

Universidad Nacional del Este.
Facultad Politécnica.

Carrera Análisis de Sistemas.
Cátedra Informática VIII.

Redundancia de túnel para centralización de datos a través de VPN.

Por: Pedro Luis López

Profesor Orientador: **Lic. Aldo Ariel Gómez Ortega**

Trabajo final de grado presentado a la Facultad Politécnica de la Universidad Nacional del Este como parte de los requisitos para optar al título Lic. Análisis de Sistemas.

Ciudad del Este, Alto Paraná. Paraguay.

Marzo y 2016

FICHA CATALOGRÍFICA
BIBLIOTECA DE LA FACULTAD POLITÉCNICA
DE LA UNIVERSIDAD NACIONAL DEL ESTE

López, Pedro
Luis, 1985.

Redundancia de túnel para centralización de datos a través de VPN.
Ciudad del Este, Alto Paraná. Año: 2016
Páginas:108.

Orientador:Lic. Aldo Ariel Gómez Ortega
Área de estudio: Ingeniería de Software.
Carrera: Lic. Análisis de Sistemas.
Titulación: Lic. Análisis de Sistemas.
Trabajo Final de Grado. Universidad Nacional del Este,
Facultad Politécnica.

Descriptores: 1. Mikrotik, 2. VPN, 3. Radio Enlace.
Tunel redundancy for data centralization through VPN
Key words: 1. Mikrotik, 2. VPN,
3. Radio Link.

Yo, Lic. Aldo Ariel Gómez Ortega, documento de identidad No. 1.504.349, Profesor Orientador del TFG titulado “Redundancia de túnel para centralización de datos a través de VPN.”, del Alumno Pedro Luis López, documento de identidad No. 4.009.082, de la carrera Análisis de Sistemas de la Facultad Politécnica de la Universidad Nacional del Este; certifico que el mencionado Trabajo Final de Grado ha sido realizado por dicho Alumno, de lo cual doy fe y en mi opinión reúne las condiciones para su presentación y defensa ante la Mesa Examinadora designada por la institución.

Marzo de 2016

Lic. Aldo Ariel Gómez Ortega

Nosotros, los miembros de la Mesa Examinadora del Trabajo Final de Grado titulado “Redundancia de túnel para centralización de datos a través de VPN.”, de la carrera Análisis de Sistemas de la Facultad Politécnica de la Universidad Nacional del Este, hacemos constar que el citado trabajo ha sido evaluado en fondo y forma por esta Mesa, la que por _____ ha resuelto asignar la calificación _____

Ciudad del Este, _____ de _____ de 2016

Profesor _____
Presidente de la Mesa Examinadora

Profesor _____

Miembro de la Mesa Examinadora

Profesor _____

Miembro de la Mesa Examinadora

Me gustaría dedicar este trabajo de investigación a toda mi familia y colegas de trabajo.

*Agradezco infinitamente,
A Dios Todopoderoso,
A mi madre Amada, a mis hermanos Victor, Ylse, Margarita,
Raquel, Aldo y David, porque siempre estan cuando necesito.
A mis amigos David, Diego y Jorge por no dejarme decaer con
el ánimo para hacer este trabajo.
A mis colegas de trabajo Justo, Arnaldo, Aldo, Alcides, Jorge,
Gabriel, Cynthia y Liz por ayudarme e incentivar me con la
práctica.
A mi encargado Andeson Lorenzon Cesar por la paciencia para
enseñarme a usar esta herramienta.
A mi orientador, Licenciado Aldo Gómez
Esta investigación ha tenido apoyo, en parte, de la empresa
MCA Solution S.A, Datapar S.A, a la empresa Agrofertil S.A
por proveer la estructura.
A mi prima Sonia Weiss y su esposo John Vaan Derpool.
He dejado de nombrar a muchas personas que me han dado su
ayuda de una u otra manera para la culminación de este trabajo.
Expreso mi más sincera gratitud a todas ellas.*

El universo no se importa con tus sentimientos, levántate y camina hacia adelante, tienes las piernas para hacerlo.

Resumen

El presente proyecto, implementó una alternativa para mejorar la seguridad de los datos de una empresa media-grande centralizando servidores, mediante la implementación de una VPN por medio de radio frecuencias y respaldo de enlace vía Internet. Los beneficios de esta implementación fueron inmediatos, ya sea con la reducción de costos de infraestructura, reducción de los gastos administrativos, y aumento de la resiliencia del servicio, entre otros.

Una conexión por medio VPN, permitió la centralización y el mejor manejo de la información, sin muchas dificultades para su mantenimiento, ni la necesidad de comprar equipamientos caros o complejos (servidores físicos tradicionales).

Centralizar los servidores ayudó en la administración de los mismos, redujo los costos y facilitando el manejo de los datos; además con la disminución de servidores el respaldo se hace en menos tiempo.

Para implementar esta infraestructura se hizo uso del sistema operativo RouterOS basado en GNU/Linux por su alta confiabilidad y su fácil administración por medio de un entorno gráfico, así como accesos vía Telnet, SSH y web; teniendo en cuenta lo citado, el enrutador Mikrotik se presenta en el mercado como una solución robusta, profesional y económicamente factible.

Descriptores: 1. VPN, 2. Mikrotik, 3. RouterOS.

Abstract

The present project implemented an alternative to improve the security of data on a medium-large enterprise, centralizing the servers through the implementation of a VPN by means of radio frequencies and backup link via Internet.

The advantages of this implementation were immediate, be it with the reduction of the costs in infrastructure, reduction of the administrative expenses and increase in the resilience of the service among others.

A connection via VPN allowed the centralization and best management of the data without many complications for its maintenance nor the need to buy expensive or complex equipment (traditional physical servers).

Centralizing the servers helped in managing them, reduced the costs and facilitate the data management; in addition, with the reduction of servers the backup take less time.

To implement this infrastructure it was made use of the RouterOS operating system based on GNU/Linux for its high reliability and its easy management through a graphical interface, as well as access via Telnet, SSH and Web, considering the aforementioned, the router Mikrotik is represented in the market as a strong solution, professional and economically feasible.

Key words: 1. VPN, 2. Mikrotik,, 3. RouterOS.

Índice general

Resumen	VIII
Abstract	IX
Índice de figuras	xv
Índice de tablas	xvi
Acrónimos y símbolos	xviii
1. Introducción	1
1.1. Motivación	2
1.2. Definición del problema	3
1.3. Objetivos, hipótesis, justificación y delimitación del alcance del tratado	3
1.3.1. Objetivo General	3
1.3.2. Objetivo Específicos	3
1.3.3. Hipótesis	4
1.3.4. Justificación del Estudio.	4
1.3.5. Alcance del Trabajo.	4
1.4. Descripción de los Contenidos por Capítulo	5
1.5. Tipo de Investigación	5
1.5.1. Investigación Tecnológica	5
1.5.2. Modalidad	5
1.6. Resultado del Diagnóstico.	6
1.6.1. Relevamiento	6
1.6.2. Planteamiento del Problema	6
1.6.3. Pregunta General	8
1.6.4. Preguntas Específicas	8
1.7. Antecedentes	8

ÍNDICE GENERAL

ÍNDICE GENERAL

2. RadioFrecuencia	10
2.1. Marco Teórico	10
2.1.1. Radiofrecuencia	11
2.1.2. Ancho de Banda	12
2.1.3. Ondas Electromagnéticas	12
2.1.4. Polarización	13
2.1.5. Tipos de Polarización	13
2.1.6. Usos de la Polarización	14
2.1.7. Características fundamentales de las ondas de radio	14
2.1.8. Reflexión Y Refracción De Ondas	15
2.1.9. Reflexión y Transmisión	15
2.1.10. Refracción	15
2.1.11. Dispersión	17
2.1.12. Difracción	17
2.1.13. Transmisión y Recepción	18
2.1.14. Usos de la radiofrecuencia	19
2.1.15. Características y tipos de enlaces	20
2.1.16. Propagación radioeléctrica	20
2.1.17. Sistemas de radiocomunicaciones inalámbricas	21
2.1.18. Línea de vista directa	21
2.1.19. La Zona de Fresnel	22
2.1.20. Energía	22
2.1.21. Cálculo en dBs	23
2.1.22. Ventajas de un enlace inalámbrico	24
2.1.23. Estructura de un radio enlace	25
2.1.24. Enlaces Punto - Punto	26
2.1.25. Enlaces Punto - Multipunto	27
2.1.26. Conexión De Rejilla O Malla	28
2.1.27. Distribución De Acceso Inalámbrico (HotSpot)	29
2.1.28. Sistemas de microondas	29
2.1.29. Radiocomunicaciones por satélite	29
2.1.30. Red Privada	30
2.1.31. Red Pública	31
2.1.32. Red Privada Virtual	31
3. Definición de VPN	33
3.0.1. Terminología	34
3.0.2. Clasificación	36
3.0.3. VPNs provistas por el cliente o por el proveedor	37
3.0.4. VPNS provistas por el cliente (CE o CPE VPN)	37
3.0.5. VPNs provistas por el Proveedor (PPVPN)	38

3.0.6. VPNs Sitio a Sitio y de Acceso Remoto	40
3.0.7. VPNs de capa 2 y capa 3	42
3.0.8. Integración de las clasificaciones	42
3.0.9. VPN VPWS	43
3.0.10. VPN VPLS	43
3.0.11. VPN IPLS	44
3.0.12. VPN Sitio a Sitio Provistas por el Proveedor de Capa 3 (L3VPN)	44
3.0.13. Confiables y Seguras	45
3.0.14. Overlay y Peer	45
3.0.15. VPNs de capa de transporte/aplicación	47
3.0.16. VPN multiservicio	48
3.0.17. Aplicaciones	48
3.0.18. Extranets	49
3.0.19. Servicio VPN provisto por un proveedor	50
3.0.20. Calidad de servicio (QoS) y Acuerdos de nivel de servicio (SLA)	51
3.0.21. Creación de Túneles	54
3.0.22. Tunneling	54
3.0.23. Comparativa entre tecnologías VPN	54
3.0.24. Aspectos Legales	56
4. Software RouterOS.	57
4.1. Winbox.	57
4.2. Configuración IP.	59
4.3. Telnet	63
4.4. Webbox	65
4.5. SSH	65
4.6. Radio Mobile	66
4.7. Google Earth	68
5. Procedimientos generales para la instalación de los enlaces	70
5.1. Equipos a ser utilizados	71
5.2. Configuración de radios	73
5.2.1. Mikrotik RouterOS - enlaces punto - punto.	73
5.2.2. Configuración AP	74
5.2.3. Configuración Estación.	81
5.3. Configuración de VPN	86
5.3.1. Configuración VPN Server	86
5.3.2. Configuración VPN Cliente	93

ÍNDICE GENERAL**ÍNDICE GENERAL**

6. Conclusión y recomendaciones	98
Glosario	99
Anexo A.	102
6.1. Configuraciones del MK1	102
6.2. Configuraciones del MK2	103
6.3. Configuraciones del MK3	104
6.4. Configuraciones del MK4	107
Referencias bibliográficas	110

Índice de figuras

1.1. Situacion Actual, donde cada filial tiene un servidor para cada servicio	7
1.2. Situacion Esperada, con la implementacion de los tuneles redundantes, los servidores quedan centralizados	7
2.1. Escala del espectro electromagnético [1]	12
2.2. Tipos de Polarización [2]	13
2.3. Rayo incidente y reflejado [2]	16
2.4. Rayo incidente y refractado [2]	16
2.5. Difracción a través de una ranura pequeña [1]	17
2.6. Interferencia de ondas: constructiva (izquierda) y destructiva (derecha) [1]	18
2.7. Longitud de onda, amplitud, y frecuencia [1]	19
2.8. Propagación de las ondas sobre la superficie terrestre [3]	20
2.9. La zona de Fresnel está bloqueada parcialmente en este enlace aunque la línea visual (line of sight) no está obstruida [1]	23
2.10. Enlace Punto - Punto [1]	27
2.11. Enlace Punto Multipunto [1]	28
2.12. Conexión Malla [1]	28
3.1. Componentes de una VPN [4]	36
3.2. VPN Provista por el Cliente [4]	38
3.3. VPN Sitio a Sitio [4]	40
3.4. VPN de Acceso Remoto [4]	41
3.5. Clasificación de las VPN [4]	42
3.6. Adyacencias del Ruteo [4]	45
3.7. Infraestructura del proveedor [4]	46
3.8. VPNs tipo Peer [4]	47
4.1. RouterOS	57
4.2. Winbox	58

4.3. Escaneo de Router con Winbox	58
4.4. Reset RouterOS	59
4.5. Remover Configuraciones	59
4.6. Configura IP WAN	60
4.7. Configurar IP LAN	60
4.8. Address List	60
4.9. Puertas de Enlaces	61
4.10. Puerta de enlace predeterminada	61
4.11. Listado de puertas de enlace	61
4.12. DNS	62
4.13. Prueba de ping	62
4.14. Firewall - General	62
4.15. Firewall -Action	62
4.16. Lista reglas Nat	63
4.17. Prueba de ping	63
4.18. Acceso vía Telnet	64
4.19. Credenciales vía telnet	64
4.20. Entorno Telnet	64
4.21. Webbox	65
4.22. Putty - Autenticación	66
4.23. Entorno de trabajo SSH	66
4.24. Radio Mobile, Enlace de Radio	67
4.25. Vista con Radio Mobile	68
4.26. Vista con Google Earth	69
5.1. Escenario para la Simulación	70
5.2. Escenario ya en limpio	71
5.3. Prueba de funcionamiento de los equipos	71
5.4. MK4 y MK3	72
5.5. MK2 y MK1	72
5.6. Notebook Central	73
5.7. Maquina Sucursal 1	73
5.8. Escaneo de Routers	74
5.9. Reseteo de configuraciones	75
5.10. Remover configuración	75
5.11. Interface Wireless disponible	76
5.12. Configurar AP	77
5.13. Habilitar Bridge - WDS	78
5.14. Equipos ya conectado	78
5.15. Nombre Bridge	79
5.16. Agregar Interface al Bridge	79

5.17. Lista de Puerto del Bridge	80
5.18. Prueba de ping al MK3	80
5.19. Prueba de Ancho de banda	80
5.20. Una vez conectado, ya muestra al escanear todas las radios	81
5.21. Prueba de ping desde la Red Central	81
5.22. Reestablecer Configuraciones MK3	82
5.23. Remover configuraciones	83
5.24. Crear Bridge	83
5.25. Lista de interfaces en el Bridge	84
5.26. Configurar IP	84
5.27. Lista Interfaces Wireless disponibles	84
5.28. Configurar Wireless Station	85
5.29. Configura interface en la Bridge y WDS	85
5.30. Restaurar configuraciones MK1	86
5.31. Winbox con el MK1 ya con las configuraciones de fabrica	87
5.32. Remover configuraciones	87
5.33. Configurar IP	88
5.34. Conectar al WIFI del Celular	88
5.35. Configuraciones de Seguridad del WIFI	89
5.36. MK1 y MK4 conectado al Celular	90
5.37. Habilitar Server PPTP	91
5.38. Crear usuario para Túnel por medio del Enlace	91
5.39. Crear usuario para el Túnel por medio de Internet	92
5.40. Túnel ya online	92
5.41. Listado de IP del MK1	92
5.42. Remover configuraciones	93
5.43. Remover configuraciones por defecto	93
5.44. configurar WIFI	94
5.45. Perfil de seguridad del WIFI	94
5.46. Lista de IP configurado MK4	95
5.47. Lista de Discadores Clientes	95
5.48. Datos Discador Cliente por Internet	96
5.49. Datos Discador Cliente VPN por Enlace	96
5.50. Configuraciones de Puertas de enlace	97
5.51. Prueba de Traceroute desde la maquina Sucursal 1	97

Índice de Tablas

3.1. SSH v1, SSH v2	48
3.2. SSH, SSL	48

Acrónimos y símbolos

.kml Keyhole Markup Language. [69](#)

AP Access Point. [73](#)

AtoM Any Transport over MPLS. [41](#)

BGP Border Gateway Protocol. [43](#)

DLCI Frame Relay Data Link Connection Identifier. [42](#)

ERP Sistemas de planificación de recursos empresariales. [2](#)

GRE Generic Routing Encapsulation. [38](#)

HTTPS Hypertext Transfer Protocol Secure. [48](#)

IPLS IP only Private Lan Service. [39](#), [43](#)

IPsec Internet Protocol security. [38](#)

ITM Irregular Terrain Model. [66](#)

L2F Layer 2 Forwarding. [41](#)

L2TPv3 Layer 2 Tunneling Protocol version 3. [41](#)

M2M Multipunto a Multipunto. [43](#)

MAC Media Access Control. [42](#)

MPLS Multiprotocol Label Switching. [40](#)

MPLS LSP MPLS Label Switched Path. [41](#)

NAS Network Access Server. 35

P2P Punto a Punto. 43

PPTP Point to Point Tunneling Protocol. 41, 86

QoS Quality of Service. 48, 50

SLA Service Level Agreement. 52

SLO Service Level Objective. 52

SLS Service Level Specification. 52

SSL Secure Sockets Layer. 55

TI Técnología de la Información. 4

VPLS Virtual Private Lan Service. 39, 43

VPN Virtual Private Network. 2–5, 8

VPWS Virtual Private Wire Service. 39, 43

WAN Wide Area Network. 30

Capítulo 1

Introducción

En la actualidad las redes informáticas, se han vuelto indispensables, tanto para las personas, como para las organizaciones, les da oportunidad de interactuar con el resto del mundo, ya sea por motivos comerciales, personales o emergencias.

Organizaciones con cientos de oficinas dispersas en una amplia área geográfica esperan de manera rutinaria poder examinar el estado actual incluso de la sucursal más distante con solo presionar un botón.

La aplicación de medidas de seguridad en las redes supone desplegar diversos productos: sistemas de detección de intrusos, controles de autenticación y autorización, cortafuegos y otros servicios. Habitualmente este despliegue se realiza utilizando productos y tecnologías de diferentes fabricantes. Cuando se habla de aspectos de seguridad, las empresas suelen seleccionar los productos con *pedigrí*: en cada categoría se selecciona siempre el producto con mayor renombre y mejor prensa. Esta es una tendencia que no parece cambiar a corto o medio plazo.

Esta disparidad de fabricantes origina diversas dificultades, como la problemática de gestión de los dispositivos (cada elemento de seguridad dispone de su propia aplicación de gestión), las dificultades para la interoperabilidad (los productos de seguridad tienen una mentalidad de funcionamiento aislado) y la centralización de la información generada.

Este último aspecto es posiblemente uno de los principales talones de Aquiles en virtualmente cualquier red con un mínimo nivel de complejidad. A medida que van aumentando los sistemas de seguridad, se reduce proporcionalmente la capacidad de poder disponer de una visión global del estado de la seguridad corporativa.

Ahora bien, en la red, esta visión global del estado de la seguridad no lo proporcionan únicamente los dispositivos tradicionales de seguridad, como son los cortafuegos y los sistemas de detección de intrusos. También otros

muchos sistemas están generando una información vital para poder construir esta imagen: sistemas operativos, bases de datos, detectores de virus, servidores de archivos, **Sistemas de planificación de recursos empresariales (ERP)**. Ignorar estos datos sólo nos hará tener una visión distorsionada del estado de la seguridad. De hecho, son más importantes aquellas informaciones que nos puedan transmitir los otros elementos, que son clave para el funcionamiento de la empresa.

Y existe otro factor, de una importancia notable: esta visión debe ser generada en tiempo real. No importa cuántos dispositivos tengamos, ni su dispersión geográfica o los diferentes métodos que tengan para representar las alertas. La visión del estado de la seguridad estará totalmente distorsionada si esta no se genera en tiempo real.

Una vez que dispongamos de las informaciones de seguridad centralizadas, podemos aplicar reglas de correlación. De esta forma podemos identificar tendencias y similitudes en los posibles ataques que reciba la red. Con la información que se obtiene de la correlación, los equipos de seguridad pueden responder rápidamente ante un incidente, ajustando sus sistemas para ofrecer la respuesta adecuada ante el ataque (desactivar una determinada dirección, reforzando las medidas de seguridad de los sistemas más expuestos a ataques).

Otra ventaja en disponer de toda la información relativa a seguridad centralizada es la facilidad en la generación de informes, que nos presenten los diferentes ataques que sufren nuestra infraestructura, el status de las diferentes líneas de negocio, el tiempo de respuesta ante los incidentes, etc. Esta información será básica para evaluar la idoneidad de las medidas de seguridad existentes y en la justificación de las inversiones necesarias. [5].

1.1. Motivación

La elaboración de este trabajo obedece a la necesidad de satisfacer las necesidades de centralizar los **Servidores**, con la finalidad de unificar la red y por ende los datos e informaciones de suma sustancialidad para una empresa. En este sentido se propone dotar al sistema de una infraestructura sólida, segura y económica mediante el uso de radio enlaces entre sucursales de una empresa ya sea de medio o grande porte, teniendo como respaldo el uso de **Virtual Private Network (VPN)** con fin de garantizar la comunicación del servicio aumentando su resiliencia, y por lo tanto la robustez del enlace, y contribuyendo con la seguridad de los datos, el activo primordial de toda empresa u organización.

1.2. Definición del problema

Las empresas de medio/grande portes en Paraguay, a fin de optimizar sus infraestructuras y sus recursos económicos, se ven obligados a buscar alternativas a los medios recurrentes tales como fibras ópticas, satélites o servicios de banda ancha. Ya que en muchas localidades servicios no se encuentran disponibles por el alto costo que implica su cobertura para las operadoras. Por tales motivos soluciones robustas como el uso de radio enlaces utilizando espectros libres, son una opción ideal.

Debido a factores imprevisibles como inclemencias del tiempo, hurtos u hechos vandálicos, se propone respaldar la conexión por medio de VPNs via internet a fin de dar mayor estabilidad a la comunicación.

Además desde el punto de vista económico, la centralización de los servidores acarrea un menor costo de implementación y mantenimiento, ya que por ejemplo para una empresa con 30 sucursales se ahorraría el costo de contar con servidores para cada local, lo que a su vez denota un ahorro tanto en simplicidad de mantenimiento como en el costo del recurso humano necesario para su correcto funcionamiento.

1.3. Objetivos, hipótesis, justificación y delimitación del alcance del tratado.

1.3.1. Objetivo General

- Implementar una infraestructura de redundancia de enlaces por medio de **VPNs** para la centralización de servidores.

1.3.2. Objetivo Específicos

- Estudiar tecnologías y metodologías para el desarrollo del proyecto.
- Realizar un radio enlaces.
- Configurar **VPN**.
- Configurar conexión respaldo por medio de Internet.
- Realizar pruebas de conexión entre máquinas/clientes y servidores.

1.3.3. Hipótesis

El desarrollo de este proyecto puede generar tanto beneficiarios directos como indirectos. Por el lado de los beneficiarios directos tenemos a los funcionarios **Tecnología de la Información (TI)** al facilitar la administración de la red.

Por otro lado, como beneficiarios indirectos se pueden mencionar a los funcionarios de las sucursales, por mejorar la continuidad del servicio.

Además de que dicho proyecto, puede servir de base para la generación de una empresa de servicios para brindar seguridad en redes a cualquier tipo de entidad sea cual fuere su tamaño.

1.3.4. Justificación del Estudio.

La elaboración de este trabajo obedece a la necesidad de satisfacer las necesidades de centralizar los servidores, con la finalidad de unificar la red y por ende los datos e informaciones de suma sustancialidad para una empresa. En este sentido se propone dotar al sistema de una infraestructura sólida, segura y económica mediante el uso de radio enlaces entre sucursales de una empresa ya sea de medio o grande porte, teniendo como respaldo el uso de **VPNs** a fin de garantizar la comunicación del servicio aumentando su resiliencia, y por lo tanto la robustez del enlace, y contribuyendo con la seguridad de los datos, el activo primordial de toda empresa u organización.

1.3.5. Alcance del Trabajo.

La solución propuesta deberá atender específicamente las necesidades de la empresa a ser utilizada para la implementación.

Se pretende utilizar las instalaciones de Agrofértil S.A. y a los funcionarios seleccionados para su implementación.

La principal característica del proyecto es la redundancia y seguridad del enlace que representa el uso de **VPNs** entre sucursales, a fin de asegurar la comunicación de los clientes a los servidores centralizados en la casa matriz. En el proyecto se prevé la utilización de la infraestructura existente de la empresa mencionada, por lo tanto no está contemplada la compra de ningún equipo.

1.4. Descripción de los Contenidos por Capítulo

El trabajo está organizado en seis (VI) capítulos:

El Capítulo I: Se presenta una introducción, el planteamiento del proyecto, motivación y los objetivos.

El Capítulo II: Se presenta conceptos de la Radiofrecuencia, su historia, sus protocolos de señalización; además su clasificación.

El Capítulo III: Se presenta información sobre **VPN**

El Capítulo IV: Se presenta una breve reseña sobre el funcionamiento del Software RouterOS

El Capítulo V: Realizar un radio enlace y túnel redundante

El Capítulo VI: Por último se exponen las conclusiones del trabajo y las recomendaciones para trabajos futuros.

1.5. Tipo de Investigación

1.5.1. Investigación Tecnológica

La investigación tecnológica busca una aplicación práctica de los conocimientos que sean útiles a la realidad, para lograr una solución factible de las problemáticas abordadas; por lo que usualmente está ligada a un campo de aplicación en particular, normalmente con un lenguaje propio, especializado y utilitario [6].

1.5.2. Modalidad

Esta investigación se enmarca de acuerdo con el tipo de conocimiento que se genera, correspondiendo al tipo adaptativo de esta clasificación.

La investigación adaptativa es aquella cuya finalidad es implementar, en el contexto que presenta el problema, soluciones que ya existen y que se aplicaron con éxito en otras situaciones [7].

1.6. Resultado del Diagnóstico.

Dar un solución rápida a los problemas de servidores, en especial cuando estas están en alguna regiones donde el acceso se hace difícil, ya sea por inclemencia de tiempo o algún otro factor, puede provocar que no se pueda poner el linea a estos, por días e inclusive semanas, dejando a las unidades sin funcionamiento. ya que resulta mas fácil para el usuario común conectarse desde otra máquina en algun lugar con conexión a **Internet**, que intentar reparar el servidor.

