ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

SOLUCIÓN DE FIREWALL CON ALTA DISPONIBILIDAD PARA REDES CORPORATIVAS UTILIZANDO VYATTA CON VIRTUALIZACIÓN

AUTOR: FELIPE ANDRÉS ORDÓÑEZ GALIANO

SANGOLQUÍ – ECUADOR

2012

AGRADECIMIENTO

A la Escuela Politécnica del Ejército, que me acogió durante un largo periodo de mi vida para formar mi carácter, mi capacidad de razonamiento y en conclusión por enseñarme a ser libre mediante el conocimiento.

Al Ing. Carlos Romero, Director de la presente tesis de grado, por guiarme en cada uno de los pasos que debía tomar para el desarrollo de este proyecto con paciencia y objetividad.

Al Ing. Darwin Aguilar, Codirector, por su apoyo constante para la ejecución de este proyecto, por su comprensión, interés e incentivo para la finalización de esta meta.

A mi madre por ser la amiga que me ayudó en cada lapso de mi vida mediante su incondicional amor, ejemplo y por ser mi más grande orgullo.

A mi padre por ser el promotor de mi educación, por su preocupación, por su apoyo incondicional en todo momento de mi vida.

A mi hermano querido, por ser mi más grande amigo.

A mi hermana querida, por recibir su apoyo cuando más lo necesito.

A mi familia materna, por que en su seno he encontrado permanentemente, comprensión, cariño y apoyo incondicional.

A mi familia paterna, por cultivar en mí valores humanos, espirituales y carácter apropiado para enfrentar los desafíos del mundo.

DEDICATORIA

A mis padres...

Ya que este logro de mi vida se dá gracias a su esfuerzo, trabajo y dedicación por cultivar una enseñanza de valores humanos y espirituales en su primogénito; por que de su sacrificio obtuve todo en la vida para poder educarme; extiendo mi compromiso de continuar entregándoles satisfacciones, por que han sido mi ejemplo y mis mejores amigos.

Con amor Felipe Andrés Ordóñez Galiano

PRÓLOGO

En la actualidad las redes de datos se han convertido en uno de los puntos más relevantes para el desarrollo de una organización, de tal manera que la misma debe tener grandes capacidades de desempeño y funcionalidad, debe ser tolerante a fallos como también tener sistemas de seguridad para mantenerla protegida de intrusos, ataques, etc.

Existen diversas soluciones para hacer que una red de datos este protegida, una de estas es usando un firewall, que es un sistema diseñado para permitir o denegar el paso de paquetes a través de la red de datos, dicho de diferente forma, es un sistema que delimita la conexión entre dos redes.

La alta disponibilidad es un protocolo o sistema diseñado que asegura un cierto grado absoluto de continuidad operacional durante un periodo de medición dado. Las redes de datos tienen que haber sido configuradas para producir la menor cantidad de tiempo de inactividad o falta de disponibilidad, la alta disponibilidad se puede conseguir mediante el buen uso de las herramientas que el hardware y software proporcionan para que la red sea robusta, por ejemplo, se pueden usar componentes redundantes.

En conclusión una red de datos robusta es aquella que está protegida y tiene características de alta disponibilidad. Vyatta es un software que permite dar estas características a redes de cualquier tamaño, en este proyecto se analizará la capacidad que tiene Vyatta para proveer alta disponibilidad y administración a una red corporativa siendo este implementado con los mínimos recursos físicos.

ÍNDICE DE CONTENIDO

CAPÍTULO I

ASPECTOS GENERALES

1.1. ANTECEDENTES

Las redes de datos son sistemas que se diseñan y construyen en arquitecturas que pretenden servir de la mejor forma a sus objetivos de uso, estos sistemas enlazan dos puntos a través de medios físicos, para así movilizar los paquetes de datos, durante esta movilización, dichos medios físicos llegan a producir errores, o bien pueden terminar deshabilitándose por algún fallo.

Una red de datos tiene que ser lo suficientemente robusta, para poder soportar cualquier tipo de eventualidad, aún así, siempre quedan brechas por donde los problemas pueden filtrarse, una de las soluciones consiste en por lo menos, mantener los puntos más críticos de las redes de datos lo más protegidos posible, tanto nivel físico como también en el resto de los niveles de una arquitectura TCP/IP, así la información que recorre a través de la red siempre estará disponible, sin errores y lo más fluida posible.

Dentro de las redes de datos, uno de los dispositivos críticos importantes son los routers, debido a que estos son los equipos periféricos en la red y mantienen la conexión con internet junto a un firewall de protección; debido a esto los routers deben ser protegidos, pero siempre queda una brecha en la que un fallo inminente puede producirse, entonces se deberá buscar una solución más segura. A partir de estos problemas nacen los conceptos de redundancia y alta disponibilidad de las redes de datos que se definen a continuación:

- “La “redundancia” se basa en la filosofía de utilizar distintas tecnologías para enlaces primarios y secundarios de tal forma que los fenómenos que afectan al primero no interrumpan al segundo, así aumentando la disponibilidad de la doble conectividad” [1].

- La “alta disponibilidad” consiste en una serie de medidas tendientes a garantizar la “disponibilidad” de que el servicio funcione durante las veinticuatro horas que hace referencia a la probabilidad de que un servicio funcione adecuadamente en cualquier momento. “La disponibilidad se expresa con mayor frecuencia a través del índice de disponibilidad, un porcentaje, que se mide dividiendo el tiempo durante el cual el servicio está disponible por el tiempo total, entonces por ejemplo un índice de disponibilidad del 99.99% es determinado si es que en 24 horas el servicio fallo 53 minutos, un índice de disponibilidad del 99.9999% se determina si en 24 horas el servicio falló 32 segundos” [2]. Ninguna organización debe dejar de prestarle atención a la efectividad de sus redes de datos, un fallo en esta podría producir la perdida de muchos bienes, es por esta razón que toda red de datos debe tener planes de contingencia para conseguir la alta disponibilidad. Mediante un estudio realizado txsolutions que es una empresa con trayectoria y confiable, “se demuestra la pérdida que sufre una empresa que factura alrededor de 2,000,000,000.00 USD al año. Una forma rápida de hacer el cálculo es: 2,000,000,000 USD se dividen por 4380 horas de trabajo al año y se multiplica por 3 horas perdidas, lo que nos arroja un total de 1′369,863.01 USD” [3].

Cuando se piensa en alta disponibilidad no necesariamente se debe pensar en arquitectura de hardware y software de alto costo, existen soluciones de alta disponibilidad que se ajustan a la realidad de muchas empresas. “Una solución de alta disponibilidad va a ser aquella que permite que los sistemas de información operativos de nuestra empresa estén disponibles las 24 horas de los 7 días de la

semana. Al implementar esta solución las empresas pueden contar con la seguridad de no perder negocios ni información debido a fallas en los sistemas" [4].

1.2. JUSTIFICACIÓN

Mediante la virtualización de algunos dispositivos críticos de red se logra abastecer de alta disponibilidad a esta red, uno de estos puntos críticos es el firewall, este dispositivo permite filtrar los datos que entran o salen de la red local, evitando la invasión de intrusos, por esta razón se lo considera crítico.

La virtualización permite optimizar la infraestructura de red, ya que podemos conseguir los mayores beneficios sin tener que gastar más dinero en equipos, también nos permite balancear la carga de trabajo de un dispositivo de los recursos existentes, se pueden replicar máquinas virtuales de los servidores críticos y probar varios entornos sobre un pequeño número de entornos físicos.

"En la actualidad, la importancia de los servicios que se brindan en una red corporativa y el avance del software para la creación de máquinas virtuales, han permitido desarrollar sistemas operativos que se pueden levantar a un bajo costo, los mismos que dotarían a la red de funcionalidades de redundancia y alta disponibilidad, tal es el caso del software desarrollado por la organización Vyatta" [5], el cual corre en arquitecturas x86 y proporciona funciones avanzadas de networking, tiene similares características a los equipos Cisco pero a costos inferiores. Vyatta mantiene una plataforma libre así como una pagada, la libre se diferencia de la comercial principalmente por el soporte que ofrecen los técnicos de esta organización.

Los equipos Cisco son de los más vendidos en el mercado, por la gran estabilidad que tienen y las soluciones que ofrecen, al comparar un equipo cisco

de gama media frente a un equipo clon común que tenga instalado Vyatta como sistema operativo, los resultados son prácticamente los mismos en cuanto a desempeño en software y hardware, pero al momento de tomar en cuenta el costo, Vyatta tiene las de ganar. Así se puede destacar la gran importancia que genera la posibilidad de virtualizar un firewall con Vyatta para obtener alta disponibilidad en una red de datos, Vyatta no sólo permitirá reemplazar en un momento de riesgo un firewall, sino que también nos ahorrará grandes cantidades de dinero en la implementación del sistema tolerante a fallas.

1.3. FUNDAMENTO TEÓRICO

1.3.1. Introducción

En la actualidad las redes de datos se han convertido en uno de los puntos más relevantes para el desarrollo de una organización, de tal manera que la misma debe tener grandes capacidades de desempeño y funcionalidad, debe ser tolerante a fallos como también tener sistemas de seguridad para mantenerla protegida de intrusos, ataques, etc.

Existen diversas soluciones para hacer que una red de datos este protegida, una de estas es usando un firewall, que es un sistema diseñado para permitir o denegar el paso de paquetes a través de la red de datos, dicho de diferente forma, es un sistema que delimita la conexión entre dos redes, cifra y descifra el tráfico entre diferentes ámbitos en base a un conjunto de normas y criterios. La tecnología firewall surgió a finales de 1980, cuando internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad.

“Sus predecesores directos fueron los routers, que mantenían a las redes separadas unas de otras. Existen diversos tipos, de entre ellos están:

- Nivel de Aplicación de Pasarela.- Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet.

- Circuito a Nivel de Pasarela.- Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida.

- Firewall de Capa de Red.- Funciona a nivel de red como filtro de paquetes IP.

- Firewall de Capa de Aplicación.- Trabaja en el nivel de aplicación, de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel.

- Firewall Personal.- Es un caso particular de firewall que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red.

