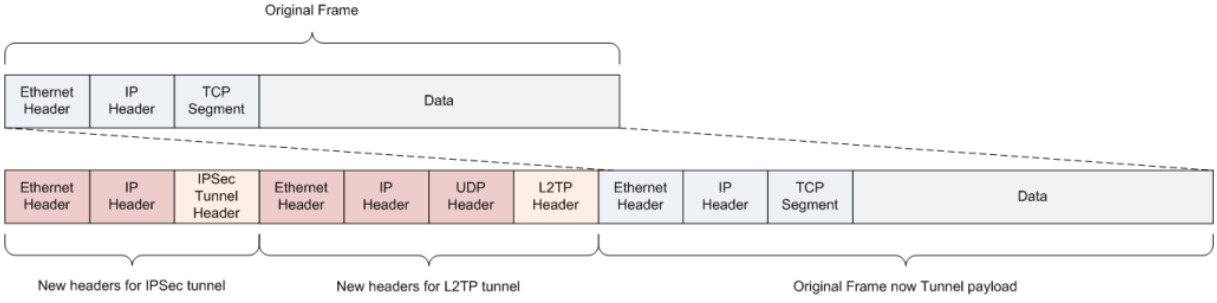
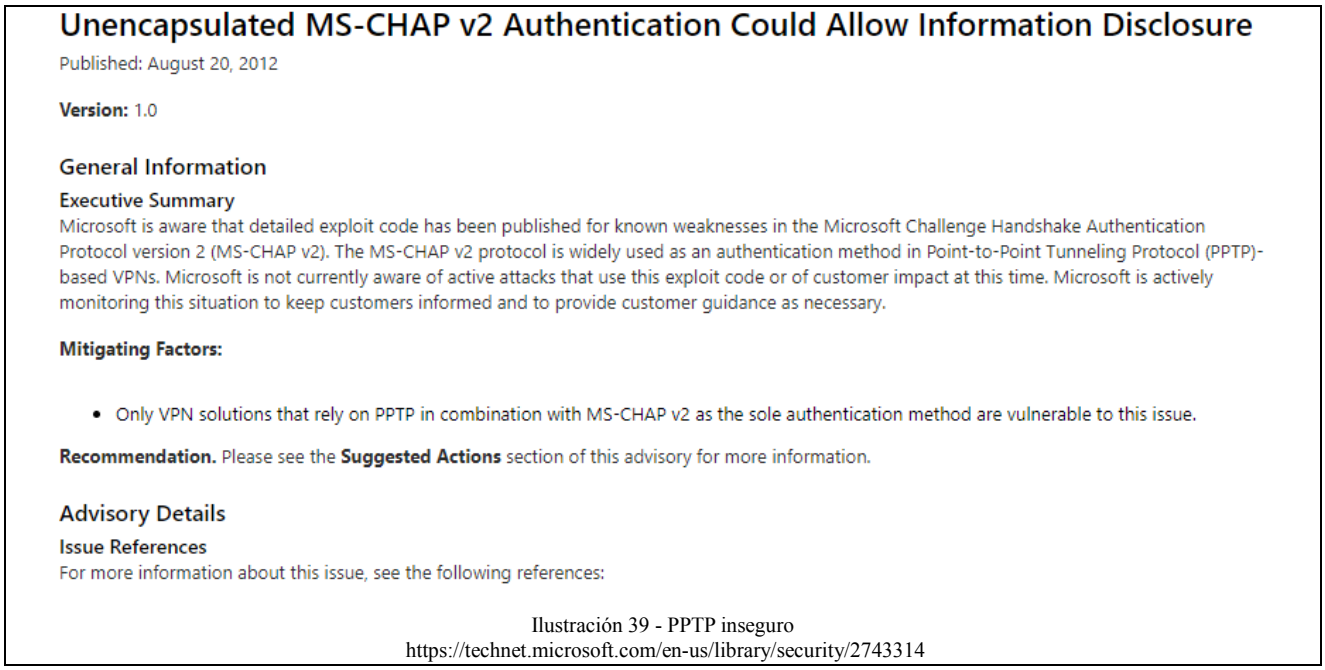


Ilustración 38 - Tunelamiento L2TP/IPsec
https://infrastructureadventures.wordpress.com/tag/vpn/page/2/

El uso de estos 2 protocolos es debido a que L2TP no brinda las funcionalidades de encriptación y autenticación como IPsec. Y este último no posee soporte multicast.

Con respecto a PPTP, que es el protocolo de VPN más utilizado actualmente por su fácil implementación y utilización, podemos citar:



Unencapsulated MS-CHAP v2 Authentication Could Allow Information Disclosure

Published: August 20, 2012

Version: 1.0

General Information

Executive Summary

Microsoft is aware that detailed exploit code has been published for known weaknesses in the Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2). The MS-CHAP v2 protocol is widely used as an authentication method in Point-to-Point Tunneling Protocol (PPTP)-based VPNs. Microsoft is not currently aware of active attacks that use this exploit code or of customer impact at this time. Microsoft is actively monitoring this situation to keep customers informed and to provide customer guidance as necessary.

Mitigating Factors:

- Only VPN solutions that rely on PPTP in combination with MS-CHAP v2 as the sole authentication method are vulnerable to this issue.

Recommendation. Please see the **Suggested Actions** section of this advisory for more information.

Advisory Details

Issue References

For more information about this issue, see the following references:

Ilustración 39 - PPTP inseguro
https://technet.microsoft.com/en-us/library/security/2743314

Protocolo de tunelamiento a utilizar

Se decidió utilizar IPsec como protocolo para implementar la VPN.
IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que, para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

En cuanto a L2TP, este encapsula en un paquete UDP la trama ethernet completa lo que implica la disminución del tamaño de los datos, un MTU menor. A su vez como L2TP o demás protocolos de encapsulamiento de capa de red no implementan encriptación, es necesario utilizar IPsec si se requiere esta característica.

IPsec está implementado por un conjunto de protocolos criptográficos para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos.
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 es simplemente el paquete de

algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Modos de funcionamiento

IPsec, al ser un conjunto de protocolos definen 2 modos de funcionamiento.

Modo transporte: En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo, traduciendo los números de puerto TCP y UDP). El modo transporte seutiliza para comunicaciones host a host.

Una forma de encapsular mensajes IPsec para atravesar NAT ha sido definido por RFCs que describen el mecanismo de NAT-T.

El propósito de este modo es establecer una comunicación segura punto a punto, entre dos hosts y sobre un canal inseguro.

Modo túnel: En el modo túnel, todo el paquete IP (datos más encabezados) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones host a red u host a host sobre Internet. El propósito de este modo es establecer una comunicación segura entre dos redes remotas sobre un canal inseguro.

Protocolos - Encabezados

IPsec define 2 protocolos para proveer seguridad de tráfico. Autentification header (encabezado de autenticación) AH y encapsulation security payload (encapsulamiento seguro de datos) ESP.

El encabezado IP de autenticación, AH, provee integridad de conexión (que el mensaje no ha sido modificado a través del trayecto en la red), autenticación de datos de origen (se asegura que el que envió el mensaje es realmente el) y servicio anti reproducción.

El encabezado de encapsulamiento seguro de datos, ESP, provee encriptación y limita el flujo de tráfico confidencial. A su vez provee autenticación. ESP es el protocolo más utilizado siendo que AH más obsoleto y brindas las mismas características de autenticación sumándole la integridad de los datos, pero sin el beneficio de la encriptación.

Estos protocolos pueden ser usados solos o en conjunto. A continuación, se muestran las diferentes variantes en modos de funcionamientos y en protocolos utilizados.

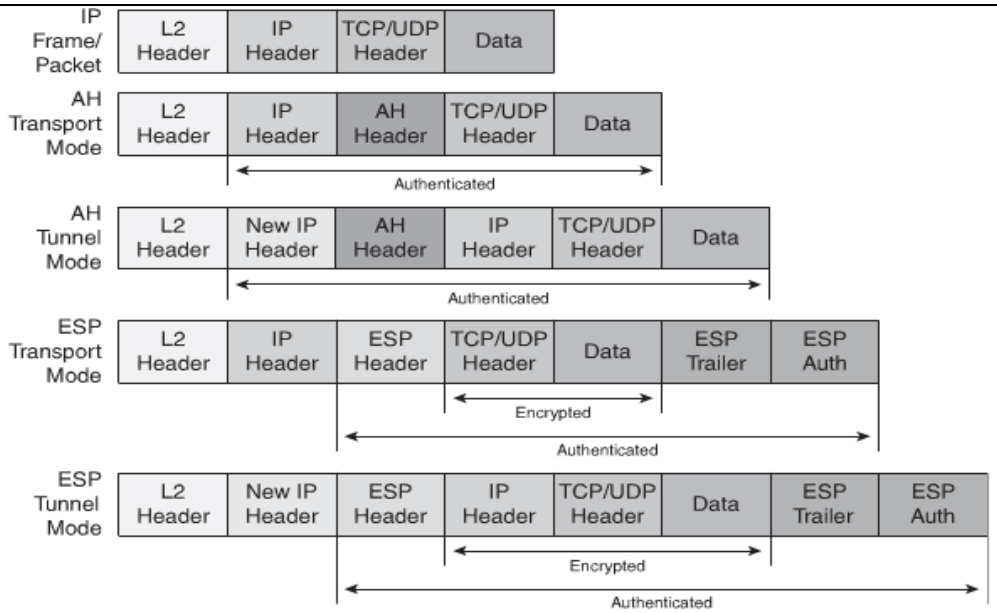


Ilustración 40 - Modos y protocolos IPsec

Elección de modo de funcionamiento y protocolo

El motivo de la implementación de una VPN en este trabajo es poder registrar cualquier softphones, PC, laptop, Tablet y celular de las personas que pertenecen a la institución, organización, empresa, etc. Y que utilizan el servicio de telefonía IP mediante una dirección IP privada. De manera tal que el registro de un softphone con la central de telefonía, y la comunicación entre estos se realice mediante direcciones de red privada.

El hecho anterior solamente puede ser implementado con IPsec en modo túnel. De manera tal de encapsular el encabezado de red original, con dirección IP origen y destino privadas en un paquete IP con las direcciones públicas correspondientes.

El segundo punto de vital importancia en una comunicación de voz-audio-video en tiempo real es la confidencialidad y seguridad de los datos. Evitando de esta manera la escucha por personas externas. Debe resaltarse que debido a que los paquetes de audio y video son transportados en la red pública, estos deben protegerse.

La información de una empresa o institución en cuanto a la comunicación entre agentes deben protegerse. En el siglo XXI, la información es poder, dinero, etc.
Este nivel de encriptación solamente lo provee el conjunto de protocolos en IPsec. El protocolo elegido para el trabajo es ESP, que brinda encriptación y autenticación de los datos.

Nivel de encriptación

La encriptación elegida para utilizar es AES-256. Recomendada por NSA (National Security Agency), Agencia de Seguridad Nacional de los Estados Unidos, ya que es la encriptación utilizada por esta para sus comunicaciones.

"The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use". CNSS Policy No. 15, Fact Sheet No. 1 (pág. 1)

AES Brinda 3 variantes en la longitud de sus claves: 128, 196 y 256 bits.

Considerando una clave de 128 bits, existen $2^{128} = 3.4 * 10^{38}$combinaciones.

Considerando una clave de 256 bits, existen $2^{256} = 1.15 * 10^{77}$combinaciones.

A su vez para agregar más portabilidad se configurará la encriptación 3DES, de manera tal de que no impida o restrinja a un cliente a utilizar solamente la encriptación AES256.

El algoritmo 3DES (Triple Data Encryption Standard), se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado, empleando una clave criptográfica. 3DES es el algoritmo que hace triple cifrado del DES; se basa en aplicarlo tres veces, con tres claves distintas, por lo que resulta mucho más seguro.

Este método está siendo paulatinamente sustituido por el AES, ya que éste tiene una velocidad hasta seis veces más rápida, sin embargo, aún existen medios de pago electrónicos, tarjetas de crédito, etc. que utilizan el estándar 3DES, por lo que continúa estando muy vigente.

Autenticación e integridad

El método de autenticación elegido es PSK (Pre Shared Key) + Auth. Pre Shared Key es la clave previamente compartida donde adicionalmente se agrega un usuario y una contraseña. De esta manera, además de tener una clave previamente compartida y conocida por los usuarios, la cual se usará para la encriptación, se posee un usuario y una clave particular para cada uno, identificándolo.

Con respecto a la integridad, se utiliza el algoritmo SHA1 (Secure Hash Algorithm, Algoritmo de Hash Seguro) donde se produce una firma digital y se comprueba que el mensaje proviene de un cliente seguro y que no ha sido modificado en su trayecto. Brindando autenticación e integridad simultáneamente.

SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. No obstante, en el año 2004, un número de ataques significativos fueron divulgados sobre funciones criptográficas de hash con una estructura similar a SHA-1; lo que ha planteado dudas sobre la seguridad a largo plazo de SHA-1.

El 23 de Febrero de 2017, un equipo formado por Google y CWI Amsterdam, han anunciado la primera colisión de SHA-1, la cual ha sido nombrada como SHAttered.

La importancia de la rotura de una función hash se debe interpretar en el siguiente sentido:
Un hash permite crear una huella digital, teóricamente única, de un archivo. Una colisión entre hashes supondría la posibilidad de la existencia de dos documentos con la misma huella.

Si bien es posible configurar en el router Mikrotik algoritmos SHA256 y SHA512. Este algoritmo de integridad no es manejado por el cliente VPN de Android, si por el cliente SHREW que será utilizado en Windows.

Código a implementar en RouterOS

La implementación de lo definido y especificado anteriormente en RouterOS es la siguiente:

```
/ip ipsec mode-config
add address-pool=poolIPv4-VPN name=cfg1
```

```
/ip ipsec peer
add address=0.0.0.0/0 auth-method=pre-shared-key-xauth dh-group="ec2n185,ec2n155\
   ,modp8192,modp6144,modp4096,modp3072,modp2048,modp1536,modp1024,modp768" \
   enc-algorithm=aes-256 generate-policy=port-override mode-config=cfg1 \
   passive=yes secret=123456
/ip ipsec user
add name=user1 password=123456
add name=user2 password=123456
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=aes-256-cbc
```

Además de lo ya descripto anteriormente podemos observar la línea:

```
/ip ipsec mode-config
add address-pool=poolIPv4-VPN name=cfg1
```

Esto implica que cuando un usuario realice una conexión IPsec en modo túnel, el router le brindará una IP perteneciente al pool "poolIPv4-VPN", que es un pool diferente al utilizado por el DHCP server en la LAN, de manera tal de tener una configuración más limpia.
Dicho pool tiene el rango: 100.64.1.0/24

De esta manera, el cliente en el extremo del túnel tendrá una dirección IP privada y se podrá comunicar con los hosts de la red LAN. Por lo tanto, se extiende la red desde el punto de vista de la capa 3 del modelo OSI. Recordando que el protocolo DHCP trabaja sobre esta. No así el protocolo ARP que trabaja sobre la capa de enlace por lo que no es posible obtener o visualizar el equipo remoto dentro de la tabla ARP de los hosts; aspecto no necesario para la implementación que estamos realizando.

Se creó 2 usuarios a modo de ejemplo con sus respectivas claves:

```
add name=user1 password=123456
add name=user2 password=123456
```

Además, agregamos las siguientes líneas en el Firewall del router para permitir la conexión:

```
/ip firewall filter
add action=accept chain=input comment=IPsec dst-port=500 protocol=udp
add action=accept chain=input comment=IPsec dst-port=4500 protocol=udp
add action=accept chain=input comment=IPsec protocol=ipsec-esp
add action=accept chain=output comment=IPsec protocol=ipsec-esp
```

add action=accept chain=forward comment=IPsec protocol=ipsec-esp

Y reglas de NAT

/ip firewall nat

add action=masquerade chain=srcnat comment=IPSec protocol=ipsec-esp

add action=accept chain=IPsec in-interface=WAN protocol=ipsec-esp

Tipos de conexiones

Podemos diferenciar 2 tipos de conexiones cuando se trata de una VPN implementando IPsec.
El primer tipo de conexión es entre redes LAN donde un router media como servidor y otro como cliente, como se puede observar en la siguiente imagen.