1.6.1. Relevamiento

La elaboración de este trabajo obedece a la necesidad de satisfacer las necesidades de centralizar los servidores de una empresa, con la finalidad de unificar la red y por ende los datos e informaciones de suma sustancialidad para la empresa. En este sentido se propone dotar al sistema de una infraestructura sólida, segura y económica mediante el uso de radio enlaces entre sucursales de la empresa seleccionada, teniendo como respaldo el uso de VPN a fin de garantizar la comunicación del servicio aumentando su resiliencia, la robustez del enlace, y contribuyendo con la seguridad de los datos, el activo primordial de toda empresa u organización. El alcance del trabajo no cubre la implementación de la seguridad en los servidores, solo la conexión de las filiales con la central y se limita exclusivamente a la orientación técnica partiendo de requisitos básicos necesarios para la centralización de datos a través de conexiones redundantes utilizando túneles VPN.

1.6.2. Planteamiento del Problema

El problema que se desea solucionar es la perdida de señal entre la central y las filiales, la replicación de los datos. Como se muestra en la (Fig. 1.1), cada sucursal tiene su propio servidor, dificultando la replicación de los datos a los servidores de la central

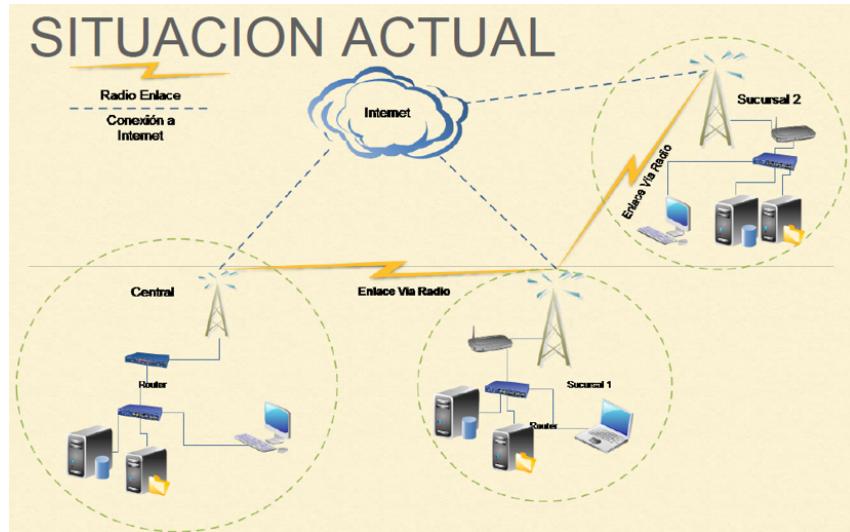


Figura 1.1: Situacion Actual, donde cada filial tiene un servidor para cada servicio.

Una vez realizado la conexión por medio de tuneles redundantes, como se puede ver en la (Fig. 1.2), los datos quedan almacenado en el servidor de la central, de esta manera reducir al minino los problemas de incoherencia a causas de replicaciones.



Figura 1.2: Situacion Esperada, con la implementacion de los tuneles redundantes, los servidores quedan centralizados.

1.6.3. Pregunta General

¿Cuál es la manera para conectar sucursales con la central a través de VPNs?

1.6.4. Preguntas Específicas

¿Cuál es el modelo de infraestructura que responde de manera más eficiente para la centralización de datos utilizando VPN?

¿Cuáles son los equipos hardware y software a ser utilizado para la implementación de la centralización de datos a través de VPN?

¿Qué cantidad de recursos humanos serán necesarios y cuál será el orden de desarrollo del trabajo para la implementación de la centralización de datos a través de VPN?

¿Cuáles son las recomendaciones para tener una seguridad mínima en la centralización de los datos a través de VPN?

1.7. Antecedentes

La importancia de la tecnología de las redes de datos para las comunicaciones en las organizaciones (empresas, instituciones gubernamentales, no gubernamentales) ha sido fundamental para su desarrollo y crecimiento, tanto en el aspecto económico y funcional, siendo una herramienta estratégica que brinda soporte y permite el desenvolvimiento y transformación de dichas organizaciones. Hoy en día no se puede concebir, a nivel organizacional, algún cambio, fusión u unión sin considerar las comunicaciones y las tecnologías de información que le dan soporte.

Ya se realizaron varios trabajos relacionados a **VPN**, cada una de ellas con sus particularidades. Cabe destacar “*Redes VPNs de Acceso Remoto*”, realizado por Mario Rubén Mansilla y Eduardo Rodolfo Colombres, donde los objetivos generales fueron: Investigar las características, componentes, mecanismos de una VPN de acceso remoto y como solucionan la necesidad de un ingreso seguro a los recursos informáticos de la organización desde cualquier sitio y Aplicar los conceptos de VPN de acceso remoto a través de una solución que implemente un cliente VPN portátil que evite la instalación de programas para esta tarea. [4] “*Las comunicaciones en las redes privadas virtuales*” de Jesús y Juan Hernández donde el objetivo principal es implementar VPN en una plataforma Windows. [8] En otro trabajo similar, “*Estudio e implementación de un radio enlace con tecnología mikrotik para el ISP Sistemas en el cantón gualaque, provincia morona santiago*”, de Klever Mauricio Suqui

Conceptos fundamentales, teorías y antecedentes

Carchipulla . Estos autores estudian las propiedades de los radios enlaces a profundidad. [2]

Capítulo 2

RadioFrecuencia

2.1. Marco Teórico

Es de sobra conocido que vivimos en la era de la información. Este hecho tiene unas connotaciones inmediatas que también son conocidas universalmente. La primera de ellas es que en la sociedad actual la información tiene un gran valor, es más, en muchas ocasiones la información es el propio “valor” o, al menos, la información es el valor que marca la diferencia.

Muchas empresas y organizaciones, solo gestionan y negocian con información. Para ellas, la información es el único activo y, por lo tanto, el más valioso. Como tal elemento de valor, la información debe ser custodiada con el máximo cuidado porque, sin lugar a duda, será buscada por otros. [9]

Hoy en día así como han crecido potencialmente las tecnologías, la masificación del uso de Internet y el uso de aplicaciones en red, también han crecido las amenazas informáticas, las cuales pueden provocar desde una infección en la computadora con virus hasta interrumpir completamente la funcionalidad de un sistema empresarial. [10]

A fin de garantizar la seguridad de este bien de las empresas u organizaciones, es imprescindible protegerla, de forma a que se evite las pérdidas por eventos accidentales o intencionales.

Entre los términos de seguridad dentro del ámbito de las Tics, se pueden definir los siguientes:

- Amenaza es un evento que puede desencadenar un incidente en la organización propietaria, produciendo daños materiales o perdidas inmateriales en sus activos.
- Activos son recursos para que la organización funcione correctamente

con el fin de alcanzar sus objetivos propuestos. En el caso que nos compete, el activo principal es la información y los activos secundarios son los propios sistemas informáticos (hardware).

- Vulnerabilidad es la posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.
- Impacto es la consecuencia sobre un activo de la materialización de una amenaza sobre el activo.
- Riesgo es la probabilidad de que se produzca un impacto determinado en un activo de la organización. [11]

Desde del inicio de las telecomunicaciones, cuando una información es transmitida por un canal de comunicación está sometida a riesgos porque existe amenazas y el canal de comunicación tiene vulnerabilidades (un canal de comunicación es, en la mayoría de los casos, esencialmente inseguro e inestable). [12]

2.1.1. Radiofrecuencia

Cuando hablamos de radio, la mayoría de la gente piensa en la radio FM, que usa una frecuencia de alrededor de 100 MHz. Entre la radio y el infrarrojo encontramos la región de las microondas con frecuencias de 1 GHz a 300 GHz, y longitudes de onda de 30 cm a 1 mm.

Las frecuencias más importantes para nosotros son las de 2 400 - 2 495 MHz, usadas por los estándares 802.11b y 802.11g (correspondientes a longitudes de onda de alrededor de 12.5 cm), y las de 5.150 - 5.850 GHz (correspondientes a longitudes de onda de alrededor de 5 a 6 cm), usadas por 802.11a. El estándar 802.11n puede trabajar en cualquiera de estas bandas. en la (Fig. 2.1) nos muestra el uso de cada frecuencia.

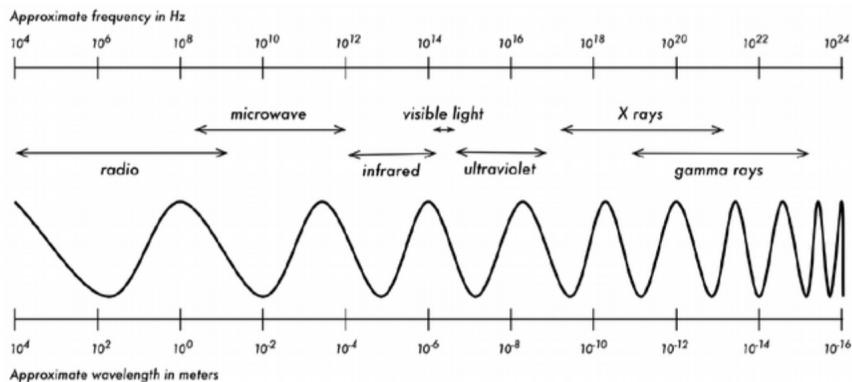


Figura 2.1: Escala del espectro electromagnético [1]

2.1.2. Ancho de Banda

Un término que vamos a encontrar a menudo en la física de radio es ancho de banda. El ancho de banda es simplemente una medida de rango de frecuencia. Si un dispositivo usa el rango de 2.40 GHz a 2.48 GHz, decimos que el ancho de banda sería 0.08 GHz (es decir 80 MHz). Se puede ver fácilmente que el ancho de banda que definimos aquí está muy relacionado con la cantidad de datos que se pueden transmitir a mayor cantidad de frecuencias disponibles, mayor cantidad de datos se pueden transmitir en un momento dado. El término ancho de banda es a menudo utilizado para algo que deberíamos más bien denominar tasa de transmisión de datos, por ejemplo “mi conexión a Internet tiene 1 Mbps de ancho de banda”, lo que significa que ésta puede transmitir datos a 1 megabit por segundo. [1]

2.1.3. Ondas Electromagnéticas

La forma de propagación de las ondas electromagnéticas se genera por la aceleración de una carga eléctrica. Estas viajan a una velocidad cercana a los 300.000 km/s, sin embargo cuando esta viaja a través de la materia las velocidades que alcanza son mucho menores, a mayor densidad menor velocidad. [1]

La radiación electromagnética se propaga por el universo como ondas interactivas de campos eléctricos y magnéticos; y se puede ordenar en un espectro que va desde ondas de frecuencias elevadas hasta ondas con frecuencia muy bajas.

Existe una división del espectro de frecuencias que fue establecida por el

Consejo Consultivo Internacional de las Comunicaciones de Radio (**CCIR**) en el año 1953. [13]

2.1.4. Polarización

Es aquel fenómeno que se produce cuando el campo eléctrico oscila solo en un plano determinado, denominado plano de polarización. Este plano puede definirse por dos vectores, uno de ellos paralelo a la dirección de propagación de la onda y otro perpendicular a esa misma dirección el mismo que indica la dirección del campo eléctrico.

2.1.5. Tipos de Polarización

Como se describió anteriormente la polarización está definida por la trayectoria que describe el campo eléctrico o magnético sobre un plano, en función de esto la polarización se clasifica en: polarización lineal, circular, elíptica. En el siguiente grafico se ilustra de mejor manera dicha clasificación, en donde el campo eléctrico está representado por el color azul, los componentes X, Y por el color rojo y verde, el eje vertical representa el tiempo, y el color púrpura es la trayectoria que describe el vector en el plano.

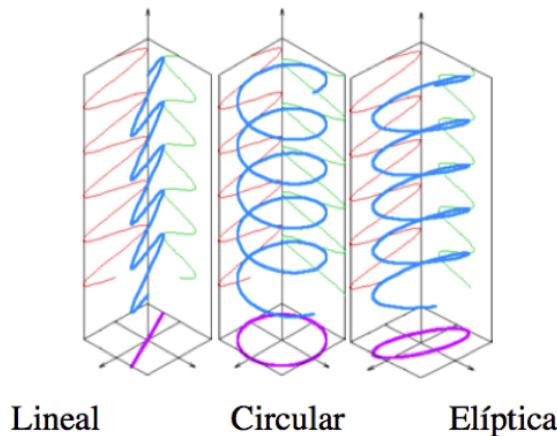


Figura 2.2: Tipos de Polarización [2]

2.1.6. Usos de la Polarización

Cada vez que se realiza un radioenlace, necesitamos el uso de antenas para conseguir un mayor alcance para la señal a emitir, sin embargo, en el momento de instalarlas nos encontramos con la posibilidad de elegir entre una polarización horizontal o vertical, la diferencia está prácticamente que cuando se alineada verticalmente (el trozo de alambre recto), los electrones solo se mueven de arriba a abajo, no hacia los lados (porque no hay lugar hacia donde moverse) y por consiguiente los campos eléctricos solo apuntan hacia arriba o hacia abajo verticalmente. El campo que abandona el alambre y viaja como una onda tiene una polarización estrictamente lineal (y en este caso vertical). Por otra parte la polarización horizontal tendremos un movimiento de los electrones de izquierda a derecha, por lo tanto el campo que abandona el alambre viaja como una onda con polarización lineal horizontal. Cabe señalar que cuando se alinean dos antenas, así consigamos los mejores niveles de señal, y si estas no se encuentran polarizadas correctamente, no podremos transmitir información por el enlace

2.1.7. Características fundamentales de las ondas de radio

El comportamiento de las ondas dependerá del medio de transmisión, del tipo de información que se desee enviar, y de los equipos a utilizar. En resumen las características principales de las ondas de radio son:

- La distancia que pueden llegar a recorrer, ya que dependerá de la potencia del equipo transmisor.
- La cantidad de información que se podrá transmitir, esto dependerá de la cantidad de ondas que puedan entrar en un periodo de un segundo (frecuencia). Cuanto más rápida sea la oscilación o ciclo de la onda, mayor cantidad de información puede transportar.
- Cuanto más corta sea la onda más alta será su frecuencia.
- Las ondas con longitudes de onda más larga tienden a viajar más lejos que las que tienen longitudes de onda más cortas.
- Las ondas más largas rodean los obstáculos. La distancia que una onda puede viajar depende de la relación entre la longitud de onda de la misma y el tamaño de los obstáculos en su camino de propagación.

2.1.8. Reflexión Y Refracción De Ondas

Si bien es cierto las ondas electromagnéticas pueden viajar en el vacío, pero por lo general estas se propagan por un medio que puede ser elástico u homogéneo. Cuando las ondas viajan a través de un medio inicial, su trayectoria se ve afectada, produciéndose así los efectos conocidos como reflexión, refracción y dispersión de ondas.

2.1.9. Reflexión y Transmisión

Cuando una onda viaja, y esta se encuentra con otro tipo de superficie, la mayor parte de la onda incidente que se refleja sobre dicha superficie se conoce como reflexión. La reflexión puede ser de dos tipos: especular cuando la superficie de incidencia es lisa (el ángulo de incidencia es igual al reflejado), y difusa cuando la superficie de incidencia tiene imperfecciones. La reflexión y transmisión de perturbaciones oscilatorias es común tanto a las ondas mecánicas como a la luz y ondas electromagnéticas.

Las dos leyes que resumen el fenómeno de la reflexión con respecto al medio de separación son:

- (I) Cada rayo de la onda incidente y el rayo correspondiente de la onda reflejada están contenidos en un mismo plano, que es perpendicular a la superficie de separación entre los dos medios en el punto de incidencia.
- (II) El ángulo que forman el rayo incidente y el rayo reflejado con la recta perpendicular a la frontera son iguales. Estos ángulos se conocen, respectivamente, como ángulo de incidencia y ángulo de reflexión. Es decir, los rayos incidentes y reflejados se encuentran en el mismo plano, que es perpendicular al de incidencia, y forman un mismo ángulo con la normal en el punto de incidencia.

2.1.10. Refracción

Durante la transmisión de una onda cuando esta se encuentra con un segundo medio, parte de la onda se refleja, y resto es absorbida por el segundo medio (onda refractada), a este fenómeno se conoce con el nombre de refracción, resumiendo tenemos que la refracción se rige por dos leyes principales:

- (I) Cada rayo de la onda incidente y el rayo correspondiente de la onda refractada forman un plano que es perpendicular a la superficie de separación entre los medios en el punto de incidencia.

$$\alpha_i = \alpha_r$$

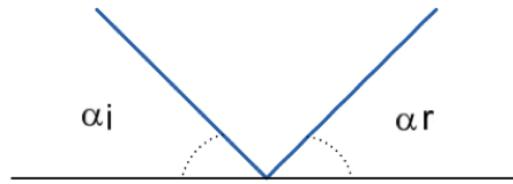


Figura 2.3: Rayo incidente y reflejado [2]

- (II) El ángulo que forma el rayo refractado con la normal, llamado ángulo de refracción, está relacionado con el ángulo de incidencia por una formula denominada ley de Snell, (1580-1626). Expresada matemáticamente esta ley indica que: los rayos incidentes y refractados están situados en un mismo plano, que es perpendicular al de la superficie de separación entre los medios. Los ángulos que determinan la dirección de propagación guardan entre sí una relación regida por la ley de Snell. [14]

$$n_1 \operatorname{sen} \alpha_i = n_2 \operatorname{sen} \alpha_r$$

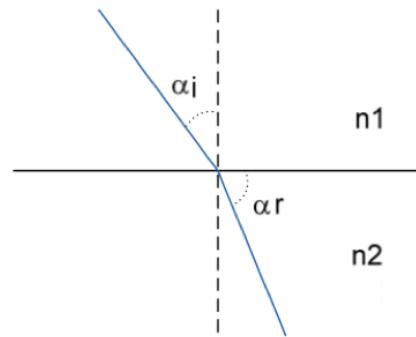


Figura 2.4: Rayo incidente y refractado [2]

2.1.11. Dispersión

La velocidad de la luz en un medio dado depende de la longitud de onda. De este modo, al incidir sobre una superficie de separación con un mismo ángulo de incidencia, se refracta con un ángulo de refracción diferente para cada longitud de onda (y, por tanto, para cada frecuencia, que determina el color). Así, si se hace incidir un haz de luz blanca sobre una superficie de separación, cada color de la luz se refracta con un ángulo diferente, para formar un efecto de arco iris. Este fenómeno se denomina dispersión de la luz.

2.1.12. Difracción

Difracción es el comportamiento de las ondas cuando al incidir en un objeto dan la impresión de doblarse. Es el efecto de ¿ondas doblando las esquinas?. Imagine una onda en el agua viajando en un frente de onda plana, tal como una ola llegando a una playa oceánica. Ahora ponemos en su camino una barrera sólida, como una cerca de madera, para bloquearla. Luego practicamos una estrecha rendija en esa pared, como una pequeña puerta. Desde esta abertura va a comenzar una onda circular, y por supuesto va a alcanzar puntos que están en una línea directa detrás de esa abertura, pero también a ambos lados de ella. Si miramos este frente de onda, y pudiera ser también una onda electromagnética, como un haz de luz, sería difícil explicar cómo logra alcanzar puntos que están ocultos por una barrera. Este fenómeno se puede apreciar mejor en la siguiente figura:

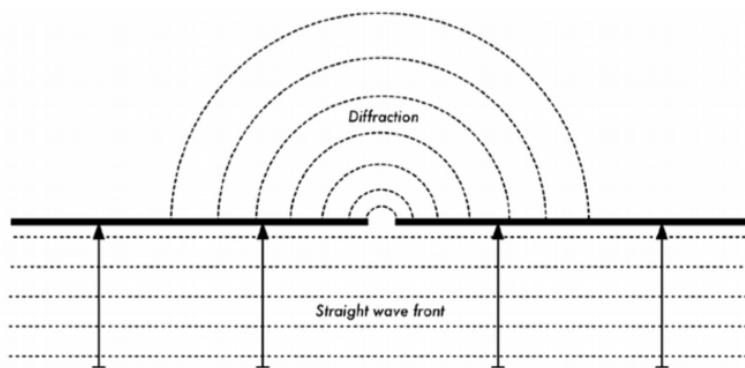


Figura 2.5: Difracción a través de una ranura pequeña [1]

Se debe tener en cuenta que en la difracción se genera una pérdida de po-

tencia, la potencia de la onda difractada es significativamente menor que el frente de onda que la provoca. Pero en algunas aplicaciones muy específicas, se puede aprovechar el efecto de difracción para rodear obstáculos. Interferencia de ondas electromagnéticas

Es fenómeno se produce cuando dos ondas de la misma frecuencia avanzan más o menos en la misma dirección y tienen una diferencia de fase que permanece constante en el transcurso del tiempo, pueden combinarse de tal manera que su energía no se distribuye uniformemente en el espacio, sino que es máxima en ciertos puntos y mínima en otros Los múltiples sistemas

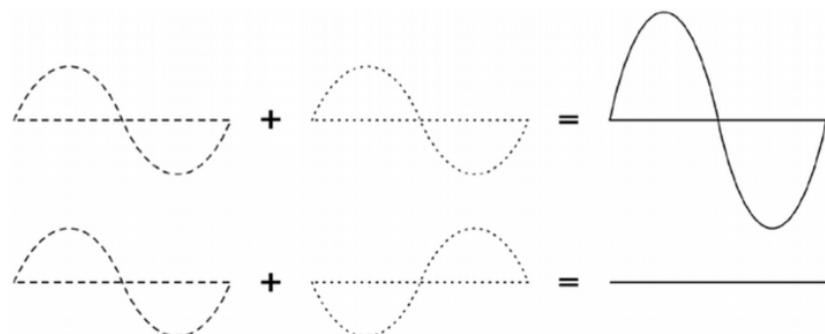


Figura 2.6: Interferencia de ondas: constructiva (izquierda) y destructiva (derecha) [1]

radio eléctricos existentes en nuestro medio operan sobre un único rango de frecuencias, y para poder tener acceso a él es necesario obtener un permiso previo de la entidad encargada de administrar el espectro en cada país. Los sistemas radioeléctricos actuales pueden soportar varias interfaces permitiendo incorporar diferentes equipos de radioenlaces a una red ya instalada. La información de un sistema de radioenlaces se difunde desde un transmisor hacia un receptor por medio de una frecuencia fija.

2.1.13. Transmisión y Recepción

Para conseguir la propagación de las ondas electromagnéticas, se sigue todo un proceso que inicia en el emisor cuya función es la de producir una onda portadora, en donde características son modificadas dependiendo del tipo de señal a transmitir, una vez que se ha propagado la onda a través de una frecuencia fija, el receptor capta la onda y la desmodula con el fin de obtener así la señal original.

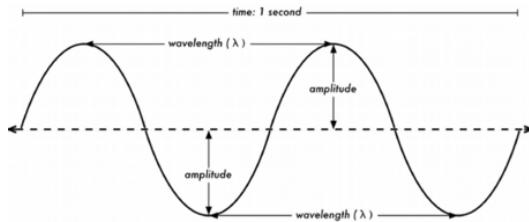


Figura 2.7: Longitud de onda, amplitud, y frecuencia [1]

En el sistema de modulación de amplitud (**AM**), la señal (de baja frecuencia) se superpone a la amplitud de ondas hertzianas portadora (de alta frecuencia). En el sistema de modulación de frecuencia (**FM**), la amplitud de la onda portadora se mantiene constante, pero la frecuencia varía según la cadencia de las señales moduladoras. Este sistema permite eliminar parásitos e interferencias, y reproduce el sonido con mayor fidelidad.

2.1.14. Usos de la radiofrecuencia

Originalmente los sistemas de radiofrecuencia se utilizaron para la comunicación naval, hoy en día, este término abarca muchas más aplicaciones entre las cuales se incluye las redes inalámbricas, comunicaciones móviles de todo tipo, y la radiodifusión. A continuación describiremos más detalladamente en que aplicaciones se usa los sistemas de radio frecuencia.

- Audio
 - Transmisión voz y servicios interactivos con el sistema de radio Digital
 - Servicios civiles y militares en alta frecuencia (HF) en la banda de Onda Corta, para comunicación con barcos en alta mar y con poblaciones o instalaciones aisladas y a muy largas distancias.
 - Sistemas telefónicos celulares digitales para uso cerrado (policía, defensa, ambulancias, etc.) Distinto de los servicios públicos de telefonía móvil.
- Telefonía
- Video
- Navegación

- Servicios de emergencia
- Transmisión de datos por radio digital

2.1.15. Características y tipos de enlaces

Una vez conocido como se propaga las ondas en nuestro medio, debemos tener en cuenta algunas características con respecto a un enlace inalámbrico, desde que es, como funciona, y hasta los factores que debemos considerar para establecer un enlace.

2.1.16. Propagación radioeléctrica

La propagación a través del espacio dependerá de la superficie de la tierra, su forma y su constitución (mar, tierra cultivada, desierto, etc.), y la atmósfera, tanto la troposfera como la ionosfera.

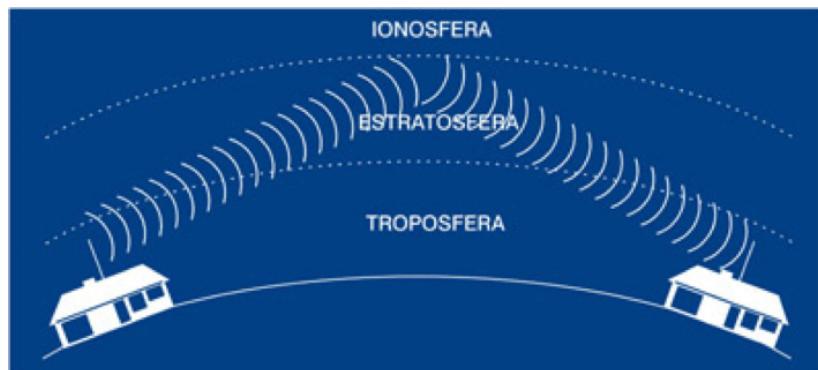


Figura 2.8: Propagación de las ondas sobre la superficie terrestre [3]

Cuando la señal se transmite esta viaja en todas direcciones, aunque la energía sigue la curvatura de la tierra, es decir que la propagación está relacionada directamente con la banda de frecuencia en la que se trabaja.