Un firewall es excelente al momento de bloquear el acceso a personas y/o aplicaciones no autorizadas a redes privadas, pero también se debe tener presente que un firewall no puede proteger de las amenazas a las que está sometido por ataques internos.” [7]

Hoy en día toda organización debe tener implementado un sistema de seguridad firewall en su red de datos, de tal manera que vuelva a esta más robusta y confiable, el no tomar en cuenta este tipo de sistemas provocará que la red se vea frágil ante cualquier intruso y por tanto a ataques de denegación de servicio, robo de información, ataques por fuerza bruta, etc.

1.3.2. Alta disponibilidad en redes de datos

1.3.2.1. Conceptos

"La alta disponibilidad es un protocolo o sistema diseñado que asegura un cierto grado absoluto de continuidad operacional durante un periodo de medición dado. Consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio." [9]

"Las redes de datos tienen que haber sido configuradas para producir la menor cantidad de tiempo de inactividad o falta de disponibilidad" [10], la alta disponibilidad se puede conseguir recurriendo al mínimo el error que se puede producir por hardware o software, también es posible mediante el buen uso de las herramientas que el hardware y software proporcionan para que la red sea robusta, por ejemplo, se pueden usar componentes redundantes y aislantes.

"El objetivo es eliminar los periodos de falta de servicio al usuario, a estas se las llama paradas y pueden ser de dos tipos:

- Paradas planificadas: Aquellas debidas a actualizaciones de software, hardware o mantenimiento preventivo.

- Paradas no planificadas: Son las causadas por un mal funcionamiento del hardware, software o bien un desastre natural." [11]

Toda red de datos debe ser tolerante a para poder alcanzar la alta disponibilidad. Los sistemas tolerantes a fallos implican la redundancia de los componentes de hardware, por tanto un gasto económico, mientras que los sistemas que usan técnicas de clustering o VRRP implican un menor costo,

puesto que no hace falta usar hardware específico, también ofrecen balanceo de carga, esto provocaría que los costos se vean mucho más disminuidos en relación a la redundancia.

1.3.2.2. Redundancia

Dependiendo de la disponibilidad que requiera cada organización, se necesitará que no exista puntos intolerantes a fallas, respecto a hardware o software, todos estos puntos en la red deben ser redundantes.

Los sistemas de red redundantes son aquellos en los que se repiten datos o hardware de carácter crítico, mismos que se quiere asegurar ante los posibles fallos que puedan surgir.

Algunos componentes de hardware son diseñados para proveer servicios de alta disponibilidad, por tanto es posible configurarlos con capacidades redundantes, esto quiere decir que si un equipo falla, inmediatamente otro entrará en funcionamiento para reemplazar este.

Cuando se considera diseñar una red con alta disponibilidad, se debe determinar el tipo de comunicación que se espera que los usuarios reciban, y cualquier conexión de software a otros servicios. Los protocolos usados, el almacenamiento de datos de una sesión o del usuario, determinan los puntos donde debe existir redundancia para generar alta disponibilidad.

1.3.2.3. Medida e interpretación

La alta disponibilidad consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio.

Índice de Disponibilidad	Duración del Tiempo de Inactividad
97 %	11 días
98 %	7 días
99 %	3 días y 15 horas
99.9 %	8 horas y 48 minutos
99.99 %	53 minutos
99.999 %	5 minutos
99.9999 %	32 segundos

Tabla. 1.1. Índice de disponibilidad

La Tabla 1.1 determina ejemplos de representación del índice de disponibilidad de una red de datos en un tiempo total de un año, “si la red falló 11 días durante los 365 días del año entonces el índice de disponibilidad es del 97%.” [12]

1.3.1. Virtualización

“La virtualización es una técnica usada para crear una versión virtual de algún recurso tecnológico, como una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.” [13]

“La virtualización permite crear sistemas más reactivos o de alta disponibilidad, ya que el servidor virtual no es más que un archivo en comparación con un equipo físico, entonces puede ser desplegado fácilmente de un servidor físico a otro servidor físico, el tiempo de no disponibilidad es de algunos minutos y se comienza de nuevo con un servidor idéntico al que acaba de caer, algunos sistemas de virtualización permiten el cambio en caliente, esto quiere decir que no existirá el periodo de no disponibilidad por tanto los datos o bien las configuraciones estarán siempre actualizadas en las distintas máquinas virtuales.” [14]

La virtualización se puede dar para distintos tipos de software, se puede virtualizar desde un sistema operativo Windows en un sistema operativo Linux host y viceversa, hasta avanzados sistemas de ruteo o firewall.

Existen diversos tipos de virtualización:

- “Virtualización por Hardware: Son extensiones en la arquitectura de procesador x86 para facilitar las tareas de virtualización al software ejecutándose sobre el sistema.

- Virtualización de almacenamiento: Se refiere al proceso de abstraer el almacenamiento lógico del almacenamiento físico, por lo general es usado en áreas de red de almacenamiento.

- Particionamiento: Es una técnica para dividir un solo recurso, por ejemplo el espacio de disco o bien el ancho de banda de red, en un número más pequeño y con recursos del mismo tipo que son más fáciles de utilizar.

- Máquina virtual: Es un sistema de virtualización el cual podría especificarse como una forma de compartir recursos locales físicos entre varios dispositivos virtuales.

- Hypervisor de almacenamiento: Es un conjunto portátil de gestión centralizada, que se usa para optimizar el valor combinado de los sistemas de disco de almacenamiento múltiples, incluyendo modelos distintos e incompatibles.” [10]

1.3.1.1. Ventajas de la virtualización

Existen muchas ventajas por las cuales la virtualización es una vía mucho más conveniente ante otras técnicas para adquirir alta disponibilidad en una red corporativa. De entre ellas las más destacables son:

- “Las máquinas virtuales pueden contener sistemas de muy distinta índole: es absolutamente posible y factible tener en nuestro servidor de virtualización, coexistiendo, por ejemplo una solución Endian, otra Vyatta, Solaris y Windows, todo ello en una única máquina física. De aquí se puede apreciar dos ventajas, el bajo costo económico y el aprovechamiento óptimo de los recursos.

- La seguridad es otra de las principales razones por las que es factible usar virtualización, ya que las máquinas virtuales sólo pueden comunicarse con otras máquinas virtuales y con el exterior a través de conexiones correctamente configuradas. Esto hace ideales a las máquinas virtuales, en las que se hace posible contaminar un sistema y observar su comportamiento con fines de conocer la seguridad del mismo.” [15]

- Mediante la virtualización se puede dar uso a hardware existente que estaba inutilizado y optimizar el aprovechamiento de recursos de la organización.

- Se puede conseguir una rápida incorporación de nuevos recursos para los servidores virtualizados.

- Administración global centralizada y simplificada.

- El hecho de que una máquina virtual falle es irrelevante para cualquier otra en funcionamiento, esto produce una condición favorable de aislamiento.

- No sólo aporta el beneficio directo en la reducción del hardware necesario, sino también los costos asociados.

- En alta disponibilidad reduce los tiempos de parada.

- Se puede hacer migraciones de máquinas virtuales de un servidor a otro sin pérdida de servicio, eliminando las paradas planificadas por mantenimientos de otros equipos físicos.

- Provee a la red capacidades de balanceo dinámico entre servidores físicos que componen el conjunto de recursos.

- “En virtualización se han realizados estudios basados sobre el ahorro de energía que genera la empresa para sus clientes, muestra que las soluciones de virtualización reducen los costos y emisiones de CO_2.” [16]

1.3.1.2. Software de virtualización seleccionado

Al igual que en cualquier otra plataforma de software existen dos tipos de programas: los que son de pago y los de versión libre.

Dentro de los programas de pago existen soluciones como:

- VMware, que es uno de los referentes en el mercado, pero también existen versiones de VMware que son gratuitas, como por ejemplo VMware Player que permite virtualizar a través de una máquina virtual ya configurada, también está VMware ESXi que es una máquina virtual de primer nivel.

- Otro gran ejemplar es Windows Server 2008 R2 Hyper-V cuya función de virtualización está incluida sin cargo en la licencia del servidor.

- Por otra parte existen organizaciones que nos permiten llenar un formulario web y así descargar una máquina virtual adecuada a cada organización, como por ejemplo EasyVMX!.

- Parallels, es otro de los programas de pago famosos, que permite la virtualización a nivel de sistema operativo o hardware, este está especialmente diseñado para uso en computadores Mac con procesadores Intel.

Dentro de los programas de código libre tenemos algunos como:

- “Xen que es un monitor de máquina virtual desarrollado por la Universidad de Cambridge. La meta del diseño es poder ejecutar instancias de sistemas operativos con todas sus características, de forma completamente funcional en un equipo sencillo.” [17]

- “OpenVZ es una tecnología de virtualización en el nivel de sistema operativo para Linux. OpenVZ permite que un servidor físico ejecute instancias de sistemas operativos aislados, conocidos como Servidores Privados Virtuales.” [18]

- “VirtualBox es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana Innotek GMBH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización.” [19]

Tomando en cuenta todas esta especificaciones y en relación a la funcionalidad que tiene cada una de estas máquinas virtuales respecto al firewall que se va a usar en este proyecto, la solución más viable es la de VMware.

Una de las ventajas con VMware es que el manejo del firewall en cuestión, fue diseñado con funcionalidades adaptativas a este software de virtualización, es por esto que, tomando en cuenta que se desea llevar al máximo las capacidades de desempeño del firewall la mejor opción sería instalarlo virtualmente en VMware.

VMware otorga licencias de funcionamiento gratis por periodos de tiempo, en este caso se ha adquirido una licencia para usar VMware.