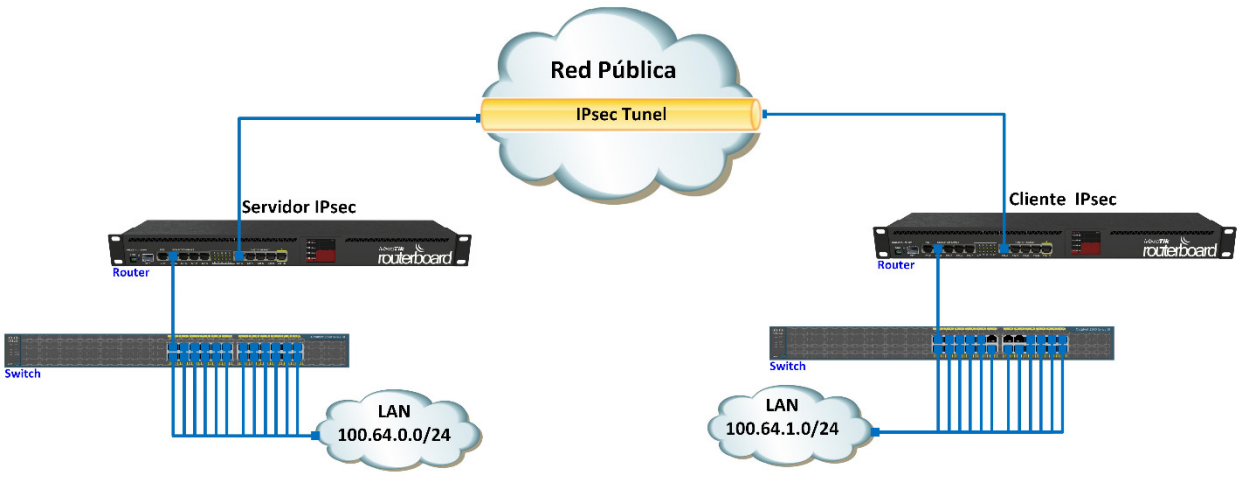


Ilustración 41 - IPsec túnel red a red

De la misma forma se puede implementar una conexión entre la red LAN con un router como servidor y diferentes hosts como clientes, los cuales se conectan en la red pública.

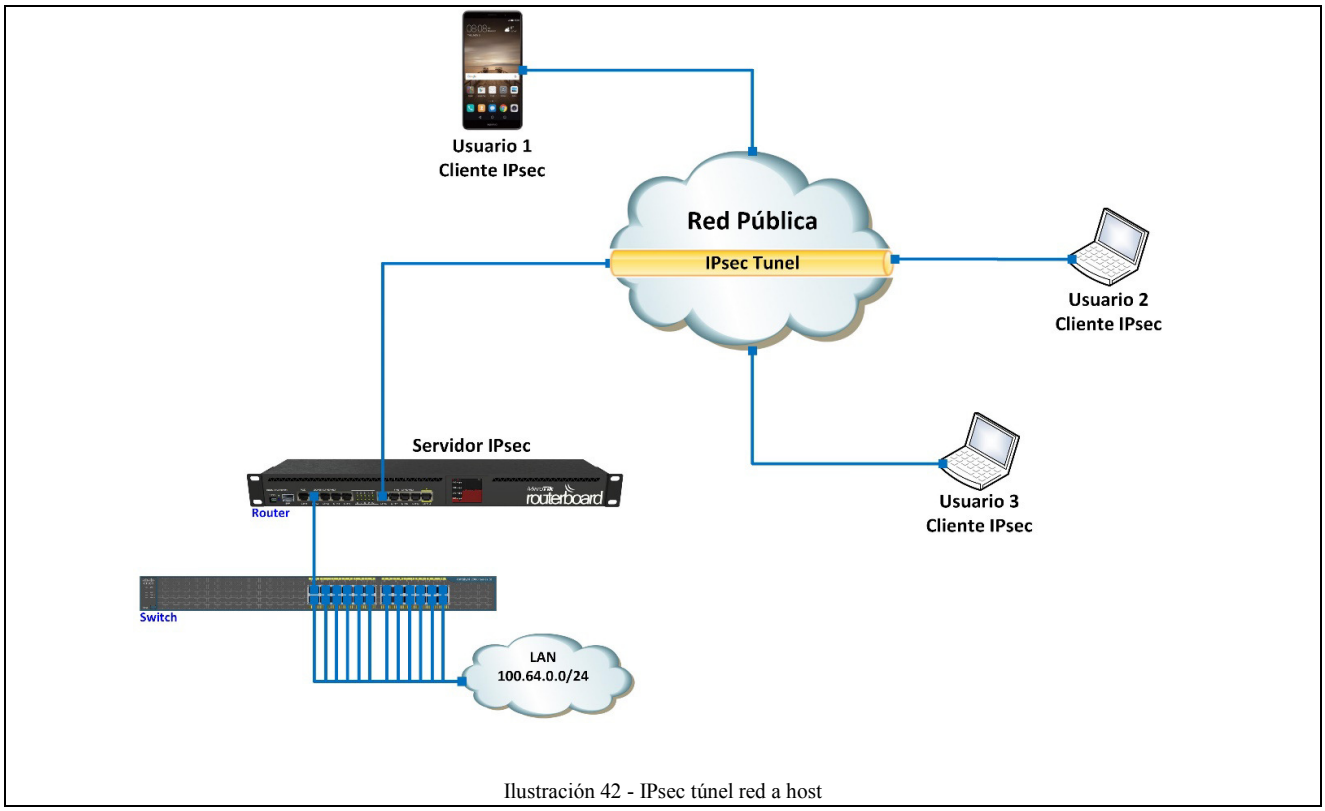


Ilustración 42 - IPsec túnel red a host

Ambos tipos de conexiones pueden implementarse complementariamente, si así se desea.

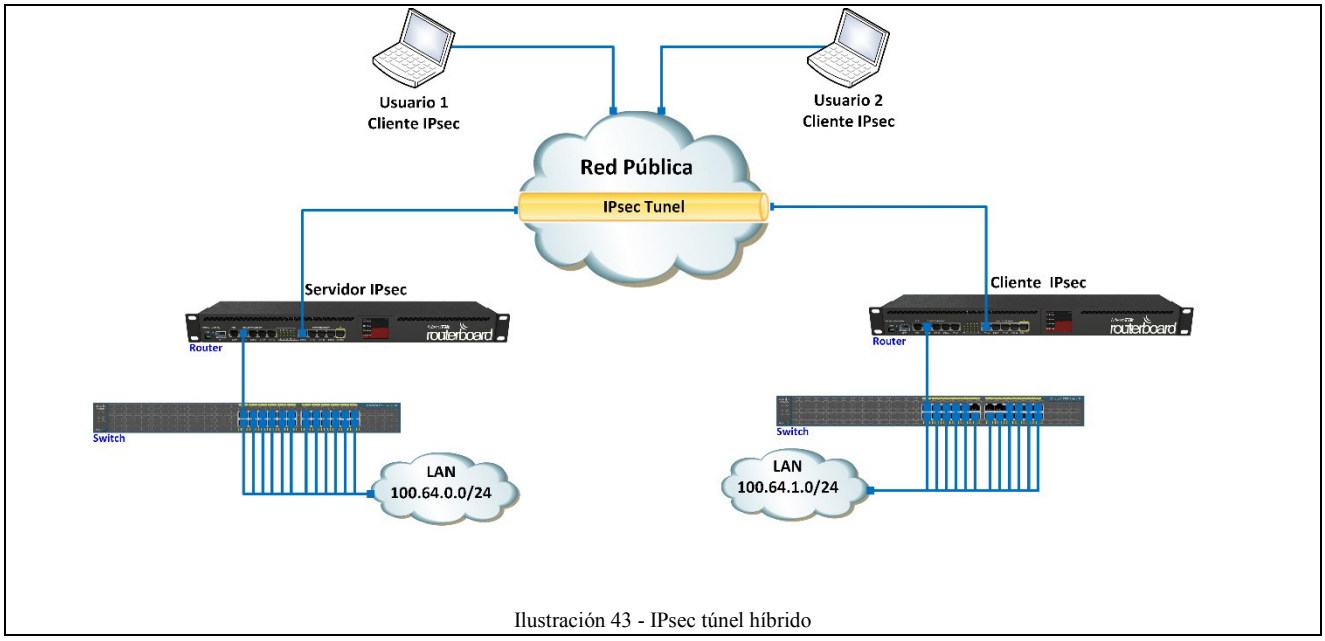


Ilustración 43 - IPsec túnel híbrido

Problemas - NAT

Cuando se estable un túnel IPsec entre routers en la red pública no es necesario considerar el NAT ya que los routers de los ISP no realizan el proceso de la traslación de direcciones, ni filtrado. Ahora bien, si el paquete de red encapsulado mediante el encabezado ESP necesita "cruzar" un router que realiza un NAT se encontrará con un gran inconveniente según el protocolo de funcionamiento del Network Address Traslation.

Un NAT es una traslación de direcciones que muchas veces se realiza para enmascarar direcciones privadas en una pequeña cantidad de direcciones públicas, o una dirección solamente como es la mayoría de los casos. Este mecanismo funciona "leyendo" los puertos de la capa de transporte, es decir, los puertos de los paquetes TCP y los paquetes UDP. Ahora bien, recordando el frame de IPsec modo túnel.

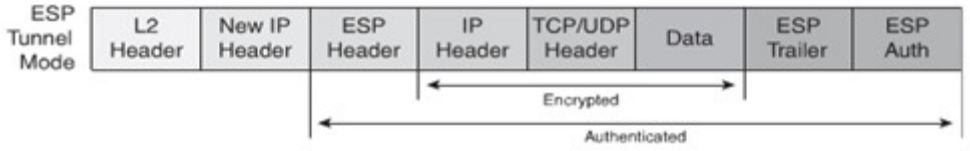


Ilustración 44 - IPsec ESP túnel

Vemos como los datos de la capa de red, que implican la capa de transporte (capa 4 del modelo OSI) en un paquete IP tradicional, ahora existe el ESP header que encripta los encabezados siguientes por lo que no es posible leer los puertos del paquete TCP o UDP. Además, rompe con el estándar TCP/IP tradicional ya que como datos de la capa de red tenemos otro paquete de red.

Este inconveniente imposibilita que se realice un NAT y trae consecuencias si un usuario, que está por ejemplo en un hotel, se quiere conectar con la central de telefonía mediante la VPN y el router de dicha LAN, que implementa direcciones privadas, no puede hacer el NAT.

Para esto existe un mecanismo o modificación del frame IPsec definido en la documentación RFC2637 donde el encabezo ESP y toda la trama siguiente está incluido como datos en un paquete UDP. Este mecanismo es denominado NAT-T.

NAT traversal es un término aplicado a las técnicas que establecen y mantienen conexiones en redes utilizando los protocolos TCP/IP o UDP que atraviesan (NAT) gateways.

Para permitir el funcionamiento de IPsec a través de NAT; los siguientes protocolos deben estar permitidos en el firewall:

- Internet Key Exchange (IKE) - User Datagram Protocol (UDP) puerto 500
- Encapsulating Security Payload (ESP) - IP protocol number 50
- IPsec NAT-T - UDP puerto 4500

Habitualmente se consiguen los mismos efectos habilitando en routers domésticos la opción "IPsec Passthrough".

Como puede observarse en el código anterior, habilito los puertos 500 y 4500 en el firewall. Además, añado la siguiente línea de código a /ip ipsec peer

```
nat-traversal=yes
```

Por lo que

```
/ip ipsec peer
add address=0.0.0.0/0 auth-method=pre-shared-key-xauth dh-group="ec2n185,ec2n155\
   ,modp8192,modp6144,modp4096,modp3072,modp2048,modp1536,modp1024,modp768" \
```

```
enc-algorithm=aes-256 generate-policy=port-override mode-config=cfg1 \
passive=yes secret=123456 nat-traversal=yes
```

Aunque debe tenerse en consideración que, si un usuario se conecta desde un hotel, iCafe, etc. El firewall y el NAT de estos no debe filtrar los paquetes con esos puertos.

Clientes VPN

La configuración anterior corresponde al servidor VPN en el router de una red local, LAN, en la cual se encuentra la central de telefonía IP. Si bien es posible conectar 2 o más redes LAN mediante IPsec, donde los router son los mediadores. Muchas veces un usuario necesitará ingresar a la VPN desde su celular, computadora, laptop en una locación externa a la oficina, a través de una conexión en la red pública.
Para esto es necesario que el sistema corra un cliente VPN.

El sistema operativo Android posee un cliente para una conexión IPsec en modo túnel con método de autenticación PSK+Auth y diferentes modos de encriptación, entre estas AES256. No así Windows.

Windows por defecto posee PPTP, L2TP/IPsec pero no una implementación IPsec puro en modo túnel.

Si bien existen una gran variedad de clientes comerciales para un túnel IPsec, no así gratuitos. Por ejemplo, la empresa Global Eagle Entertaiment utiliza como cliente VPN Pulse Secure, que es una empresa que brinda seguridad informática.

El cliente gratuito que implementaré para Windows es: SHREW cliente.

Página oficial: https://www.shrew.net/download

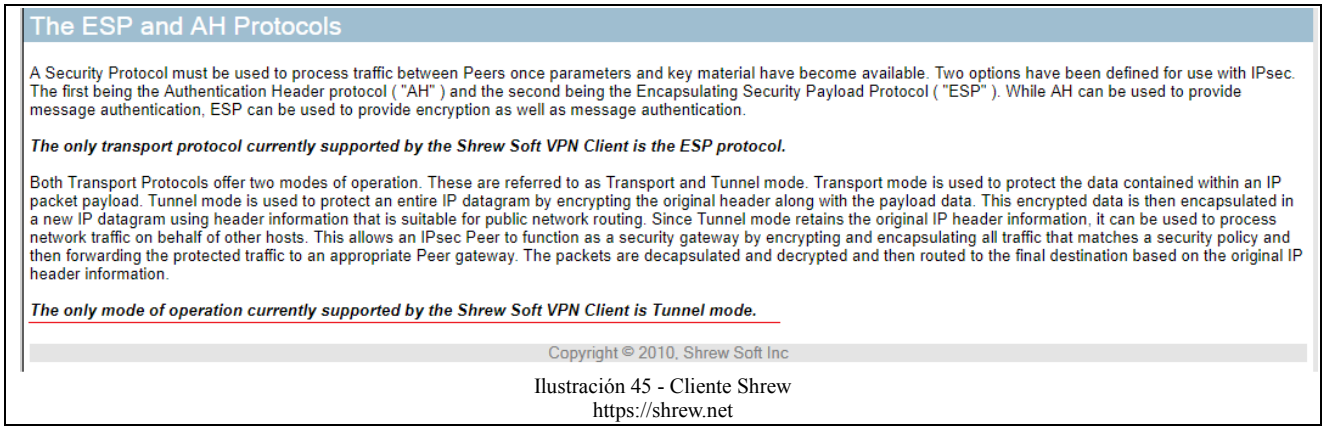
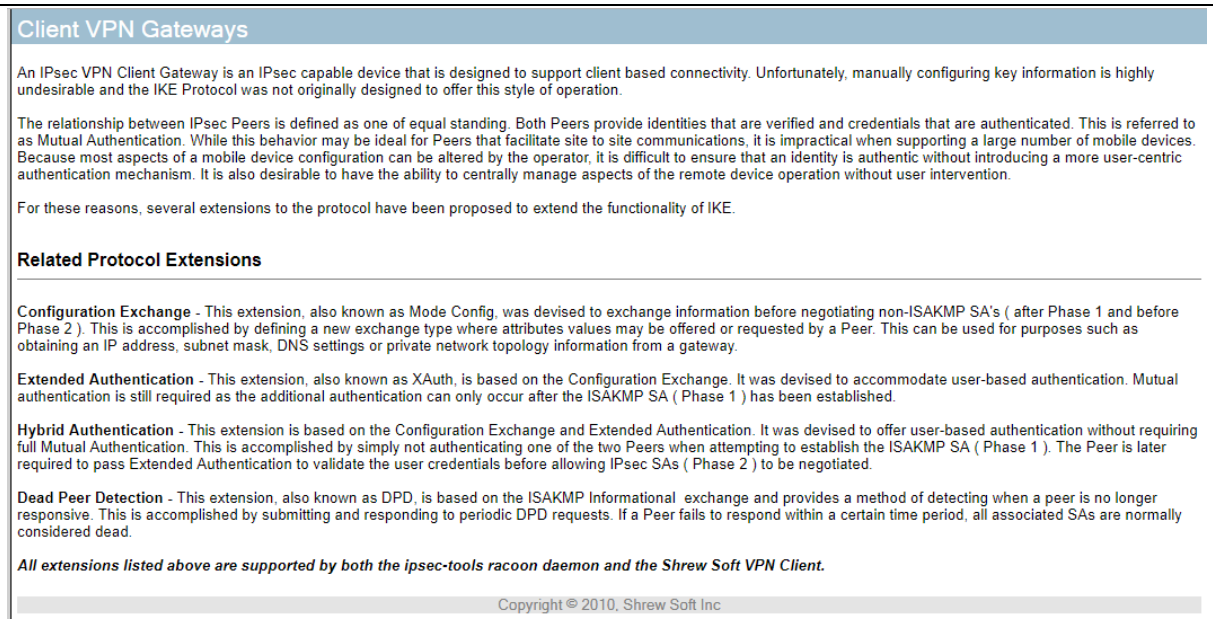


Ilustración 45 - Cliente Shrew
https://shrew.net



Client VPN Gateways

An IPsec VPN Client Gateway is an IPsec capable device that is designed to support client based connectivity. Unfortunately, manually configuring key information is highly undesirable and the IKE Protocol was not originally designed to offer this style of operation.