- En frecuencias inferiores a 30 **KHz**, existe un mecanismo de propagación por guía-ondas tierra ionosfera.
- En frecuencias desde 10KHz y hasta 3 **MHz** el principal mecanismo de propagación utilizado es la onda de superficie.
- En frecuencias por encima de 3 MHz (1 MHz) y hasta unos 30 MHz el mecanismo fundamentalmente utilizado es la onda ionosférica. Por

reflexión ionosférica se consiguen enlaces de hasta 4000 Km en un solo salto, y más por múltiples reflexiones ionosfera tierra (mar).

- En frecuencias por encima de unos 30 MHz, el principal mecanismo es la onda espacial. Debido a la curvatura de la superficie terrestre, a partir del horizonte el mecanismo posible de propagación son las ondas difractadas, que a estas frecuencias tienen alcances muy pequeños.
- A partir de 40 o 50 MHz la ionosfera no refleja las ondas electromagnéticas por lo que puede utilizarse para comunicaciones extraterrestres.

2.1.17. Sistemas de radiocomunicaciones inalámbricas

La comunicación inalámbrica inicio con la postulación de las ondas electromagnéticas por James Clerk Maxwell (1860), la demostración de la existencia de estas ondas fueron confirmadas por Heinrich Rudolf Hertz (1880), y con la invención del telégrafo inalámbrico por Guillermo Marconi. Pero no fue sino hasta el año de 1896 en donde se concedió la primera patente de comunicaciones inalámbricas a Guillermo Marconi en el Reino Unido. Desde aquel momento, entonces el número de desarrollos en el campo de las comunicaciones inalámbricas tomaron ese sitio. La comunicación inalámbrica fue un suceso novedoso y muy importante ya que este permitió cruzar barreras a la que las conexiones guiadas nos mantenían atadas, especialmente por las distancias que se podía conseguir con estas. [15]

Un enlace inalámbrico es aquel que no necesita de un medio guiado para la transmisión de información, este presenta grandes ventajas frente a la conexión por cable, ya que su instalación puede llegar a lugares geográficos imposible para una red cableada, con la facilidad de transportar datos y voz. En la actualidad las redes inalámbricas ofrecen igual o hasta mejor confiabilidad, calidad y velocidad en comparación con algunas conexiones de Internet vía satélite, estos enlaces se realizan desde un punto donde existe la posibilidad de contratar un acceso a Internet hasta el punto donde sea necesaria dicha conexión.

2.1.18. Línea de vista directa

El término línea vista, a menudo abreviada como LOS (por su sigla en inglés, Line of Sight), es fácil de comprender cuando se habla acerca de la luz visible, si podemos ver un punto B desde un punto A donde estamos, tenemos línea de vista directa. La línea visual que necesitamos para tener una conexión inalámbrica optima desde un punto A hasta otro B, es más que

simplemente una línea delgada, su forma es más bien la de un cigarro, un elipsoide. Su ancho puede ser descrito por medio del concepto de zonas de Fresnel.

2.1.19. La Zona de Fresnel

La teoría exacta de las zonas de Fresnel es algo complicada. Sin embargo el concepto es fácilmente entendible, se sabe por el principio de Huygens que por cada punto de un frente de onda comienzan nuevas ondas circulares, por ende se sabe que los haces de microondas se ensanchan. También que las ondas de una frecuencia pueden interferir unas con otras. La teoría de zona de Fresnel simplemente examina a la línea desde A hasta B y luego al espacio alrededor de esa línea que contribuye a lo que está llegando al punto B. Algunas ondas viajan directamente desde A hasta B, mientras que otras lo hacen en trayectorias indirectas. Consecuentemente, su camino es más largo, introduciendo un desplazamiento de fase entre los rayos directos e indirectos. Siempre que el desplazamiento de fase es de una longitud de onda completa, se obtiene una interferencia constructiva, las señales se suman óptimamente. Tomando este enfoque, y haciendo los cálculos, se encuentra con que hay zonas anulares alrededor de la línea directa de A hacia B que contribuyen a que la señal llegue al punto B. Se debe tener en cuenta que existen muchas zonas de Fresnel, pero para este caso interesa principalmente la zona 1. Si ésta fuera bloqueada por un obstáculo, por ejemplo un árbol o un edificio, la señal que llegue al destino lejano será atenuada. Entonces, cuando se planea enlaces inalámbricos, se debe estar seguro de que esta zona va estará libre de obstáculos. En la práctica de redes inalámbricas ya se puede trabajar con que al menos el 60 por ciento de la primera zona de Fresnel esté libre. [16]

La siguiente ecuación es la fórmula para calcular la primera zona de Fresnel:

$$r = 17,31 * \sqrt{((d1 * d2) / (f * d)))} \quad (2.1)$$

Donde r es el radio de la primera zona en metros, d1 y d2 son las distancias desde el obstáculo a los extremos del enlace en metros, d es la distancia total del enlace en metros, y f es la frecuencia en MHz. Note que esta fórmula calcula el radio de la zona. Para calcular la altura sobre el terreno, debe sustraerse este resultado de una línea trazada directamente entre la cima de las dos torres.

2.1.20. Energía

La potencia P es clave para lograr que los enlaces inalámbricos funcionen, se necesita cierto mínimo de potencia para que el receptor le dé sentido a

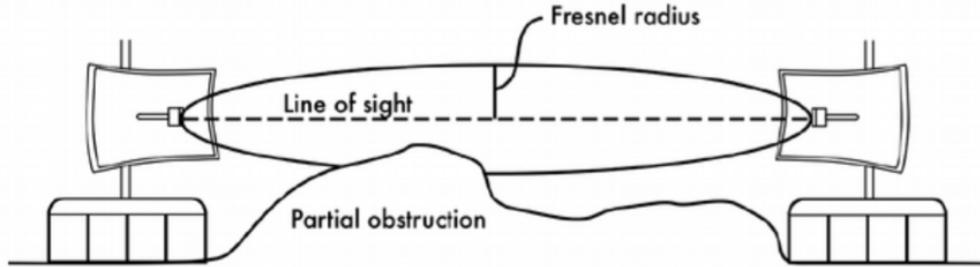


Figura 2.9: La zona de Fresnel está bloqueada parcialmente en este enlace aunque la línea visual (line of sight) no está obstruida [1]

la señal. Ahora vamos a discutir brevemente cómo se define y calcula la potencia P . El campo eléctrico se mide en V/m , la potencia contenida en él es proporcional al campo eléctrico al cuadrado, expresado en la ecuación.

$$P \approx E^2 \quad (2.2)$$

En la práctica, se mide la potencia por medio de algún tipo de receptor, por ejemplo una antena y un voltímetro, un medidor de potencia, un osciloscopio, o inclusive una tarjeta inalámbrica y una computadora portátil. La potencia es proporcional al cuadrado del voltaje de la señal.

2.1.21. Cálculo en dBs

La técnica sin duda más importante para calcular la potencia es por decibeles (dB). No hay física nueva en esto, es solamente un método conveniente que hace que los cálculos sean muy simples. El decibel es una unidad sin dimensión, es decir, define la relación entre dos medidas de potencia. Se define como en la ecuación:

$$dB = 10 * \log(P1/P0) \quad (2.3)$$

Donde $P1$ y $P0$ pueden ser de los dos valores cualesquiera que se quiere comparar. Típicamente, en este caso, se tratará de potencia. Aquí hay algunos valores utilizados comúnmente que es importante recordar:

- +3 dB = doble potencia

- -3 dB = potencia media
- +10 dB = orden de magnitud (10 veces la potencia)
- -10 dB = un décimo de potencia

Además de los dBs a dimensionales, hay cierto número de definiciones relacionadas que están basadas en una referencia P0 fija. Los más relevantes para nosotros son:

- dBm relativo a P0 = 1 mW
- dBi relativo a una antena isotrópica ideal

Una antena isotrópica es una antena hipotética que distribuye uniformemente la potencia en todas direcciones. La antena que más se aproxima a este concepto es el dipolo, pero una antena isotrópica perfecta no puede ser construida en la realidad. El modelo isotrópico es útil para describir la ganancia de potencia relativa de una antena real.

2.1.22. Ventajas de un enlace inalámbrico

A continuación se da a conocer algunas ventajas de este tipo de redes permitiendo comprender cuál es su alcance real.

- Accesibilidad: en la actualidad existen equipos que permiten enlazar zonas geográficas imposibles de llegar con una red cableada, o que simplemente resultaría costoso, permitiendo a un usuario final tener acceso a esta red, siempre y cuando se encuentre dentro del área de cobertura, lugar en donde se encuentran los equipos de difusión.
- Movilidad: especialmente para los usuarios que disponen de una línea celular, permitiéndoles acceder a la red, cuando este en movimiento y desde cualquier lugar siempre y cuando este en un lugar en donde haya cobertura.
- Productividad: El poder tener acceso a la información permite disminuir la brecha digital existente en algunos sectores. El Internet en la actualidad es una herramienta fundamental en cada negocio, porque esta no solo permite establecer una comunicación, sino que también la mayoría de transacciones se las hace a través del internet.

- Fácil Instalación: El hecho de no utilizar un medio guiado, la instalación se la puede realizar en un tiempo más corto, y por ende resultará más rentable.
- Escalabilidad: A medida que una empresa crece, necesita también ampliar su cobertura, como es el caso de los I.S.P. que generalmente su área de cobertura no se ve limitado, y conforme crecen pueden expandirse a otros sectores, con solo establecer el nuevo punto de enlace para poder llegar con el servicio al usuario que lo necesite.
- Seguridad: Las instalaciones inalámbricas son fáciles de monitorear, y por ende poseen seguridades sólidas, permitiendo únicamente al personal capacitado, poder acceder a estas.
- Costos: Con una red inalámbrica se puede reducir los costes, ya que se eliminan o se reducen los costes de cableado durante los trasladados configuraciones o expansiones.

2.1.23. Estructura de un radio enlace

Un radio enlace está constituido por estaciones terminales y repetidoras intermedias, con equipos transceptores, antenas y elementos de supervisión y reserva. Además de las estaciones repetidoras, existen las estaciones nodales donde se desmodula la señal y de la baja a banda base y en ocasiones se extraen o se insertan canales. Al tramo terminal estación nodal se lo denomina sección de conmutación y es una entidad de control, protección y supervisión. En cuanto a los repetidores se los puede clasificar en activos o pasivos.

- Activos: En ellos se recibe la señal en la frecuencia de portadora y se la baja a una frecuencia intermedia (FI) para amplificarla y retransmitirla en la frecuencia de salida. No hay demodulación y son transceptores.
- Pasivos: Se comportan como espejos que reflejan la señal y se los puede dividir en pasivos convencionales, que son una pantalla reflectora y los pasivos back-back, que están constituidos por dos antenas espalda a espalda. Se los utiliza en ciertos casos para salvar obstáculos aislados y de corta distancia.

Los enlaces son estructuralmente sistemas en serie, de tal manera que si uno falla se pierde la comunicación a través de la red. Por ello se le exige los equipos en cada nodo posean una alta disponibilidad y confiabilidad. Esto también implica que utilicen sistemas de supervisión y control de alto rendimiento para detectar fácilmente una falla en el sistema. Conceptos de diseño

Radiofrecuencia, su historia, sus protocolos de señalización

Como se mencionó anteriormente la forma de garantizar el correcto funcionamiento del enlace es necesario que entre dos puntos a conectar exista línea de vista directa, es decir que entre el enlace exista una altura libre de obstáculos para la adecuada propagación en toda época del año, tomando en cuenta las variaciones de las condiciones atmosféricas de la región. Para poder calcular las alturas libres debe conocerse la topografía del terreno, así como la altura y ubicación de los obstáculos que puedan existir en el trayecto. El diseño de un radio enlace se puede resumir en los siguientes pasos:

- Definir el modo de transmisión, es decir en condiciones de visibilidad directa, este puede ser punto a punto o transmisión omnidireccional.
- Tener en cuenta los diferentes factores que pueden degradar nuestra señal como por ejemplo el ruido.
- El alcance deseado dependerá especialmente de la potencia de los equipos a transmitir.
- Tener en cuenta bajo qué condiciones se producirá las pérdidas o atenuación de la señal.

Una vez analizado la parte técnica, para la implementación del enlace se debe considerar:

- Elección del sitio de instalación.
- Relevamiento del perfil del terreno y cálculo de la altura del mástil para la antena.
- Cálculo completo del radio enlace, estudio de la trayectoria del mismo y los efectos a los que se encuentra expuesto.
- Prueba posterior a la instalación del radio enlace, y su posterior puesta en servicio con tráfico real.

2.1.24. Enlaces Punto - Punto

Las redes punto a punto son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos. En una red punto a punto, los dispositivos en red actúan como socios iguales, o pares entre sí. Los enlaces que interconectan los nodos de una red punto a punto se pueden clasificar en tres tipos según el sentido de las comunicaciones que transportan:

- Simplex: La transacción sólo se efectúa en un solo sentido.
- Half-dúplex: La transacción se realiza en ambos sentidos, pero de forma alternativa, es decir solo uno puede transmitir en un momento dado, no pudiendo transmitir los dos al mismo tiempo.
- Full-Dúplex: La transacción se puede llevar a cabo en ambos sentidos simultáneamente.

Cuando la velocidad de los enlaces Semi-dúplex y Dúplex es la misma en ambos sentidos, se dice que es un enlace simétrico, en caso contrario se dice que es un enlace asimétrico. Los enlaces punto - punto pueden conseguir un

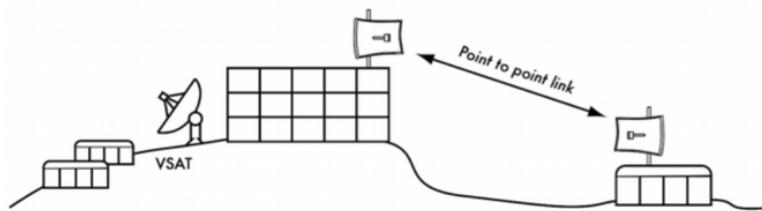


Figura 2.10: Enlace Punto - Punto [1]

mayor alcance utilizando antenas de grilla o plato tanto en el receptor como en el transmisor, permitiendo expandir a una red de forma fácil y rápida. La velocidad de transferencia conseguida con estos tipos de enlaces tiene un promedio 20Mbytes, sin ninguna dificultad.

2.1.25. Enlaces Punto - Multipunto

El enlace punto a multipunto es la versión del punto a punto para la conexión rápida y fiable de más de dos instalaciones. Para reducir costes, este sistema consta de una instalación central dotada de una antena multidireccional, a la que apuntan las antenas direccionales del resto de centros. Esto permite una capacidad igual a la del punto a punto, pero extensible hasta a 16 centros. Algunas de las aplicaciones de este tipo de redes permiten:

- Mantener una constante comunicación con las diferentes sucursales de una empresa, permitiéndome compartir base de datos, acceso, etc.
- Implementar redes de voz sobre IP, permitiéndome reducir costos de llamadas entre sucursales.

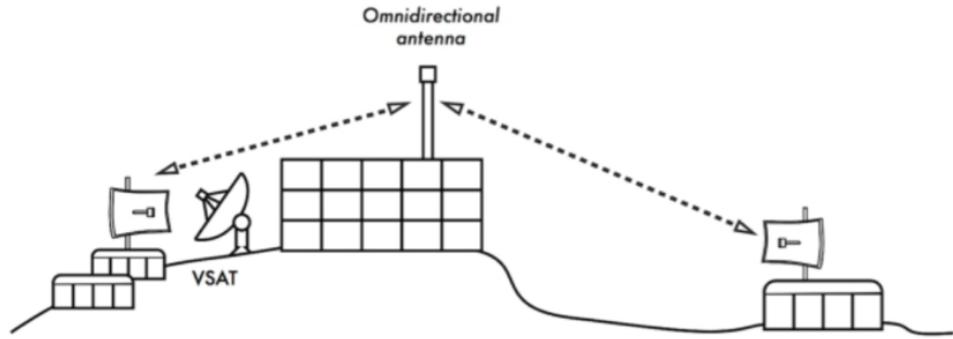


Figura 2.11: Enlace Punto Multipunto [1]

- Venta de acceso a Internet (I.S.P.).
- Monitoreo a través de cámaras de vigilancia.

2.1.26. Conexión De Rejilla O Malla

La siguiente configuración es una consecuencia de las dos anteriores usada especialmente en redes inalámbricas privadas. Es configuración conocida como rejilla o malla en donde cada punto o nodo puede trasmitir a cualquier otro que esté disponible o accesible. Esta configuración es muy flexible ya que permite a un nodo trasmitir a otro vía cualquier otro nodo.

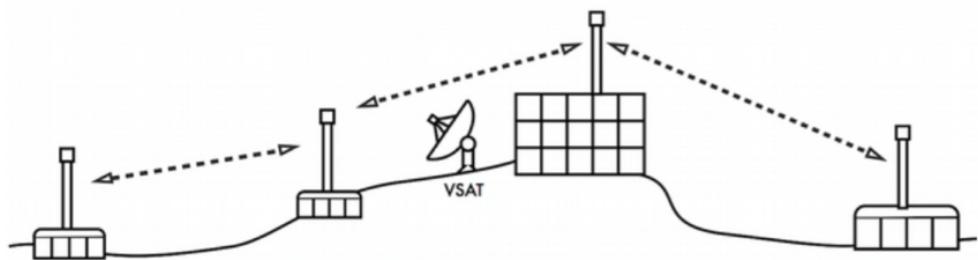


Figura 2.12: Conexión Malla [1]

2.1.27. Distribución De Acceso Inalámbrico (HotSpot)

La distribución HotSpot, no es un tipo de enlace, sino más bien parte de uno. El HotSpot consiste en puntos de conexión en zonas públicas o privadas como aeropuertos, parques, institutos educativos, restaurantes, etc., permitiendo que el usuario que disponga de un equipo WIFI acceda al internet banda ancha. Los HotSpots permiten que el acceso inalámbrico sea una realidad mucho más compleja y extensible que el Internet que hoy se conoce. No se trata solo de estar en un lugar físicamente y poder conectarte a la Red sin el cable, es mucho más. El concepto lleva a que Internet, la oficina, la empresa, se va con el usuario, por lo que se puede arriesgar a pensar en una incursión similar a la del móvil.

2.1.28. Sistemas de microondas

El control de tráfico aéreo, navegación marina, control de misiles, aviación, telecomunicaciones, son algunas de las aplicaciones de las microondas, en la actualidad las frecuencias de microondas son utilizadas cada vez más en telecomunicaciones, cuando se utilizan antenas repetidoras, necesarias a lo largo de un camino o trayecto de comunicación. Las microondas comprenden frecuencias que trabajan en el rango de los 109 a 1012 Hertz, que corresponden a longitudes de onda que van de los 30 cm. (centímetros) a 0.3 mm. (Milímetros). Estas longitudes de onda son del mismo orden de magnitud que las dimensiones de los circuitos empleados en su generación. La transmisión en un sistema de microondas se utiliza para cubrir distancias mayores, el receptor recibe la señal enviada por un transmisor en una frecuencia inicial, la convierte a sus propiedades eléctricas y la retransmite a otra estación de microonda, en algunos casos puede hacerlo cambiando de frecuencia para retransmitir. [17]

2.1.29. Radiocomunicaciones por satélite

Podemos definir a la comunicación por satélite como: “un repetidor radioeléctrico ubicado en el espacio, recibe señales generadas en la tierra, las amplifica y las vuelve a enviar a la tierra”. Un satélite ofrece grandes ventajas con respecto a otros sistemas, entre los más importantes está mayor potencia de transmisión y mayor área de cobertura. La transmisión por satélite se ha utilizado comúnmente en nuestro medio, para comunicaciones de larga distancia, y comunicaciones internacionales transatlánticas. Pero el elevado costo que implica el disponer de una estación terrestre, equipos electrónicos para la conexión satelital, ocasionan que el usuario opte por otro medio de co-

municación como la microonda, fibra ópticas, radioenlaces, etc., cuyos costos de instalación son mucho menores cada día, mientras que los costos para un enlace satelital se mantienen siempre elevados. Con los sistemas por satélite se dispone de gran cantidad de ancho de banda puesto que el espectro de frecuencias puede asignarse a una base de acceso fijo o bajo demanda. Puesto que la señal se debe transmitir al satélite situado a 22300 millas, el costo de alquiler de un canal no es sensible a la distancia, por lo que las ventajas que presentan los satélites en el momento de transmisión, pesan más que los inconvenientes que ocasionan.

Con respecto a las desventajas, cabe citar el elevadísimo costo inicial, el cual solo podría ser afrontado mediante la gestión de grandes emprendimientos, aunque puede considerarse que no constituye obstáculo insalvable, sino que el principal inconveniente estaría dado en la necesidad de tomar una decisión política a través de la cual, se superen intereses sectoriales y contradictorios en lo que atañe a este tema, y se implemente definitivamente el sistema teniendo en miras fundamentalmente el bien de toda la comunidad. [18]

2.1.30. Red Privada

Las redes de datos interconectaban, en un principio en forma local, las computadoras personales de una organización, permitiendo compartir la información, y el trabajo en grupo de una forma más ágil y eficiente. Sin embargo esto requirió considerar el aspecto de la seguridad, ya que si bien se trabajaba en un mismo ámbito, es decir dentro de la misma empresa, no todos los usuarios debían acceder a los datos por igual. Este esquema funcionó para pequeñas organizaciones, pero para aquellas cuyas estructuras, incluida sitios geográficamente alejados, surgió la necesidad de interconectar también dichos lugares.

La solución vino de la mano de los proveedores de servicio de red de área amplia de datos o **Wide Area Network (WAN)**, a través de la contratación de enlaces dedicados, los cuales conectaban las redes distantes con la red central. Esta solución implicaba un costo, que resultó prohibitivo para la mayoría, excepto para aquellos que podían abonar un costo fijo de contratación más un valor que variaba proporcionalmente a la distancia existente entre los sitios a interconectar (mile-age fee). En la actualidad existen tecnologías WAN (Frame Relay, ATM) donde el costo está en función del caudal de datos o ancho de banda comprometido del enlace, que una organización está dispuesta a pagar, sin considerar ya la distancia geográfica. De esta forma se cuenta con una red privada o estructura de comunicación propia, en el sentido de que el control y la administración de la red están bajo el dominio de la orga-

nización. Las políticas de uso, los servicios suministrados, los medios activos y pasivos de comunicación por donde fluyen los datos están bajo un control propio. Si bien las comunicaciones de área amplia son suministradas por un proveedor, este se compromete a respetar los requerimientos de la organización cliente, además, los datos que atraviesan su red, no estarán al alcance de otros clientes.

2.1.31. Red Pública

Uno de los eventos más importantes que acompañó al desarrollo de las redes en las organizaciones, fue la rápida evolución de la mayor de las redes IP existentes, Internet. Esta se define como un sistema cooperativo de interconexión de redes que suministra un servicio de comunicación universal. De esta manera satisface la necesidad de los usuarios de comunicar dos puntos cualesquiera, también denominados sistemas o nodos finales, pudiendo acceder a recursos más allá de los disponibles en un único sistema y ubicados fuera de los límites de la red local. Los datos atraviesan redes intermedias hasta llegar a su destino, en una operación no orientada a la conexión, mediante el uso de equipos especiales denominados routers, también conocidos como sistemas o nodos intermedios. La naturaleza no orientada a la conexión de Internet, significa que no hay una ruta preestablecida o circuito virtual dedicado entre los sistemas que se comunican, tampoco niveles de servicio, priorización o separación de tráfico que puedan aplicarse a los datos que se transmiten.

La función de los routers es interconectar al menos dos redes, transfiriendo paquetes desde una red a otra. Estas pertenecen a diversas organizaciones y proveedores. Esto convierte a Internet en una red pública, en el sentido de que son muchos los que participan en su conformación y los medios de transmisión son compartidos. Dependerá de quien utilice la infraestructura de Internet para comunicar dos sistemas finales, tomar las medidas de seguridad apropiadas para asegurar la confidencialidad, autenticidad, integridad y no repudio de los datos transmitidos. [4]

2.1.32. Red Privada Virtual

El funcionamiento de algunas organizaciones, determinaron la necesidad de permitir el acceso a la red propia a usuarios que se encontraban geográficamente fuera de los límites de ésta. Éstos requerían desplazarse con frecuencia y en algún momento acceder a sus archivos en la red local, revisar su correo electrónico o utilizar un sistema de información. En un principio se utilizaron servicios de acceso remoto mediante la implementación de servidores para tal

Radiofrecuencia, su historia, sus protocolos de señalización

fin o RAS (Remote Access Server), el uso de líneas discadas para la conexión y pools de módems para atender las llamadas. Toda esta infraestructura era costeada por la organización la cual era responsable de su administración y mantenimiento. Si bien se solucionaba el problema de acceso a la red local, se lograba a un costo económico alto.

Otra necesidad fue la de encontrar una alternativa más económica de interconectar diversas redes entre sí y ya no solamente las de una misma organización, sino redes de diferentes organizaciones. Razones de política estratégica justificaban este desafío, ya sea a nivel empresarial, universitario o gubernamental. Ambos requerimientos tuvieron su solución a partir de la idea de utilizar Internet, teniendo en cuenta su alcance global y su capacidad de entrega de datos a casi cualquier sistema final a un bajo costo. Dado que se utiliza Internet para transmitir datos, no hay garantía de que estos no puedan ser captados por terceros. También es claro que los sistemas finales que se comunican están expuestos.

En la actualidad no solo se considera a Internet como medio donde una organización puede implementar una VPN. Los proveedores de servicios de comunicaciones o SP (Service Provider) ofrecen servicios de VPN de acuerdo a las necesidades del cliente a través de su red backbone. Un SP puede administrar múltiples VPNs pertenecientes a varios clientes operando a través de su backbone.