1.3.2 Vyatta

1.3.2.1. Concepto

Es una organización que provee software base para routers, firewall y VPN que trabajan con protocolo IPv4 e IPv6. El sistema está basado en Debian, que es una distribución de Linux con aplicaciones de red como Quagga, Open VPN entre otras. La intención de la organización es desarrollar software que pueda reemplazar sistemas operativos Cisco, con un gran énfasis en el costo y la flexibilidad por el hecho de ser una fuente libre. Los sistemas que provee la organización son basados en Linux y corren muy establemente en arquitecturas con hardware x86 o bien en máquinas virtuales Xen o VMware. “Vyatta también provee una guía de reemplazo Cisco que puede ser descargada de su página web, misma que muestra varios de los productos cisco y la solución comparable con Vyatta/x86.” [20]

1.3.2.2. Utilidades de Vyatta en su versión libre

Vyatta ofrece su software de manera libre, pero también tiene una versión que es pagada y esta última se diferencia de la otra por el soporte que ofrece la organización, la cantidad de usuarios que pueden conectarse a la red, el tipo de conexiones Ethernet o inalámbricas que se pueden usar, plataforma gráfica o algunas configuraciones avanzadas del sistema entre otros. Los costos que tienen los paquetes de Vyatta de acuerdo al soporte que ofrecen pueden ir desde los $5000 hasta un poco mas de $35000, estos también varían de acuerdo al número de licencias que se adquieran. Otras de las ventajas que se adquiere al comprar la licencia por ejemplo de un paquete que cuesta $7500 son:

- “10 Licencias VSE
- 10 Casos de soporte por año
- 12 Horas de Respuesta SLA
- Servicio Telefónico de 6am a 6pm
- 5 clases de capacitación en línea” [6]

Respecto a su versión libre se puede notar que es posible implementar la mayor parte de las funcionalidades de Vyatta, entre ellas las más destacadas son:

- Protocolos de enrutado avanzados: BGP/OSPF/RIP usando Quagga.
- Monitorización de Redes: SNMP, Wireshark y tcpdump.
- QoS en limitación del ancho de banda.
- Firewall Avanzado: NAT, DMZ, balanceo de carga, filtrado de tráfico, VLAN.
- Servicio de acceso remoto: SSH y Telnet.
- Servidor DHCP.
- Cliente y servidor de VPN (OpenVPN).
- Encapsulación y túneles: Cisco HDLC, Frame Relay, PPP, PPPoE, Multilink.

- Clustering y VRRP.
- DNS forwarding, dynamic DNS.
- URL filtering.
- Virtualizar funciones de networking Xen, XenServer, VMware.

1.3.2.3. Ventajas de usar Vyatta

Como ya se había hablado antes, el enfoque de Vyatta es generar software para redes que sea una mejor alternativa ante hardware dedicado. En la Tabla 1.2 se puede apreciar una comparación entre el software de Vyatta y el sistema operativo que maneja una de las grandes compañías que diseñan hardware especializado para redes como es Cisco.

Requerimientos de Red		
Características	Vyatta Network OS	Cisco IOS
Multifunción	Si	Si
Escalabilidad en Hardware	Mínimo plataformas x86	Limitado a Cisco
Desempeño de Software	Ilimitado	Plataforma limitada
Disponibilidad en Máquina Virtual	Si - Vmware, Xen, XenServer y Red Hat KVM	No
Manejo Abierto de API	Si	No
Integración en Dispositivos de Borde	Si	No
Disposición de Servicio Cloud	Si	No
Actualización en Caliente	Si	No

Tabla. 1.2. Comparación de software Vyatta y Cisco [21]

Otras de las ventajas que podemos recalcar al usar Vyatta:

- Correcto Dimensionamiento de Red: como un sistema operativo de red que se ajusta para satisfacer necesidades, Vyatta pone la libertad de poder variar el tamaño de la red cuando sea necesario, sin necesidad de cambiar los componentes del sistema, Vyatta mata el paradigma de tener que comprar nuevo hardware para poder aumentar las capacidades de red.

- Precio/Rendimiento en Hardware: Los estándares de redes se han convertido en una carga de trabajo pesada para cualquier servidor. Hoy en día las arquitecturas x86 pueden fácilmente alcanzar un gran desempeño a un pequeño costo. Y el universo x86 dice que sistemas más rápidos a menor costo son siempre la mejor opción.

- Virtualización: Vyatta da la gran opción de correr funciones de red como una máquina virtual. Estas implementaciones permiten que Vyatta incremente de forma radical la flexibilidad de la infraestructura y produce un substancial retorno de inversión a diferencia de otras soluciones propietarias.

CAPÍTULO II

ANALISIS Y DISEÑO DE LA SOLUCIÓN DE FIREWALL PARA RED CORPORATIVA

2.1 ANÁLISIS DE LOS REQUERIMIENTOS DE SEGURIDAD EN UNA RED CORPORATIVA.

2.1.1. Seguridad que emplea la red de datos

El objetivo de una red de datos como internet, es permitir la comunicación entre distintos usuarios, sin embargo, no es factible que esta información esté disponible todo el tiempo o para cualquier tipo de usuario, por lo mismo se crean distintos parámetros para permitir o negar el acceso a las redes de datos. Pero además del acceso a la información confidencial, existen otras amenazas que pueden ser incluso más peligrosas; por ejemplo, un ataque que deje fuera de servicio a sistemas críticos de la red que aparte de generar pérdidas económicas, también puede provocar perdida de datos, insatisfacción en el usuario o pérdida de credibilidad.

La seguridad en redes es el proceso mediante el cual se logra proteger los activos digitales de la red. Este objetivo se desglosa en tres aspectos principales:

- Confidencialidad.- La información debe estar protegida de accesos no autorizados.

- Integridad.- La información no debe ser cambiada o eliminada, debe establecerse formas de restricción para distintos tipos de usuarios, así como permisos de modificación en la información.

- Disponibilidad.- La información debe estar disponible para los usuarios autorizados en el momento que lo requieran. En caso de presentarse algún fallo en hardware o software que interrumpa el funcionamiento de un servicio de red, este debe tener recuperación inmediata.

  Términos importantes en la seguridad de redes de datos:

- Identificación.- Proceso de identificar una entidad de otra o determinar la identidad de una entidad con quién se está comunicando.

- Autenticación.- Verificar que la identidad de una entidad es válida, probar que es quien dice ser.

- Autorización.- Controlar los niveles de acceso y privilegios que una entidad o usuario tienen en un sistema.

- No repudio.- Prevenir que usuarios o entidades nieguen la realización de un evento, como: envío, recibo, acceso o alteración de información o archivos.

Seguridad en la red de acceso

Esta capa permite efectuar un enlace físico real con los medios y enviar paquetes IP sobre la red. Esta capa incluye los detalles de la tecnología LAN, WAN, capa física y capa enlace de datos del modelo OSI. Existen muchos protocolos que operan en esta capa, entre ellos:

- ATM – Asynchronous Transfer Mode

  Es una tecnología de red orientada a la conexión, su arquitectura es basada en celdas, permite transmitir voz, video y datos a través de redes públicas y privadas a alta velocidad y con distintos niveles de calidad de servicio. Esta tecnología nos provee seguridad como integridad, autenticación, alta

seguridad en conexiones punto-multipunto multicast, también tiene la posibilidad de levantar VPN que son circuitos virtuales, estos ofrecen confidencialidad en el internet.

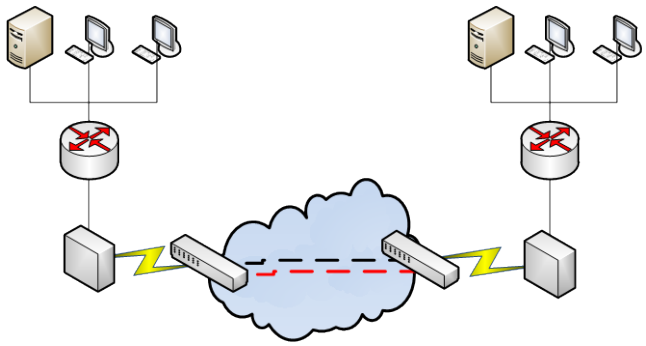


Figura. 2.1. Red ATM

- PPP – Point to Point Protocol

Es utilizado en conexiones seriales, con comunicación síncrona y asíncrona. A través de este protocolo se puede establecer seguridad mediante autenticación, encriptación, control de errores.

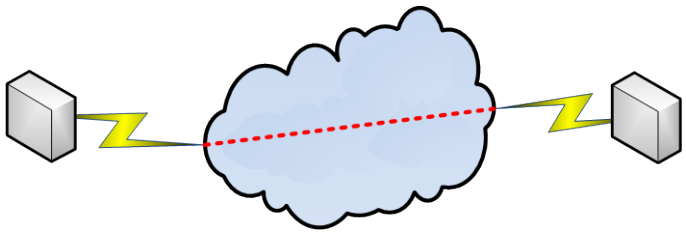


Figura. 2.2. Conexión PPP

- L2TP – Layer 2 Tunneling Protocol

Transporta en un túnel tráfico PPP sobre varias redes como IP, ATM, etc. Opera en la capa de enlace de datos del modelo OSI, por lo que su

implementación se realiza nodo a nodo en la red. Los parámetros que este puede ofrecer al nivel de seguridad son los de autenticación y cifrado proporcionados por PPP, y dependiendo del tipo de red por el que se esté transmitiendo se podrán ofertar otros tipos de seguridad.

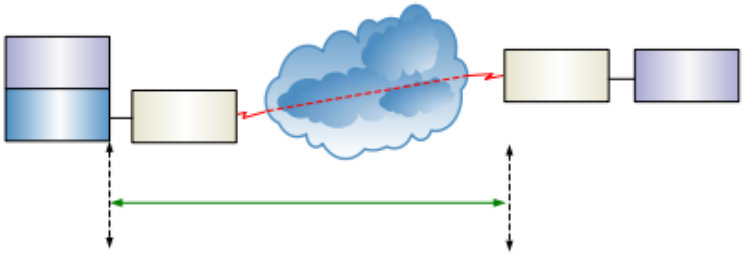


Figura. 2.3. Ejemplo De LTP2

Seguridad en la capa de internetworking

Esta capa se encarga de seleccionar la mejor ruta para transmitir paquetes y determina la conmutación de los mismos. Algunos de los mecanismos de seguridad que se pueden implementar en esta capa son:

- Filtros de Paquetes o Firewalls

  Su función es impedir el paso de paquetes a menos que cumplan con las reglas de acceso impuestas. Por ejemplo un router con capacidad de configurar ACL (Access Control List) se convierte en un filtro de paquetes y por lo general se ubican en el borde de la red interna y externa, también permiten controlar el flujo de datos entrante y saliente.