The relationship between IPsec Peers is defined as one of equal standing. Both Peers provide identities that are verified and credentials that are authenticated. This is referred to as Mutual Authentication. While this behavior may be ideal for Peers that facilitate site to site communications, it is impractical when supporting a large number of mobile devices. Because most aspects of a mobile device configuration can be altered by the operator, it is difficult to ensure that an identity is authentic without introducing a more user-centric authentication mechanism. It is also desirable to have the ability to centrally manage aspects of the remote device operation without user intervention.

For these reasons, several extensions to the protocol have been proposed to extend the functionality of IKE.

Related Protocol Extensions

Configuration Exchange - This extension, also known as Mode Config, was devised to exchange information before negotiating non-ISAKMP SA's (after Phase 1 and before Phase 2). This is accomplished by defining a new exchange type where attributes values may be offered or requested by a Peer. This can be used for purposes such as obtaining an IP address, subnet mask, DNS settings or private network topology information from a gateway.

Extended Authentication - This extension, also known as XAuth, is based on the Configuration Exchange. It was devised to accommodate user-based authentication. Mutual authentication is still required as the additional authentication can only occur after the ISAKMP SA (Phase 1) has been established.

Hybrid Authentication - This extension is based on the Configuration Exchange and Extended Authentication. It was devised to offer user-based authentication without requiring full Mutual Authentication. This is accomplished by simply not authenticating one of the two Peers when attempting to establish the ISAKMP SA (Phase 1). The Peer is later required to pass Extended Authentication to validate the user credentials before allowing IPsec SAs (Phase 2) to be negotiated.

Dead Peer Detection - This extension, also known as DPD, is based on the ISAKMP Informational exchange and provides a method of detecting when a peer is no longer responsive. This is accomplished by submitting and responding to periodic DPD requests. If a Peer fails to respond within a certain time period, all associated SAs are normally considered dead.

All extensions listed above are supported by both the ipsec-tools racoon daemon and the Shrew Soft VPN Client.

Ilustración 46 - Cliente Shrew
https://shrew.net

Calidad de Servicio - QoS

En una red LAN existen diferentes tipos de servicios y tráfico. De allí el término intranet definiéndose como una red que brinda servicios especiales y definidos.

En el caso del proyecto estamos implementado una red con servicio de telefonía. Siendo los paquetes de comunicación en tiempo real (RTP) los prioritarios. Utilizados para una comunicación de voz y video, videollamadas o videoconferencias. Así como también los paquetes de señalización SIP entre softphones y la central de telefonía.

Son prioritarios los paquetes que transportan la información de telefonía porque deben cumplir con la calidad de servicio que permite una comunicación fluida y que pueda ser entendida entre los usuarios.

Una red síncrona con sus jerarquías de sincronización como lo es PDH y su avance en SDH tienen como base el transporte de información un paquete de 8 bits de resolución, tomando 8000 muestras por segundo dando un ancho de banda total de 4KHz. Esto sigue el teorema de Shannon-Nyquist que considerando el ruido del canal y un previo filtrado permite un ancho de banda de voz de 300 Hz a 3.4 KHz, y de esta manera la tasa total de información base es de 64Kbps. En lo que se conoce como códec A-law y U-law, definidos en la documentación – estándar ITU-T G.711.

En una red de paquetes basadas en el protocolo IP, estandarizadas principalmente bajo el conjunto de protocolos ethernet, el cual tiene definiciones en capa física y capa de enlace, se comparte el ancho de banda entre diferentes servicios y usuarios, donde el acceso y la ocupación de la red dependerá del uso en el momento específico.
Para poder priorizar tráfico la operación debe realizarse en el equipo de capa de red, el cual tiene como objetivo el enrutamiento de los paquetes entre las redes.

Calidad de servicio en RouterOS

La siguiente imagen, obtenida de la documentación de Mikrotik, corresponde al flujo del paquete en el router.

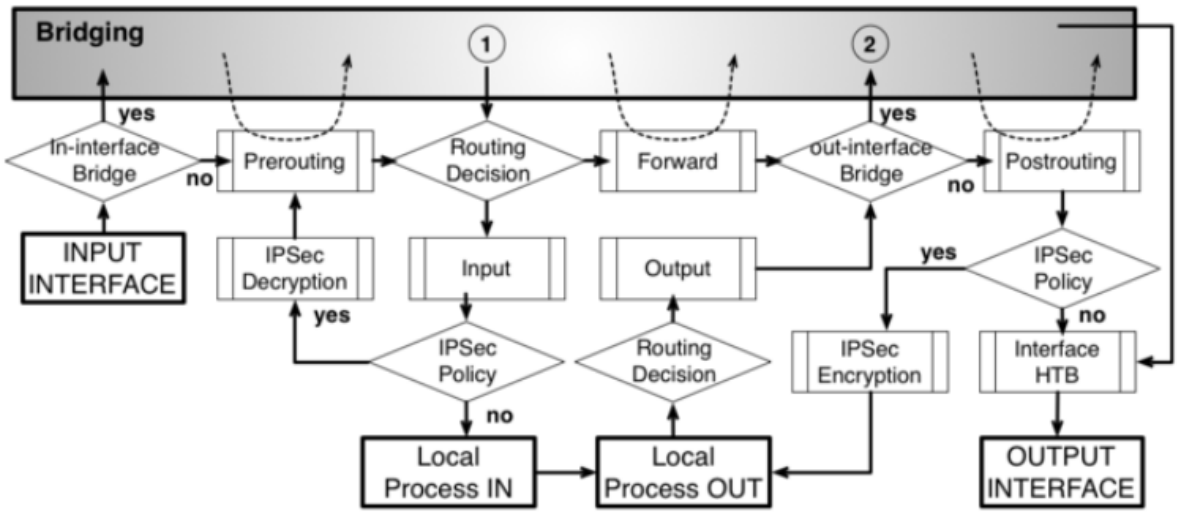


Ilustración 47 - Flujo de paquetes RouterOS
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Bridging corresponde a la capa 2 del modelo OSI, MAC layer o capa de enlace. Haciendo referencia al switch integrado en Mikrotik RB2011.

Podemos observar cuando un paquete es enviado desde una interfaz de entrada (INPUT INTERFACE), como puede ser una interfaz ethernet o una interfaz virtual (como una interfaz 6to4), y se realiza una decisión lógica si el paquete debe ser manejado por la capa de enlace o la capa de red. La interfaz de salida (OUTPUT INTERFACE) puede ser tanto una interfaz ethernet o una interfaz virtual.

El siguiente ejemplo corresponde al flujo de un paquete entre interfaces ethernet.

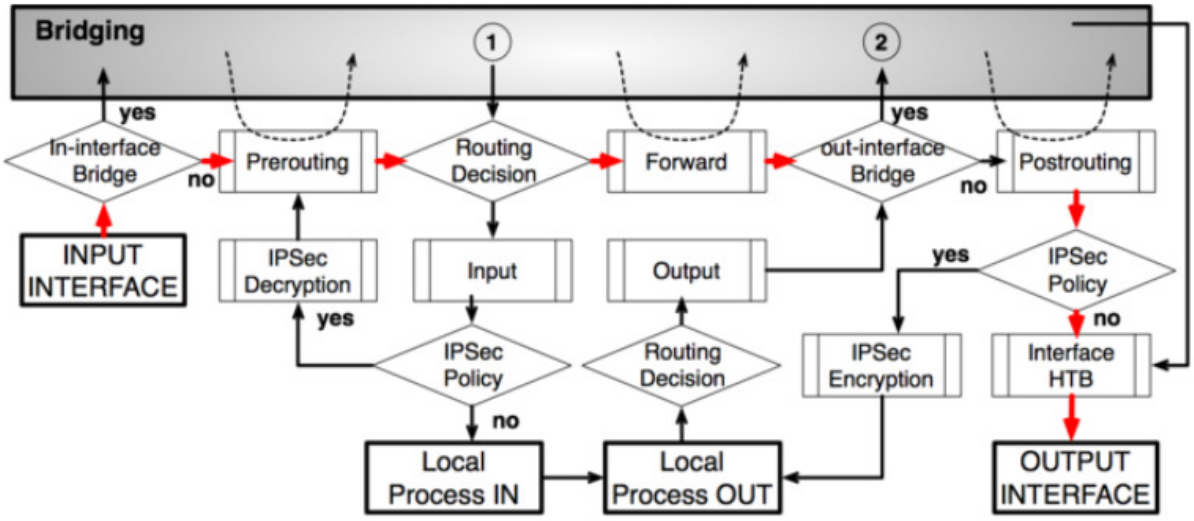


Ilustración 48 - Flujo de paquetes entre puertos RouterOS
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Las siguientes imágenes muestran el proceso de paquetes con encriptación y desencriptación IPsec.

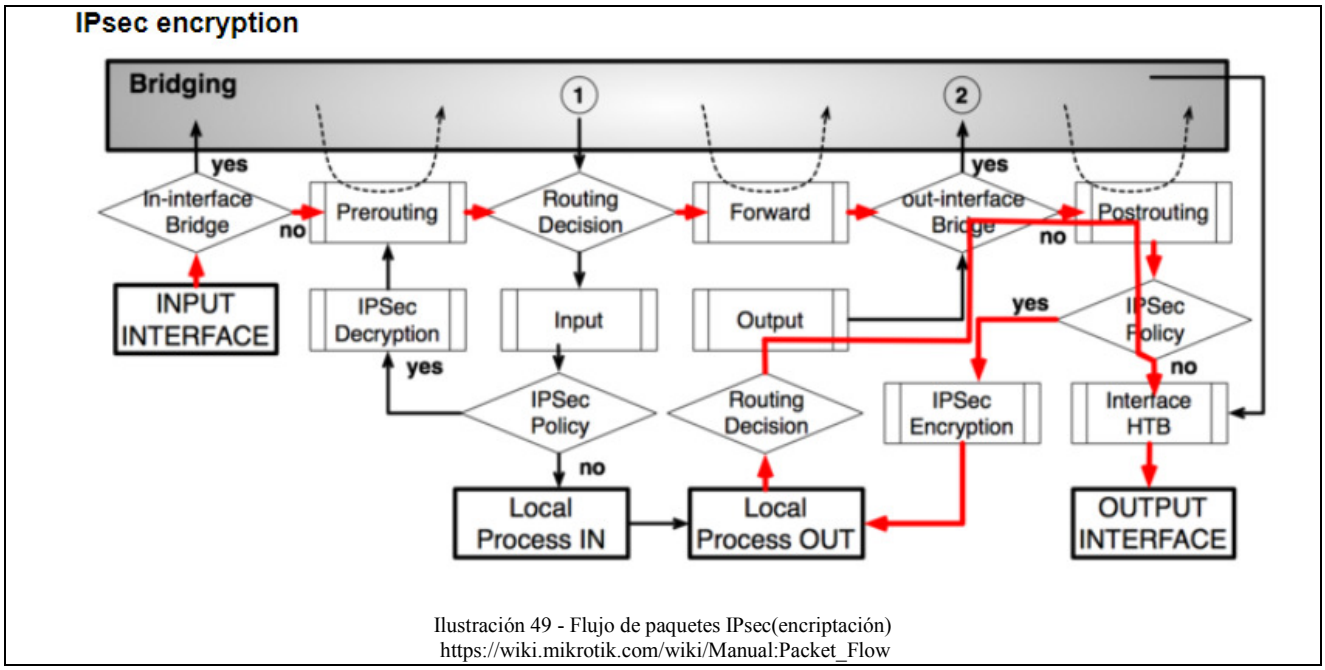


Ilustración 49 - Flujo de paquetes IPsec(encriptación)
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

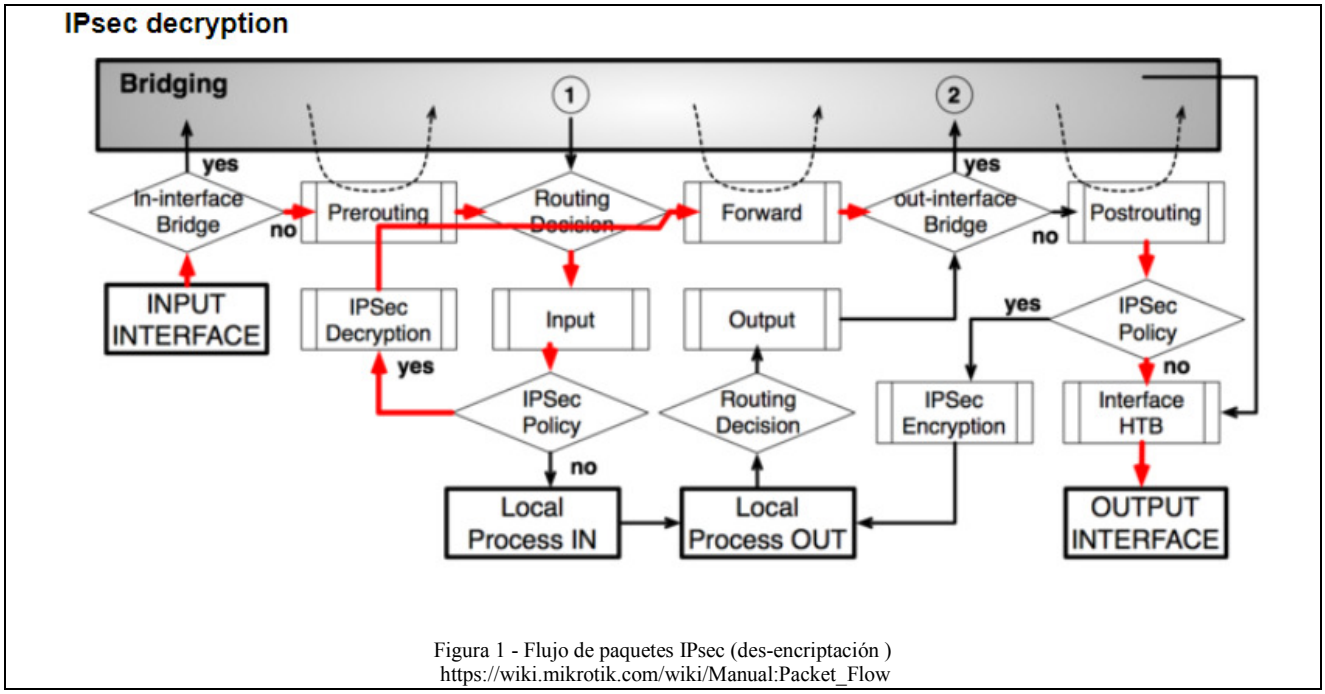


Figura 1 - Flujo de paquetes IPsec (des-encriptación)
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Las funciones de cada instancia: input, output, prerouting, forward y postrouting están especificadas en la siguiente imagen:

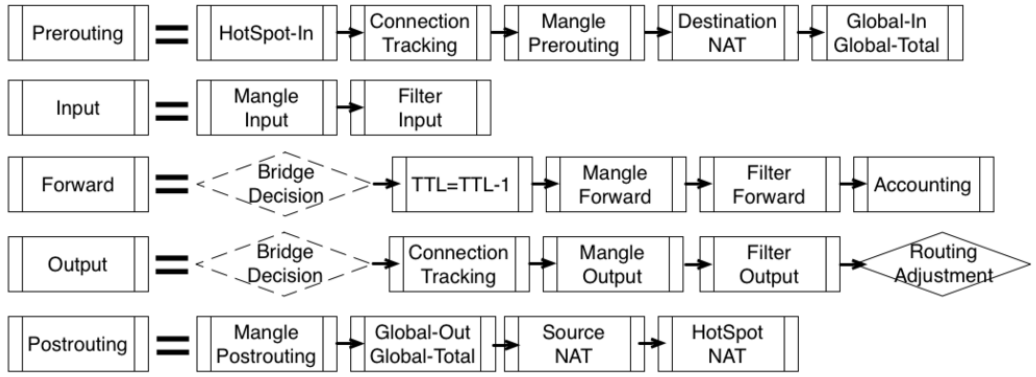


Ilustración 50 - Referencia en flujo de paquetes RouterOS
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

A partir de la versión 6 de RouterOS, se implementa el manejo de colas de paquetes:

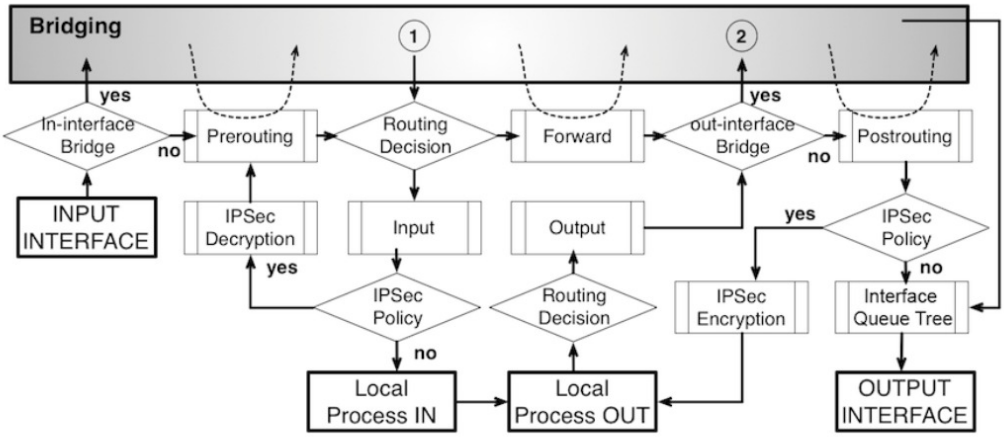


Ilustración 51 - Flujos de paquetes RouterOS v6
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

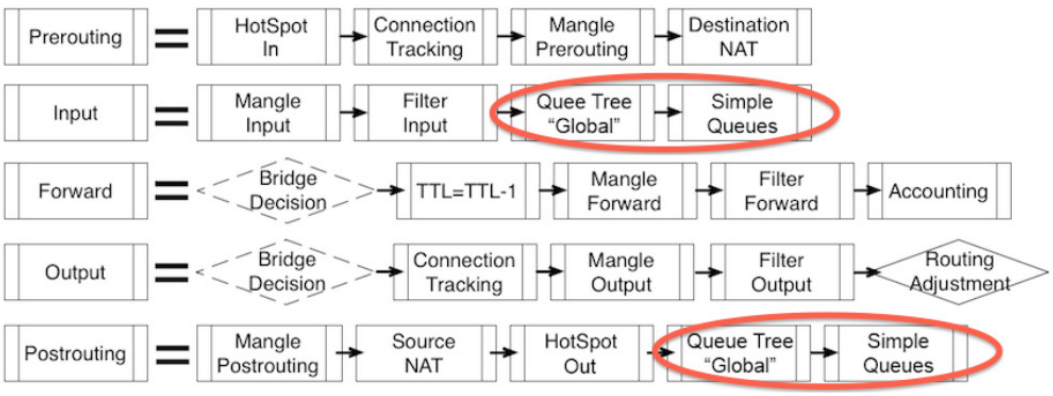


Ilustración 52 - Flujos de paquetes y arboles de colas RouterOS v.6
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Cada una de estas secciones tiene un menú particular en RouterOS, muchas de las cuales ya se han configurado anteriormente en este trabajo.