Capítulo 3

Definición de VPN

Es habitual encontrar varias definiciones sobre VPN, aunque éstas no difieren en esencia. Algunas de ellas pueden ser:

- “Una VPN es una red privada construida dentro de una infraestructura de red pública, como la red Internet”
- “La idea básica de una VPN es muy simple. Una corporación podría tener un número de oficinas (o grupos de ellas) en diferentes lugares, y en cada uno de estos tener su propia red local. Muchas corporaciones han aumentado la cantidad de empleados que deben trabajar en forma remota, ya sea desde sus hogares o en forma itinerante. Interconectar estas redes y lugares mediante una red compartida (no privada) crea una VPN”
- “Una red privada virtual basada en Internet utiliza la infraestructura abierta y distribuida de Internet para transmitir datos entre sitios corporativos”
- “Una red privada virtual es una red privada de datos que utiliza una infraestructura de telecomunicación pública, manteniendo la privacidad mediante protocolos de túnel y procedimientos seguros. El propósito principal de una VPN es dar a la compañía la misma capacidad que otorgan los enlaces dedicados contratados pero a un costo menor, utilizando medios de comunicación públicos.”

Se puede definir a una VPN de manera más formal. Esta definición aparece publicada en el artículo *What Is a VPN? Part 1* escrito por Ferguson y Houston para la publicación mensual The Internet Protocol Journal de Cisco System en Marzo de 2001: “*Una VPN es un ambiente de comunicaciones en el cual existe un control de acceso, para permitir la conexión entre sistemas*

pares únicamente dentro de una comunidad de interés definida, y está creado considerando alguna forma de participación de un medio de comunicación subyacente, donde este brinda servicios a la red de una forma no exclusiva.” De acuerdo a estas definiciones se puede decir que una red privada virtual es una red, que comunica dos o más dispositivos finales (estos a su vez pueden interconectar una red completa) que pueden estar ubicados geográficamente distantes y representan una comunidad de interés. Para esto se utiliza como medio de transmisión una estructura compartida común a varios usuarios. Ésta puede ser Internet o la red principal o backbone de un proveedor de servicios de comunicaciones.

Se dice privada porque los dispositivos que no participan en esta comunicación no tienen acceso al contenido de la misma y de hecho no son conscientes de su establecimiento. El acceso a esta red y su administración está restringido solo a un número limitado de dispositivos. La privacidad se aplica también al espacio de direccionamiento y esquema de enrutamiento utilizado en una VPN, en el sentido de que están separados o difieren de aquellos instrumentados en alguna otra red privada existente o en la infraestructura de red subyacente por donde ocurre la comunicación.

El concepto de virtual, por definición es la representación de un objeto no existente mediante la ejecución de funciones que simulan su existencia. En el contexto de una VPN, significa que esta última representa una red de comunicaciones, que no tiene una contraparte física real. Este concepto fundamenta la naturaleza discreta o de separación, de una red lógica privada funcionando sobre una infraestructura de comunicaciones compartida y real. El aspecto de privacidad, definido en el párrafo anterior, está en función de la virtualización. [19]

3.0.1. Terminología

La literatura relacionada con redes privadas virtuales está llena de acrónimos, siglas, términos muy específicos que tornan difícil la interpretación de cualquier lectura relacionada con el tema. Esta sección define los principales elementos que componen un escenario VPN.

- Sitio: ubicación geográfica con uno o más usuarios o uno o más servidores o una combinación de servidores y usuarios. El usuario refiere al host o estación de trabajo.
- Servidor VPN: software o firmware VPN el cual se ejecuta en un dispositivo. Tiene la función de establecer un túnel con un cliente VPN. Previamente verifica la identidad del cliente para autorizar su acceso y determinar los permisos de este para acceder a los recursos locales. El

VPN - Definición - Tipos

dispositivo donde se ejecuta el servidor VPN puede ser un host, router o switch. Este equipo comunica la red local con la red pública. Otras acepciones pueden ser: gateway VPN, servidor de túneles.

- Cliente VPN: software o firmware VPN ejecutándose en un dispositivo, cuya función es establecer un túnel con un servidor VPN. Previamente, debe presentar las credenciales correctas al servidor. Otra acepción puede ser cliente de túnel.
- Túnel: Enlace lógico entre el servidor y cliente VPN, creado por un protocolo de túnel. Por este canal se envían los datos que han sido encapsulados y quizás encriptados por el protocolo. Es posible transmitir datos sin encriptar por un túnel. Un túnel puede establecerse en diferentes capas del modelo ISO/OSI de protocolos de comunicaciones.
- Extremos de un túnel: dispositivos que gestionan la creación, el establecimiento y la finalización de un túnel mediante la ejecución de software o firmware dedicado para tal fin, por lo tanto se encargan también del procesamiento relacionado con la des/encapsulación, des/encriptación y transmisión de los paquetes recibidos.
- **Network Access Server (NAS)** : servidor de acceso de red, un dispositivo que representa una interface entre un medio de acceso como la red de telefonía y una red de conmutación de paquetes, como el backbone de un proveedor o Internet. En una VPN este dispositivo permite que un usuario utilizando un acceso telefónico acceda a su red mediante un túnel creado por el NAS hacia el servidor de acceso remoto de la red destino.
- Túnel voluntario (Voluntary Tunnel): Túnel creado y configurado a partir de la solicitud de un cliente VPN. Esta clase de túnel es común en las VPN de acceso remoto, donde uno de los extremos es una computadora personal o notebook de un usuario hogareño o móvil.
- Túnel obligatorio (Compulsory Tunnel): Túnel asociado con las VPN de acceso remoto. Su creación y configuración está a cargo de un dispositivo denominado servidor de acceso de red o NAS. Éste se ubica entre la PC del usuario y el servidor VPN. En el NAS se ubica el extremo del túnel donde funciona el cliente VPN. Es posible que múltiples usuarios conectados al servidor de acceso de red, compartan el túnel en forma concurrente. En general el NAS es propiedad y es administrado por un proveedor de servicios.

VPN - Definición - Tipos

- Dispositivo de borde: Es el dispositivo ubicado en la frontera entre la red local y la red pública.
- CE: Dispositivo de borde del cliente (Customer Edge Device). Es el equipo perteneciente a un cliente de un servicio de comunicaciones que se sitúa en el borde de la red privada local y conecta con la red del proveedor del servicio a través de un PE. Un CE puede ser un router o switch.
- C: Dispositivo que pertenece al cliente y que se ubica dentro de la red del mismo. Estos no tienen conectividad directa con la red del Proveedor ni participan de la VPN. Pueden ser routers o switches.
- PE: Dispositivo de borde del proveedor (Provider Edge Device). Este es propiedad del proveedor de servicio de comunicaciones. Se conecta directamente a la red del cliente a través del CE. Un PE puede ser un router, switch o un dispositivo que combine ambas funciones.
- P: Dispositivos que componen el núcleo de la red del Proveedor. No tienen conectividad directa con la red del cliente ni participan de las VPN. Estos son equipos como routers y switches.

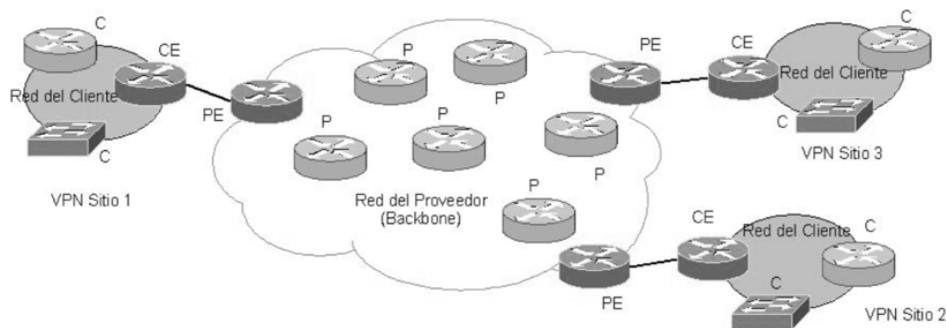


Figura 3.1: Componentes de una VPN [4]

3.0.2. Clasificación

Se pueden encontrar varias clasificaciones de las VPN, lo cual puede generar cierta confusión. Esto se debe a que existen diversos tipos de tecnologías y clases de redes privadas virtuales, lo que permite más de un criterio de organización. Las clasificaciones generales y más habituales son:

VPN - Definición - Tipos

- De acuerdo a quien implementa y administra el servicio: la propia organización o un proveedor de servicios.
- Según que comunican: redes entre sí o usuarios a la red.
- Según la capa del modelo de referencia de pila ISO/OSI para comunicaciones donde se establece la VPN: capa 2, 3 y las VPNs de capa de aplicación/transporte que utilizan el protocolo **SSL/TLS**. Estas representan una clase particular de VPN que se describen aparte. [20]

Otros criterios pueden ser:

- Según si los dispositivos de borde de un proveedor participan o no en el enrutamiento del tráfico de datos del cliente: VPN peer to peer o VPN overlay.
- Según si son orientadas o no a la conexión.
- Si son confiables o seguras.

3.0.3. VPNs provistas por el cliente o por el proveedor

Uno de los principales criterios para clasificar las VPN, define quien está a cargo de la implementación y administración de la red privada virtual, ya sea el cliente (la organización) o el proveedor de servicios de comunicaciones. Esto se refiere a la definición de las políticas a cumplir con esta solución, los requerimientos para la implementación, la adquisición y configuración de equipamiento, mantenimiento, resolución de problemas y monitoreo, especificación del espacio de direccionamiento a utilizar, esquema de enrutamiento etc.

3.0.4. VPNS provistas por el cliente (CE o CPE VPN)

También denominadas VPNs del ámbito del cliente (Customer Promises VPN). Estas VPNs son definidas e implementadas por el cliente de un servicio de comunicaciones. Generalmente este tiene acceso al backbone de un proveedor o bien posee un servicio de acceso a Internet. En este contexto el cliente puede tener más de un sitio propio, geográficamente distante que desea conectar o bien requiere hacerlo con otra red fuera de su dominio, también remota. En este tipo de VPN, el túnel se establece, únicamente, entre los equipos del cliente. Estos representan los extremos del o los túneles. Los equipos del proveedor o PE, no participan de la VPN. Tampoco del esquema de direccionamiento que esta utiliza o del enrutamiento necesario. Tratan a

VPN - Definición - Tipos

los paquetes o tramas como proveniente de un cliente del servicio, es decir solo lo reenvían. En el caso de la utilización de Internet, los routers intermedios también lo hacen con los paquetes IP, sin tener en cuenta el contenido encapsulado por el túnel de la VPN.

La ventaja de esta clase de VPN radica en que el cliente tiene el control de la seguridad aplicada a los datos que transmite. Para el proveedor sus dispositivos de borde no requieren ninguna configuración especial para el tratamiento de los paquetes de las VPN, además no surgen problemas de escalabilidad al momento de aumentar la cantidad de VPNs o los sitios a interconectar mediante estas ya que, como se mencionó anteriormente, estos equipos no participan en este escenario virtual.

Como desventaja, el cliente debe hacerse cargo básicamente de todo. Esto puede implicar un gran costo, tanto en la compra de equipamiento, como en la preparación de personal para la configuración y el mantenimiento de la VPN. Esta solución presenta problemas de escalabilidad para el cliente cuando existen varios sitios para interconectar.

Los tipos de VPN provistas por el cliente son:

- VPN **Internet Protocol security (IPsec)**
- VPN **Generic Routing Encapsulation (GRE)**
- VPN **SSL/TLS**



Figura 3.2: VPN Provista por el Cliente [4]

3.0.5. VPNs provistas por el Proveedor (PPVPN)

En esta clase de VPN el proveedor de servicio se encarga de su implementación. Los equipos de borde o PE participan activamente de la red virtual

VPN - Definición - Tipos

como así también, pero en menor grado, los dispositivos de borde del cliente. Esto significa que los PE realizan la mayor parte del procesamiento específico de la VPN, permitiendo que los equipos CE puedan ser routers o switches estándar sin necesidad de comprar equipamiento especial. El proveedor es responsable de la administración de la VPN, liberando al cliente de estas tareas. Esto resulta, para este último, en un menor costo de implementación respecto de un emprendimiento propio. Actualmente los proveedores ofrecen un servicio de VPN mejorado, donde suman además de la conectividad, acuerdos de nivel de servicio, calidad y diferenciación de servicio, seguridad, ingeniería de tráfico, etc. Esto redunda en un producto con valor agregado que beneficia a ambas partes. Las soluciones VPN de esta clase, pueden operar en la red de un único proveedor, entre un conjunto de proveedores de servicio y sobre Internet. En este último caso se asume que los routers de núcleo de Internet, no mantendrán información referida a la VPN, sin considerar si se utilizan protocolos de enrutamiento para distribuir o no dicha información. Existen cuatro escenarios donde pueden desplegarse estas VPN6:

- Único Proveedor, único Sistema Autónomo o AS (Autonomous System): escenario más simple, el servicio se brinda a través del AS de un único proveedor.
- Único Proveedor, múltiples AS: un proveedor administra varios AS (adquisición de varias redes). Este escenario implica la distribución con restricciones de la información de enrutamiento entre los diversos Sistemas Autónomos.
- Multi Proveedor: es el caso más complejo, debido a que es necesario negociar relaciones de confianza entre los backbones de los diversos proveedores para cumplir con las medidas de seguridad y niveles de servicio acordados para la VPN de un cliente. En este caso el servicio se denomina VPN inter-AS o inter proveedor.
- Proveedor de Proveedores (Carrier's Carrier): este es un caso especial del primer escenario, excepto que los clientes son proveedores de servicios de comunicaciones que contratan el servicio de VPN a un proveedor principal, para ofrecerlo a su vez a sus propios clientes.

Los tipos de VPN provistas por el Proveedor son:

- VPN **Virtual Private Wire Service (VPWS)**
- VPN **Virtual Private Lan Service (VPLS)**
- VPN **IP only Private Lan Service (IPLS)**

- VPN basada en routers virtuales
- VPN IPSec
- VPN **Multiprotocol Label Switching (MPLS)**

3.0.6. VPNs Sitio a Sitio y de Acceso Remoto

Otra forma general de distinguir las VPN es en función de si conectan redes entre sí o usuarios a una red. Una VPN sitio a sitio (site-to- site VPN) conecta dos o más redes entre sí que están geográficamente dispersas, estas pueden pertenecer a una o varias organizaciones. Si las redes pertenecen a una misma organización, esta clase de VPN se denomina intranet. Si las redes pertenecen a varias organizaciones se conoce como extranet. La intención en este último caso es comunicar organizaciones diferentes que persiguen un objetivo común y requieren compartir información útil para el conjunto. El servicio de VPN entre sitios debería ser independiente del alcance geográfico de la implementación.

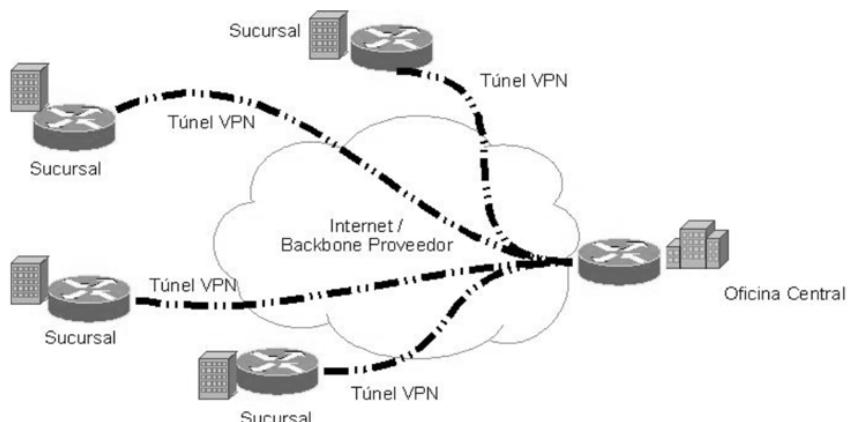


Figura 3.3: VPN Sitio a Sitio [4]

Las VPN de Acceso Remoto o RAVPN (Remote Access VPN), también denominadas VPN de acceso, permiten a los usuarios móviles o itinerantes y a los usuarios hogareños de una organización o tele trabajadores, acceder en forma remota a la red. Esta clase de VPN puede establecer un túnel en modo voluntario u obligatorio.

VPN - Definición - Tipos

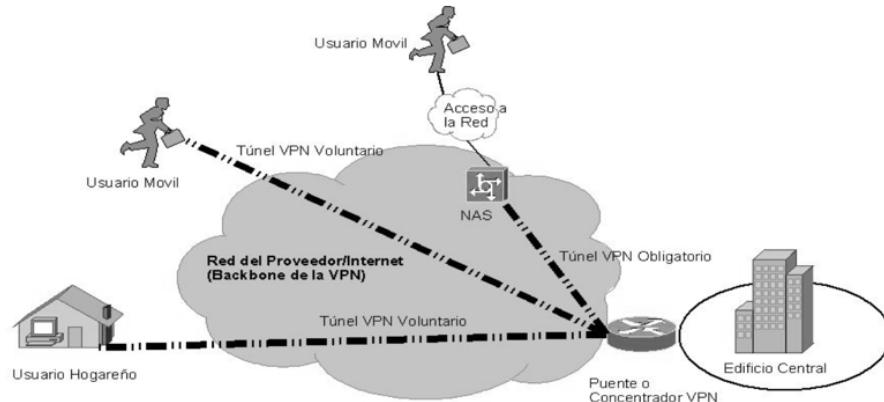


Figura 3.4: VPN de Acceso Remoto [4]

Las tecnologías y protocolos asociados a esta clasificación son: VPNs sitio a sitio:

- IPSec
- GRE
- Any Transport over MPLS (AtoM) (Any Transport over MPLS)
- Layer 2 Tunneling Protocol version 3 (L2TPv3) (Layer 2 Tunneling Protocol version 3)
- IEEE 802.1Q
- MPLS Label Switched Path (MPLS LSP) (MPLS Label Switched Path)

VPNs de acceso remoto:

- Layer 2 Forwarding (L2F)
- Point to Point Tunneling Protocol (PPTP)
- L2TPv2/v3
- IPSec
- SSL/TLS

3.0.7. VPNs de capa 2 y capa 3

El criterio de esta clasificación se basa en las capas, del modelo de referencia ISO/OSI de protocolo de comunicaciones, por donde se establece el túnel de la VPN. Esta clasificación surge a partir de la variedad de tecnologías existentes que se utilizan para implementar la VPN. Esta distinción tiene sentido cuando se la aprecia en el contexto de las clasificaciones anteriores. Las VPN de capa 2 permiten la conectividad a nivel de la capa de enlace de datos y puede ser establecida entre switches, routers o hosts. La comunicación está basada en el direccionamiento de capa 2 y el reenvío del tráfico está basado respecto del enlace entrante y la información de encabezados de dicha capa, tales como direcciones **Media Access Control (MAC)** o **Frame Relay Data Link Connection Identifier (DLCI)**.

Las VPN de capa 3 interconectan hosts o routers, la comunicación se basa en el direccionamiento a nivel de capa de red. El reenvío del tráfico se lleva a cabo teniendo en cuenta el enlace entrante y las direcciones del encabezado IP.

3.0.8. Integración de las clasificaciones

Las clasificaciones anteriores se pueden integrar para tener una perspectiva más práctica y operativa de las VPN. Esta integración muestra las VPN provista por el cliente o proveedor como el criterio de clasificación más general, dentro de la cual se pueden diferenciar las VPN sitio a sitio y remota. Finalmente se consideran según las tecnologías VPN de capa 2 y 3. El siguiente esquema muestra esta relación:

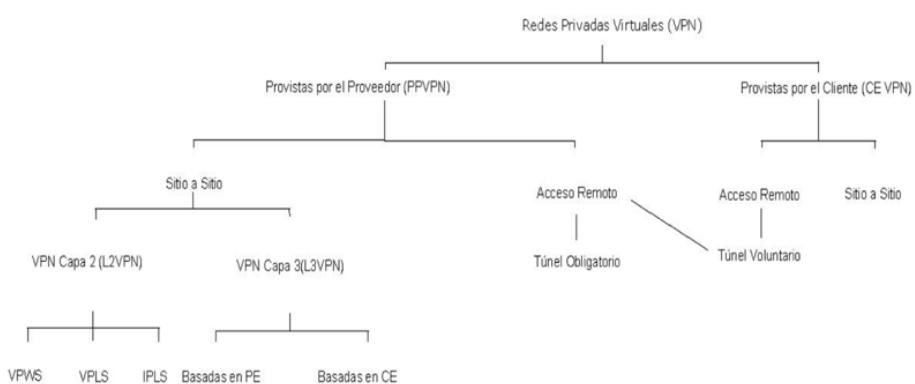


Figura 3.5: Clasificación de las VPN [4]

VPN - Definición - Tipos

VPN Sitio a Sitio Provistas por el Proveedor de Capa 2 (L2VPN) Estas VPN pueden ser establecidas entre switches, routers y hosts, permitiendo la conectividad a nivel de capa de enlace entre sitios separados. Tanto el direccionamiento como el reenvío del tráfico de la VPN se llevan a cabo en función del enlace entrante y de la información del encabezado de capa 2. Dentro de las L2VPN se pueden distinguir dos categorías:

- VPNs basadas en circuitos **Punto a Punto (P2P)**: conocidas también como **VPWS**. Se implementan usando MPLS o circuitos emulados (pseudowires) L2TPv3.
- VPNs **Multipunto a Multipunto (M2M)**: en esta categoría entran las VPN **VPLS** e **IPLS**

3.0.9. VPN VPWS

La red del proveedor puede considerarse como una emulación de un conjunto de enlaces punto a punto o pseudowires entre los sitios del cliente. Es útil en escenarios donde el cliente ya posee circuitos virtuales **ATM** o Frame Relay que interconectan sus redes. En lugar de que el tráfico del cliente atraviese el backbone hasta su destino en su formato nativo de capa 2, éste es encapsulado y enrutado sobre la infraestructura IP del Proveedor. El cliente mantiene las conexiones de capa 2 al backbone. Los routers CE deben seleccionar el circuito virtual a usar para enviar el tráfico al sitio destino.

Este esquema permite el reemplazo de redes con topologías estrella que requieren la interconexión de redes satélites hacia una red central, permitiendo alternativas de rutas hacia un destino. Una de las tecnologías habituales, en el núcleo de la red del proveedor, para esta clase de VPN es MPLS junto a extensiones conocidas como PWE3 (Pseudowire Emulation Edge to Edge). Un enfoque más escalable, respecto de la administración del servicio, utiliza **Border Gateway Protocol (BGP)** (Border Gateway Protocol) como protocolo de señalización y auto detección. En este caso, los dispositivos PE usan BGP multiprotocolo para anunciar los dispositivos CE y VPN que controlan, junto con las etiquetas MPLS utilizadas para encaminar el tráfico. De esta forma, cuando los otros CE reciben esta información, saben cómo establecer los pseudowires.

3.0.10. VPN VPLS

En este caso la red LAN ethernet de cada sitio del cliente se extiende hasta el borde de la red backbone del proveedor. Luego, una vez allí, se emula la

función de un bridge o switch para conectar todas las LANs del cliente. De esta forma se emula, en la red del proveedor, una única LAN ethernet. Esta solución provee un servicio punto a multipunto donde los routers CE envían todo el tráfico, destinados a los otros sitios, directamente al router PE. Este servicio se basa en la utilización de pseudowires, combinados en una topología de malla completa (full mesh) de interconexiones entre los dispositivos PE que participan en una VPN determinada. Éstos llevan a cabo el aprendizaje de las direcciones MAC, de la misma forma que un switch ethernet para reenviar las tramas desde un CE a otro. Así, un CE puede reenviar tráfico en una forma punto a multipunto a otros CE. Existe un problema de escalabilidad con este servicio, y tiene que ver con el incremento de sitios del cliente. Es necesario mantener en los PE un gran número de direcciones MAC para el reenvío de tramas por sitio de cliente.

3.0.11. VPN IPLS

Si se requiere intercambiar tráfico IP exclusivamente y los dispositivos CE son routers IP, entonces es posible el servicio IP sobre LAN. Si bien se transmiten datagramas IP, el mecanismo de reenvío se basa en información de encabezado de capa 2. Dado que el siguiente salto o hop para cada datagrama IP es otro CE, las únicas direcciones MAC que un PE debe aprender, cuando reenvía las tramas de capa 2, son aquellas de los routers CE. Esto es una ventaja respecto del servicio VPLS por el reducido número de direcciones MAC a preservar por sitio de cliente.

3.0.12. VPN Sitio a Sitio Provistas por el Proveedor de Capa 3 (L3VPN)

Esta clase de VPN se basa en tecnologías más estables que las empleadas en las L2VPN, debido al estudio y desarrollo de las mismas. Esto le permite al proveedor de servicio tener mayor seguridad al momento de implementar una u otra solución. Se pueden dividir a su vez en:

- VPN basadas en PE: Los dispositivos PE participan en el enrutamiento y reenvío del tráfico del cliente basado en el espacio de direcciones de la red del cliente. En este caso los CE no participan de la VPN. El tráfico del cliente se reenvía entre los PE a través de túneles MPLS LSP, IPSec, L2TPv3 o GRE.
- VPN basadas en CE: En este caso los túneles son creados entre los equipos CE, mientras los PE no participan en la VPN, solo reenvían el tráfico del cliente. Se utiliza IPSec o GRE para establecer los túneles.

3.0.13. Confiables y Seguras

Esta es una clasificación donde se tiene en cuenta si es o no necesaria la encriptación y autenticación de los datos a transferir entre los nodos de la VPN. Los proveedores que no utilizan encriptación para los datos de sus clientes debido a que utilizan circuitos virtuales de capa 2 se pueden definir como VPN Confiables. Podemos mencionar las redes FRAME RELAY, ATM y MPLS. En cambio en las VPN Seguras el tráfico de datos es autenticado y encriptado sobre el backbone del proveedor del servicio. Utilizan los protocolos IPSEC, SSL, L2TP asegurado mediante IPSEC, PPTP asegurado con MPPE (Microsoft Point-to-Point Encryption).