- Filtros Basados en Direcciones IP

  Se basa en la dirección origen y destino de un paquete para permitir o negar su paso.

Regla	Dirección Origen	Dirección Destino	Acción
1	172.13.2.*	118.56.5.*	Permitir
2	118.56.5.*	172.13.2.*	Permitir
3	*	*	Negar

Tabla. 2.1. Reglas de filtraje basadas en direcciones IP

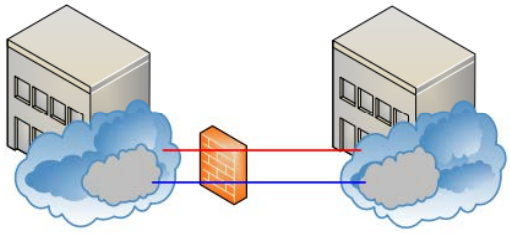


Figura. 2.4. Firewall de filtraje de paquetes

- Filtros Basados en Direcciones IP y Números de Puerto

Se añade un parámetro más, el número de puerto TCP o UDP.

Reglas	Conexión	Tipo	Dirección Origen	Dirección Destino	Puerto Fuente	Puerto Destino	Acción
1	entrada	tcp	externa	interna	>=1024	25	permitir
2	entrada	tcp	interna	externa	25	>=1024	permitir
3	salida	tcp	interna	externa	>=1024	25	permitir
4	salida	tcp	externa	interna	25	>=1024	permitir
5	*	*	*	*	*	*	negar

Tabla. 2.2. Reglas de filtraje basadas en direcciones IP y puertos TCP/UDP

Conexión de Entrada: Es iniciada desde un cliente sobre un host externo.

Conexión de Salida: Es iniciada desde un cliente sobre un host interno.

Otras acciones además de permitir o negar una conexión pueden implementarse como autenticación de usuario o cifrado.

- NAT - Network Address Translation

Es un mecanismo que permite reemplazar la dirección IP de un paquete por otra. Por lo general se configura en un equipo de borde como un firewall o router.

Red Interna		NAT	Red Externa	
Dirección Origen	Dirección Destino		Dirección Fuente	Dirección Destino
116.72.2.5	218.5.4.1	→	166.87.12.6	218.5.4.1
218.5.4.1	116.72.2.5	←	218.5.4.1	166.87.12.6

Tabla. 2.3. Traducción de direcciones de red

La dirección IP fuente de un paquete se traduce de una dirección IP privada a una dirección pública, y de la misma forma sucede con los paquetes de respuesta. Este mecanismo permite una conservación de las direcciones de IP las cuales son limitadas y además da cierta seguridad a los dispositivos de la intranet ya que su dirección IP permanece oculta.

- IPSec – Internet Protocol Security

Es una extensión de IP que asegura su comunicación, para esto utiliza un conjunto de protocolos de seguridad y algoritmos. Provee integridad de datos, autenticación y confidencialidad; así como, asociaciones de seguridad y administración de llaves. Es usado para implementar VPNs en ambientes intranet e internet.

- Seguridad para DNS

  DNS es un sistema que asocia direcciones IP con nombres de dominio de host. La mayoría de ataques a DNS tratan de direccionar el tráfico de datos a un sitio incorrecto. Una forma de lograr su objetivo es ingresar al registro DNS y modificarlo, así la respuesta del servidor DNS será una dirección IP incorrecta. Otra forma es suplantar al verdadero servidor DNS, y responder a una solicitud de resolución de dirección IP con un valor falso.

- NIDS – Network Based Intrusion Detection System

  Un sistema de protección contra intrusos debe proveer los siguientes mecanismos de defensa:

  - Detección.- Identificar ataques maliciosos sobre recursos de la red y el host.

  - Prevención.- Parar la ejecución del ataque detectado.

  - Reacción.- Inmunizar el sistema de futuros ataques de fuentes maliciosas.

  Un IDS está formado por uno o varios sensores y un analizador los cuales pueden estar separados o formar parte de un mismo componente. El analizador examina la información aplicando alguno de los métodos de detección de intrusos. Los métodos de análisis son: detección de anomalías y detección de usos indebidos.

  Un NIDS inspecciona el tráfico entrante o saliente a nivel de red, si detecta una acción maliciosa realiza una acción correctiva propia o notifica al

administrador del sistema para que realice una acción correctiva propia o notifica al administrador del sistema para que realice la acción correspondiente.

Seguridad en la capa de transporte

Esta capa proporciona servicios de transporte de datos desde el host origen hacia el host destino. Forma una conexión lógica entre los extremos de la comunicación. Algunos de los mecanismos que se ofrecen para dar seguridad a esta capa son los siguientes:

- Proxy a nivel de circuito

Un Proxy es un servidor que se ubica entre el cliente de una aplicación y un servidor real, permitiendo su comunicación de manera controlada. El cliente debe ejecutar un software de cliente especial para que el Proxy a nivel de circuito funcione.

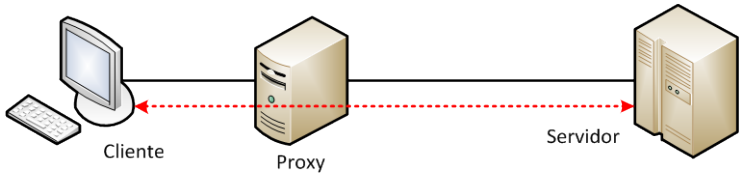


Figura. 2.5. Ejemplo de conexión proxy en capa de transporte

- SSL – Secure Sockets Layer

Fue desarrollado con la intención de proveer seguridad cuando se transmite información sobre internet. Utiliza cifrado de llave asimétrica y simétrica para establecer y transferir datos en modo seguro sobre una red insegura. Un ejemplo sería la establecer una sesión entre un navegador web y un servidor World wide web, usualmente http sobre SSL se lo denomina https.

- TLS – Transport Layer Security

  El desarrollo de TLS se basa en el protocolo SSLv3, al ser una versión avanzada proporciona mejores características de seguridad. TLS proporciona integración de datos, confidencialidad de datos, y autenticidad de entidades de la comunicación. Se ubica sobre un protocolo de transporte confiable, tal como TCP.

Seguridad en la capa de aplicación

La capa de aplicación se encarga del manejo de protocolos de alto nivel, entre los principales se tiene SMTP, http, FTP, los que soportan aplicaciones como transferencia de archivos, e-mail, conexión remota, etc. Algunos de los mecanismos de seguridad a este nivel son:

- Proxy de aplicación

  También es conocido como Gateway de aplicación y es un mecanismo instalado en un firewall que actúa como intermediario entre cliente y servidor de la aplicación. Controla el establecimiento de las conexiones y el tráfico que pasa sobre una red confiable y una no confiable. Por lo general también proporciona autenticidad del usuario, de la dirección fuente-destino y del protocolo.

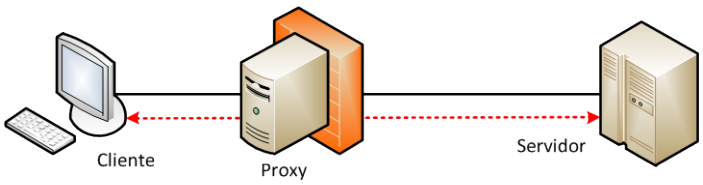


Figura. 2.6. Ejemplo de conexión proxy en capa de aplicación

- Filtros de contenidos

Los filtros de contenido son programas que se ejecutan sobre el firewall y analizan el tráfico en base a reglas a nivel de aplicación.

- Controles de acceso y autorización

El control de acceso a la red y a sus recursos es el punto principal de seguridad de redes. Los principales protocolos para autenticidad y autorización son RADIUS (Remote Authentication Access Control System) o TACACS (Terminal Access Controller Access Control System), estos se implementan en la mayoría de firewall.

- Seguridad en sistemas operativos

Todos los ataques se realizan con la finalidad de afectar a un dispositivo de red, muchas veces ese dispositivo es un host o servidor. Es por esto, que la seguridad en un sistema operativo es tan importante como la de cualquier otro control de seguridad. Algunos de los mecanismos que se deben considerar para manejar seguridad en sistemas operativos son los siguientes:

  - Configurar el monitoreo de logs, logs fallados y toda la actividad de la red en cada sistema que conforma la red y en especial en sistemas críticos como servidores.

  - Revisar periódicamente el archivo de log, si es posible diariamente para ver los intentos de acceso a la red y prevenir futuros ataques.

  - Respaldar los archivos de log constantemente, una copia impresa puede ser una buena opción ya que existe la posibilidad de que los archivos sean alterados.

- Controlar el acceso y definir los niveles de privilegios de uso de aplicaciones en cada sistema.

- Utilizar mecanismos de cifrado sobre información de administración y monitoreo.

- Instalar únicamente los componentes, servicios y programas necesarios.

- Actualizar las versiones del sistema operativo.

- HIDS – Host Based Intrusion Detection System

  Detecta actividades maliciosas dentro de una sola computadora, para esto revisa los archivos de log del host y del sistema. Puede monitorear un proceso del sistema operativo o un recurso crítico del sistema que requiera mayor protección.

2.1.2. Tráfico transmitido

La cantidad y tipo de tráfico que se transmite en una red, es uno de los factores más importantes que se debe tener en cuenta al momento de implantar nuevos sistemas de seguridad para la misma. La cantidad de tráfico que circule por la red determinará el dimensionamiento de muchos factores, para dimensionar la cantidad de tráfico que de manera coherente debería circular por una red de datos, se hace uso de una herramienta matemática que se denomina teoría de colas, y concretamente esta hace uso de modelos capaces de representar el comportamiento óptimo de la red frente a volúmenes de tráfico deseados, es decir que en función de los resultados de estos modelos se debería diseñar y dimensionar por ejemplo la capacidad de los enlaces, la capacidad de los equipos, el grado de atención de los servidores, etc., frente a condiciones esperadas; sin embargo este enfoque es netamente teórico, por lo que no es muy

aplicable a situaciones prácticas como las que se mostrarán a continuación, este análisis está dirigido y focalizado hacia la obtención de resultados en cuanto al tráfico que circula en la red corporativa.