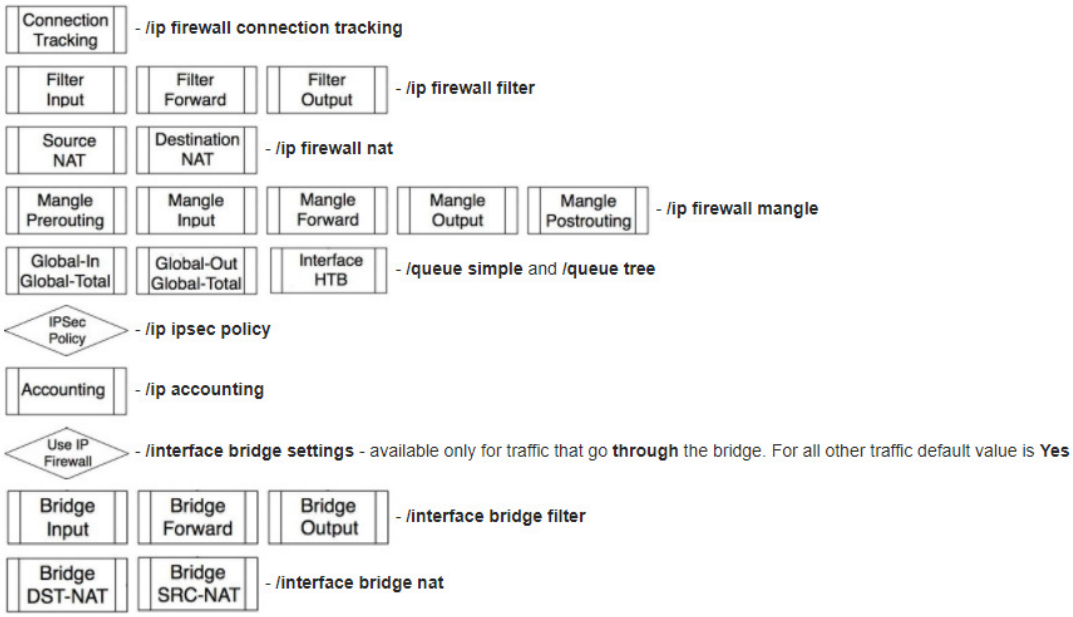


Ilustración 53 - Referencias - RouterOS
https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

El proceso para implementar QoS en este trabajo está dado por la implementación de árboles de colas. Pero para esto primeramente debemos implementar un marcado de paquetes mediante mangle.

Mangle

Mangle es un 'marcador' que marca paquetes para el procesamiento futuro con marcas especiales. Muchas opciones en RouterOS hacen uso de estas marcas, p. árboles de cola, NAT, enrutamiento. Identifican un paquete basado en su marca y lo procesan en consecuencia. Las marcas de mangle solo existen dentro del router, no se transmiten a través de la red.

Para este proyecto marcaremos los paquetes de señalización SIP y paquetes RTP, identificándolos mediante el puerto de destino. También se marcará los paquetes de la VPN, identificándolos mediante el protocolo ESP.

```
/ip firewall mangle
add action=mark-packet chain=prerouting dst-port=5060-5070 new-packet-mark=VoIP
passthrough=yes protocol=udp
add action=mark-packet chain=prerouting dst-port=10000-20000 new-packet-mark=VoIP
passthrough=yes protocol=udp
add action=mark-packet chain=prerouting new-packet-mark=VPN passthrough=yes protocol=ipsec-
esp
add action=mark-packet chain=prerouting comment="todo lo demas" new-packet-mark=paquetes-
TCP passthrough=yes protocol=tcp
```

Arboles de colas

En esta sección configuramos las prioridades de los paquetes marcados y el ancho de banda máximo (MIR) y mínimo (CIR). Como podemos ver en la siguiente imagen.

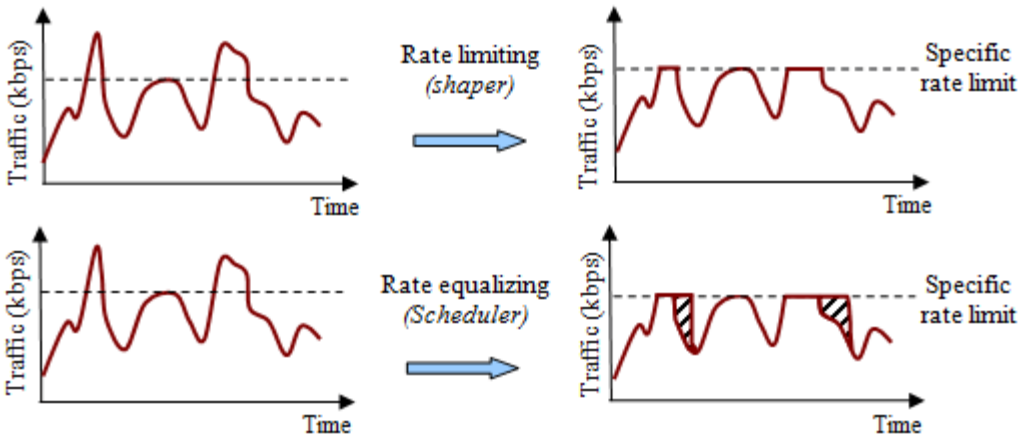


Ilustración 54 - CIR y MIR RouterOS
https://wiki.mikrotik.com/wiki/Manual:Queue

El código es el siguiente.

```
/queue tree
add limit-at=1048576 max-limit=10485760 name=VPN packet-mark=VPN parent=global priority=3
add limit-at=1024 max-limit=8388608 name=TCP packet-mark=paquetes-TCP parent=global
priority=8
add limit-at=2097152 max-limit=10485760 name=VoIP packet-mark=VoIP parent=global priority=1
queue=default
```

Prioridad 1 para los paquetes de telefonía (SIP y RTP), prioridad 3 para los paquetes IPsec y prioridad 8 para los demás paquetes TCP, el cual incluye el protocolo de aplicación HTTP y HTTPS.
El ancho de banda está en bytes por segundo.

Se estable un ancho de banda mínimo de 2Mbps y máximo de 10Mbps para los paquetes de telefonía. Se estable un ancho de banda mínimo de 1Mbps y máximo de 10Mbps para los paquetes IPsec. Se estable un ancho de banda mínimo de 1Kbps y máximo de 8Mbps para los paquetes de TCP, en general.

Conexión a red PSTN

Para realizar una migración paulatina de los servicios de telefonía a VoIP se debe considerar la utilización actual de las redes de telefonía tradicional PSTN.

Si una empresa o institución decide implementar una central de telefonía IP para la comunicación del personal debe tener en consideración las llamadas externas, entrantes y salientes de las redes IP.

Esto será necesario si la comunicación debe ser abierta a personas como clientes, proveedores, asociados, etc. que no posean esta nueva tecnología de comunicación.

La conexión a la red PSTN se realiza a partir de un par de cables (dos hilos) que forman una línea telefónica básica. La señal se transmite en forma analógica desde el terminal de abonado hasta la central de telefonía donde se digitaliza, según el estándar G.711, y mediante un proceso de conmutación el mensaje se integra en un times slot en una trama primaria T1 o E1 sobre el soporte físico que enlaza las diferentes centrales conmutadas.

La señalización, que indica el número al cual se desea llamar, es una señal en banda entre el terminal de abonado y la central de telefonía. Esta señalización es por tonos, denominados DTMF. La señalización entre centrales de telefonías es fuera de banda, por un canal dedicado.

Antes de que se establezca el canal para la comunicación de información entre los terminales finales, las centrales de telefonía conmutadas deben establecer un camino. La conmutación de circuitos es un tipo de conexión que realizan los diferentes nodos de la red para lograr una ruta apropiada y de esta manera conectar los usuarios. A diferencia de lo que ocurre en la conmutación de paquetes, en esta se establece un canal de comunicaciones dedicado entre dos estaciones, se reservan recursos de transmisión (times slots) para su uso exclusivo en el circuito durante la conexión.

La comunicación por conmutación de circuitos implica tres fases: el establecimiento del circuito, la transferencia de datos y la desconexión del circuito. Una vez que el camino entre el origen y el destino queda fijado, queda reservado un ancho de banda fijo hasta que la comunicación se termine. Para comunicarse con otro destino, el origen debe primero finalizar la conexión establecida. Los nodos deben tener capacidad de conmutación y de canal suficiente como para gestionar las conexiones solicitadas; los conmutadores deben contar con el soporte necesario para realizar estas reservas y establecer una ruta a través de la red.

Interfaces FXO/FXS

FXS y FXO son los nombres de los puertos usados por las líneas telefónicas analógicas. Para conocer su función es necesario entender el funcionamiento de la línea de telefonía en la última milla.

La central de telefonía conmutada genera una tensión continua (generalmente 48[V] con respecto a tierra, aunque varía en función de la empresa). Cuando el teléfono es descolgado, existe una variación en la impedancia del “teléfono” y la tensión cae por debajo de una tensión umbral (generalmente 8[V]) en el mismo, la central de telefonía registra este cambio y envía un tono con una frecuencia de 1KHz. El teléfono al registrar este tono puede enviar la marcación, DTMF (marcación por tonos). Todas estas señales se superponen a la tensión de 8[V].

En el sentido inverso, cuando suena un teléfono debido a que se está realizando una llamada a este, a la tensión de continua se le suma una tensión alterna que genera el ring.

Podemos especificar los niveles de impedancia del teléfono en su estados colgados y descolgados:
Umbral de teléfono descolgado (captura de línea): Rdc < 1000 ohmios
Umbral de teléfono colgado (liberación de línea): Rdc >10 000 ohmios

Ambos puertos siempre funcionan de a pares, como se puede ver en la siguiente imagen.

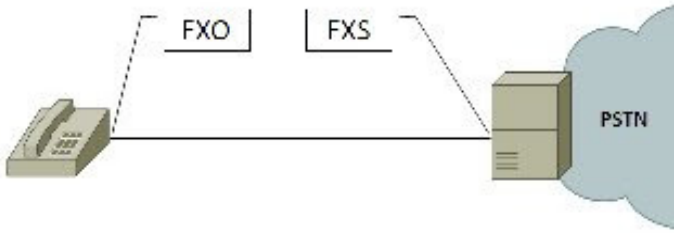


Ilustración 55 - Puertos línea telefónica analógica
https://www.3cx.es/voip-sip/fxs-fxo

Una interfaz FXS proporciona alimentación eléctrica para la tensión continua en la línea y mediante la variación de corriente o variación de caída de tensión en su impedancia interna registra el descolgado y colgado. A su vez, genera la señal de tensión alterna para la señal de habilitación de marcado y la señal de generación del ring.

La interfaz FXO produce una variación en la impedancia para generar el cuelgue y descuelgue, así como también registra la señal de habilitación de marcado y produce la marcación mediante tonos, DTMF.

Por lo tanto, para utilizar un teléfono analógico e integrarlo con una central de telefonía IP asignándole un número interno, es necesario un voice gateway con puerto FXS.

Para conectar o enlazar la central de telefonía IP con la red PSTN, es necesario un voice gateway con puerto FXO.

Voice Gateway Grandstream HT503

El voice gateway que se utilizará en este proyecto es el HT503 dela empresa Grandstream por sus prestaciones y su coste económico. Podemos ver sus características en la página oficial de Grandstream.

Características:

- 1 puerto FXS para teléfonos analógicos (RJ11), 1 puerto FXO de línea PSTN, dos puertos de 10/100 Mbps con router NAT integrado
- Las funciones de telefonía avanzada incluyen identificador de llamadas y llamada en espera
- Conferencia de voz de 3 vías, transferencia, desvío, no molestar, indicador de mensajes, avisos de voz en múltiples idiomas, fax T.38, plan de marcación flexible y más
- Soporta hasta 2 cuentas SIP
- LED de estatus para energía eléctrica, puertos para teléfono y red e indicación de mensaje en espera

Ilustración 56 - Características Grandstream HT503
http://www.grandstream.com

Ilustración 57 - Grandstream HT503
http://www.grandstream.com

El HT503 es un adaptador de teléfono analógico que incluye 1 puerto FXS para teléfono analógico y 1 puerto FXO para línea PSTN. La integración de un puerto FXO y FXS permite la iniciación y terminación de llamadas remotas a y desde la línea PSTN, lo que se conoce como "llamada hop-on y hop off". El puerto FXS permite la extensión de un servicio VoIP a un teléfono analógico.

Configuración

Se configura en la central de telefonía Asterisk un número interno para el puerto FXS y para el puerto FXO.

Sip.conf

```
[telefonoanalogico]
type=friend
host=100.64.0.7
secret=123456   ;contraseña para el registro del usuario al asterisk
context=users
qualify=yes
nat=force_rport
dtmfmode=rfc2833
voicemail=1700@default

[Externo-PSTN]
callerid=800
canreinvite=no
dtmfmode=rfc2833
port=5062
type=friend
context=users
```

allow=ulaw

allow=gsm

host=Dynamic

extensions.conf

exten => 1700,1,GotoIf($[${DEVICE_STATE(SIP/telefonoanalogico)}=UNAVAILABLE]?skip_dial)

same => n,Dial(SIP/telefonoanalogico,30)

same => n,GotoIf($["${DIALSTATUS}"="BUSY" | "${DIALSTATUS}"="DONTCALL"]?dialed_busy)

same => n,NoOp(Do More Stuff here, like dial another extension, whatever) ;no answer

same => n,Hangup

same => n(skip_dial),Playback(extension&is-curntly-unavail&please-try-again-later&goodbye)

same => n,Hangup

same => n(dialed_busy),Playback(extension&is-curntly-busy)

same => n,Hangup(17) ; generate busy signal

exten => 800,1,Answer()

exten => 800,n,Dial(SIP/Externo-PSTN)

exten => 800,n,Hangup()

Puede observarse que la extensión para el teléfono analógico es 1700.

Para realizar una llamada a través de la red PSTN es necesario marcar la extensión 800, paso seguido marcar una contraseña (puede configurarse o no) y por último en número al cual se desea llamar.

La configuración en el Voice gateway es la siguiente. Primeramente, se debe indicar la dirección IP del servidor SIP.