3.0.14. Overlay y Peer

Las VPN overlay se dan entre dispositivos CE, los dispositivos PE no participan en el enrutamiento de los clientes de la red, sino que reenvían tráfico de clientes basados en direccionamiento globalmente único, por lo tanto no tiene conocimiento del direccionamiento utilizado por el cliente. Los túneles son configurados entre dispositivos CE usando protocolos como IPsec y GRE. Cabe observar que el modelo overlay tiene serios problemas de escalabilidad debido a que si se cuenta con muchos nodos de egreso el número de adyacencias se incrementa en directa proporción con el número de nodos.

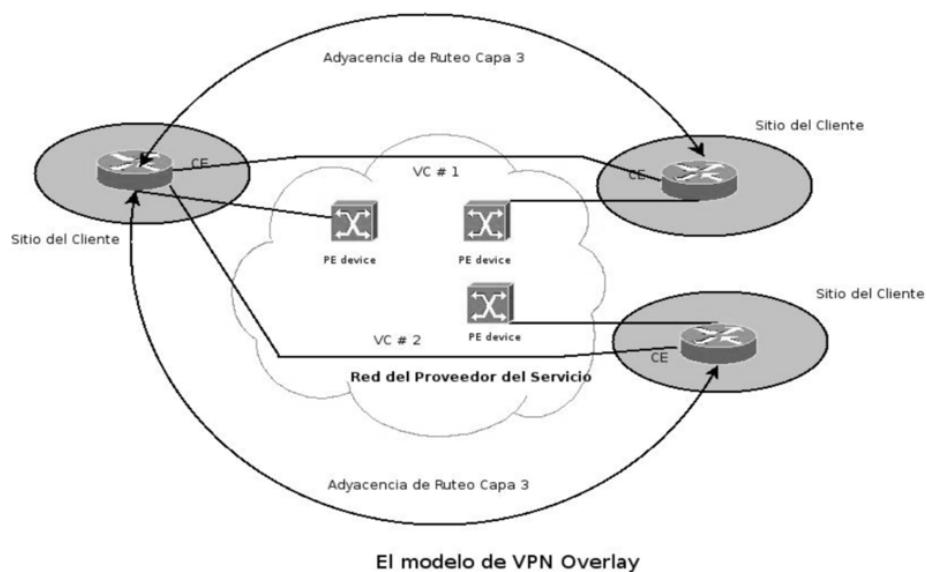
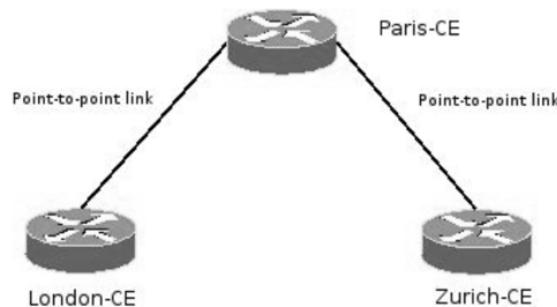


Figura 3.6: Adyacencias del Ruteo [4]

VPN - Definición - Tipos

Pueden ser implementadas a nivel de capa física usando líneas telefónicas (dialup), a nivel de capa 2 utilizando Frame Relay, X-25 y ATM, o a nivel de capa 3 utilizando túneles IP o GRE. Con el fin de clarificar veamos un ejemplo, un esquema en el que figuran tres sitios. Un sitio se conecta a través de los circuitos virtuales $VC1^o$ Y $VC2^o$ con otros dos sitios. Si suponemos que el sitio principal es Londres y los otros son Paris y Zurich podríamos ver que la percepción que poseen los routers CE



Percepcion de la Infraestructura del proveedor desde los routers CE

Figura 3.7: Infraestructura del proveedor [4]

Si son reemplazados los dispositivo PE por routers y estos participan en el enrutamiento entonces es una VPN tipo Peer. Los routers tienen que poseer conocimiento del direccionamiento que utiliza el cliente. Esto es necesario debido a que las rutas se intercambian entre dispositivos CE y los dispositivos PE. Estas VPN son provistas por un proveedor de servicios.

VPN - Definición - Tipos

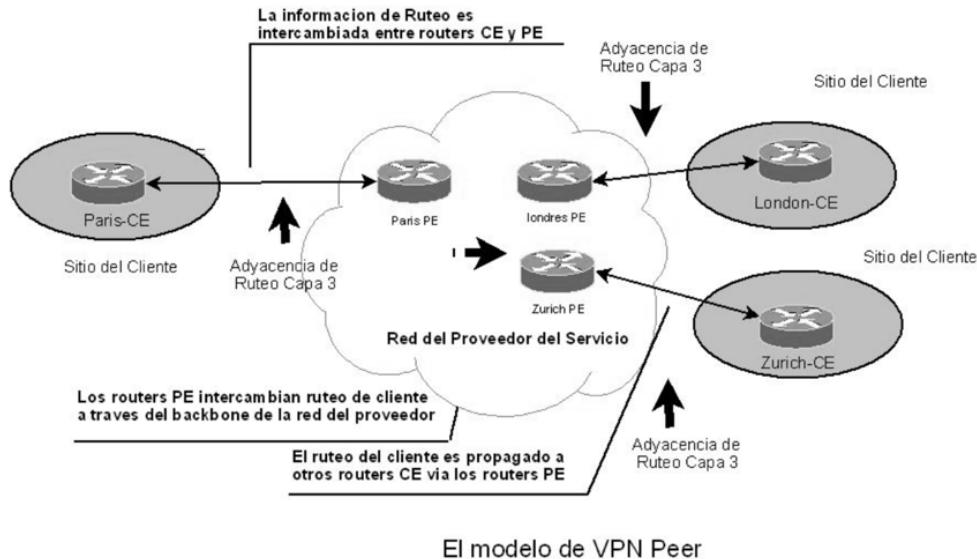


Figura 3.8: VPNs tipo Peer [4]

En la Figura anterior podemos observar que al reemplazar los switches por routers se convierte en una VPN tipo Peer. No Orientadas y orientadas a la conexión

Son orientadas o no orientadas a la conexión dependiendo si el proveedor provee o no circuitos virtuales dedicados.

Orientada a la conexión: Son en las que provee el proveedor un circuito virtual dedicado. Por ejemplo FRAME RELAY y ATM.

No orientadas a la conexión: Son las que no poseen un circuito virtual. Por ejemplo las VPN basadas en IP.

3.0.15. VPNs de capa de transporte/aplicación

El protocolo SSH (Secure Shell) desarrollado por Communications Security Ltd., permite acceder a otro dispositivo a través de una red insegura, ejecutar comandos a una máquina remota y mover archivos de una computadora a otra. Utilizando encriptación sobre canales inseguros provee una fuerte autenticación y encriptación.

Existen dos versiones incompatibles entre sí. Son dos protocolos totalmente diferentes que usan distinto cifrado.

Tabla 3.1: SSH v1, SSH v2

	SSH v1	SSH v2
Autenticación de Sistemas	Llaves de servidor y clientes	Llaves de hosts
Autenticación	Llaves	Certificados

SSH2 es una completa reescritura del protocolo que lo hace más seguro y utiliza una implementación de red totalmente distinta que SSH1. Debido a la diferente implementación ambos protocolos son incompatibles. Por ejemplo se lo utiliza para asegurar un túnel PPP. El principio de funcionamiento es el mismo que el de SSL diferenciándose en la capa en la que actúan y el método de autenticación.

Tabla 3.2: SSH, SSL

	SSH	SSL
Capa en la que trabaja	Aplicación	Transporte
Autenticación	Certificados	Llaves

También es posible establecer túneles en la capa de aplicación. Para esto se utiliza un browser del lado del cliente, por lo que no es necesario instalar ningún programa. La conexión se realiza a un sitio web seguro mediante el protocolo **Hypertext Transfer Protocol Secure (HTTPS)**. Además, existen otros productos los cuales ofrecen una combinación de gran flexibilidad, seguridad y que intentan lograr una configuración que no requiera mucho conocimiento. La seguridad es lograda mediante cifrado del tráfico usando el protocolo SSL/TLS.

3.0.16. VPN multiservicio

Trabajan sobre MPLS, cuyo sello distintivo es la calidad de servicio o **Quality of Service (QoS)**. El objetivo de estas VPN es integrar diferentes aplicaciones en una sola conexión: voz, datos, multimedia, etc.

3.0.17. Aplicaciones

Las VPN se utilizan en situaciones donde es necesario establecer una comunicación en forma segura utilizando un medio o infraestructura compartida de transmisión. Además de comunicar redes propias de la organización,

usuarios móviles, tele trabajadores etc., también es posible comunicar distintas organizaciones entre sí. Esta alternativa surge a partir de la necesidad de establecer lazos de negocios, o la concreción de intereses comunes. La extranet refleja dichos intereses mediante la interconexión de las redes de datos de las distintas organizaciones. En realidad solo comparten los recursos necesarios para cumplir con los objetivos comunes, por lo que el acceso es parcial y controlado.

Finalmente las VPN se pueden considerar como un negocio con valor agregado en la forma de un servicio. El hecho de que hoy en día las organizaciones dependan fuertemente de las tecnologías de información para su desarrollo y que sus necesidades sean diferentes, plantea un mercado donde las soluciones de comunicaciones de datos son casi a la medida del cliente. No existe una única solución para todos los tipos de organizaciones. Es por esto que los proveedores de servicios han sumado a su oferta de soluciones empresariales, el servicio de VPN, donde una buena relación costo-beneficio para el cliente es posible.

3.0.18. Extranets

Una extranet es un conjunto de intranets de organizaciones diferentes que se interconectan entre sí para cumplir con objetivos comunes. Esta relación está bien definida y es establecida bajo un estricto control del acceso. Se puede definir también como la intersección de un grupo de intranets de varias empresas, lo cual indica que solo se comparte una porción de la intranet hacia el resto de la extranet.

Por otro lado Internet es el medio común que resuelve problemas de incompatibilidad entre sistemas de empresas muy diferentes. Es decir, ofrece una interfaz común que permite una interacción difícil de lograr con otras tecnologías. Por lo tanto, como en el caso de las intranets, adoptan las tecnologías basadas en estándares abiertos propias de Internet para lograr comunicación dentro de la extranet.

Una extranet puede tener un impacto notable en las relaciones e interrelaciones con las demás empresas que la integran. De hecho puede modificar notablemente la posición de la organización frente a sus clientes y competidores. Por esta razón la decisión de su implementación debe responder a fines estratégicos, por lo cual deberá ser tomada por la alta gerencia de la organización.

Las VPNs son la forma más efectiva de implementar las extranets, ya que pueden hacer uso de Internet para lograr la interconexión de los diferentes sitios. Nuevamente los puntos más importantes a considerar son la seguridad en cuanto al acceso solo de los usuarios autorizados mediante mecanismos

de autenticación, como también el transporte a través de la encapsulación y encriptado de los datos. Como se ha visto en este capítulo, existen diversos protocolos de túnel utilizados en VPNs, los cuales se aplican obviamente en las extranets. Algunos de ellos como IPSec, encapsulan los paquetes originales y encriptar la información sensible, otros como PPTP y L2TP se valen de IPSec para brindar la confidencialidad.

3.0.19. Servicio VPN provisto por un proveedor

Las corporaciones y organizaciones dependen cada vez más de las telecomunicaciones y redes de datos. Es muy importante la interconexión de redes propias en diferentes sitios. Esta necesidad fue resuelta por proveedores de servicios de telecomunicaciones, principalmente a través de conexiones Frame Relay, ATM y más recientemente mediante Ethernet y túneles basados en IP. Estas organizaciones, requieren con más frecuencia, servicios de conectividad sobre uno o más backbones, incluso a través de Internet, pero que este servicio incluya contratos de nivel de servicio (Service Level Agreement), **QoS**, y otros parámetros que permitan una comunicación segura, estable, con alto grado de disponibilidad, con un umbral de ancho de banda, con priorización de tráfico, etc.

Estas características son difíciles de lograr cuando la comunicación entre sitios debe atravesar redes de diferentes proveedores más la Internet, es decir un entorno compartido y de naturaleza no orientada a la conexión.

Las VPN permiten una comunicación segura y privada mediante la encapsulación y encriptación. Es decir, aislan el tráfico de datos privados de una organización del resto con el cual pueda compartir un canal de comunicación. Actualmente la relación costo-beneficio en la implementación de este mecanismo ha determinado la conveniencia de la contratación del servicio a proveedores, en lugar de la puesta en funcionamiento y control por parte de la propia organización.

Para poder diferenciar y aislar los tráficos pertenecientes a varios clientes, el proveedor utiliza conexiones de capa 2 (VPNs tradicionales) o túneles de capa 2 o 3. Para el caso de conexiones a través de Internet, las VPN se han basado en IPSec para brindar la mayor seguridad.

El concepto de servicio VPN provisto por el proveedor debe soportar los tipos tradicionales de VPN, también debe funcionar con las clases de otros proveedores ya definidos anteriormente, además de Internet: único proveedor, conjunto de proveedores y proveedor de proveedores. Existen requerimientos generales para esta clase de VPNs, un análisis detallado se expresa en la RFC 3809 . Estos requerimientos pueden clasificarse en:

- Requerimientos del servicio: atributos del servicio que el cliente puede observar o medir, por ejemplo: disponibilidad y estabilidad, garantías de seguridad, servicio de tramas o datagramas.
- Requerimientos del proveedor: características que el proveedor evalúa para determinar la viabilidad en términos de la relación costo-efectividad del servicio, por ejemplo escalabilidad y grado de administración.
- Requerimientos de Ingeniería: características de implementación que permiten cumplir con los requerimientos del proveedor y del servicio. Estos a su vez pueden clasificarse en:
 - Requerimientos en el plano de reenvío: asociados a los mecanismos de reenvío de datos.
 - Requerimientos en el plano de control: asociados al mecanismo de distribución de la información de enrutamiento.
 - Requerimientos relacionados a la uniformidad de los mecanismos en esta clase de VPN respecto de otros esquemas y en general con la forma de operación de Internet.

3.0.20. Calidad de servicio (QoS) y Acuerdos de nivel de servicio (SLA)

En general calidad de servicio se refiere a la habilidad de brindar servicios de redes y comunicaciones de acuerdo a un conjunto de parámetros especificados un contrato de nivel de servicio o SLA. La calidad está caracterizada por la disponibilidad del servicio, tasa de demora, de variación de la demora (jitter), tasa de proceso de paquetes (throughput), de perdida de paquetes. En particular, y desde una perspectiva de recurso de red, calidad de servicio se refiere a un conjunto de herramientas que permiten a un proveedor de servicio priorizar tráfico, controlar el ancho de banda y la demora en la red. Existen dos maneras de lograrlo en redes IP, mediante Servicios Integrados y a través de Servicios Diferenciados.

El ámbito en el cual un servicio VPN cumple con calidad de servicio dependerá del proveedor de servicio. En la mayoría de los casos de VPN definida en el sistema autónomo de un único proveedor es posible cumplir con este requerimiento. El soporte de QoS en ambientes de multi proveedores o diversos sistemas autónomos estará en función de los acuerdos de cooperación entre los involucrados en la provisión del servicio y de que todos utilicen los mismos mecanismos. Es decir que los dispositivos CE y/o PE ejecuten al

VPN - Definición - Tipos

menos formateo y apliquen políticas al tráfico (shaping y policing).

La necesidad de aplicar calidad de servicio ocurre principalmente en la red de acceso al backbone del proveedor y no en el interior del mismo, de hecho QoS sobre las conexiones PE a PE no son un inconveniente. En cuanto a la calidad de servicio en el acceso, se pueden distinguir dos enfoques:

- Desde el CE a través de la red de acceso al PE
- Desde el PE a través de la red de acceso al CE

Los dispositivos CE y PE deberían poder soportar QoS sin importar la tecnología de acceso ya sea de capa 2 o 3: circuitos virtuales ATM y Frame Relay, acceso basado en MPLS, DSL etc.

Se pueden distinguir dos modelos de servicio para QoS:

- Servicio de administración del acceso: este provee QoS sobre el acceso entre CE y los puertos del lado de cliente en el PE. No es requerido en el núcleo del backbone.
- QoS borde a borde: brinda QoS sobre el backbone del proveedor, ya sea entre pares de dispositivos CE o pares de PE, dependiendo de los límites del túnel.

Un acuerdo de nivel de servicio **Service Level Agreement (SLA)** es una documentación donde se expresan los resultados de una negociación entre un cliente y un proveedor de servicios. En este documento se especifican los niveles de disponibilidad, performance, nivel de servicio, forma de operación y otros atributos del servicio.

A partir de un SLA se pueden determinar objetivos de nivel de servicio o **Service Level Objective (SLO)**, considerando métricas individuales con los valores deseados e información operacional para controlar el SLA. Estas se pueden implementarse como políticas.

Una especificación de nivel de servicio o **Service Level Specification (SLS)** engloba a las dos anteriores, es decir especifica un acuerdo negociado y las métricas individuales y datos operacionales, para garantizar la calidad de servicio del tráfico de red para ese cliente. Una SLS puede definirse sobre la base de los siguientes objetivos y parámetros, los cuales se pueden considerar sobre la base de conexiones a la red de acceso, VPNs o sitios:

- Disponibilidad del sitio, VPN o conexión de acceso.
- Duración de los intervalos de no disponibilidad del servicio.
- Tiempo de activación del servicio.

VPN - Definición - Tipos

- Tiempo de respuesta para la resolución de un problema.
- Tiempo de aviso de un inconveniente.
- Límites para la variación del delay y jitter.

El sistema de administración y monitoreo del proveedor deberá medir y generar reportes respecto si el desempeño medido cumple o no los objetivos de la SLS. Muchas veces el nivel garantizado para los parámetros de los objetivos de nivel de servicio, dependen del alcance de la VPN, por ejemplo ciertos niveles pueden ser garantizados en el ámbito de un solo sistema autónomo, mientras que otro, aún más estricto, se puede cumplir en un dominio de un único proveedor pero con varios sistemas autónomos bajo su cargo. En un escenario multi proveedor es más difícil cumplir con aquellos parámetros que requieran un alto grado de cumplimiento, por ejemplo el requerimiento de QoS.

Resumiendo, Mediante las VPNs se obtiene:

- La administración de la red a bajo costo.
- Seguridad para conectarse vía Internet.
- Confidencialidad, integridad de los datos.
- Permite conexión de cualquier equipo que tenga autorización.
- Son sencillas de manejar, etc.

No sólo es necesario mencionar las ventajas de las VPN sino que se debe presentar sus desventajas para cuidar el rendimiento de la intranet y optimizar sus recursos, las desventajas más conocidas son:

- Se deben establecer correctamente las políticas de seguridad y de acceso.
- Mayor carga en el cliente VPN porque debe encapsular los paquetes de datos y encriptarlos.
- Fallo en seguridad debido a los usuarios que accesan remotamente pueden utilizar las computadoras para abrir otras aplicaciones que amenazan la red.

3.0.21. Creación de Túneles.

El túnel es el camino lógico o sentido que los paquetes encapsulados viajan a través de la red interna de tránsito, se pueden crear muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura, el tunneling tiene implicaciones notorias para las VPNs.

3.0.22. Tunneling

Es un método que consiste en utilizar la infraestructura de una interred, para transportar datos de una red a otra, además hace el proceso de colocación de cada paquete de información que se envía dentro de otro encapsulado, lo que permite que los usuarios se conecten de forma segura estén donde estén a la organización.

Los componentes básicos de un túnel son:

- Un iniciador de túnel
- Dispositivos de enrutamiento
- Terminadores de túneles.

3.0.23. Comparativa entre tecnologías VPN

PPTP

- Puntos Fuertes
 - Proporciona una capacidad multiprotocolo.
 - Integración con IPsec
- Puntos Débiles
 - Precisa un servidor NT como terminador del túnel.
 - Está siendo sustituido por el L2TP, ya no se utiliza porque la IETF no lo reconoció como estándar.

L2F

- Puntos Fuertes
 - Proporciona el tunneling multiprotocolo.

VPN - Definición - Tipos

- Soportado por la gran mayoría de fabricantes.
- Puntos Débiles
 - No hay encriptación
 - No hay control de flujo en el túnel
 - Seguridad débil.

L2TP

- Puntos Fuertes
 - Combina L2F y PPTP.
 - Necesidad de únicamente una red de paquetes para operar bajo X.25 y Frame Relay.
- Punto Débil
 - Da problemas la definir una encriptación estándar.

IPSEC

- Puntos Fuertes
 - Subconjunto de Ipv6.
 - Transparente a aplicaciones (por debajo de la capa de Transporte).
 - Provee seguridad para usuarios individuales.
- Puntos Débiles
 - No estandarizado
 - No hace gestión de usuarios.
 - Protocolo complejo que requiere una configuración complicada.
 - Puede afectar el rendimiento en recursos del CPU.
 - Requiere la instalación de software cliente

Secure Sockets Layer (SSL)

- Punto Fuerte
 - No es necesario instalar software cliente para la vpn.

VPN - Definición - Tipos

■ Puntos Débiles

- No se usa para conexiones red a red.
- Funciona a través de un servidor NAT.
- No da seguridad en la estación de trabajo.
- No se ajusta a unir redes completas sino al modelo negocio/cliente.
- No trabaja bien con gateways.

SSH

■ Puntos Fuertes

- Simplicidad de implementación
- Todos los datos que se envían en una conexión son cifrados.

■ Punto Débil

- No soporta UDP y solo por TCP tuneliza.

MPLS (Multiprotocol Label Switching)

■ Puntos Fuertes

- Las capacidades más relevantes son: Calidad de servicio QoS, soporte multiprotocolo.
- Permite transportar diferentes tipos de tráfico IP, incluyendo tráfico de voz y datos
- Fácil de configurar y administrar.
- Soporta multicast

■ Puntos Débiles

- Puede crear túneles IP a través de la red sin necesidad de encriptación o aplicación en el usuario final lo que es propensa a ataques.
- No se pueden mantener los vínculos en Internet entre etiquetas MPLS y los hosts.

3.0.24. Aspectos Legales

Todos los aspectos legales se rigen por las leyes de la Compañía Nacional de Telecomunicaciones CONATEL.

Capítulo 4

Software RouterOS.

El software ruteadores viene pre instalado en el mainboard el mismo que podemos acceder por medio de un software conocido como Winbox que nos servirá de interfaz entre las diferentes configuraciones de nuestro RouterBOARD y el usuario.

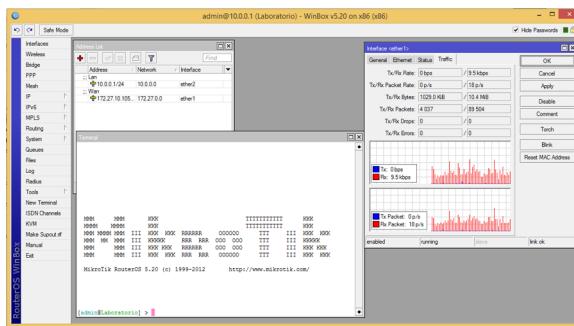


Figura 4.1: RouterOS

El MikroTik RouterOS es un sistema operativo basado en el Kernel V3.5.5 de Linux y es muy estable, la facilidad de acceso a las múltiples configuraciones dependerá del tipo de licencia a la que tengamos acceso con nuestro RouterBOARD. La licencia que este establecida en nuestro mainboard no tiene fecha de expiración, pero si un tiempo de duración en la que se podrá tener acceso a una nueva actualización. [21]

4.1. Winbox.

Winbox es un programa ejecutable en Windows, en Linux y Mac OSX por medio de WINE, que me permite acceder a las múltiples configuraciones

Fucionamiento del Software RouterOS

de mi mainboard desde mi PC por medio de un entorno amigable. Es un software liviano que se lo puede descargar de la página Mikrotik [22]

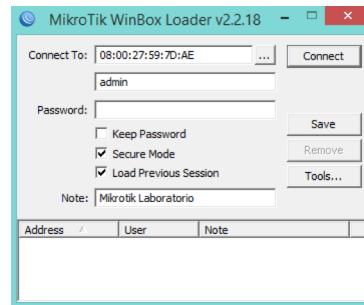


Figura 4.2: Winbox

Conectamos nuestro RouterBoard a nuestra máquina y le damos escanear en el botón “...” y nos mostrara todos los RouterBoard conectados. Se selecciona el equipo con el usuario por defecto es *admin* sin contraseña

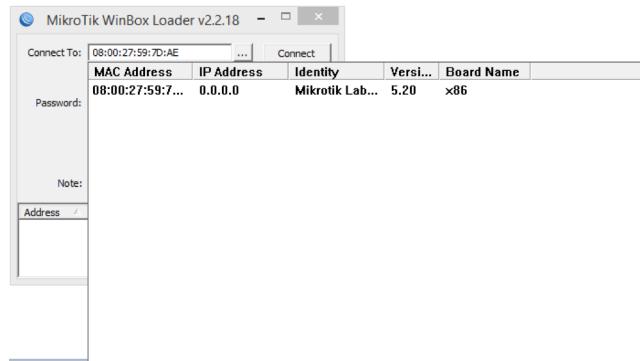


Figura 4.3: Escaneo de Router con Winbox

Una vez dentro del RouterBoard se selecciona: **New Terminal** y digitando “*system reset*” para que vuelva a sus configuraciones de fábrica y evitar algún problema por otras configuraciones que pueden estar dentro del Router.

Fucionamiento del Software RouterOS

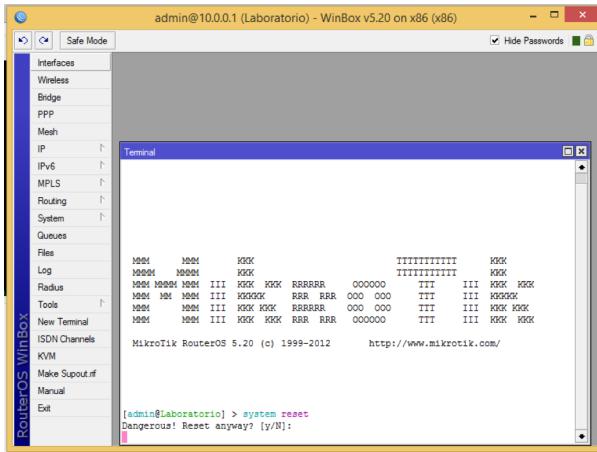


Figura 4.4: Reset RouterOS

Una vez que el RouterBoard reinicie, se accede vía WinBox, para ver como quedo la configuración.