Dentro de una red corporativa los servicios más usados son los de:

- Telefonía.- La red corporativa tendrá alrededor de 50 usuarios por lo que estos deberán estar comunicados no sólo mediante la transferencia de datos sino también mediante voz.

- Servicio Web.- Actualmente es necesario que todas las empresas manejen páginas web para poder generar publicidad y se ofrezcan servicios a clientes, por tanto es obvio que este tráfico estará moviéndose dentro de la red.

- Servicio de e-mail.- Este es un recurso de red que a menudo se suele implementar debido a que permite generar privacidad dentro de las corporaciones y también es una manera de seguridad contra virus, spam entre otros.

- Servicio de transferencia de archivos.- Este servicio es fundamental ya que ayudará a que muchos de los usuarios descarguen documentos esenciales para su trabajo desde un servidor que por lo general esta ubicado en la intranet.

- Tráfico de control como DHCP, DNS entre otros.

- Se debe también tomar en cuenta que existirá otro tipo de tráfico debido a las descargas de internet generadas por algunos usuarios de la intranet.

2.2. DISEÑO DE LA SOLUCIÓN DE FIREWALL PARA UNA RED CORPORATIVA.

2.2.1. Análisis de hardware

Una red corporativa podría abarcar dentro de su red distintos tipos de tecnologías, así como también distintas topologías física y lógicas. En este inciso se describirán los equipos que formarán parte de la red corporativa.

Para este proyecto se analizarán dos tipos de usuarios que conformarán la red, estos son: usuarios de poder y usuarios de no poder.

Los usuarios de poder son aquellos que tendrán comunicación tanto con los usuarios de no poder como con los servidores principales de la empresa, estos también tendrán libre acceso al internet, debido a esto, los equipos que generalmente manejarán este tipo de usuarios serán computadores de escritorio como portátiles, teléfonos inteligentes, PDAs, por otra parte estos usuarios también deberán contar con servicio de telefonía.

Respecto a los usuarios de no poder, estos tan sólo tienen la necesidad de comunicarse con los servidores internos para descargar documentos importantes o bien para hacer consultas sobre alguna base de datos por lo que no les hace falta tener acceso a internet, con estas condiciones se puede notar que tan sólo dispondrán de computadores de escritorio y también contarán con servicio de telefonía.

Ahora centrándose un poco más en el hardware que se usará para generar la conectividad dentro de la empresa se deben analizar otros equipos como routers, switch.

Dentro de una red corporativa es muy común encontrar distintas áreas de trabajo, para este proyecto como ya se había dicho antes se tomarán en cuenta dos tipos de usuarios, estos dos tipos de usuarios generan dos tipos de áreas que son: usuarios de poder y usuarios de no poder, por último se establecerá una última área que será la DMZ, esta área es la zona desmilitarizada misma donde se encontrarán todos los servidores que tenga la corporación. Cada una de estas áreas deberá tener un switch que permita la conectividad inmediata entre los distintos usuarios que la conformen, estos switch también deberán tener configurada un puerto troncal por el que se conectarán a un router que será el que viabilice la comunicación entre las distintas áreas, además de tener configurado una vlan por cada área, es decir el área de usuarios de no poder, pertenecerá a la vlan 10, el área de usuarios de poder pertenecerá a la vlan 20 y el área DMZ pertenecerá a la vlan 30.

Focalizando en el tema del router que permite la conectividad entre las distintas áreas es necesario tener en cuenta que se deben generar políticas que determinen el comportamiento de este dispositivo, para este proyecto este dispositivo será el sistema Vyatta que también funcionará como router de borde, ya que permite la comunicación con el internet, funcionará como firewall y dotará a la red de algunos servicios típicos. Las capacidades físicas de la máquina donde se instalará este software son las siguientes:

- Computador de escritorio con arquitectura x86
- Procesador Intel Core 2 Duo de 2,13 GHz
- 2 GB de RAM
- Bus de datos de 32 bits
- Tarjeta Madre Intel DG33BU

Respecto a las características de software el sistema operativo host es Windows 7 sobre el que se instalará una máquina virtual VMware y con este programa instalar los dos sistemas Vyatta, esta configuración fue necesaria ya que para poder usar una máquina virtual de primer nivel se debía contar con un servidor de características específicas avanzadas y la intención de este proyecto es usar los menores recursos posibles.

2.2.2. Análisis de los servicios

Mediante la implementación del sistema Vyatta se hace posible levantar servicios comunes dentro de la red como DHCP, DNS, NAT, QoS, SSH, HTTP.

DHCP.- Es un servicio TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red, dentro de Vyatta este servicio es muy versátil en su configuración, permite configurarlo como prioritario en caso de que existan otros servidores que intente proveer direcciones IP en la intranet, otra de las ventajas es que permite proveer una dirección para consultas DNS, nombre de dominio y puerta de enlace predeterminada.

DNS.- Se utiliza para proveer a las computadoras de los usuarios un nombre equivalente a las direcciones IP, el uso de este servicio es transparente para los usuarios cuando éste está bien configurado en los servidores, Vyatta asigna una cantidad de memoria caché para guardar las consultas hechas más recientemente, si una consulta no es encontrada en su memoria caché entonces la remite a otro servidor DNS que deberá ser configurado dentro del sistema Vyatta, su configuración se puede implementar para dar servicio sólo a ciertas interfaces.

NAT.- Este servicio permite la traducción de direcciones IP, en este caso su implementación será necesaria dentro del sistema Vyatta para que las distintas áreas tengan conectividad con el internet, debido a que Vyatta se encuentra como router de borde entonces deberá cumplir con esta tarea, la configuración es

bastante sencilla y se la ejecuta tomando en cuenta que interfaz Ethernet, vlan o bond se desea dar el servicio.

QoS.- Dentro del sistema Vyatta la calidad de servicio trabaja directamente con la prioridad de los paquetes que van llegando al sistema, es decir si llegan tres paquetes y el tipo de paquete que llegó en tercer lugar se ha configurado con mayor prioridad dentro de Vyatta, entonces a éste se le dará mayor importancia que a los otros dos paquetes. Para su implementación se tomarán en cuenta las distintas áreas dividiendo para cada una de ellas el ancho de banda que ocuparán de la conexión a internet.

HTTP y SSH.- Dentro de Vyatta es posible también levantar una página web mediante la cuál se puede configurar el sistema de forma gráfica, para este proyecto tan sólo se levantará la página web pero no se hará mayor configuración desde ésta se usará línea de comandos para modificar el sistema, para que algún tipo de configuración sea levantada desde la página web que levanta Vyatta sea posible es necesario también levantar el servicio SSH que es un acceso remoto seguro al sistema Vyatta. Los cambios hechos en la página web no serán ejecutados dentro de Vyatta sino está levantado el servicio SSH también.

2.2.3. Análisis de redundancia en la red

La redundancia directamente trata sobre la capacidad de que un dispositivo reemplace a otro para que la red se mantenga en correcto funcionamiento, en este caso se toma en cuenta un dispositivo en especial como es un firewall, al implementar esta redundancia automáticamente la red de datos gana alta disponibilidad.

Una estructura de firewall en alta disponibilidad presenta las siguientes ventajas:

- Continuidad de servicio frente a fallas de hardware o software.

- Permitir actualizaciones de software sin interrupción del servicio.

El sistema Vyatta permite la alta disponibilidad entre dos sistemas Vyatta configurados con el protocolo VRRP, otro de los requerimientos es que los dos sistemas deben manejar las mismas versiones de Vyatta en esta caso es la versión 6.2, VRRP que hace posible que un sistema secundario reemplace al principal cuando este deje de funcionar, además Vyatta permite configurar un servicio llamado stateful, este servicio permite la actualización del sistema principal y el secundario, logrando así que si por ejemplo una dirección DHCP fue prestada por el sistema primario, cuando éste falle el secundario que sería quien lo reemplace no la vuelva a entregar a un nuevo usuario.

Las condiciones para que un sistema de alta disponibilidad sea posible con Vyatta es que los dos tengan las mismas configuraciones, mediante Vyatta se puede sincronizar el sistema primario y el secundario, es decir que si un cambio de configuración se realiza en el sistema primario este se verá automáticamente reflejado el sistema secundario.

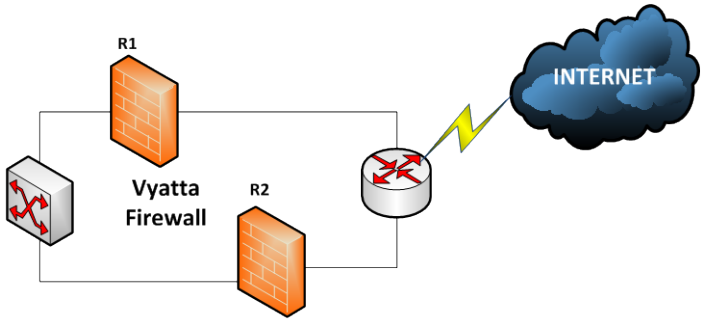


Figura. 2.7. Red con redundancia en firewall para alta disponibilidad

Un nodo principal filtra todo el tráfico y un nodo de backup espera a entrar en acción en caso de fallo del primero. La principal consecuencia es el desaprovechamiento de los recursos del nodo de backup, que en circunstancias normales no hará nada.

2.2.4. Diseño de la topología física y lógica

Como ya se había hablado anteriormente la intranet se dividirá en distintas áreas que de aquí en adelante se las llamarán zonas, entonces existe la zona de usuarios de no poder, usuarios de poder y una zona DMZ, estas zonas son las que típicamente tiene toda corporación.