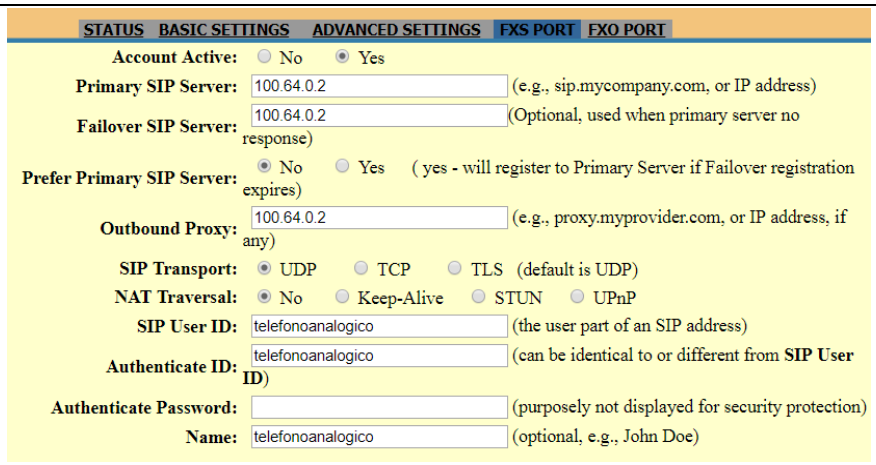


Ilustración 58 - HT503 configuración por Browser

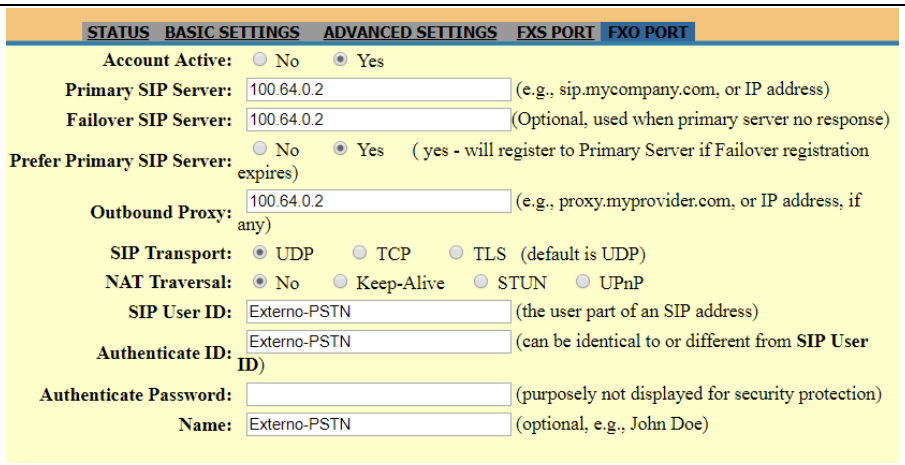


Ilustración 59 - HT503 configuración por Browser

Se asigna un puerto para la señalización SIP, tanto para el puerto FXS que será el puerto 5060 y para el puerto FXO, que será el puerto 5062. Ambos puertos deben ser diferentes debido a que es necesario esto para realizar llamadas simultaneas en ambos puertos.

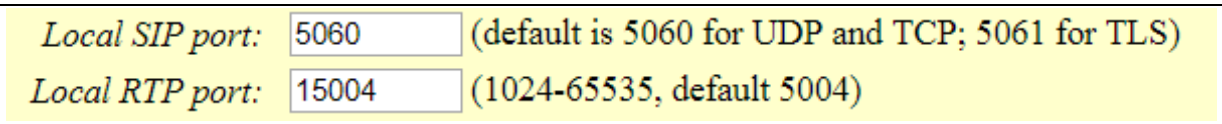


Ilustración 60 - HT503 configuración por Browser

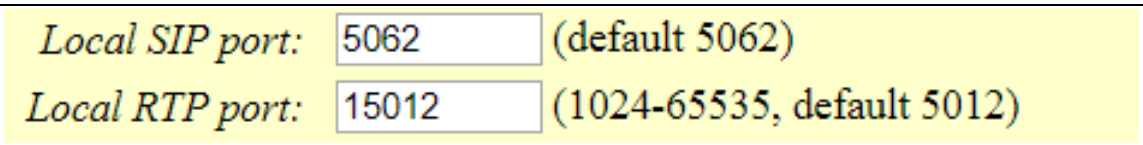


Ilustración 61 - HT503 configuración por Browser

Se configura el método DTMF de señalización por tonos, en ambos.

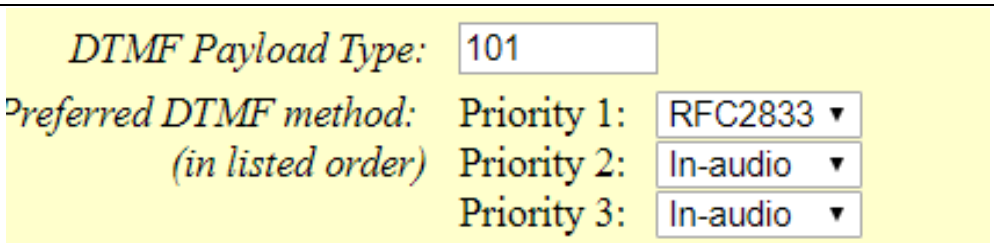


Ilustración 62 - HT503 configuración por Browser

Y el tipo de codificación de voz.

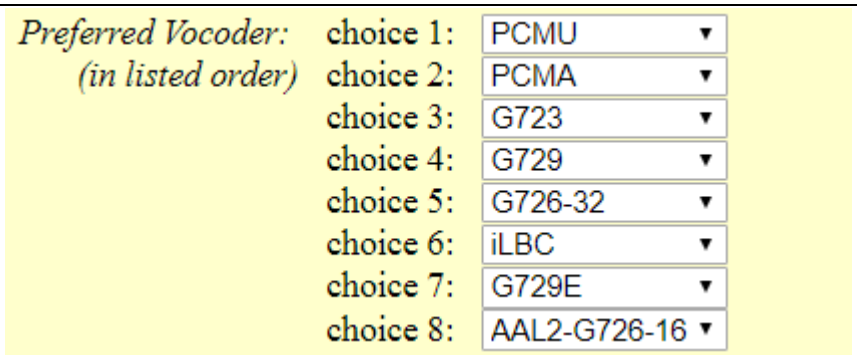


Ilustración 63 - HT503 configuración por Browser

En el puerto FXS se configuran los parámetros de la señal, en este caso se dejan los parámetros por defecto. SLIC es el circuito de interfaz de línea de suscriptor (SLIC, Subscriber Line Interface Circuit), el cual especifica todos los niveles de tensión e impedancia de la línea de abonado. En este caso seleccionamos el estándar europeo, de Italia, ya que las líneas telefónicas en Argentina utilizan e implementan el hardware proveniente de dicha región.

El caller ID scheme hace referencia al número telefónico de identificación del interlocutor llamante que se transmite en una llamada telefónica. En este caso, las identificaciones de llamadas se realizan mediante tonos con modulación FSK durante el timbrado inicial.

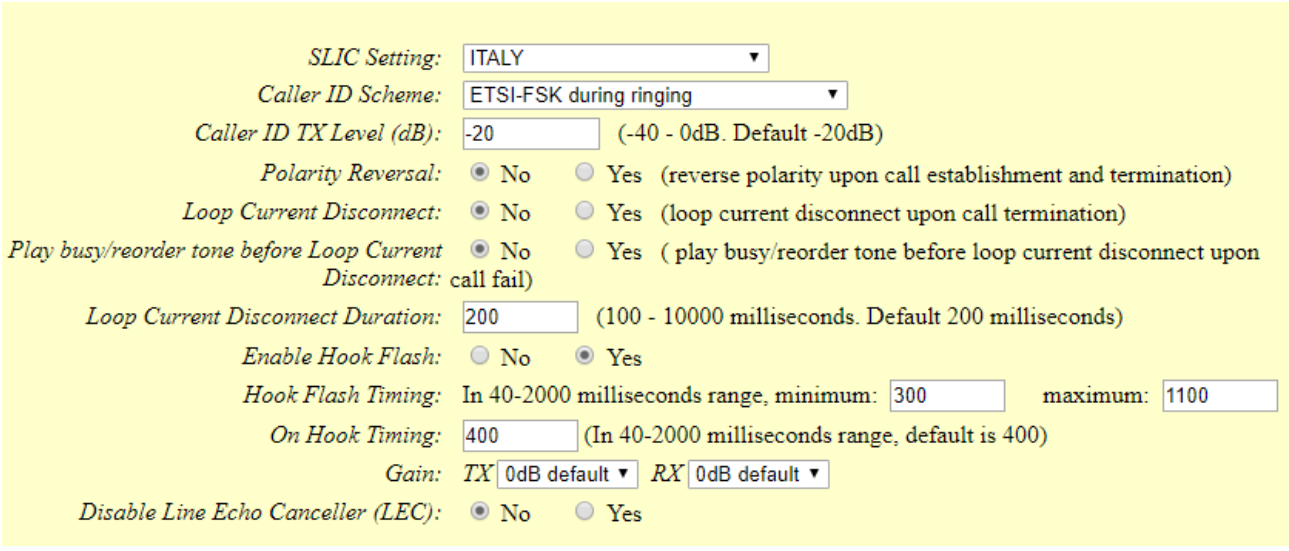


Ilustración 64 - HT503 configuración por Browser

Y se configuran los tonos de ring para el teléfono analógico, en el puerto FXS

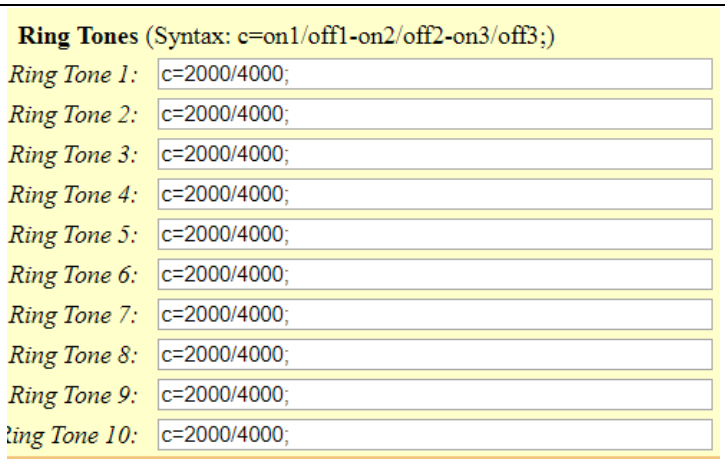


Ilustración 65 - HT503 configuración por Browser

En cambio, para el puerto FXO, debe configurarse de manera tal que se integre con los valores de la línea PSTN. Como se detallan a continuación, si la configuración no es la correspondiente es posible un daño en el dispositivo.

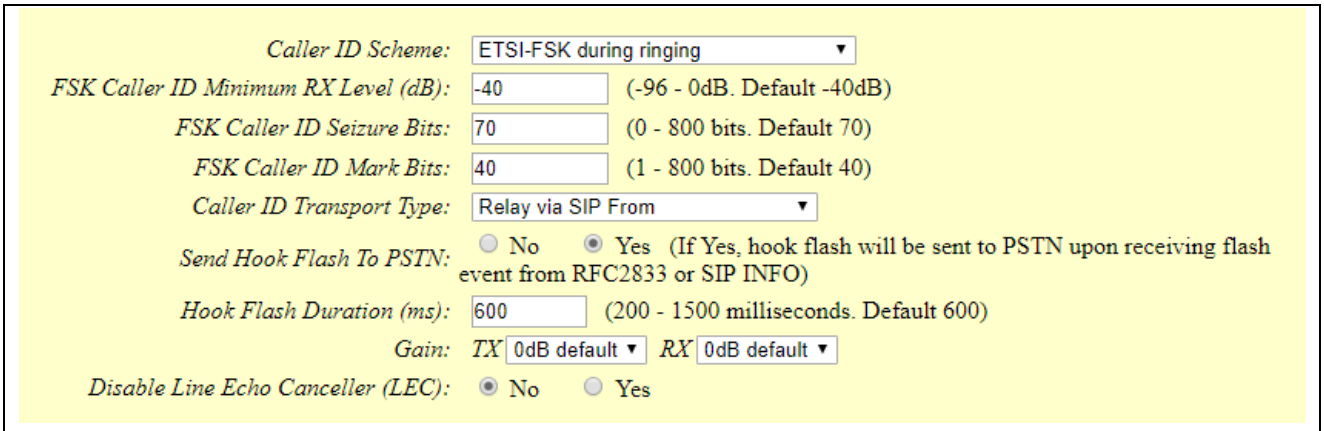


Ilustración 66 - HT503 configuración por Browser

Se debe definir el valor de impedancia de la línea que corresponde al teléfono descolgado, que en Argentina corresponde a 900Ohms.

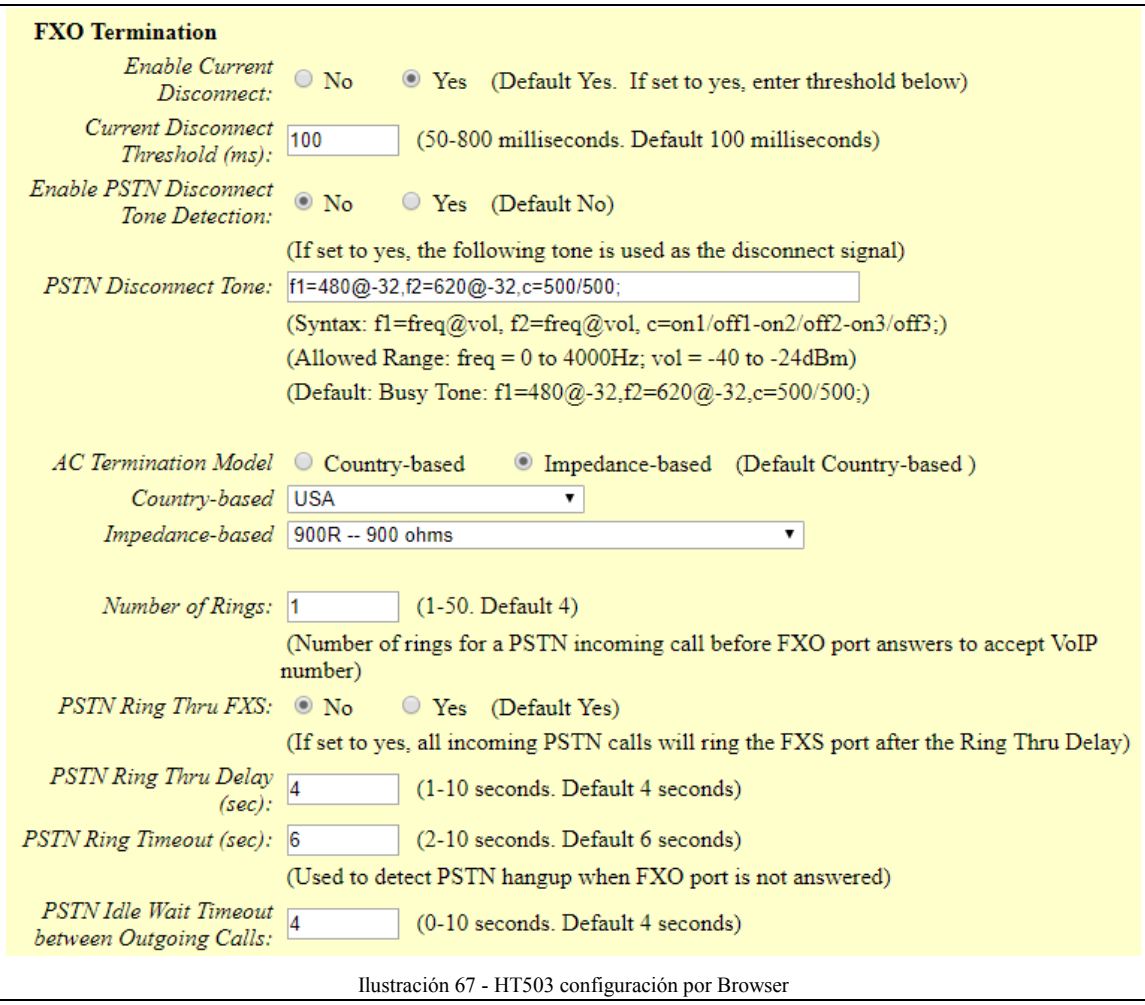


Ilustración 67 - HT503 configuración por Browser

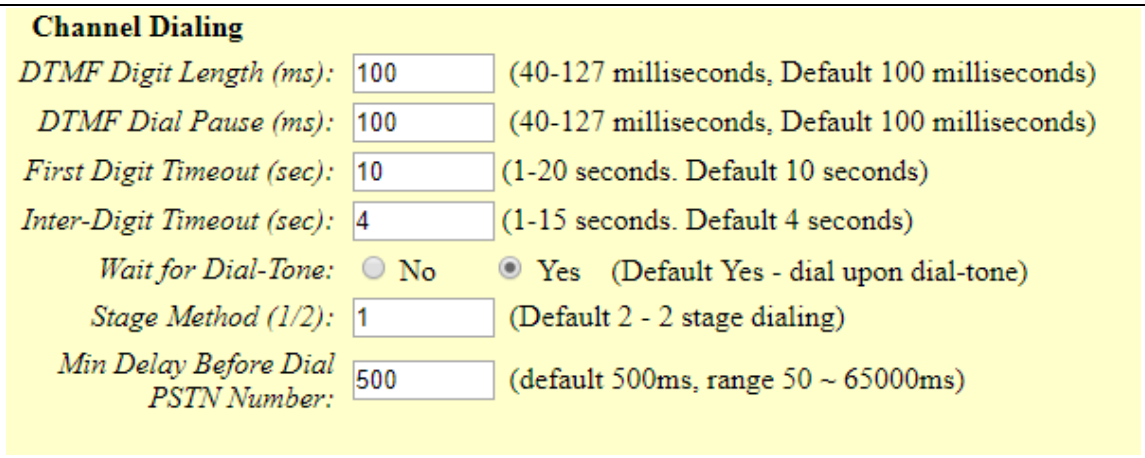


Ilustración 68 - HT503 configuración por Browser

Por último, en la pestaña advance seeting se debe especificar las frecuencias de las siguientes señales.