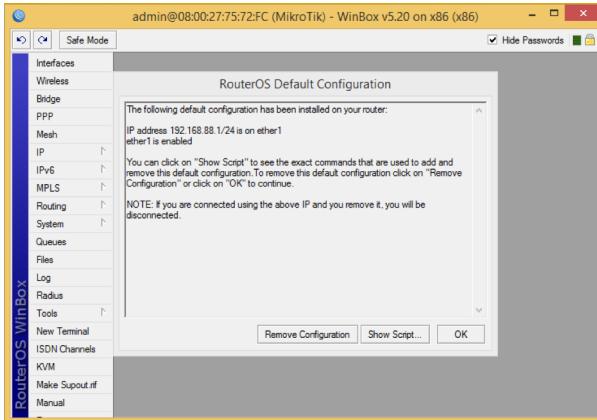


Figura 4.5: Remover Configuraciones

4.2. Configuración IP.

Las IP (Internet Protocol) son muy importantes en cada uno de los enlaces ya que por medio de ellas se establecerá la comunicación el enlace. Para asignar una dirección IP a una interfaz tenemos que.

Escoger el menú **IP → Address → +**

Fucionamiento del Software RouterOS

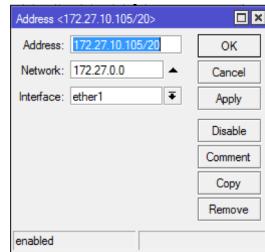


Figura 4.6: Configura IP WAN

Escoger el menú **IP** → **Address** → **+**



Figura 4.7: Configurar IP LAN

Escoger el menú **IP** → **Address**

Address List		
<input type="button"/> <input type="button"/> <input type="button"/> <input type="button"/> <input type="button"/> <input type="button"/> <input type="text"/> <input type="button"/>		
Address	/	Network
... Lan	<input type="checkbox"/>	10.0.0.1/24
... Wan	<input type="checkbox"/>	172.27.10.105...

Figura 4.8: Address List

Escoger el menú **IP** → **Routes**

Funcionamiento del Software RouterOS



Figura 4.9: Puertas de Enlaces

Escoger el menú IP → Routes → +

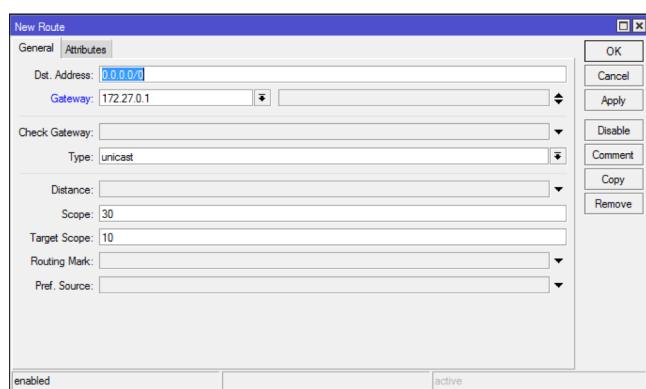


Figura 4.10: Puerta de enlace predeterminada

Escoger el menú IP → Routes



Figura 4.11: Listado de puertas de enlace

Escoger el menú IP → DNS

Fucionamiento del Software RouterOS

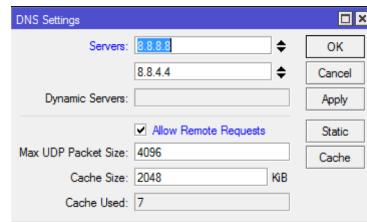


Figura 4.12: DNS

Escoger el menú New Terminal → ping google.com

```
[admin@Laboratorio] > ping google.com
HOST                                SIZE TTL TIME   STATUS
186.16.31.109                         56 57 23ms
186.16.31.109                         56 57 8ms
186.16.31.109                         56 57 7ms
186.16.31.109                         56 57 9ms
186.16.31.109                         56 57 9ms
186.16.31.109                         56 57 7ms
186.16.31.109                         56 57 8ms
sent=7 received=7 packet-loss=0% min-rtt=7ms avg-rtt=10ms max-rtt=23ms
```

Figura 4.13: Prueba de ping

Escoger el menú IP → Firewall → +

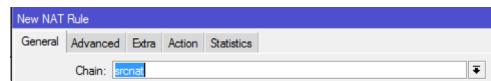


Figura 4.14: Firewall - General

Escoger el menú IP → Firewall

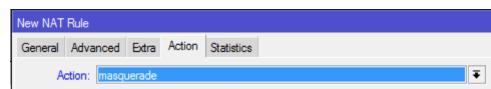


Figura 4.15: Firewall -Action

Escoger el menú IP → Firewall

Funcionamiento del Software RouterOS



Figura 4.16: Lista reglas Nat

Escoger el menú Inicio → Ejecutar → cmd



Figura 4.17: Prueba de ping

4.3. Telnet

Telnet sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero es una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc. [23]

Fucionamiento del Software RouterOS



Figura 4.18: Acceso vía Telnet



Figura 4.19: Credenciales vía telnet

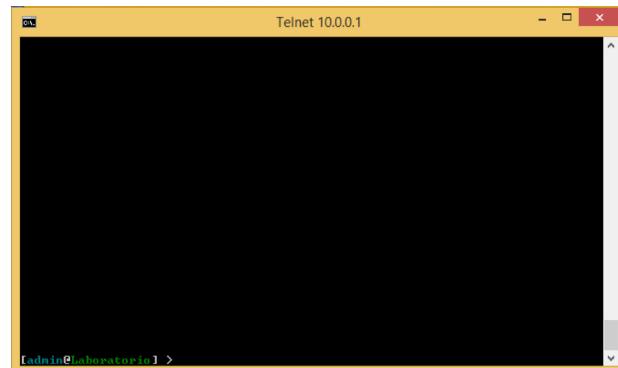


Figura 4.20: Entorno Telnet

Fucionamiento del Software RouterOS

4.4. Webbox

Es una manera de controlar y monitorear el Mikrotik RouterOS por medio de una navegador Web sin la necesidad de utilizar herramientas adicionales

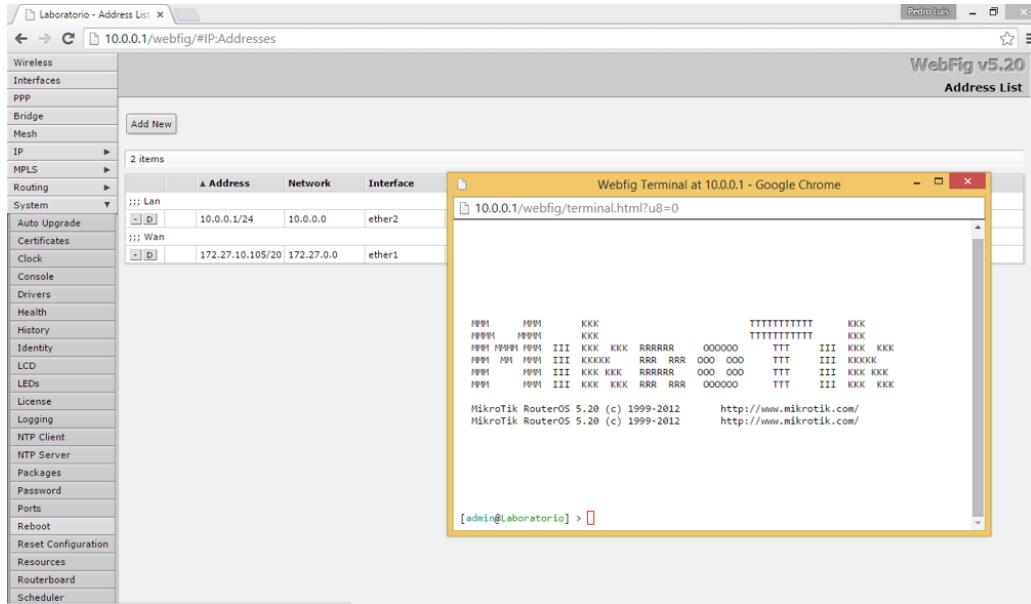


Figura 4.21: Webbox

4.5. SSH

SSH es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como **FTP** o **Gstelnet**, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como telnet o rsh [24]

Fucionamiento del Software RouterOS

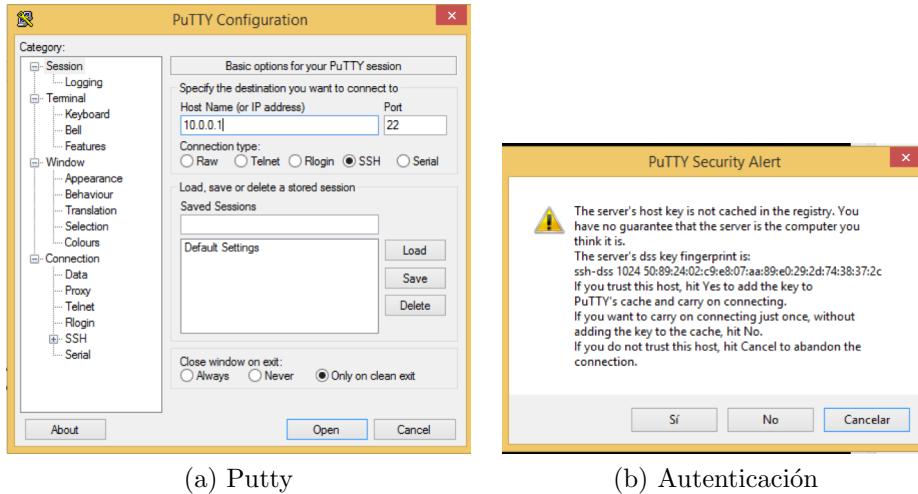


Figura 4.22: Putty - Autenticación



Figura 4.23: Entorno de trabajo SSH

4.6. Radio Mobile

Es un programa de simulación de radiopropagación gratuito desarrollado por Roger Coudé para predecir el comportamiento de sistemas radio, simular radioenlaces y representar el área de cobertura de una red de radiocomunicaciones, entre otras funciones. El software trabaja en el rango de frecuencias entre 20 MHz y 20 GHz y está basado en el modelo de propagación **Irregular Terrain Model (ITM)** o modelo Longley-Rice. Utiliza datos de elevación del terreno que se descargan gratuitamente de Internet para crear mapas virtuales.

Fucionamiento del Software RouterOS

les del área de interés, vistas estereoscópicas, vistas en 3-D y animaciones de vuelo. Los datos de elevación se pueden obtener de diversas fuentes, entre ellas del proyecto de la NASA que provee datos de altitud con una precisión de 3 segundos de arco (100m). [25]

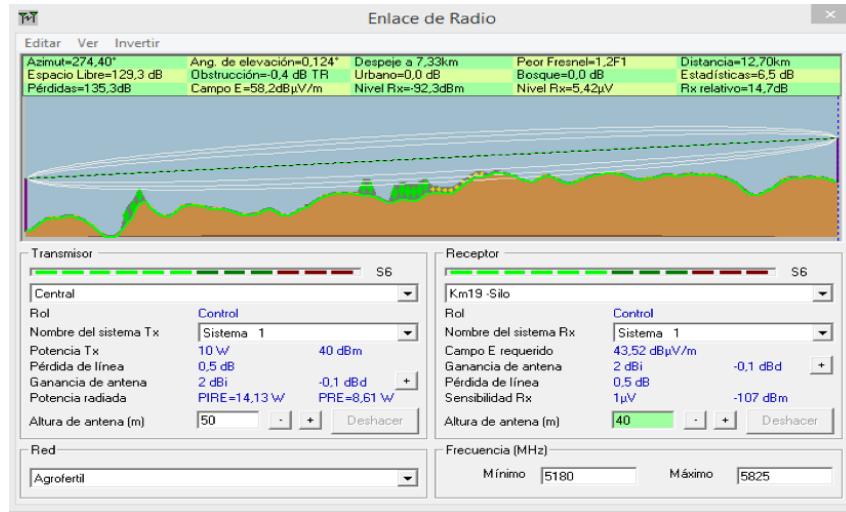


Figura 4.24: Radio Mobile, Enlace de Radio



Figura 4.25: Vista con Radio Mobile

4.7. Google Earth

Es un programa informático que muestra un globo virtual que permite visualizar múltiple cartografía, con base en la fotografía satelital. El programa fue creado bajo el nombre de EarthViewer 3D por la compañía Keyhole Inc, financiada por la Agencia Central de Inteligencia. La compañía fue comprada por Google en 2004 absorbiendo la aplicación.

El mapa de Google Earth está compuesto por una superposición de imágenes obtenidas por imágenes satelitales, fotografías aéreas, información geográfica proveniente de modelos de datos SIG de todo el mundo y modelos creados por computadora. El programa está disponible en varias licencias, pero la versión gratuita es la más popular, disponible para dispositivos móviles, tabletas y computadoras personales.

La primera versión de Google Earth fue lanzada en 2005 y actualmente está disponible en PC para Windows, Mac y Linux. Google Earth también está disponible como plugin para visualizarse desde el navegador web. En 2013 Google Earth se había convertido en el programa más popular para visualizar

Fucionamiento del Software RouterOS

cartografía, con más de mil millones de descargas.

Muchos usuarios utilizan la aplicación para añadir sus propios datos, haciéndolos disponibles mediante varias fuentes, tales como el Bulletin Board Systems o blogs. Google Earth es capaz de mostrar diferentes capas de imagen encima de la base y es también un cliente válido para un Web Map Service. Google Earth soporta datos geoespaciales tridimensionales mediante los archivos **Keyhole Markup Language (.kml)** [26]

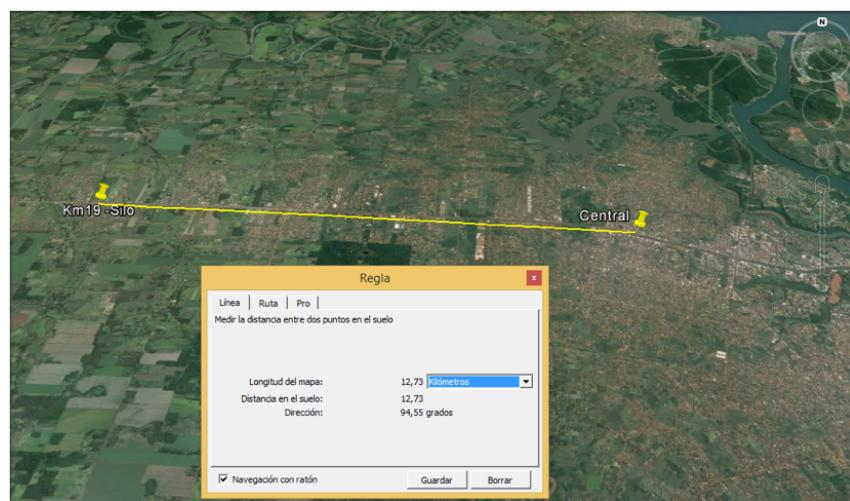


Figura 4.26: Vista con Google Earth

Capítulo 5

Procedimientos generales para la instalación de los enlaces

Para que todo se entienda mejor se procederá a una demostración bastante sencilla que se ira indicando paso a paso.

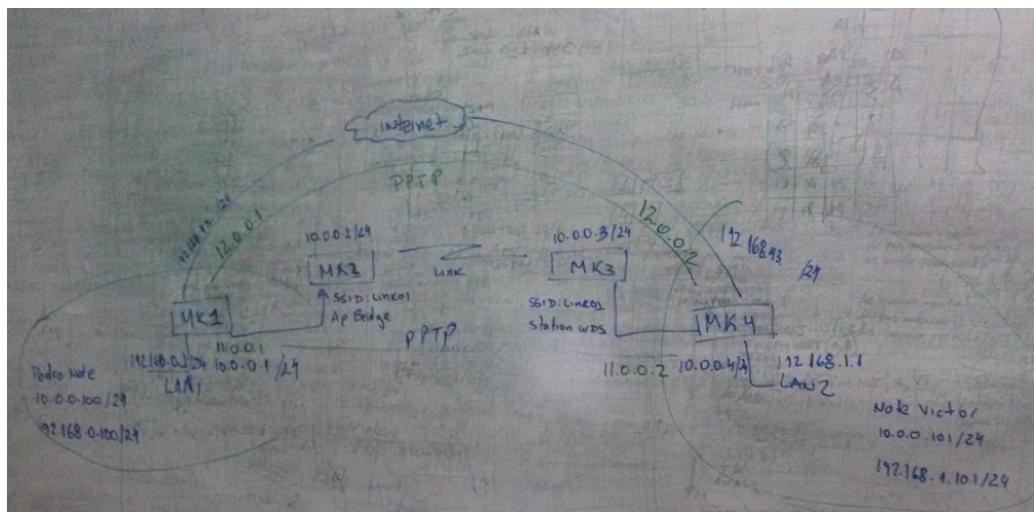


Figura 5.1: Escenario para la Simulación

Realizar un radio enlace y túnel redundante

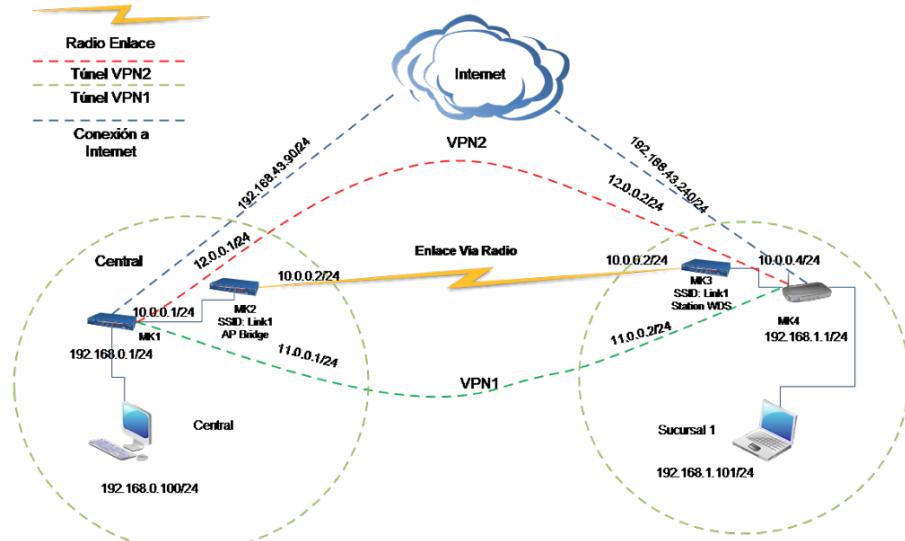


Figura 5.2: Escenario ya en limpio

5.1. Equipos a ser utilizados



Figura 5.3: Prueba de funcionamiento de los equipos

Realizar un radio enlace y túnel redundante



Figura 5.4: MK4 y MK3



Figura 5.5: MK2 y MK1

Realizar un radio enlace y túnel redundante



Figura 5.6: Notebook Central



Figura 5.7: Maquina Sucursal 1

5.2. Configuración de radios

5.2.1. Mikrotik RouterOS - enlaces punto - punto.

Para establecer la comunicación en un enlace inalámbrico punto - puntos generalmente la topología que se utiliza es la de **Access Point (AP) - Station**. Este tipo de configuración se lo hace en el modo de operación de cada main-board que forma parte del enlace.

Realizar un radio enlace y túnel redundante

Antes de iniciar con la configuración respectiva de cada equipo es importante señalar que existen algunos parámetros que se deben tomar en consideración para garantizar la conexión del enlace; entre estos parámetros se encuentra: el **SSID** de la red, seguridad WEP, la banda de operación y la frecuencia de trabajo (Únicamente en el AP, ya que la estación trabajara? en la frecuencia del AP al que se conecte.)

5.2.2. Configuración AP

Una vez inicializada nuestra consola de Winbox, accedemos al menú Interfaces, el mismo que nos presentara la ventana Interface List que me presentara? los diferentes puertos Ethernet e inalámbricos de los que disponemos.

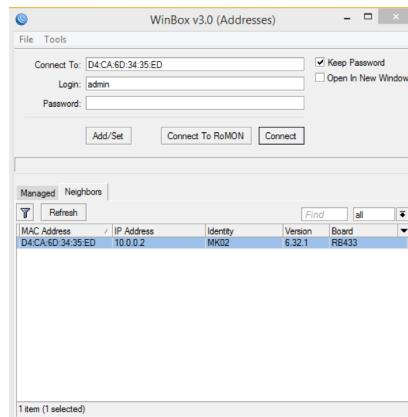


Figura 5.8: Escaneo de Routers

Realizar un radio enlace y túnel redundante

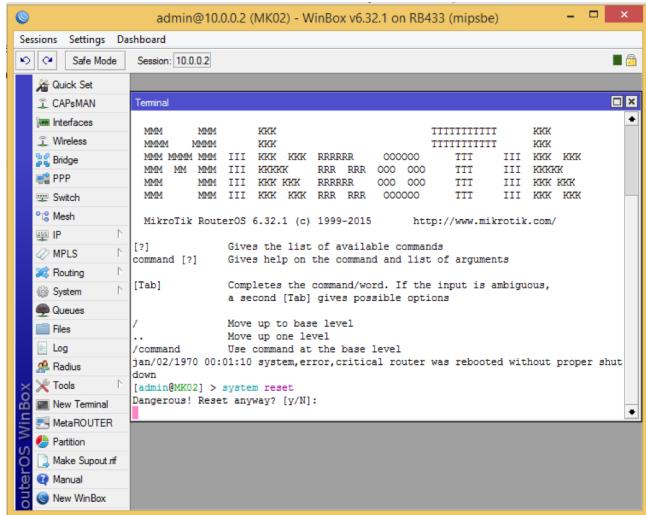


Figura 5.9: Reseteo de configuraciones

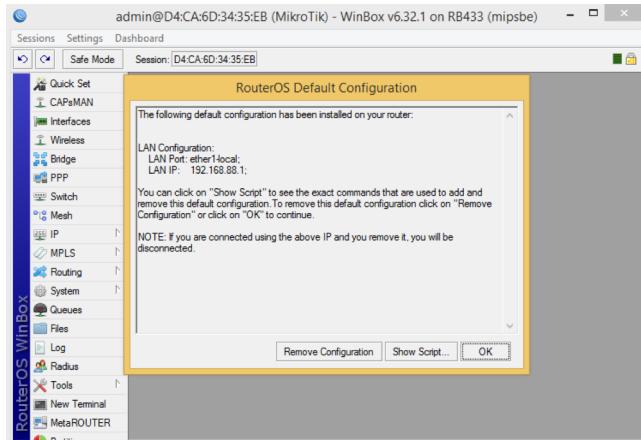


Figura 5.10: Remover configuración

Ya que la configuración es inalámbrica procedemos a la configuración de nuestra tarjeta wlan1 en el Menú Wireless wlan1 A continuación describiremos únicamente los parámetros más importantes a configurar para un enlace AP.

General

Name: Permite cambiar el nombre de la interface en la que encontramos.
Type: Muestra el tipo de chip que utiliza la mini Pci.

Realizar un radio enlace y túnel redundante

MTU: Expresa el tamaño en byte de la unidad de datos más grande que puede enviarse usando un Protocolo de Internet.

Wireless

Mode: Designa el modo de funcionamiento de la interfaz en este caso AP Bridge.

Band: hace referencia al rango de frecuencia sobre el cual se va a trabajar.
Frecuencia: Especifica el canal permanente sobre el cual se va a tratar la información.

SSID: es un código incluido en todos los paquetes que se tratan por una red inalámbrica, para identificarlos como parte de la misma.

Security Profile: Es un código Hexadecimal creado con el fin de evitar que usuarios sin una autorización formen parte de la red.

Antena Mode: Ya que las tarjetas miniPCI disponen para dos conectores, en el momento que este se conecta en el principal (main), colocamos como antena a, si por el contrario decidimos conectar al otro puerto (aux), el modo sera? antena b.

Antena Gain: Ganancia de la antena externa que estemos utilizando (en dBi). **Tx-Power:** En la opción de potencia podremos controlar la potencia de salida de las miniPCI, (en dBi).

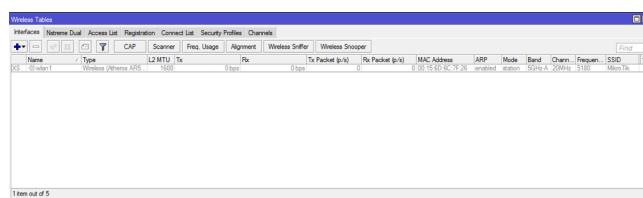


Figura 5.11: Interface Wireless disponible

Realizar un radio enlace y túnel redundante

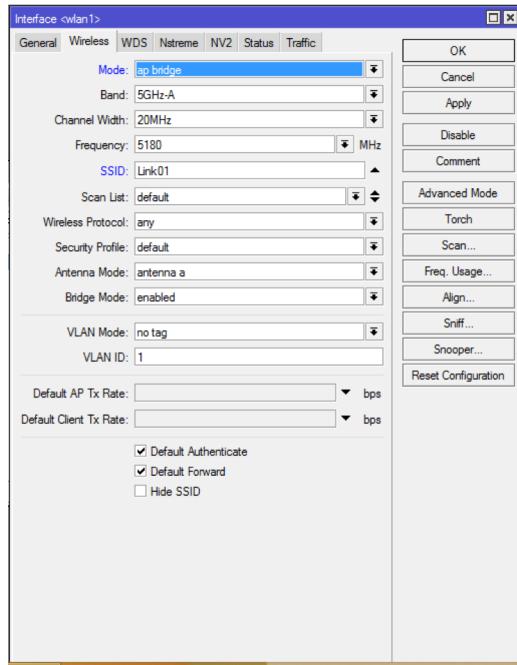


Figura 5.12: Configurar AP

Realizar un radio enlace y túnel redundante

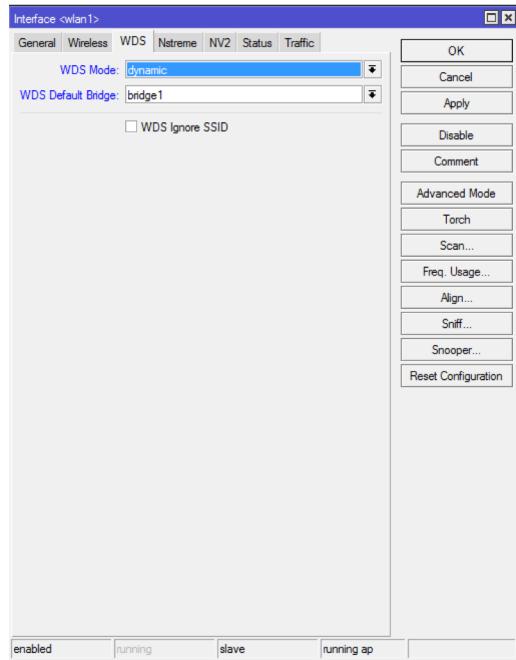


Figura 5.13: Habilitar Bridge - WDS

Wireless Tables								
Interfaces	Ntreme Dual	Access List	Registration	Connect List	Security Profiles	Channels		
[]	[]	[]	[]	[]	[]	[]	[]	[]
Radio Name / MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
00156D6...	wlan1	00:01:16	no	yes	0.000	-72/-76	6Mbps	6Mbps

Figura 5.14: Equipos ya conectado

Configuración Bridge.