Las características principales de la intranet física serán:

- Zona de usuarios de no poder
    - Capacidad de hasta 30 usuarios
    - Conexión a internet limitada
    - Conexión con la zona DMZ

- Zona de usuarios de poder
    - Capacidad de hasta 15 usuarios
    - Conexión a internet de libre acceso
    - Conexión con la zona de usuarios de no poder
    - Conexión con la zona DMZ

- Zona DMZ
    - Capacidad de hasta 5 servidores
    - Conexión a internet

También es necesario definir una nueva zona llamada la zona local esta se refiere al sistema Vyatta en si, por tanto esta nueva zona tendrá conectividad con todas la otras zonas pero no tendrá acceso a internet.

La topología física básica de la red está detallada en la Figura 2.8.

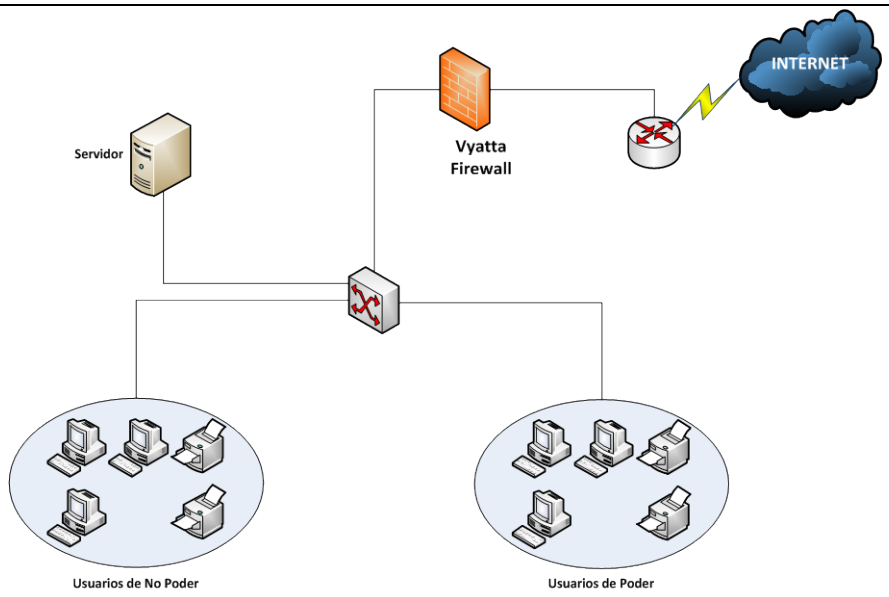


Figura. 2.8. Diagrama físico de la red corporativa

Para el diseño lógico de la red corporativa se tendrá cada dispositivo crítico de red en una subred ya que no existe seguridad en términos de acceso. El diseño de la red lógica es independiente de la conectividad física, reflejando solo el diagrama de la capa 3 de la red, como se puede ver a continuación:

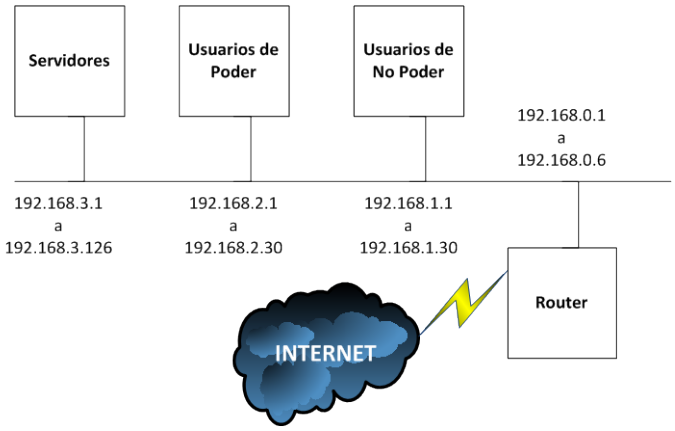


Figura. 2.9. Diseño lógico de la red corporativa

La infraestructura de la red es ahora funcional, y todos los componentes requeridos están en su lugar. La red, como sea, está aislada del internet. Conectando la red a internet se requerirán algunas otras consideraciones.

Primero, la más importante consideración es la dirección IP. Tomando en cuenta este parámetro se optó por usar direcciones del rango privado de clase C.

Obviamente para cualquier tipo de red la seguridad es imprescindible, aún con la asignación lógica privada es necesario levantar un sistema que proteja toda la red local del internet, y ese es el propósito de este proyecto, el elemento clave que aún se necesita instalar es un firewall, el cual proveerá de seguridad de alto nivel a la intranet.

El firewall se instalará directamente a la conexión de internet para luego conectar el router al firewall y el resto de la intranet, el firewall será instalado en una máquina de bajos recursos de hardware, también tendrá redundancia para ofrecer alta disponibilidad, con estos términos entonces la topología de red quedará de la siguiente forma:

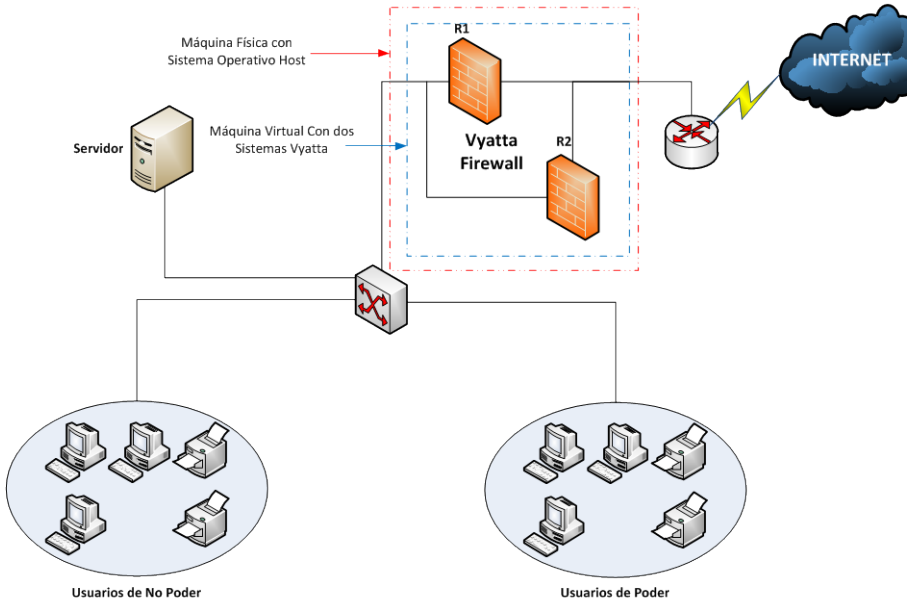


Figura. 2.10. Diagrama físico de la red corporativa con firewall

Relacionando todas las configuraciones anteriores la topología de la red final es como la de la Figura 2.11 esta sería una red corporativa común con sus distintas etapas y para dar conectividad a las distintas zonas que se han descrito,

además de que ya se propone el sistema de redundancia y alta disponibilidad con el objetivo de tener una red tolerante a fallos.

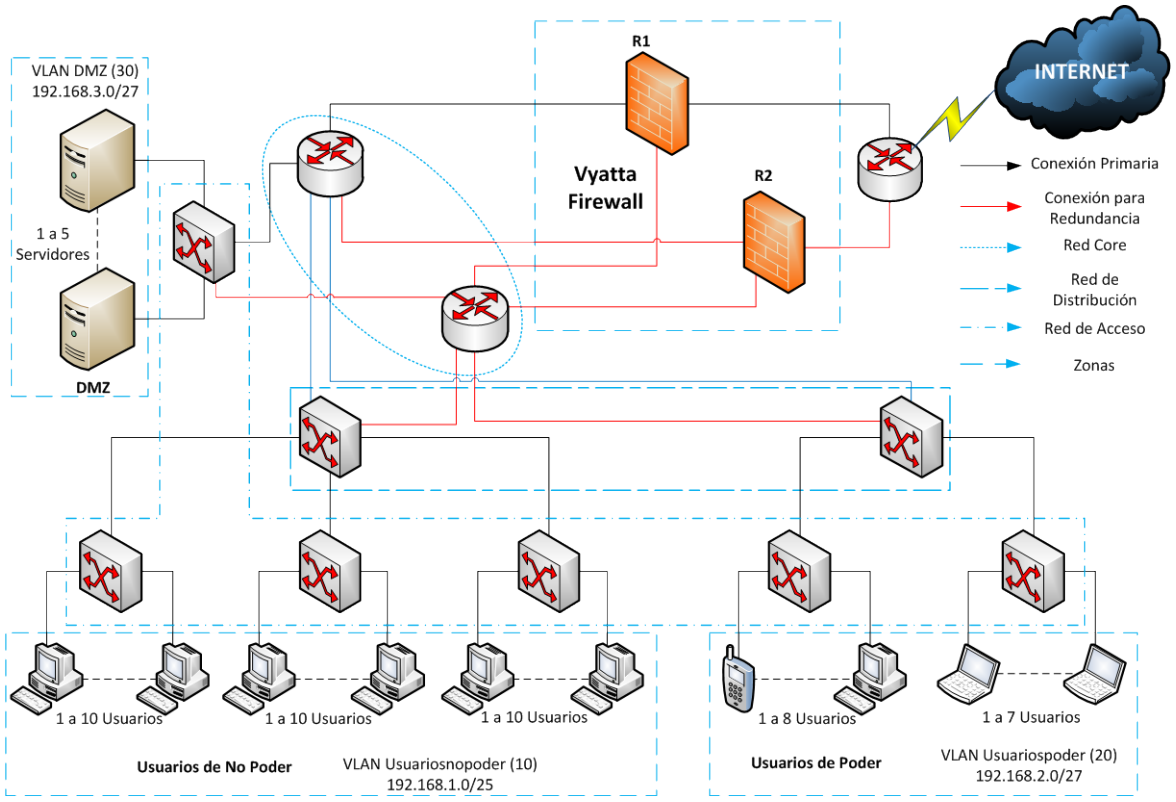


Figura. 2.11. Configuración de la red corporativa con tolerancia a fallos

CAPÍTULO III

IMPLEMENTACIÓN DE LA SOLUCIÓN DE FIREWALL PARA RED CORPORATIVA

3.1 IMPLEMENTACIÓN DE LA SOLUCIÓN DE FIREWALL PARA RED CORPORATIVA.

Para poder continuar con el desarrollo del proyecto desde ahora en adelante se conocerá como “topología proyecto” a la red que se muestra descrita en la Figura 3.1 que es un resumen de la red real para poder hacer el desarrollo del proyecto más simplificado.