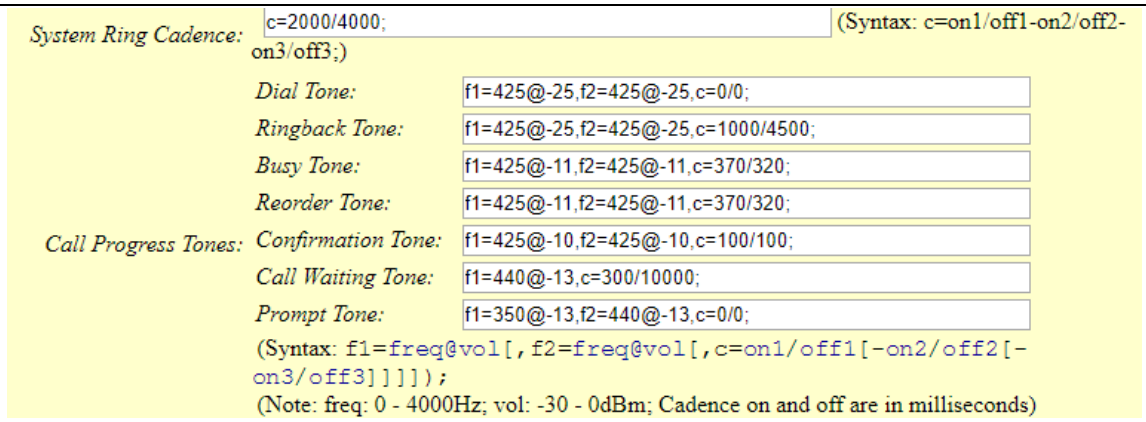


Ilustración 69 - HT503 configuración por Browser

Dichas frecuencias corresponden a los valores utilizados en las líneas de telefonía analógica en Argentina.

En basic seeting, configuramos un PIN, es decir, una contraseña para realizar llamadas hacia la línea PSTN y además definimos el interno que será llamado al momento de que se realice una llamada desde la red PSTN hacia la central de telefonía IP. En este caso el interno será el IVR (extensión 100), que especifica el menú con todos los internos en la central de telefonía.

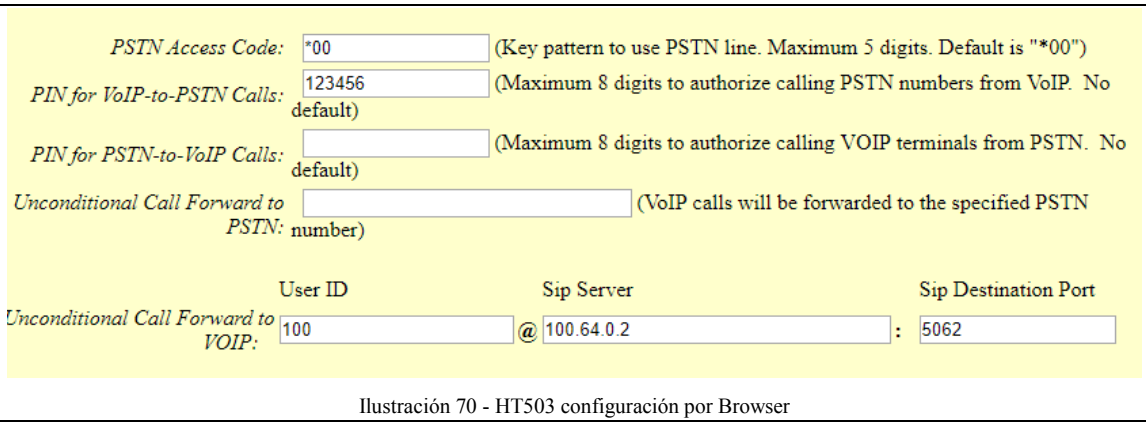


Ilustración 70 - HT503 configuración por Browser

SIP trunking - Proveedor de telefonía.

SIP trunking es una conexión troncal entre centrales de telefonía. Sin lugar a dudas, la telefonía sobre redes IP implica la comunicación tanto de señalización como paquetes de datos entre diferentes centrales.

Las centrales de telefonía deben tener canales de comunicación de manera tal de brindar un servicio extendido a nivel mundial. Efectivamente, cuando queremos realizar una llamada mediante una red PSTN a Miami. Luego del marcado, la señalización se transmite entre las centrales conmutadas por un canal especial, estableciendo un enlace físico, lógico que reservará los recursos de ancho de banda entre los diferentes nodos de la red y que se utilizará durante el tiempo de llamada. Para esto, las centrales están interconectadas y se extiende el servicio de telefonía dando una mayor cobertura.

Para centrales IP es análogo al caso de la red PSTN, dejando de lado las diferencias de la capa de física, de enlace, capa de red y capa de transporte. En la capa aplicación se debe realizar un registro entre las centrales estableciendo el número de canales (cuentas) entre estas, métodos de tarifa,

autenticación de usuarios, etc. A su vez dichas centrales además del SIP server debe poseer SIP proxys y RTP proxys para el enrutamiento de gran volumen de tráfico.

En este proyecto se implementará un enlace troncal con un proveedor de telefonía IP, el cual brinda la posibilidad de realizar llamadas a cualquier número perteneciente a centrales de telefonía IP registradas en su SIP server y la compra de números internacionales con salida a red PSTN.

El proveedor elegido es Netelip. https://www.netelip.com/ar/

Ilustración 71 - Servicio de telefonía IP
https://www.netelip.com/ar/

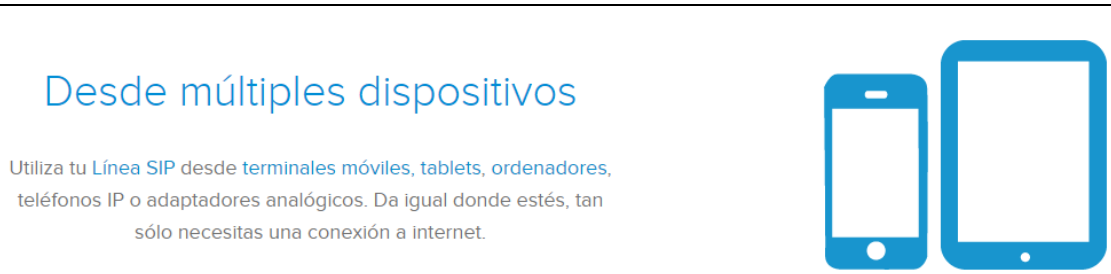


Ilustración 72 - Plataformas
https://www.netelip.com/ar/

Ilustración 73 - Troncal SIP
https://www.netelip.com/ar/

Ilustración 74 - Características de SIP trunking

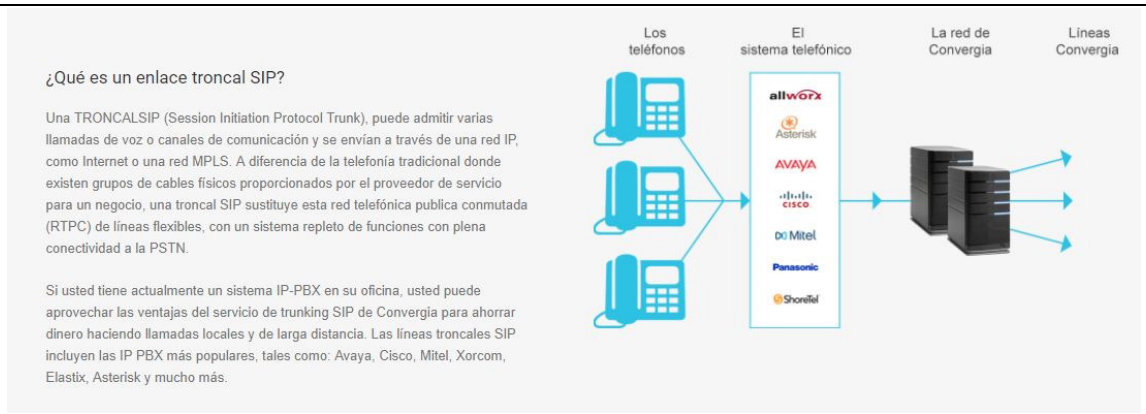


Ilustración 75 - Troncal SIP
https://www.netelip.com/ar/

Para poder implementar un enlace troncal SIP es necesario la compra de números, dicha acción puede realizarse desde el panel de control, luego de haberse registrado en Netelip.
Los números adquiridos son: 541152194194 y 541152195546. Números virtuales con conexión a red PSTN, pertenecientes a la provincia de Buenos Aires.

Luego se debe ingresar la dirección IP de nuestra central de telefonía IP y los puertos del canal, en el panel de control.

Teléfono	Expira	Destino	Dirección IP	Puerto	Acciones
541152194194	18/12/17	Servidor SIP	186.108.121.191	5060	Desactivar
541152195546	18/12/17	Línea SIP	*No definido*	*No definido*	Activar

Ilustración 76 - Números virtuales adquiridos
https://www.netelip.com/ar/

El identificador de usuario y la contraseña se envían a nuestro correo electrónico. Dicha información es necesaria para la configuración de nuestra central.

Configurando nuestra central Asterisk con SIP trunking

Debemos agregar en sip.conf

```
[trunk]
host=sip.netelip.com   ;proveedor
defaultuser=julianov  ;usuario a registrar dado por el proveedor
secret=xxxxxx ; contraseña dada por el proveedor
type=friend   ;tipo de cuenta friend necesaria para recibir y realizar llamadas.
disallow=all  ;a continuación se habilitarán los codecs
allow=alaw
allow=ulaw
allow=g722
allow=gsm
context=users   ;contexto de la cuenta
insecure=port,invite
qualify=15000
port=5060
nat=force_rport
fromuser=julianov
```

En extensions.conf

```
exten => _X.,1,Dial(SIP/trunk/${EXTEN}@trunk,60) ;llamadas salientes
exten => _X.,n,Dial(SIP/julian, 30)  ;las llamadas entrantes se dirigirán a la cuenta de julian
```

En llamadas salientes, el dialplan _X. especifica cualquier número de marcado que no sea un interno en nuestra central. De esta manera si realizamos la marcación de un número que no se corresponde a los registrados en la central Asterisk, la llamada se enviará al proveedor de telefonía.

Para llamadas se debe especificar el código del país + código de área + número.

Podemos ver las tarifas en Netelip.

Destino	Establ. llamadas (US$)	Precio/min. (US$)
Entre usuarios **netelip**	US$0.00	Gratis
Argentina	US$0.0000	US$0.0345
Argentina - (Corredor)	US$0.0000	US$0.0327
Argentina - Buenos Aires	US$0.0000	US$0.0150
Argentina - Cordoba	US$0.0000	US$0.0184
Argentina - Mendoza	US$0.0000	US$0.0184
Argentina - Moviles	US$0.0000	US$0.2324
Argentina - Resto de Corredor	US$0.0000	US$0.0345
Argentina - Rosario	US$0.0000	US$0.0150

Ilustración 77 - Tarifas nacionales
https://www.netelip.com/ar/

Y las tarifas internacionales, tomando 2 países como ejemplo.

Destino	Establ. de llamada (US$)	Precio/min. (US$)
Estados Unidos	US$0.0000	US$0.0150
Estados Unidos - P800	US$0.0000	US$0.0150

Destino	Establ. de llamada (US$)	Precio/min. (US$)
España	US$0.0000	US$0.0150
España - IP Nomada	US$0.0000	US$0.0150
España - especial 901	US$0.0600	US$0.0600
España - especial 902	US$0.1500	US$0.1500
España - gratuito	US$0.0000	US$0.0000
España - móvil	US$0.0000	US$0.0390
España - móvil M2M	US$0.0000	US$0.0390
España - número personal	US$0.1000	US$0.1000
España - premium	US$0.0000	US$1.2000
España - premium	US$0.5000	US$1.2000

Ilustración 78 - Tarifas internacionales
https://www.netelip.com/ar/

Por lo tanto, con esta implementación de SIP trunking con Netelip damos cobertura mundial a nuestra central de telefonía IP, adquiriendo números virtuales.

Capítulo 3: Resultados

En la siguiente imagen se puede apreciar el ancho de banda de la comunicación de voz bajo el codec A-law (implementado), mismo ancho de banda para el codec u-law.

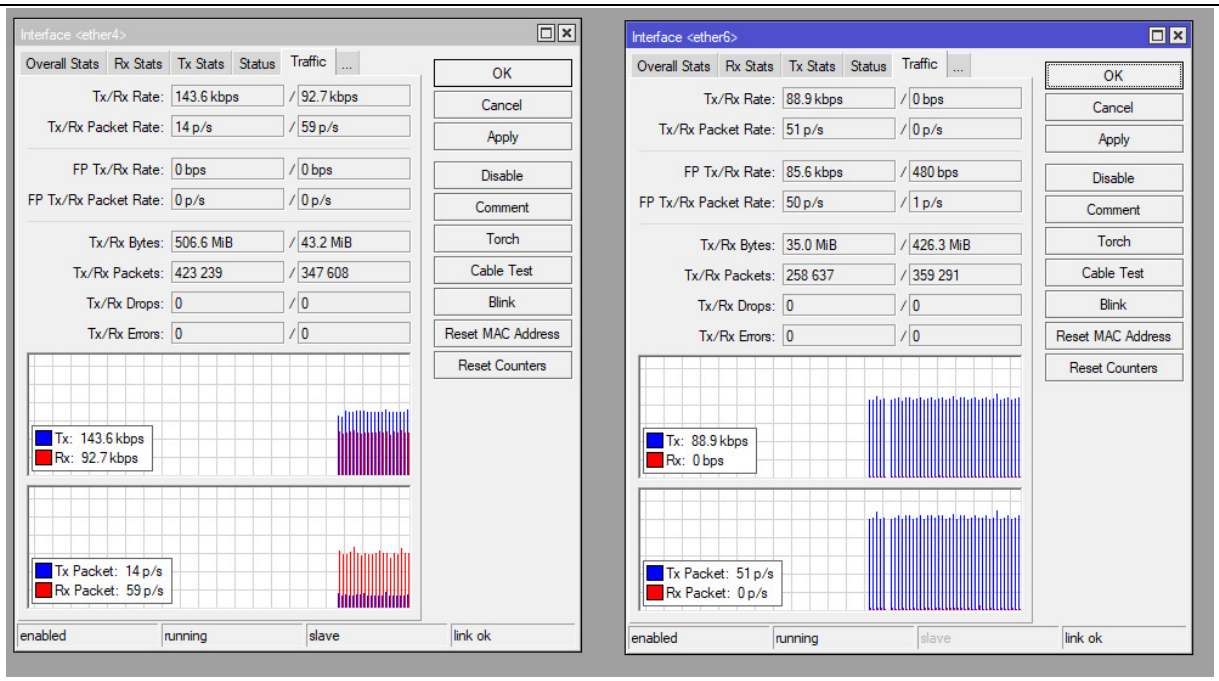


Ilustración 79 - Ancho de banda

Donde se visualiza un ancho de banda de 88 kbps.

Podemos apreciar en la siguiente imagen, el ancho de banda en una comunicación troncal SIP de un solo canal con el proveedor de telefonía Netelip, realizando una llamada desde un número interno a un número celular o teléfono analógico conectado a red PSTN. El mismo ancho de banda es el implicado cuando se realiza una llamada desde un teléfono conectado a la red PSTN o celular, al número virtual adquirido 541152194194.