El crear un bridge me permitirá comunicar dos o más interfaces dentro de una misma tarjeta; para ello seguimos los siguientes pasos:

Escoger el menú Brige → +

Realizar un radio enlace y túnel redundante

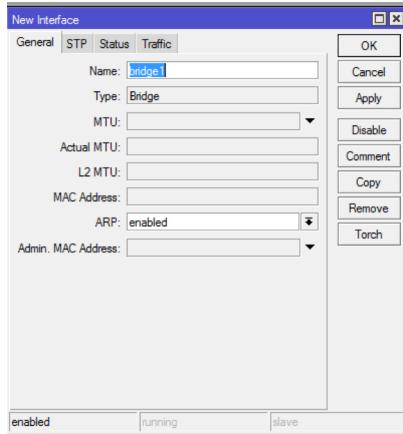


Figura 5.15: Nombre Bridge

Escoger el menú Brige → ports → +

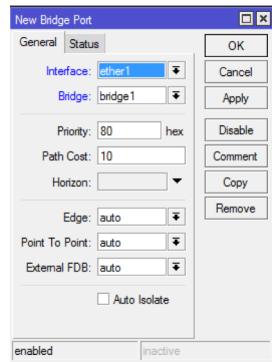


Figura 5.16: Agregar Interface al Bridge

Escoger el menú Brige → ports

Realizar un radio enlace y túnel redundante

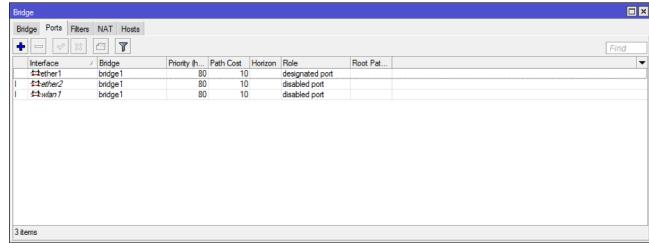


Figura 5.17: Lista de Puerto del Bridge

Escoger el menú New Terminal → ping 10.0.0.3

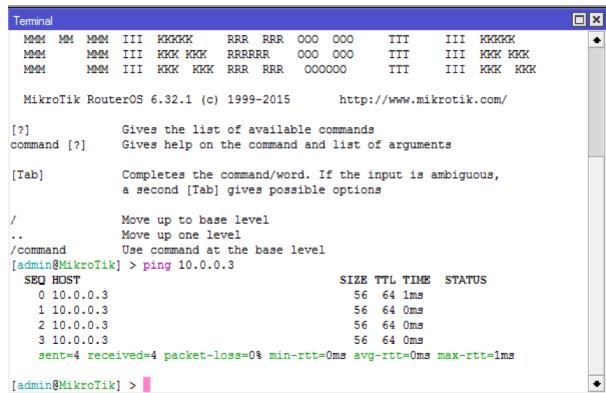


Figura 5.18: Prueba de ping al MK3

Escoger el menú Tools → Bandwidth Test

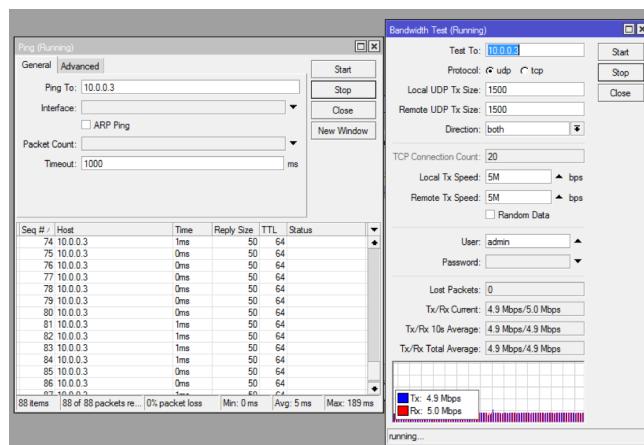


Figura 5.19: Prueba de Ancho de banda

Realizar un radio enlace y túnel redundante

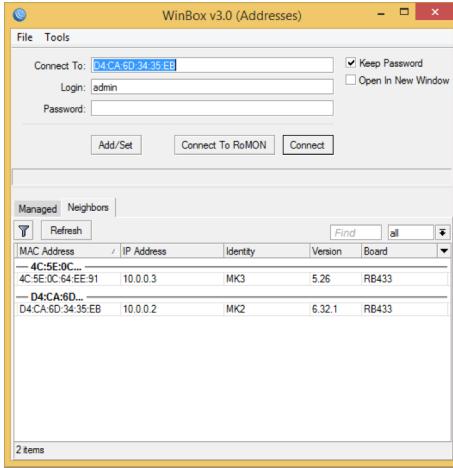


Figura 5.20: Una vez conectado, ya muestra al escanear todas las radios

Escoger el menú Inicio → ejecutar → cmd

```
C:\Windows\system32\cmd.exe
C:\Users\ect2015_up>ping 10.0.0.3
Haciendo ping a 10.0.0.3 con 32 bytes de datos:
Respuesta desde 10.0.0.3: bytes=32 tiempo=1ms TTL=64
Estadísticas de ping para 10.0.0.3:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos)
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\Users\ect2015_up>ping 10.0.0.101
Haciendo ping a 10.0.0.101 con 32 bytes de datos:
Respuesta desde 10.0.0.101: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.0.0.101: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.0.0.101: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.0.0.101: bytes=32 tiempo=15ms TTL=128
Estadísticas de ping para 10.0.0.101:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos)
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 15ms, Media = 7ms
```

Figura 5.21: Prueba de ping desde la Red Central

5.2.3. Configuración Estación.

La configuración de nuestra estación es mucho más sencilla ya que como estación tendremos que configurar únicamente los siguientes parámetros:

General

Name: Permite cambiar el nombre de la interface en la que os encontramos.
Type: Muestra el tipo de chip que utiliza la mini PCI.MTU (unidad máxima de transferencia): Expresa el tamaño en byte de la unidad de datos más grande que puede enviarse usando un Protocolo de Internet.

Realizar un radio enlace y túnel redundante

Wireless

Mode: Designa el modo de funcionamiento de la interfaz en este caso AP Bridge.

Band: hace referencia al rango de frecuencia sobre el cual se va a trabajar.

Frecuencia: Especifica el canal permanente sobre el cual se va a tratar información dado por el AP al que se conecta.

SSID: Ya que la estación pertenecerá a la misma red del AP, esta tendrá que utilizar el mismo SSID.

Security Profile: Al igual que con el SSID, la estación debe tener la misma seguridad para comunicar los dos equipos.

Antena Mode: Ya que las tarjetas miniPCI disponen para dos conectores, en el momento que este se conecta en el principal (main), colocamos como antena a, si por el contrario decidimos conectar al otro puerto (aux), el modo será antena b.

Antena Gain: Ganancia de la antena externa que estemos utilizando (en dBi).

Tx-Power: En la opción de potencia podremos controlar la potencia de salida de las miniPCI, (en dBi).

Escoger el menú **New Terminal → system reset-configuration**

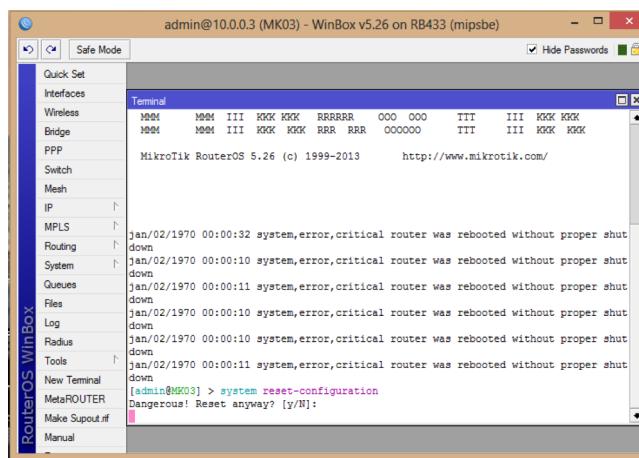


Figura 5.22: Reestablecer Configuraciones MK3

Escoger el menú **Remove Configuration**

Realizar un radio enlace y túnel redundante

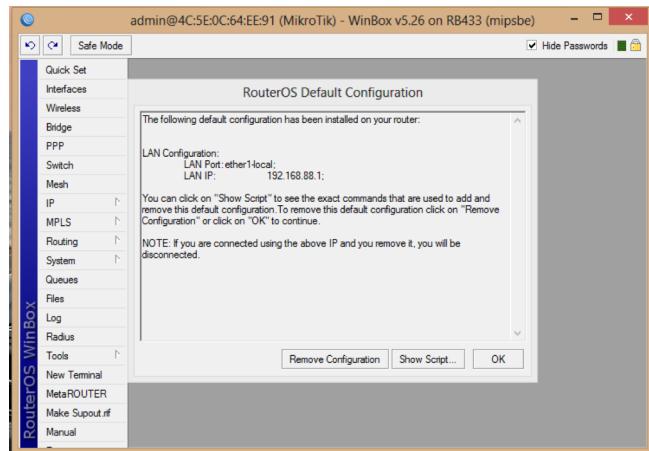


Figura 5.23: Remover configuraciones

Escoger el menú **Brige** → +

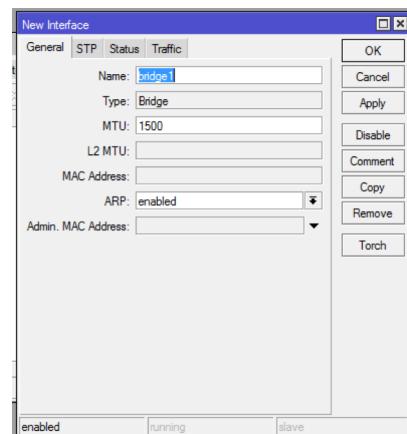


Figura 5.24: Crear Bridge

Escoger el menú **Bridge** → **Ports**

Realizar un radio enlace y túnel redundante

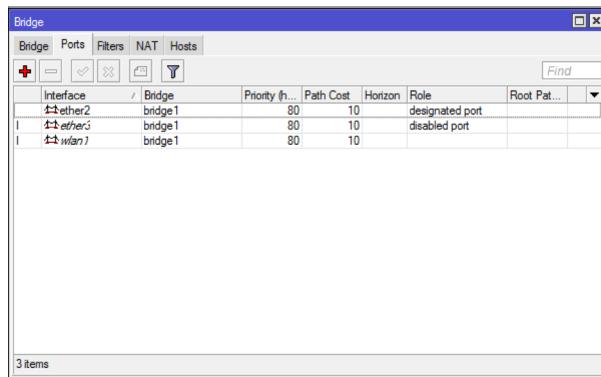


Figura 5.25: Lista de interfaces en el Bridge

Escoger el menú IP → Address → +



Figura 5.26: Configurar IP

Escoger el menú Wireless

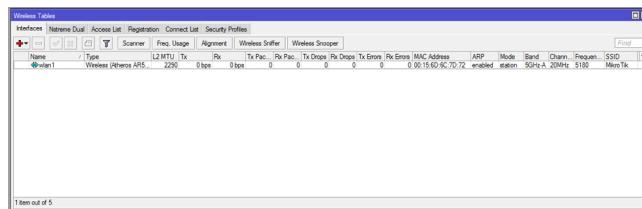


Figura 5.27: Lista Interfaces Wireless disponibles

Escoger el menú Wireless → wlan1 → Wireless

Realizar un radio enlace y túnel redundante

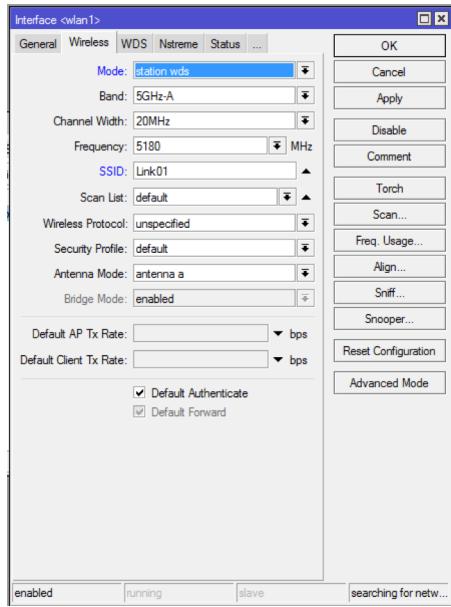


Figura 5.28: Configurar Wireless Station

Escoger el menú Wireless → wlan1 → WDS



Figura 5.29: Configura interface en la Bridge y WDS

Realizar un radio enlace y túnel redundante

5.3. Configuración de VPN

La especificación para PPTP fue publicada por el RFC 2637 [27], aunque no ha sido ratificada como estándar por el IETF.

Point-To-Point Tunneling Protocol ([PPTP](#)) permite el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual (VPN, por el anglicismo Virtual Private Network), basado en una red de trabajo vía [TCP/IP](#). El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Escoger el menú **New Terminal** → **system-reset**

5.3.1. Configuración VPN Server

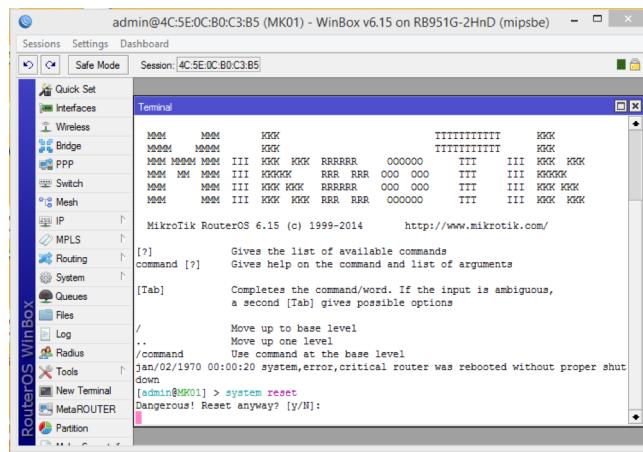


Figura 5.30: Restaurar configuraciones MK1

Escoger el menú **Mac Address** → **Connect**

Realizar un radio enlace y túnel redundante

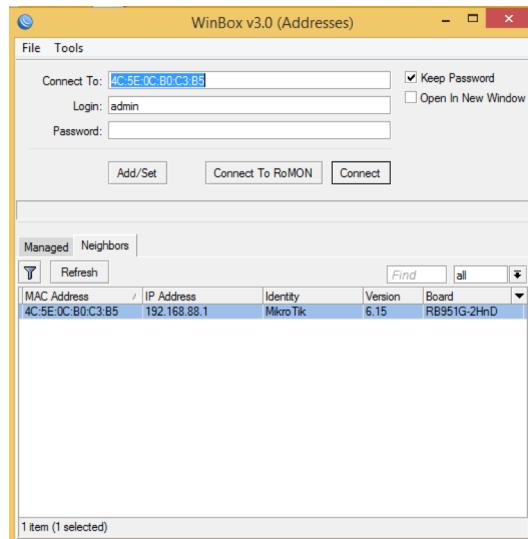


Figura 5.31: Winbox con el MK1 ya con las configuraciones de fabrica

Escoger el menú Remove Configuration

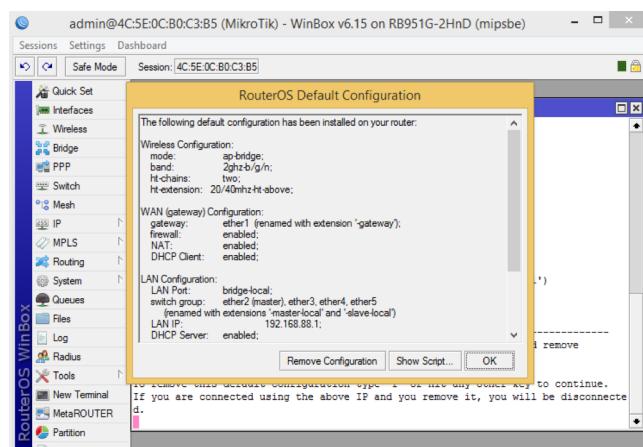


Figura 5.32: Remover configuraciones

Escoger el menú IP → Address → +

Realizar un radio enlace y túnel redundante



Figura 5.33: Configurar IP

Escoger el menú **Wireless** → **wlan1** → **Wireless**

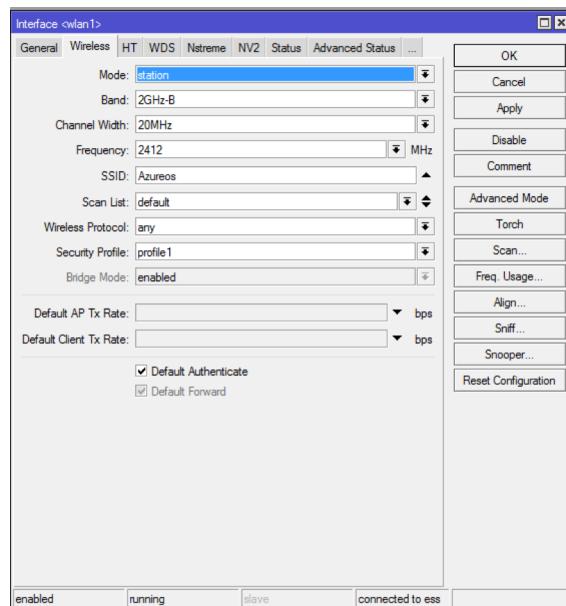


Figura 5.34: Conectar al WIFI del Celular

Escoger el menú **Wireless** → **Security Profiles** → **+**

Realizar un radio enlace y túnel redundante

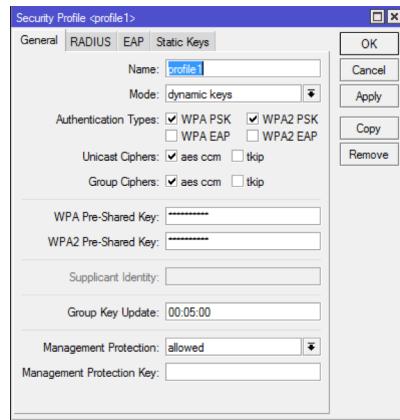


Figura 5.35: Configuraciones de Seguridad del WIFI

Realizar un radio enlace y túnel redundante



Figura 5.36: MK1 y MK4 conectado al Celular

Habilitamos el PPTP Server, para eso nos vamos a la opcion de /PPP Interface; acemos clic e el boton PPTP Server hacemos click en Enabled y en default Profile escogemos default-encryption. Aplicamos, de esta forma estamos habilitando al servidor para que permita coneccione PPTP.

Escoger el menú **PPP → PPTP-Server**

Realizar un radio enlace y túnel redundante

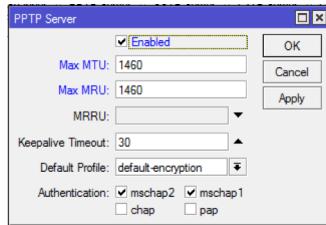


Figura 5.37: Habilitar Server PPTP

Ahora agregamos nuestros Clientes VPN, Para eso nos vamos a la pestaña Secrets, y agregamos los usuarios que sean necesarios.

Name: Nombre de Usuario VPN

Password: Contraseña del Usuario VPN

Service: Tipo de Protocolo que usara el cliente para su conección con el servidor.

Profile: Perfil de encryptación

Local Address: Dirección IP del equipo anfitrión, del router local (La IP de puerta de enlace de nuestra LAN anfitrión.)

Remote address: Dirección IP con la cual el equipo cliente se identificara en nuestra red LAN.

Escoger el menú ppp → Secret → +

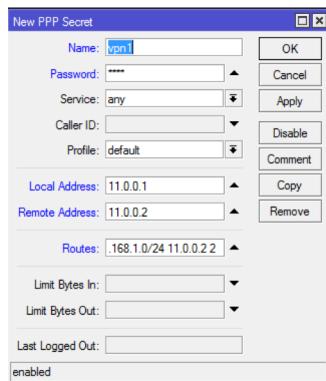


Figura 5.38: Crear usuario para Túnel por medio del Enlace

Escoger el menú ppp → Secret → +

Realizar un radio enlace y túnel redundante

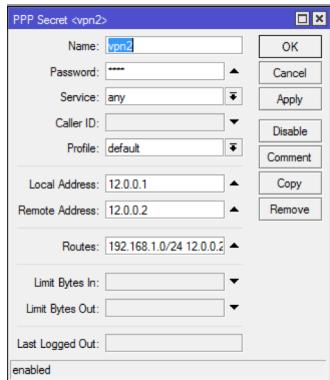


Figura 5.39: Crear usuario para el Túnel por medio de Internet

Escoger el menú **PPP → Interfaces**

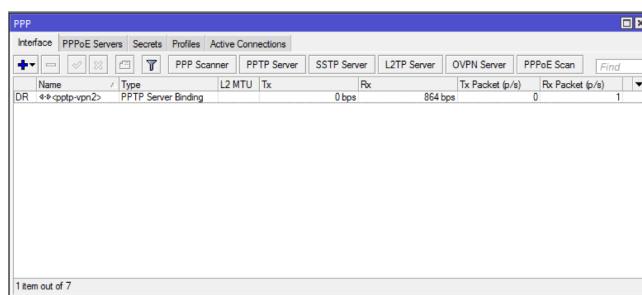


Figura 5.40: Túnel ya online

Escoger el menú **IP → Address List**

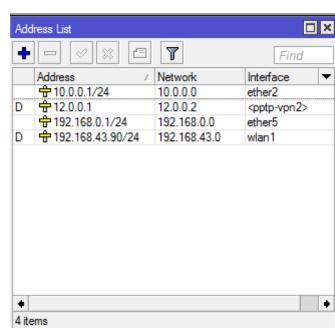


Figura 5.41: Listado de IP del MK1

Realizar un radio enlace y túnel redundante

5.3.2. Configuración VPN Cliente

Escoger el menú New Terminal → system reset-configuration

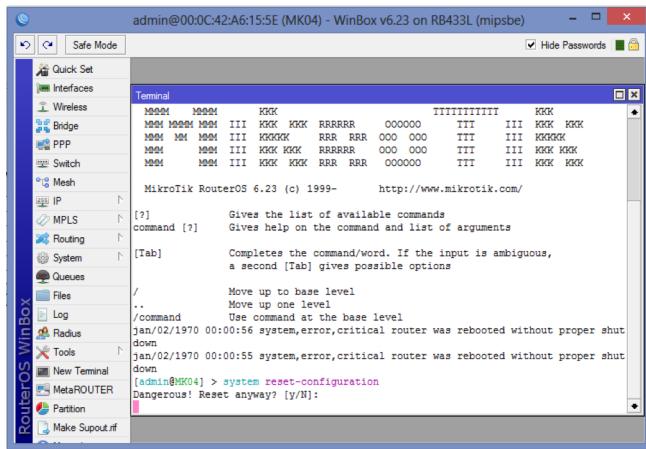


Figura 5.42: Remover configuraciones

Escoger el menú Remove Configuration

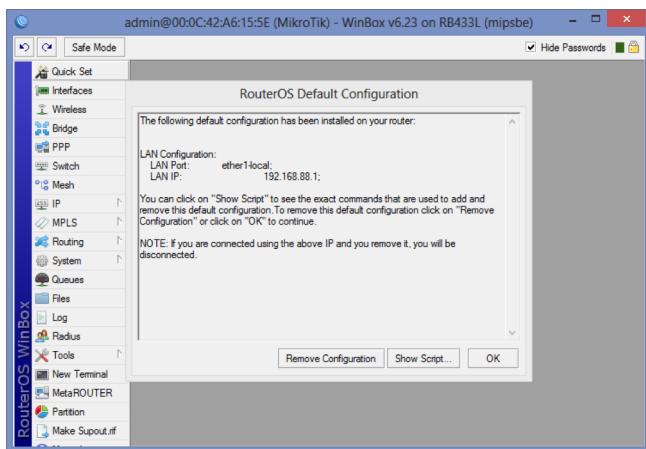


Figura 5.43: Remover configuraciones por defecto

Escoger el menú Wireless → wlan1 → Wireless

Realizar un radio enlace y túnel redundante

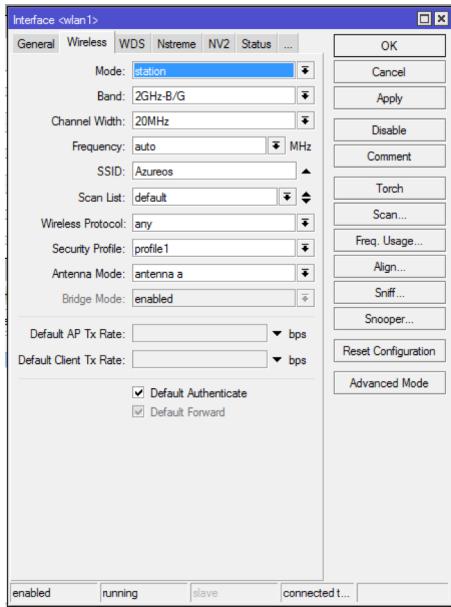


Figura 5.44: configurar WIFI

Escoger el menú **Wireless** → **Security Profiles** → **+**

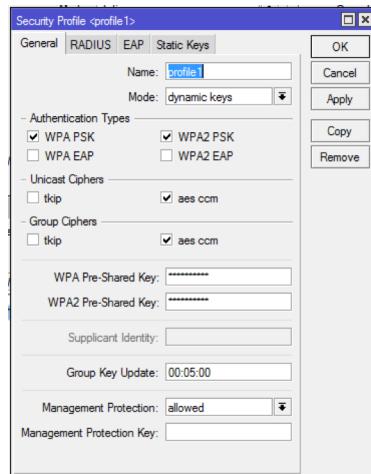


Figura 5.45: Perfil de seguridad del WIFI

Escoger el menú **IP** → **Address List**

Configurar VPN - Discadores

Address List		
Address	Network	Interface
10.0.0.4/24	10.0.0.0	ether7
D 12.0.0.2	12.0.0.1	vpn2
D 192.168.1.1/24	192.168.1.0	ether3
D 192.168.43.24...	192.168.43.0	wlan1