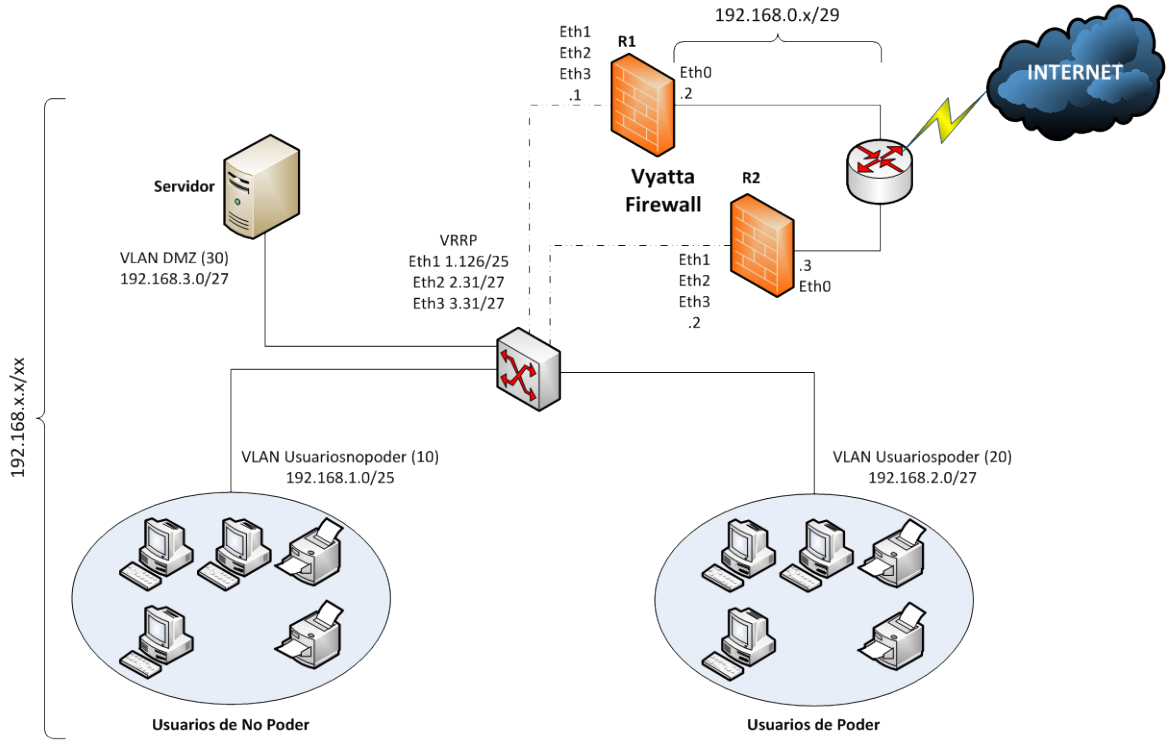


Figura. 3.1. Topología proyecto

Las direcciones de red se han establecido en la topología proyecto utilizando la configuración de la Tabla 3.1.

Interfaz		Máscara	Especificación	
	Vyatta			
LAN	Eth 1	192.168.1.0/25	192.168.1.0	Dirección de Red
			192.168.1.1	Dirección R1
			192.168.1.2	Dirección R2
			192.168.1.3	Intervalo para usuarios de no poder
			192.168.1.125	
			192.168.1.126	VRRP para R1 y R2
			192.168.1.127	Broadcast
	Eth2	192.168.2.0/27	192.168.2.0	Dirección de Red
			192.168.2.1	Dirección R1
			192.168.2.2	Dirección R2
			192.168.2.3	Intervalo para usuarios de poder
			192.168.2.29	
			192.168.2.30	VRRP para R1 y R2
			192.168.2.31	Broadcast
	Eth3	192.168.3.0/27	192.168.3.0	Dirección de Red
			192.168.3.1	Dirección R1
			192.168.3.2	Dirección R2
			192.168.3.3	Intervalo para servidores
			192.168.3.29	
			192.168.3.30	VRRP para R1 y R2
			192.168.3.31	Broadcast
WAN		192.168.0.0/29	192.168.0.1	Dirección interfaz ethernet del router
	Eth0		192.168.0.2	Interfaz ethernet en Vyatta R1 para acceso a internet
	Eth0		192.168.0.3	Interfaz ethernet en Vyatta R2 para acceso a internet

Tabla. 3.1. Topología lógica propuesta

3.1.1. Instalación del software

En este proyecto se utilizará la versión 6.2 de Vyatta la cual es libre y se puede descargar desde Vyatta.com, usaremos el livecd Vyatta que es un archivo iso, montable en una unidad lectora de discos compactos.

Una vez que empieza a cargar el programa inicial aparece la Figura 3.2.

Figura. 3.2. Boot Vyatta

En el siguiente paso aparecerá el cuadro de la Figura 3.3, el cual nos pide un nombre de user/password, que por defecto son vyatta/vyatta.

```
Starting network plug daemon: netplugd.
Starting enhanced syslogd: rsyslogd.
Loading open-vm-tools modules: vmhgfs vmmemctl vmsync.
Starting open-vm daemon: vmtoolsd.
Starting ACPI services....
Starting deferred execution scheduler: atd.
Starting periodic command scheduler: cron.
Loading cpufreq kernel modules...done (none).
Starting routing daemons: ripd ripngd ospfd ospf6d bgpd.
Mounting Vyatta Config...done.
[   99.308116] end_request: I/O error, dev fd0, sector 0
Starting Vyatta router: migrate rl-system firewall configure.

Welcome to Vyatta - vyatta tty1

vyatta login: vyatta
Password:
Linux vyatta 2.6.35-1-586-vyatta-virt #1 SMP Fri Feb 4 05:36:56 PST 2011 i686
Welcome to Vyatta.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyatta@vyatta:~$ configure
[edit]
vyatta@vyatta# _
```

Figura. 3.3. Ingreso de usuario y clave

Una vez que se inicie el sistema se deberá instalar el mismo con el comando install-system que sería una instalación basada en disco, el sistema pregunta si se desea continuar con la instalación y la opción por defecto es yes como en la Figura 3.4, por tanto se teclea enter.

```
Would you like to continue? (Yes/No) [Yes]: yes_
```

Figura. 3.4. Inicio de la instalación de vyatta

Después analiza el disco y pregunta si se desea que el particionamiento sea automático, raid de unión, manual o saltar paso si el disco ya se ha particionado antes correctamente. Se selecciona la opción automática:
- Enter para aceptar la opción [Auto] por defecto y continuar, como en la Figura 3.5.

Figura. 3.5. Tipo de partición del disco

Ahora el sistema informa de los discos encontrados en el equipo y pregunta en cual instalar la imagen. Normalmente habrá solo uno (hda o sda según el tipo de disco). Se selecciona la opción por defecto que será instalar en el HDD primario:

- Enter para instalar en el disco duro primario seleccionado por defecto [sda] y continuar, como en la Figura 3.6, el sistema avisa que se eliminarán todos los datos y pregunta si se desea continuar como en la Figura 3.6.

- Escribir Yes ya que por defecto está seleccionado [No] y pulsar Enter para continuar.

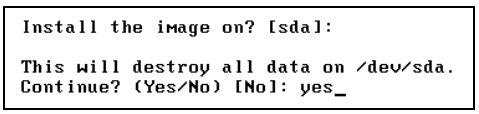


Figura. 3.6. Selección de discos del sistema

Ahora el sistema pregunta de que tamaño deberá ser la partición tal como en la Figura 3.7.

- Enter para usar todo el disco seleccionado por defecto y continuar. Tras esto se crea el sistema de archivos y se copian todos los ficheros necesarios al disco.

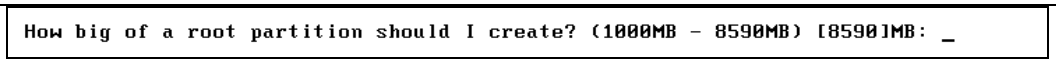


Figura. 3.7. Tamaño de la partición del disco

A continuación comunica que en el CD hay un fichero de configuración inicial "*config.boot*" y pregunta si debe copiarlo al disco local con la instalación como en la Figura 3.8.

- Enter para aceptar la opción por defecto de copiarlo y continuar.

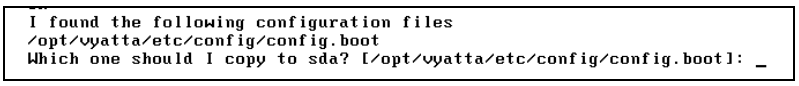


Figura. 3.8. Instalación del fichero de configuración inicial

Ahora pide la contraseña de administrador como en la Figura 3.9. que por defecto es vyatta.

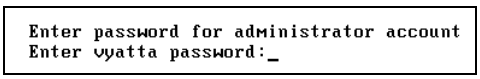


Figura. 3.9. Contraseña de administrador

Por último informa que es necesario instalar un gestor de arranque (GRUB) en el sistema, nuevamente da la información de los discos locales y pregunta a que partición ha de modificar GRUB la partición de arranque.

- Enter para aceptar la opción por defecto de instalarlo en el disco local primario.

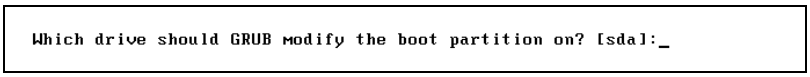


Figura. 3.10. Instalación del gestor de arranque GRUB

Después de esto se deberá reiniciar el sistema desde el disco duro ya que si lo hacemos desde el LiveCD la configuración no la podremos salvar.

Se ingresa nuevamente el usuario/contraseña por defecto vyatta/vyatta y configuramos un nombre para el sistema con el comando "*set system host-name*" como en la Figura 3.11.

```
vyatta@vyatta# set system host-name R1
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.11. Configuración nombre del sistema

Para notar cuales son las interfaces ethernet del sistema, escribimos el comando show interfaces como en la Figura 3.12.