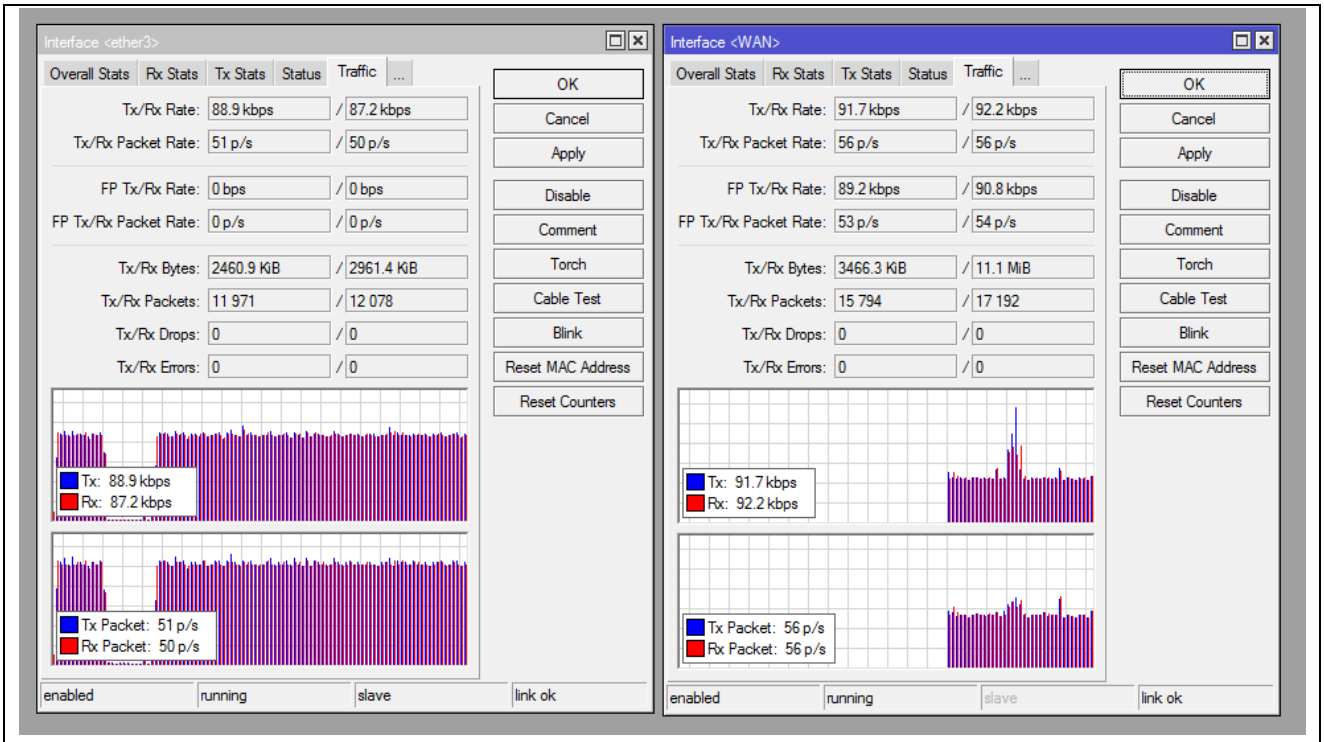


Ilustración 80 - Ancho de banda

Por lo tanto, si tenemos un ancho de banda de 2Mbps, la cantidad de llamadas que pueden realizarse es:

2048 Kbps / 88 Kbps = 23 llamadas.

Es necesario resaltar que el codec utilizado es A-law, definido en la documentación ITU-T G.711. El ancho de banda según la definición es 64Kbps y por lo tanto vemos que el ancho de banda efectivo, cuando lo implementamos, es 88 kbps. Por lo tanto existe una diferencia entre lo definido y lo implementado, como es de esperarse.

Existen codecs comerciales pagos como G729, cuyo ancho de banda es de 8kbps según su definición, siendo un ancho de banda efectivo aproximado de 32 kbps. Por lo que es una mejora importante para la implementación comercial de una central de telefonía.

2048 Kpbs /32 Kbps= 64 llamadas.

En la siguiente imagen se puede apreciar el ancho de banda de una videollamada.

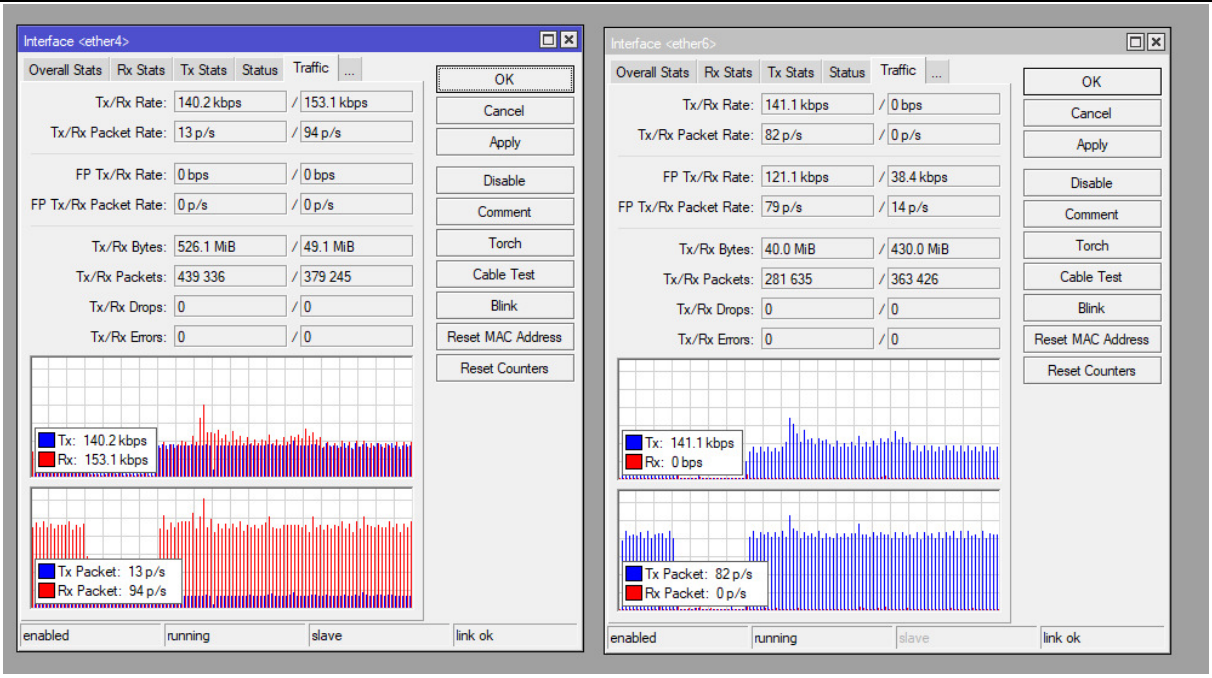


Ilustración 81 - Ancho de banda videollamada

Donde se observa una tasa de 144 Kbps. Que se corresponde a la suma de los 88 kbps + los 77 kbps de stream de video (codec H.263). Como se aprecia en la siguiente imagen.

Ilustración 82 - Streaming de video

A su vez podemos corroborar el envío del buzón de voz al correo electrónico de la persona asignada a la extensión; en la cual se ha dejado un mensaje en la casilla de mensaje. Este mensaje puede escucharse mediante el marcado de la extensión 222, que corresponde al buzón de voz y de la misma manera dicho mensaje es enviado al correo electrónico.

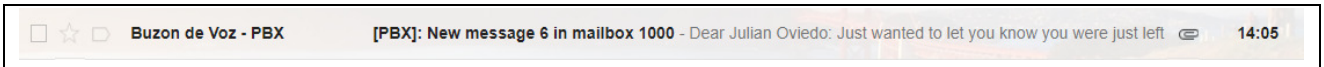


Ilustración 83 - Buzón de voz

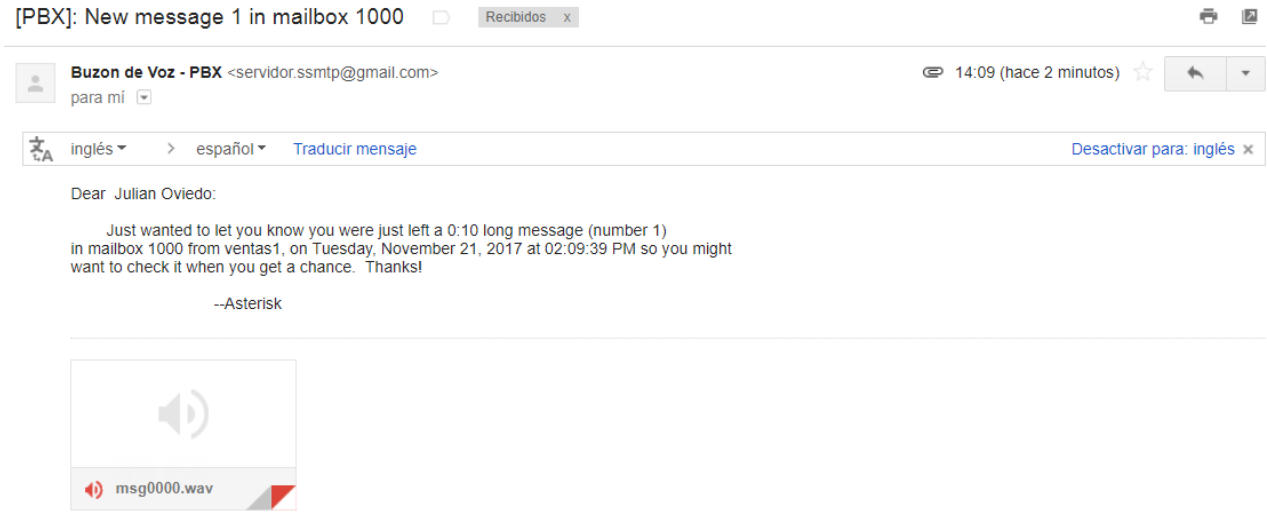
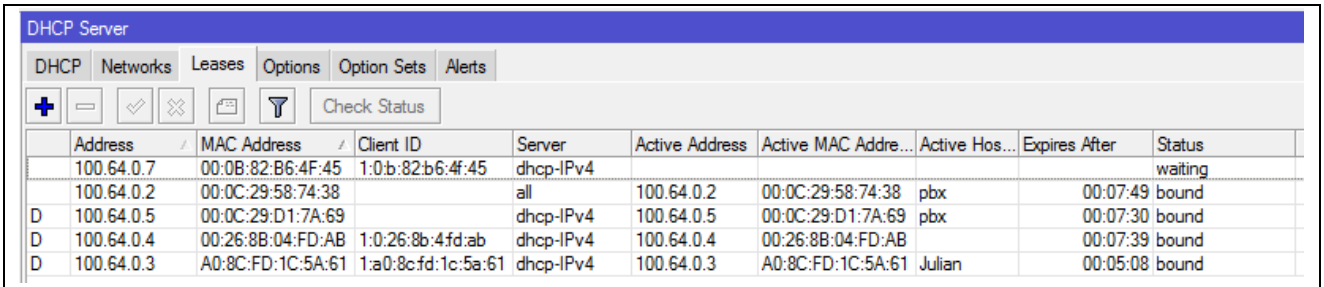


Ilustración 84 - Buzón de voz

Podemos corroborar el uso del servidor DHCP para la red LAN, considerando el protocolo de red IPv4.



	Address	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Hos...	Expires After	Status
	100.64.0.7	00:0B:82:B6:4F:45	1:0:b:82:b6:4f:45	dhcp-IPv4					waiting
	100.64.0.2	00:0C:29:58:74:38		all	100.64.0.2	00:0C:29:58:74:38	pbx	00:07:49	bound
D	100.64.0.5	00:0C:29:D1:7A:69		dhcp-IPv4	100.64.0.5	00:0C:29:D1:7A:69	pbx	00:07:30	bound
D	100.64.0.4	00:26:8B:04:FD:AB	1:0:26:8b:4:fd:ab	dhcp-IPv4	100.64.0.4	00:26:8B:04:FD:AB		00:07:39	bound
D	100.64.0.3	A0:8C:FD:1C:5A:61	1:a0:8c:fd:1c:5a:61	dhcp-IPv4	100.64.0.3	A0:8C:FD:1C:5A:61	Julian	00:05:08	bound

Ilustración 85 - IPs asignadas

Y las reglas del firewall donde se deja en evidencia que las primeras reglas actúan, memorizando las reglas anteriores y de esta manera se realiza un ahorro de recursos.

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	accept	input								2476.8 KiB	23 755
1	accept	forward								60.4 KiB	686
2	accept	output								38.8 MiB	35 337
3	drop	input								4534 B	81
	;;; IPsec										
4	accept	input			17 (udp)		500			972 B	2
	;;; IPsec										
5	accept	input			17 (udp)		4500			0 B	0
	;;; IPsec										
6	accept	input			50 (ipsec-esp)					1944 B	18
	;;; IPsec										
7	accept	output			50 (ipsec-esp)					0 B	0
	;;; IPsec										
8	accept	forward			50 (ipsec-esp)					0 B	0
	;;; FuerzaBruta										
9	add src to address list	input			6 (tcp)		22			0 B	0
	;;; FuerzaBruta										
10	add src to address list	input			6 (tcp)		22			0 B	0
	;;; FuerzaBruta										
11	add src to address list	input			6 (tcp)		22			0 B	0
	;;; FuerzaBruta										
12	add src to address list	input			6 (tcp)		22			0 B	0
	;;; FuerzaBruta										
13	drop	input			6 (tcp)		22			0 B	0
	;;; DOS										
14	tarpit	input		100.64.0.1	6 (tcp)		22-8291			0 B	0
	;;; SIP trunking										
15	accept	forward	0.0.0.0	194.140.135.80	17 (udp)					0 B	0

Ilustración 86 - Firewall

Podemos corroborar el funcionamiento del protocolo de pila dobla, donde observamos en la siguiente imagen las direcciones IPs del host conectado a la red LAN.

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . . . . : 2a01:d0:e348:0:d8ac:139f:5204:d444
   Dirección IPv6 temporal. . . . . . . . . : 2a01:d0:e348:0:d41a:10df:9e70:9618
   Vínculo: dirección IPv6 local. . . . . : fe80::d8ac:139f:5204:d444%3
   Dirección IPv4. . . . . . . . . . . . . . : 100.64.0.3
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::4e5e:cff:fe1e:8b48%3
                                               100.64.0.1
```

Ilustración 87 - IPs asignadas a host en red

Y la comprobación del funcionamiento del protocolo de red IPv6.

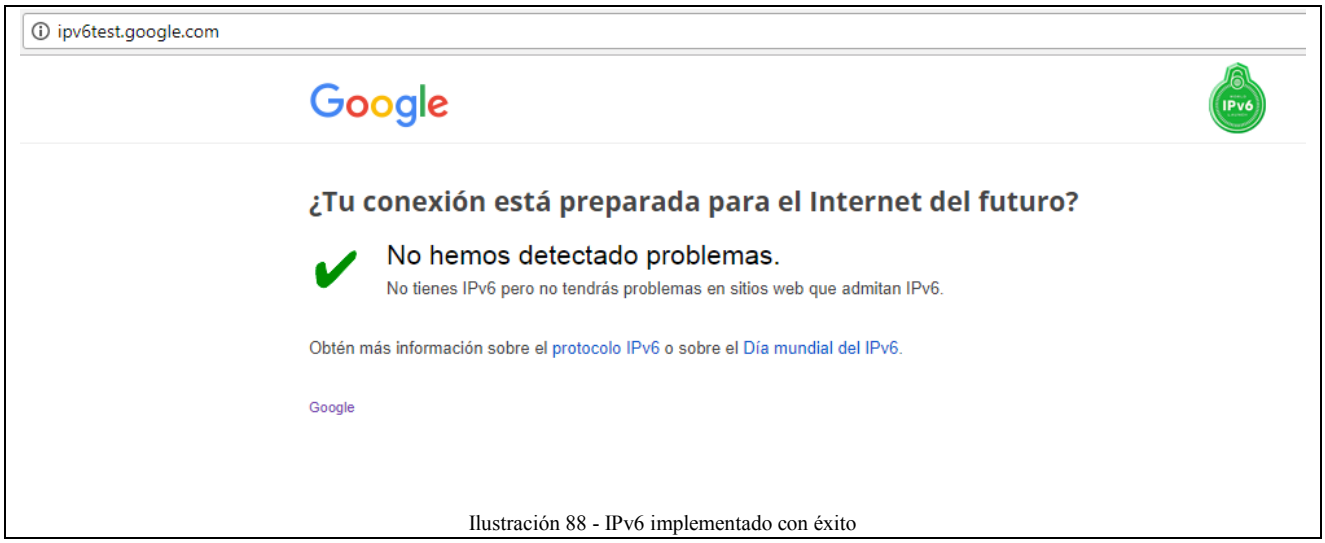


Ilustración 88 - IPv6 implementado con éxito

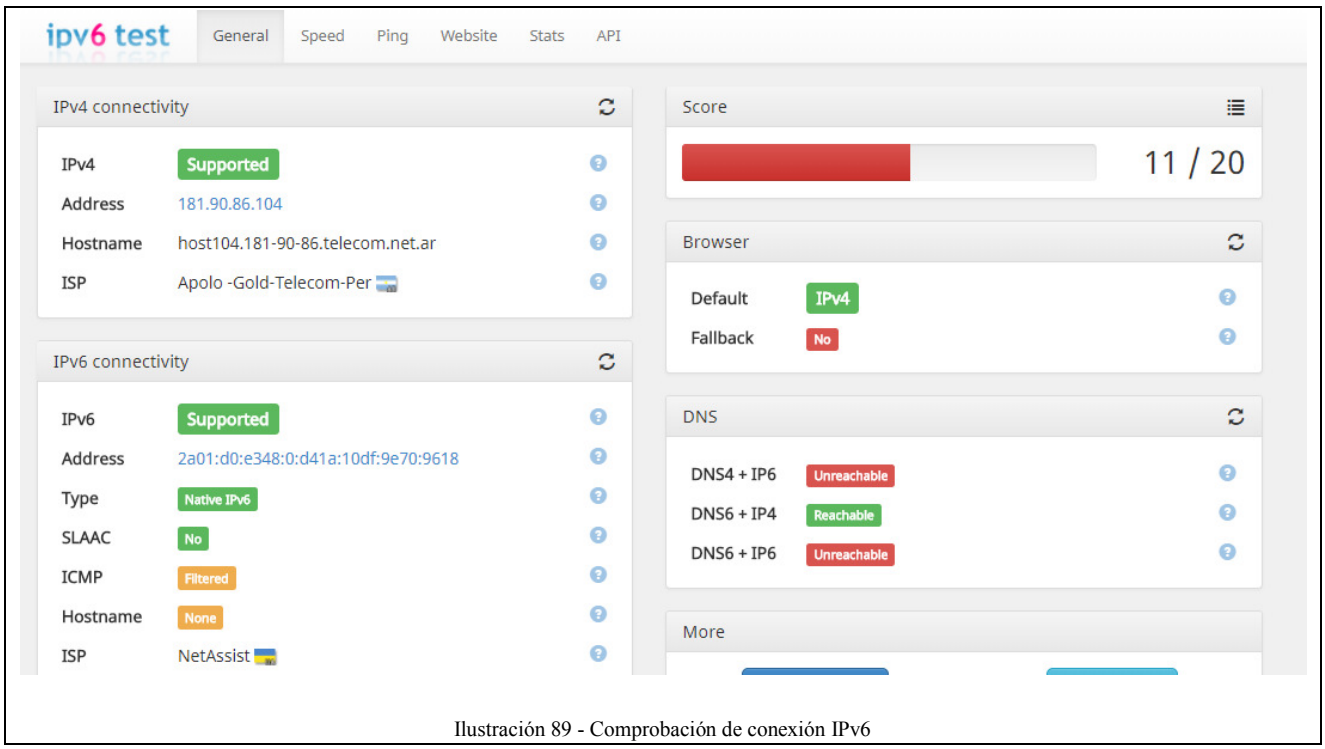


Ilustración 89 - Comprobación de conexión IPv6

Se realizó un test de ping al servidor DNS IPv6 Google.