Figura 5.46: Lista de IP configurado MK4

Escoger el menú ppp →

PPP						
Interface	PPPoE Servers	Secrets	Profiles	Active Connections	Find	
+<ether7>	PPPoE Scanner	PPTP Server	SSTP Server	L2TP Server	OVpn Server	PPPoE Scan
Name / Type	L2 MTU	Tx Rx		Tx Packet (p/s) Rx Packet (p/s)		
***vpn1 PPTP Client		0 bps 0 bps		0 0		
R ***vpn2 PPTP Client		0 bps 480 bps		0 1		

Figura 5.47: Lista de Discadores Clientes

Configurar Discadores:

Connect To: Dirección IP con la cual el equipo cliente se identificara en nuestra re LAN

Name: Nombre de Usuario VPN

Password: Contraseña del Usuario VPN

Profile: Perfil de encryptacion Escoger el menú PPP → Secret → +

Configurar VPN - Discadores

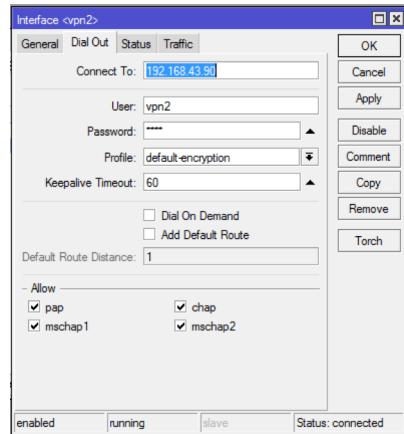


Figura 5.48: Datos Discador Cliente por Internet

Escoger el menú ppp → Secret → +

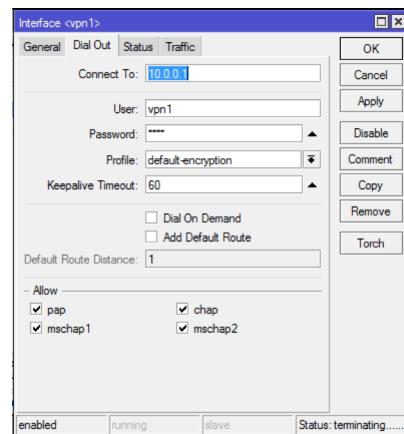


Figura 5.49: Datos Discador Cliente VPN por Enlace

Escoger el menú IP → Routes → +

Configurar VPN - Discadores

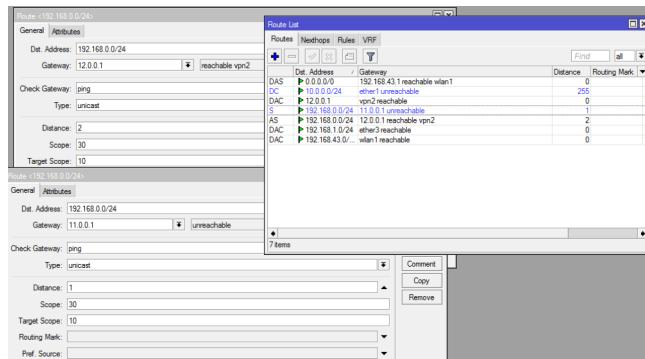


Figura 5.50: Configuraciones de Puertas de enlace

Escoger el menú Inicio → ejecutar → cmd

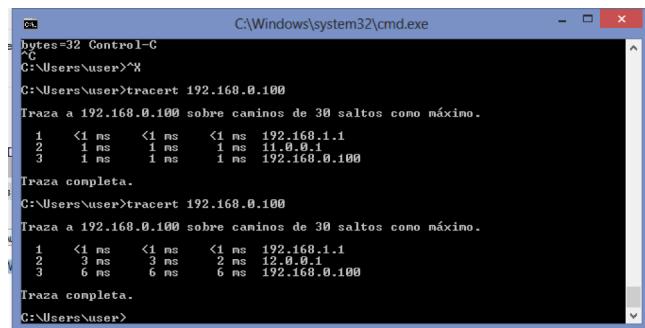


Figura 5.51: Prueba de Traceroute desde la maquina Sucursal 1

Capítulo 6

Conclusión y recomendaciones

El modelo de infraestructura que responde de manera más práctica y eficiente para la centralización de datos es utilizando VPN a través de radio enlaces y reforzando con enlaces de internet. Los equipos hardware y software utilizados para la implementación de la centralización de datos a través de VPN responden de manera eficiente al costo beneficio, la marca Mikrotik es mucha más barata que otras tecnologías de su competencia como Cisco. Presenta la robustez necesaria para los radios enlaces. La cantidad de recursos humanos necesarios y el orden de desarrollo del trabajo para la implementación de la centralización de datos a través de VPN fueron evaluados y demostraron ventajas en costos beneficios. Antes se necesitaba si o si una persona de TI por cada local, con la implementación de la centralización ya no existe esa necesidad. Además, se economiza los costos de la locomoción. Las recomendaciones para tener una seguridad mínima en la centralización de los datos a través de VPN es la administración eficiente de las mismas, ya que todos los equipos reúnen las condiciones necesarias para la implementación de la seguridad. Las 21 filiales anexadas a la central y la administración de las mismas de manera remota genera una gran economía a la empresa y es un modelo replicable a otras empresas que buscan mejor infraestructura para la administración de su información. Se recomienda la instalación de enlaces con equipamientos RouterBoard por la practicidad, robustez y economía.

Glosario

- AM** La modulación de amplitud o amplitud modulada (AM) es una técnica utilizada en la comunicación electrónica, más comúnmente para la transmisión de información a través de una onda transversal de televisión. La modulación en amplitud (AM) funciona mediante la variación de la amplitud de la señal transmitida en relación con la información que se envía.. [19](#)
- ATM** El modo de transferencia asíncrona (Asynchronous Transfer Mode, ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones, basada en la conmutación por etiquetas.. [43](#)
- CCIR** Comité Consultivo Internacional de Radiocomunicaciones (CCIR), o International Radio Consultative Committee (IRCC), con el objeto de servir como un comité de normalización de las radiocomunicaciones.. [13](#)
- dB** Expresa una razón entre cantidades y no una cantidad. El decibel expresa cuantas veces más o cuantas veces menos, pero no la cantidad exacta. Es una expresión que no es lineal, sino logarítmica. Es una unidad de medida relativa. En audiofrecuencias un cambio de 1 decibel (dB) es apenas (si hay suerte) notado.. [23](#)
- FM** La modulación de frecuencia, o frecuencia modulada (FM), es una técnica de modulación que permite transmitir información a través de una onda portadora variando su frecuencia. En aplicaciones analógicas, la frecuencia instantánea de la señal modulada es proporcional al valor instantáneo de la señal moduladora. [19](#)
- FTP** protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en

Conclusión y recomendaciones

la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.. [65](#)

IEEE 802.1Q El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).. [41](#)

Internet Internet no es del todo una red, sino un inmenso conjunto de redes diferentes que usan ciertos protocolos comunes y proporcionan ciertos servicios comunes. [\[28\]](#). [6](#)

KHz Kilohercio. [20](#)

MHz Megahercio. [20](#)

MTU es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.. [76](#)

Servidor Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como «el servidor». En la mayoría de los casos una misma computadora puede proveer múltiples servicios y tener varios servidores en funcionamiento. La ventaja de montar un servidor en computadoras dedicadas es la seguridad. Por esta razón la mayoría de los servidores son procesos diseñados de forma que puedan funcionar en computadoras de propósito específico.. [2](#)

SSH protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X (Sistema de Ventanas X) para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (en sistemas Unix y Windows).. [65](#)

SSID Service Set Identifier: es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. [74](#)

Conclusión y recomendaciones

SSL/TLS Transport Layer Security (TLS; en español seguridad de la capa de transporte) y su antecesor Secure Sockets Layer (SSL; en español capa de conexión segura) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente. [37, 38](#)

TCP/IP Protocolo de control de transmisión/Protocolo de Internet. [86](#)

Traceroute Traceroute es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de red). [97](#)

V/m Un campo eléctrico es un campo de fuerza creado por la atracción y repulsión de cargas eléctricas (la causa del flujo eléctrico) y se mide en Voltios por metro (V/m). El flujo decrece con la distancia a la fuente que provoca el campo.. [23](#)

Anexo A.

6.1. Configuraciones del MK1

```
# mar/02/2016 19:28:43 by RouterOS 6.15
# software id = SLWX-PKH2
/ip firewall nat
    add action=masquerade chain=srcnat
/system identity
    set name=MK1
/ip address
    add address=192.168.0.1/24 interface=ether5 network=192.168.0.0
    add address=10.0.0.1/24 interface=ether2 network=10.0.0.0
/ppp secret
    add local-address=11.0.0.1 name=vpn1 password=vpn1 \
        remote-address=11.0.0.2 routes="192.168.1.0/24 11.0.0.2 1"
    add local-address=12.0.0.1 name=vpn2 password=vpn2 \
        remote-address=12.0.0.2 routes="192.168.1.0/24 12.0.0.2 1"
/interface pptp-server server
    set enabled=yes max-mru=1460 max-mtu=1460
/interface wireless security-profiles
    set [ find default=yes ] supplicant-identity=MikroTik
    add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
        management-protection=allowed mode=dynamic-keys name=profile1 \
        supplicant-identity="" wpa-pre-shared-key="123.123.!" \
        wpa2-pre-shared-key="123.123.!"
/user
    add comment="system default user" group=full name=admin
/interface wireless security-profiles
    set [ find default=yes ] supplicant-identity=MikroTik
    add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
        management-protection=allowed mode=dynamic-keys name=profile1 \
        supplicant-identity="" wpa-pre-shared-key="123.123.!" \
```

Anexo A.

```
wpa2-pre-shared-key="123.123.!"  
/interface wireless  
set [ find default-name=wlan1 ] disabled=no 12mtu=2290 \  
security-profile=profile1 ssid=Azureos
```

6.2. Configuraciones del MK2

```
# mar/02/2016 19:08:54 by RouterOS 6.32.1  
# software id = U9B0-UXDW  
#  
/system identity  
set name=MK2  
  
/interface bridge  
add name=bridge1  
  
/interface bridge port  
add bridge=bridge1 interface=ether1  
add bridge=bridge1 interface=ether2  
add bridge=bridge1 interface=wlan1  
/interface bridge port  
add bridge=bridge1 interface=ether1  
add bridge=bridge1 interface=ether2  
add bridge=bridge1 interface=wlan1  
  
/ip address  
add address=10.0.0.2/24 interface=bridge1 network=10.0.0.0  
/interface wireless security-profiles  
set [ find default=yes ] supplicant-identity=MikroTik  
  
/user  
add comment="system default user" group=full name=admin  
/interface wireless  
set [ find default-name=wlan1 ] disabled=no 12mtu=1600 \  
mode=ap-bridge ssid=Link01 wds-default-bridge=bridge1 \  
wds-mode=dynamic  
  
/interface wireless security-profiles  
set [ find default=yes ] supplicant-identity=MikroTik
```

6.3. Configuraciones del MK3

```
# mar/02/2016 19:09:40 by RouterOS 5.26
# software id = IKF9-H3ZS
#
/system identity
    set name=MK3

/interface bridge
    add admin-mac=00:00:00:00:00:00 ageing-time=5m arp=enabled \
        auto-mac=yes disabled=no forward-delay=15s 12mtu=1522 \
        max-message-age=20s mtu=1500 name=bridge1 priority=0x8000 \
        protocol-mode=none transmit-hold-count=6

/interface bridge port
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=wlan1 path-cost=10 point-to-point=auto \
        priority=0x80
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=ether2 path-cost=10 point-to-point=auto \
        priority=0x80
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=ether3 path-cost=10 point-to-point=auto \
        priority=0x80
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=ether1 path-cost=10 point-to-point=auto \
        priority=0x80

/interface bridge settings
    set use-ip-firewall=no use-ip-firewall-for-pppoe=no \
        use-ip-firewall-for-vlan=no
/interface bridge port
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=wlan1 path-cost=10 point-to-point=auto \
        priority=0x80
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=ether2 path-cost=10 point-to-point=auto \
        priority=0x80
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=ether3 path-cost=10 point-to-point=auto \
        priority=0x80
    add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
        horizon=none interface=ether1 path-cost=10 point-to-point=auto \
        priority=0x80
```

Anexo A.

```
add bridge=bridge1 disabled=no edge=auto external-fdb=auto \
horizon=none interface=ether1 path-cost=10 point-to-point=auto \
priority=0x80

/ip dns
set allow-remote-requests=no cache-max-ttl=1w cache-size=2048KiB \
max-udp-packet-size=4096 servers=""

/ip address
add address=10.0.0.3/24 disabled=no interface=bridge1 \
network=10.0.0.0

/interface pptp-server server
set authentication=mschap1,mschap2 default-profile=default-\
encryption enabled=no keepalive-timeout=30 max-mru=1460 max-\
mtu=1460 mrru=disabled

/interface wireless security-profiles
set [ find default=yes ] authentication-types="" eap-met\
hods=passthrough group-ciphers=aes-ccm group-key-update=5m\
interim-update=0s \
management-protection=disabled management-protection-key=""\
mode=none \
name=default radius-eap-accounting=no radius-mac-accounting=no \
radius-mac-authentication=no radius-mac-caching=disabled \
radius-mac-format=XX:XX:XX:XX:XX:XX radius-mac-mode=as-username \
static-algo-0=none static-algo-1=none static-algo-2=none static-\
algo-3=none static-key-0="" static-key-1="" static-key-2="" \
static-key-3="" static-sta-private-algo=none static-sta-private-\
key="" static-transmit-key=key-0 supplicant-identity=MikroTik \
tls-certificate=none tls-mode=no-certificates unicast-ciphers=\
aes-ccm wpa-pre-shared-key="" wpa2-pre-shared-key=""

/user group
set read name=read policy="local,telnet,ssh,reboot,read\
,test,winbox,password,web,sniff,sensitive,api,!ftp,!write\
,!policy" skin=default
set write name=write policy="local,telnet,ssh,reboot,read, \
write,test,winbox,password,web,sniff,sensitive,api,!ftp,!po\
licy" skin=default set full name=full policy="local,telnet, \
ssh,ftp,reboot,read,write,policy,test,winbox,password,web,sn\
iff,sensitive,api" skin=default
```

Anexo A.

```
/user
    add address="" comment="system default user" disabled=no \
        group=full name=admin
/user aaa
    set accounting=yes default-group=read exclude-groups="" \
        interim-update=0s use-radius=no

/interface wireless security-profiles
    set [ find default=yes ] authentication-types="" eap-\
        methods=passthrough group-ciphers=aes-ccm group-key-\
        update=5m interim-update=0s management-protection=disa\
            bled management-protection-key="" mode=none name=default \
            radius-eap-accounting=no radius-mac-accounting=no radius-\
            mac-authentication=no radius-mac-caching=disabled radius-\
            mac-format=XX:XX:XX:XX:XX:XX radius-mac-mode=as-username \
            static-algo-0=none static-algo-1=none static-algo-2=none \
            static-algo-3=none static-key-0="" static-key-1="" static\
                -key-2="" static-key-3="" static-sta-private-algo=none \
            static-sta-private-key="" static-transmit-key=key-0 suppl\
                icant-identity=MikroTik tls-certificate=none tls-mode=no-\
                certificates unicast-ciphers=aes-ccm wpa-pre-shared-key=\
                    "" wpa2-pre-shared-key=""
/interface wireless
    set 0 adaptive-noise-immunity=none allow-sharedkey=no \
        antenna-gain=0 antenna-mode=ant-a area="" arp=enabled \
        band=5ghz-a basic-rates-a/g=6Mbps bridge-mode=enabled \
        burst-time=disabled channel-width=20mhz compression=\
            no country=no_country_set default-ap-tx-limit=0 \
            default-authentication=yes default-client-tx-limit=0 \
            default-forwarding=yes dfs-mode=none disable-running-\
            check=no disabled=no disconnect-timeout=3s distance=\
            dynamic frame-lifetime=0 frequency=5180 frequency-mode=\
            manual-txpower frequency-offset=0 hide-ssid=no hw-fragmen\
                tation-threshold=disabled hw-protection-mode=none hw-prote\
                    ction-threshold=0 hw-retries=7 12mtu=2290 mac-address=\
                    00:15:6D:6C:7D:72 max-station-count=2007 mode=station-wds \
                    mtu=1500 multicast-helper=default name=wlan1 noise-floor-\
                    threshold=default nv2-cell-radius=30 nv2-noise-floor-\
                    offset=default nv2-preshared-key="" nv2-qos=default nv2-\
                    queue-count=2 nv2-security=disabled on-fail-retry-time=100ms \
```

Anexo A.

```
periodic-calibration\
=default periodic-calibration-interval=60 preamble-mode=both \
proprietary-extensions=post-2.9.25 radio-name=00156D6C7D72 \
rate-selection=advanced rate-set=default scan-list=default \
security-profile=default ssid=Link01 station-bridge-clone-mac=\
00:00:00:00:00:00 supported-rates-a/g=\
6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,54Mbps tdma-period\
-size=2 tx-power-mode=default update-stats-interval=disabled wds-\
cost-range=50-150 wds-default-bridge=bridge1 wds-default-cost=100\
wds-ignore-ssid=no wds-mode=dynamic wireless-protocol=unspecified \
wmm-support=disabled
/interface wireless manual-tx-power-table
set wlan1 manual-tx-powers="1Mbps:17,2Mbps:17,5.5Mbps:17, \
11Mbps:17,6Mbps:17,9Mbps:17,12Mbps:17,18Mbps:17,24Mbps:17, \
36Mbps:17,48Mbps:17,54Mbps:17,HT20-0:17,HT20-1:17,HT20-2:17, \
HT20-3:17,HT20-4:17,HT20-5:17,HT20-6:17,HT20-7:17,HT40-0:17, \
HT40-1:17,HT40-2:17,HT40-3:17,HT40-4:17,HT40-5:17,HT40-6:17, \
HT40-7:17"
/interface wireless nstreme
set wlan1 disable-csma=no enable-nstreme=no enable-polling=yes \
framer-limit=3200 framer-policy=none
/interface wireless align
set active-mode=yes audio-max=-20 audio-min=-100 audio-monitor=\
00:00:00:00:00:00 filter-mac=00:00:00:00:00:00 frame-size=300 \
frames-per-second=25 receive-all=no ssid-all=no
/interface wireless sniffer
set channel-time=200ms file-limit=10 file-name="" \
memory-limit=10 multiple-channels=no only-headers=no \
receive-errors=no streaming-enabled=no streaming-max-rate=0 \
streaming-server=0.0.0.0
/interface wireless snooper
set channel-time=200ms multiple-channels=yes receive-errors=no
```

6.4. Configuraciones del MK4

```
# mar/02/2016 19:04:59 by RouterOS 6.23
# software id = K9T9-NOKR
#
/system identity
set name=MK4
```

Anexo A.

```
/ip firewall nat
add action=masquerade chain=srcnat

/ip address
add address=10.0.0.4/24 interface=ether2 network=10.0.0.0
add address=192.168.1.1/24 interface=ether3 network=192.168.1.0

/ip route
add check-gateway=ping distance=1 dst-address=192.168.0.0/24 \
gateway=11.0.0.1
add check-gateway=ping distance=2 dst-address=192.168.0.0/24 \
gateway=12.0.0.1

/interface pptp-client
add add-default-route=no allow=pap,chap,mschap1,mschap2 \
connect-to=10.0.0.1 dial-on-demand=no disabled=no \
keepalive-timeout=60 max-mru=1460 max-mtu=1460 mrru=1600 \
name=vpn1 password=vpn1 profile=default-encryption user=vpn1

add add-default-route=no allow=pap,chap,mschap1,mschap2 \
connect-to=192.168.43.90 dial-on-demand=no disabled=no \
keepalive-timeout=60 max-mru=1460 max-mtu=1460 mrru=1600 \
name=vpn2 password=vpn2 profile=default-encryption user=vpn2

/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
management-protection=allowed mode=dynamic-keys name=profile1 \
supplicant-identity="" wpa-pre-shared-key="123.123.!" \
wpa2-pre-shared-key="123.123.!"

/user
add comment="system default user" group=full name=admin

/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
management-protection=allowed mode=dynamic-keys \
name=profile1 supplicant-identity="" \
wpa-pre-shared-key="123.123.!"wpa2-pre-shared-key="123.123.!"
/interface wireless
```

Anexo A.

```
set [ find default-name=wlan1 ] band=2ghz-b/g disabled=no \
frequency=auto 12mtu=2290 security-profile=profile1 \
ssid=Azureos
```

Referencias bibliográficas

- [1] E. Pietrosemoli, *Redes Inalambricas en los paises en desarollo*, 4th ed., ser. Electric Power Engineering Handbook, J. Butler, Ed. janes-butler@networktheworld.org: networktheworld.org, 2013.
- [2] S. C. K. Mauricio, “Estudio e implementacion de un radio enlace con tecnología mikrotik para el isp jjsistemas en el cantón gualaquiza, provincia morona santiago,” 2010.
- [3] “Propagación de las ondas radioeléctricas.” [Online]. Available: <http://www.capa-f2.com/propagondas.html>
- [4] M. R. Mansilla, *Redes VPNs de acceso remoto*. Univesidad Nacional de Patagonia San juan Bosco, 2009.
- [5] Recursos-as400, “La importancia de centralizar la información de seguridad a nivel corporativo.” Febrero 2003. [Online]. Available: <http://www.recursos-as400.com/tendenciasit004.shtml>
- [6] D. X. G. Villafranca, *Fortalecimiento Tecnológico del Sector Social Mexicano*. Escuela Superior de Ingeniería Mexcánica y Eléctrica, 1986.
- [7] F. García Cordoba, *La investigación tecnológica: Investigar, idear e innovar en Ingenierías y Ciencias Sociales*. Mexico: Limusa, 2007.
- [8] J. Guitierrez, *Protocolos criptográficos y seguridad en redes*. Universidad de Cantabria, 2003.
- [9] ——, *Protocolos criptográficos y seguridad en redes*. Universidad de Cantabria.
- [10] “Diseño de un sistema de seguridad informática para la red lan de telecomunicaciones del ministerio de minas y petroleos,” 2012. [Online]. Available: <http://bibdigital.epn.edu.ec/bitstream/15000/4662/1/CD-4294.pdf>

Anexo A.

- [11] QA:NEWS, “Evaluación de la seguridad de los sistemas informáticos: Polícias, estándares y análisis de riesgos?” Abril 2013. [Online]. Available: goo.gl/VSM4Xo
- [12] “Introducción a la seguridad en internet y aplicaciones,” 2004.
- [13] ITU, “Focus on radiocommunication.” [Online]. Available: <http://www.itu.int/en/history/Pages/FocusOnRadiocommunication.aspx>
- [14] A. F. García, “La ley de snell de la refracción.” [Online]. Available: <http://www.sc.ehu.es/sbweb/fisica/ondas/snell/snell.htm>
- [15] J. L. Giordano, “La radio,” 2009.
- [16] “The internet protocol journal,” 2014.
- [17] E. Unicrom, “Las microondas aplicaciones, frecuencias, longitudes de onda.” [Online]. Available: <http://unicrom.com/las-microondas-aplicaciones-frecuencia-longitudes-onda/>
- [18] D. J. Whalen, “Communications satellites: Making the global village possible.” [Online]. Available: <http://www.hq.nasa.gov/office/pao/History/satcomhistory.html>
- [19] “The internet protocol journal,” 2001.
- [20] D. O. R. López, “El cifrado web (ssl/tls),” 2011.
- [21] mikrotik.com, “Mikrotik routeros,” 2010.
- [22] ——, “Mikrotik routeros.” [Online]. Available: <http://www.mikrotik.com/download>
- [23] J. R. J. Postel, “Especificación del protocolo telnet.” [Online]. Available: <https://www.rfc-es.org/rfc/rfc0854-es.txt>
- [24] R. H. Enterprise, “Red hat enterprise linux 4 manual de referencia - capítulo 20. protocolo ssh.” [Online]. Available: <http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/ch-ssh.html>
- [25] U. A. de México, “Radio mobile,” Octubre 2015. [Online]. Available: <http://www.cplus.org/rmw/rme.html>
- [26] G. Inc., “Google earth.” [Online]. Available: <http://www.google.com/earth/>

Anexo A.

- [27] K. Hamzeh, “Point-to-point tunneling protocol (pptp).” [Online]. Available: <https://tools.ietf.org/html/rfc2637>
- [28] A. S. Tanenbaum, *Redes de computadoras*, 4th ed., P. H. México, Ed., 2003.