```
C:\Users\julian-pc>ping 2001:4860:4860::8888

Haciendo ping a 2001:4860:4860::8888 con 32 bytes de datos:
Respuesta desde 2001:4860:4860::8888: tiempo=327ms
Respuesta desde 2001:4860:4860::8888: tiempo=334ms
Respuesta desde 2001:4860:4860::8888: tiempo=328ms
Respuesta desde 2001:4860:4860::8888: tiempo=336ms

Estadísticas de ping para 2001:4860:4860::8888:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 327ms, Máximo = 336ms, Media = 331ms

C:\Users\julian-pc>ping 2001:4860:4860::8844

Haciendo ping a 2001:4860:4860::8844 con 32 bytes de datos:
Respuesta desde 2001:4860:4860::8844: tiempo=335ms
Respuesta desde 2001:4860:4860::8844: tiempo=329ms
Respuesta desde 2001:4860:4860::8844: tiempo=334ms
Respuesta desde 2001:4860:4860::8844: tiempo=326ms

Estadísticas de ping para 2001:4860:4860::8844:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 326ms, Máximo = 335ms, Media = 331ms
```

Ilustración 90 - Ping a DNS de Google IPv6

Vemos el tiempo promedio de 330ms que es debido a que dicho paquete es encapsulado y enviado en la red publica con soporte IPv4, para luego ser desencapsulado y enviado efectivamente en la red IPv6. Podemos compararlo con un ping con los servidores DNS IPv4.

```
C:\Users\julian-pc>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=28ms TTL=54
Respuesta desde 8.8.8.8: bytes=32 tiempo=30ms TTL=54
Respuesta desde 8.8.8.8: bytes=32 tiempo=29ms TTL=54
Respuesta desde 8.8.8.8: bytes=32 tiempo=29ms TTL=54

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 28ms, Máximo = 30ms, Media = 29ms

C:\Users\julian-pc>ping 8.8.4.4

Haciendo ping a 8.8.4.4 con 32 bytes de datos:
Respuesta desde 8.8.4.4: bytes=32 tiempo=24ms TTL=53
Respuesta desde 8.8.4.4: bytes=32 tiempo=23ms TTL=53
Respuesta desde 8.8.4.4: bytes=32 tiempo=23ms TTL=53
Respuesta desde 8.8.4.4: bytes=32 tiempo=25ms TTL=53

Estadísticas de ping para 8.8.4.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 23ms, Máximo = 25ms, Media = 23ms
```

Ilustración 91 - Ping a DNS de Google IPv4

Se observa la diferencia de 300ms.

Podemos corroborar la conexión de los clientes IPsec conectados desde la red pública, de manera tal de demostrar el funcionamiento de la VPN.

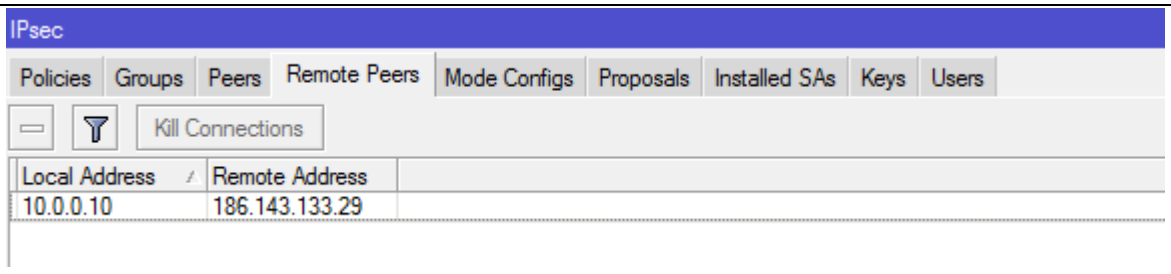


Ilustración 92 - Usuarios conectados a la VPN

Y como estos adquieren una dirección privada dentro del pool 100.64.1.0/24

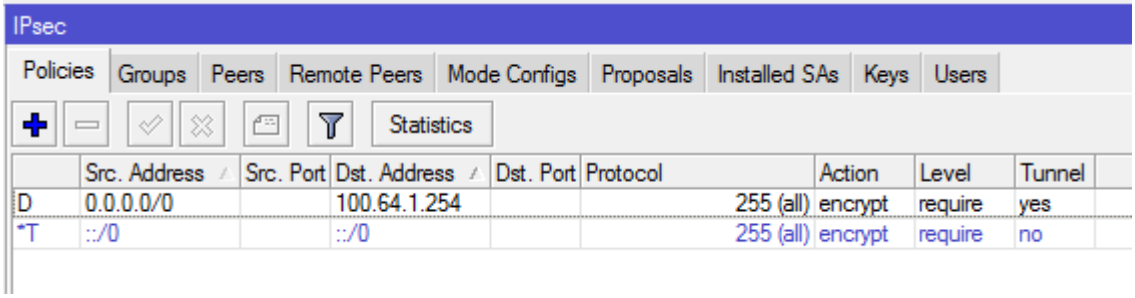


Ilustración 93 - Usuarios conectados a la VPN

En la siguiente imagen podemos observar el marcado de paquetes.

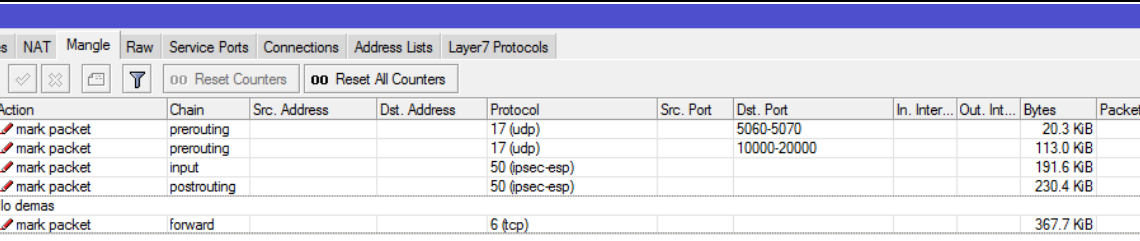


Ilustración 94 - Marcado de paquetes

Y las estadísticas del arbol de colas.

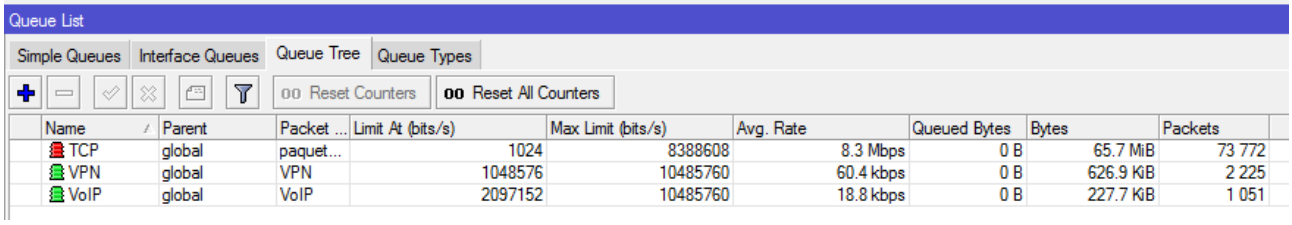


Ilustración 95 - Priorización y colas

Podemos observar y corroborar en la siguiente imagen las llamadas realizadas al número virtual adquirido, realizadas desde un número celular.

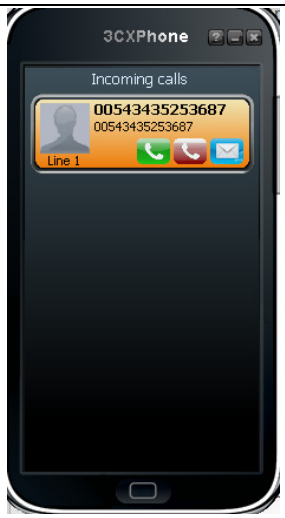


Ilustración 96 - Llamada realizada a número celular desde interno

Y las llamadas salientes.

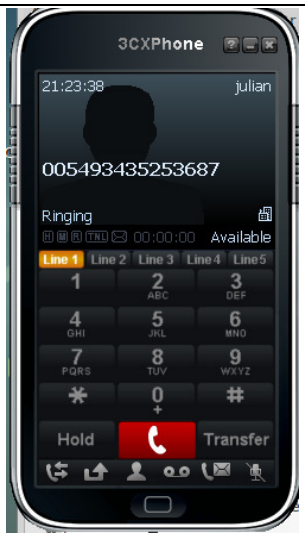


Ilustración 97 - Llamada realizada a número virtual

Capítulo 4: Análisis de Costos

A continuación, se detallarán los costos de los equipos utilizados.

- Router Mikrotik RB2011 – $ 2500
- Voice gateway Grandstream Ht 503 ATA - $ 1650
- Teléfono IP Escene Es205 - $ 800
- Compra de 2 números virtuales (DID), con numeración en la provincia de Buenos Aires - $180/mes

Costo total: $ 5130

- Infraestructura de red – precio variable dependiente de la empresa o institución

El trabajo se ha realizado en un tiempo de 4 meses e incluye conocimientos de telefonía tradicional de conmutación, networking, calidad de servicio en redes de paquetes, seguridad de información, encriptación y programación. Conocimientos adquiridos durante el cursado completo de la carrera ingeniería en electrónica y cursos extracurriculares.

Costo total mano de obra: $ 10000

Capítulo 5: Discusión y Conclusión

Las redes asíncronas de paquetes con soporte en el protocolo IP están ganando el mercado mundial de comunicaciones frente a las redes síncronas. Nombrando las redes de telefonía PSTN, ISDN y las redes de comunicaciones troncales de gran ancho de banda como FDDI y SONET, con sus jerarquías de sincronización, PHD y SHD, las cuales fueron redes basadas principalmente en el servicio de voz bajo la condición de la trasmisión base de información en 64 kbps; descriptos en la documentación ITU-T G.711.

Un texto interesante para la discusión de las nuevas redes de gran ancho de banda es el White Paper escrito por Steve Tang, Senior Engineer, TC Communications: "Advantages of Ethernet vs SONET/SDH"

"*Ethernet que ha sido el estándar elegido para redes de área local (LAN), está rápidamente reemplazando a las tecnologías tradicionales como SONET/SHD (TDM red sincrona), ATM y Frame Relay en redes de área metropolitana y redes de área extendida. En general en toda la industria de telecomunicaciones. Existen muchas razones para esta migración.*

La simplicidad de ethernet y su interoperabilidad a un costo eficiente con beneficios tangibles. Podemos mencionar: eficiencia y protección en el ancho de banda, modularidad, topologías flexibles, simplicidad, menor costo, protección en inversión a futuro.

La reciente estandarización de ethernet se ha centrado en promover y desarrollar la calidad del servicio (QoS) y administración y control. Como resultado, ethernet solucionó algunas debilidades y ahora proporciona fortalezas previamente asociadas solo con SONET / SDH". Advantages of Ethernet vs SONET/SDH (pág. 1)

"En el pasado, las redes SONET eran las únicas opciones para redes de gran cobertura. Estos sistemas estandarizados, confiables y bien entendidos, eran centrados en la voz y por lo tanto muy poco flexibles, difíciles de escalar y no optimizados para el transporte de paquetes." Advantages of Ethernet vs SONET/SDH (pág. 4)

El conjunto de protocolos ethernet abarca la capa física y capa de enlace del modelo OSI, capa 1 y capa 2. Con la característica del envió de tramas con un tamaño máximo de datos de 1500 bytes donde se encapsulan las tramas IP y los respectivos paquetes de la capa de transporte.

Por lo tanto, se debe considerar que, ante la creciente migración a este tipo de redes, los servicios sobre estas también deben modificarse para estas nuevas tecnologías, por lo que la telefonía se dirige completamente hacia ese cambio.

Un cambio que no solamente será dado por los grandes proveedores de servicio de telefonía sino también para centrales pequeñas en negocios, empresas e instituciones las cuales ya presentan una infraestructura de red ethernet.

Durante este trabajo hemos podido corroborar que es posible implementar una central de telefonía IP con implementación de softphones en una red LAN preexistente, la cual ha servido anteriormente para el uso de otros servicios. No es necesario realizar grandes cambios en la infraestructura de red ethernet para implementar una central de telefonía IP.

Con un ancho de banda de 2Mbps reservado para la comunicación de paquetes de telefonía es suficiente para implementar 23 llamadas simultaneas en un canal troncal con un servidor VoIP o llamas de softphones conectados en la red pública. La cantidad de llamadas simultaneas puede incrementarse si se aplican códecs más modernos, como G.729.

La implementación de una VPN mediante IPsec asegura los datos y autentifica a los usuarios que se conectan con la central de telefonía mediante la red pública.

El Voice gateway permite mantener operativa la central de telefonía IP a usuarios que no cuentan con servicio de VoIP y sirve como respaldo al canal de comunicaciones. Esto fue corroborado en forma efectiva y aunque la mayoría de los proveedores de telefonía VoIP brindan este servicio, siempre es conveniente tener una línea analógica por posibles inconvenientes en la conexión a internet.

Las posibles mejoras en este proyecto son las siguientes.

- Implementar diferentes codecs de manera tal de reducir el ancho de banda de una llamada; permitiendo canales troncales con mayor cantidad de comunicaciones simultaneas.
- Estudiar y solventar los problemas de latencia, pérdida de paquetes y jitter en enlaces satelitales y canales ruidosos. Mejorar la comunicación de voz en estos medios.
- Estudio e implementación de medidas de seguridad en los canales troncales, SIP trunking, con proveedores de VoIP.
- Implementar diferentes frameworks de telefonía haciendo uso de servidores SIP, SIP proxys y RTP Proxys diferentes y especializados, de manera tal de implementar una central de telefonía IP de gran capacidad, la cual puede ser utilizada como proveedor de este servicio, aplicando tarifas a clientes. Es decir, desarrollo e implementación de central de telefonía IP que brinde un servicio pago y que compita en el mercado.
- Realizar un estudio de los métodos de pago y gestión de recursos en función de tarifas, tarifas por minuto, tarifas por numeración y enrutamiento.

La propuesta para un nuevo desarrollo es implementar una central de telefonía IP con los suficientes recursos y características para comercializar el servicio.

Capítulo 6: Literatura Citada.

- Documentación RFC.
  https://www.ietf.org/rfc.html
- Documentación VMware.
  https://www.vmware.com/ar/solutions/virtualization.html
- Documentación de Asterisk.
  https://wiki.asterisk.org/wiki/display/AST/Home
- 3CX
  https://3cx.com
- IEEE 802.1D.
- Documentación Mikrotik, RouterOS.
  https://wiki.mikrotik.com/wiki/Manual:TOC
- CNSS Policy No. 15, Fact Sheet No. 1.
  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf
- Steve Tang, Senior Engineer, TC Communications: “Advantages of Ethernet vs SONET/SDH”

Universidad Tecnológica Nacional
Facultad Regional Paraná

Se certifica que …..... , DNI: …..... ha realizado la dirección del Proyecto Final:

…..... ....

De los alumnos:

- …..
- …..
- …..

Realizada durante el ciclo lectivo: ....., obteniendo el grupo un calificación final de:

….....

A fin de ser emitida la correspondiente certificación por el departamento de electrónica, se extiende la siguiente constancia.

Pañoni Sergio ***Ramos Hector*** ***Maggiolini Lucas***