```
vyatta@vyatta# show interfaces
 ethernet eth0 {
     hw-id 00:0c:29:0e:12:21
 }
 ethernet eth1 {
     hw-id 00:0c:29:0e:12:0d
 }
 ethernet eth2 {
     hw-id 00:0c:29:0e:12:17
 }
 loopback lo {
 }
[edit]
```

Figura. 3.12. Interfaces del sistema

A continuación se deberá dar una dirección IP estática a las interfaces ethernet, para esto se usa el comando "*set interfaces ethernet ethx address* ***.***.***.***/**", tal como en la Figura 3.13, seguido del comando commit.

```
vyatta@vyatta# set interfaces ethernet eth1 address 192.168.1.1/25
[edit]
vyatta@vyatta# set interfaces ethernet eth2 address 192.168.2.1/27
[edit]
vyatta@vyatta# set interfaces ethernet eth3 address 192.168.3.1/27
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.13. Configuración direcciones lógicas IP en interfaces ethernet

Para la interfaz wan el comando que se usará es "*set interface ethernet eth0 address dhcp*", con esto nos aseguramos de que la interfaz wan esta recibiendo una dirección ip desde el ISP así como una dirección para consultas DNS.

Para notar que las interfaces hayan sido levantadas correctamente entonces escribimos el comando "*show interfaces*", el sistema presentará un resultado como el de la Figura 3.14.

```
  ethernet eth1 {
      address 192.168.1.1/25
      hw-id 00:0c:29:91:15:f8
  }
  ethernet eth2 {
      address 192.168.2.1/27
      hw-id 00:0c:29:91:15:02
  }
  ethernet eth3 {
      address 192.168.3.1/27
      hw-id 00:0c:29:91:15:0c
  }
  loopback lo {
  }
 [edit]
 vyatta@vyatta# _
```

Figura. 3.14. Descripción de la configuración de las interfaces ethernet del sistema Vyatta

El siguiente paso básico consiste en levantar el servicio https para lo cual se usa el comando "*set service https*" como en la Figura 3.15, seguido del comando commit.

```
[edit]
vyatta@vyatta# set service https
[edit]
vyatta@vyatta# commit
[ service https ]
Generating a 1024 bit RSA private key
.++++++
.......................++++++
writing new private key to '/etc/lighttpd/server.pem'
-----

[ service https ]
Stopping web server: lighttpd.
Starting web server: lighttpd.
Stopping PAGER server
Starting PAGER server

[edit]
vyatta@vyatta# _
```

Figura. 3.15. Levantamiento del servicio HTTPS

De la misma manera en la que se levantó el servicio https, se procede con el servicio de ssh mediante el comando "*set service ssh*" como en la Figura 3.16, seguido del comando commit.

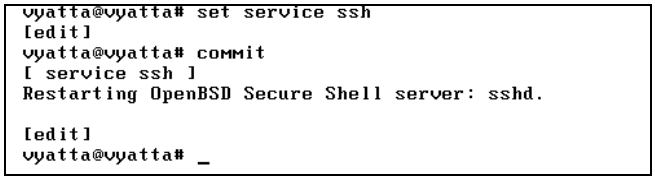


Figura. 3.16. Levantamiento del servicio SSH

Con estos pasos el sistema estará configurado básicamente.

Para probar que el servicio https este en funcionamiento, entonces desde un computador conectado en red a la interfaz lan, se abre un navegador de internet y en la dirección URL se ingresará la dirección IP de la interfaz a la que se conecto en red dicho computador, como en la Figura 3.17, aquí se debe ingresar el usuario y clave para poder administrar el sistema.

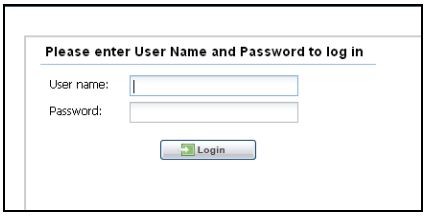


Figura. 3.17. Ingreso de usuario y clave

En seguida aparecerá la interfaz gráfica de Vyatta para su administración, como en la Figura 3.18.

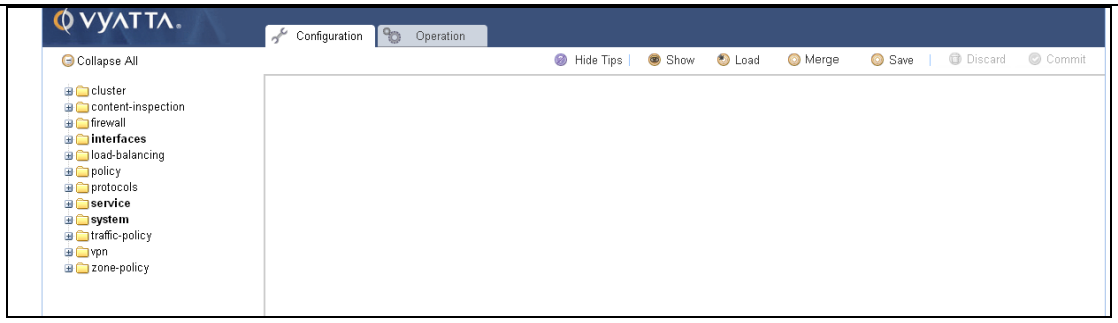


Figura. 3.18. Interfaz web de Vyatta

Por último para concluir con la configuración básica del sistema Vyatta, es necesario incluir reglas NAT las cuales permitan que las interfaces LAN accedan al internet, usando el comando "*set service nat rule*" se podrá definir una regla NAT que permita mover todo el tráfico de cada interfaz LAN hacia el internet tal como en la Figura 3.19, este procedimiento debe repetirse para cada interfaz.

```
vyatta@vyatta# set service nat rule 10 source address 192.168.1.0/25
[edit]
vyatta@vyatta# set service nat rule 10 outbound-interface eth0
[edit]
vyatta@vyatta# set service nat rule 10 type masquerade
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.19. Configuración de internet para interfaz LAN

Esta configuración deberá levantarse en cada una de las interfaces, para notar que el cambio ha sido efectuado, se usa el comando "*show service nat*", la información desplegada tiene que ser igual a la de la Figura 3.20.

```
[edit]
vyatta@vyatta# show service nat
 rule 10 {
     outbound-interface eth0
     source {
         address 192.168.1.0/25
     }
     type masquerade
 }
 rule 20 {
     outbound-interface eth0
     source {
         address 192.168.2.0/27
     }
     type masquerade
 }
 rule 30 {
     outbound-interface eth0
     source {
         address 192.168.3.0/27
     }
     type masquerade
 }
[edit]
vyatta@vyatta# _
```

Figura. 3.20. Detalle de la configuración en el sistema Vyatta del servicio NAT

3.1.2 Configuración de VRRP, stateful failover y sincronización para alta disponibilidad

Tomando en cuenta que la topología proyecto tiene redundancia entonces se necesita levantar VRRP que es un protocolo de enrutamiento redundante virtual, para esto se usa el comando "*set interfaces ethernet ethx vrrp vrrp-group*".

Primero se definirá la prioridad o jerarquía del sistema, luego la descripción del grupo y por último el tipo de autenticación. Este proceso deberá llevarse acabo en cada una de las interfaces del sistema a excepción de la interfaz WAN. En la Figura 3.21. se muestra la forma de configuración de VRRP.

```
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10
[edit]
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10 virtual-address 1
92.168.1.126/25
[edit]
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10 priority 150
[edit]
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10 preempt true
[edit]
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10 advertise-interva
l 1
[edit]
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10 authentication ty
pe ah
[edit]
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10 authentication pa
ssword vyatta
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.21. Configuración VRRP

Para notar que el sistema haya aceptado los cambios luego de haber corrido el comando “commit”, ejecutamos el comando “*show interfaces*”, el sistema deberá indicar información tal como en la Figura 3.22.

```
 ethernet eth1 {
     address 192.168.1.1/25
     hw-id 00:0c:29:91:15:f8
     vrrp {
         vrrp-group 10 {
             advertise-interval 1
             authentication {
                 password vyatta
                 type ah
             }
             preempt true
             priority 150
             virtual-address 192.168.1.126/25
         }
     }
 }
 ethernet eth2 {
     address 192.168.2.1/27
     hw-id 00:0c:29:91:15:02
     vrrp {
         vrrp-group 20 {
             advertise-interval 1
             authentication {
                 password vyatta
                 type ah
             }
             preempt true
             priority 150
             virtual-address 192.168.2.30/27
         }
     }
 }
 ethernet eth3 {
     address 192.168.3.1/27
     hw-id 00:0c:29:91:15:0c
     vrrp {
         vrrp-group 30 {
             advertise-interval 1
             authentication {
                 password vyatta
                 type ah
             }
             preempt true
             priority 150
             virtual-address 192.168.3.30/27
         }
     }
 }
 loopback lo {
 }
[edit]
vyatta@vyatta#
```

Figura. 3.22. Interfaces después de configurar VRRP

Ahora se procede a configurar la puerta de enlace predeterminada del sistema, que para la topología proyecto que se está usando vendría a ser la 192.168.0.1, para esto ejecutamos el comando “*set system gatewat-address* ***.***.***.***” como en la Figura 3.23.

```
vyatta@vyatta# set system gateway-address 192.168.0.1
[edit]
vyatta@vyatta# commit
[edit]
```

Figura. 3.23. Configuración de la dirección de la puerta de enlace

Para continuar con la configuración de alta disponibilidad ahora se levantará el modo stateful failover, este servicio nos permite mantener actualizada la configuración entre los dos routers con la finalidad de que si, por ejemplo, un host está descargando un archivo de internet entonces éste jamás pierda la conectividad en caso de que el router principal pierda la conectividad, si el caso fuese que el router principal falla, entonces el router de backup automáticamente lo reemplazará y será posible que el host que está descargando no pierda su descarga.

Para configurar este modo, se deben seguir los pasos de la Figura 3.24.

```
vyatta@vyatta# set interfaces ethernet eth1 vrrp vrrp-group 10 sync-group vyatta
10
[edit]
vyatta@vyatta# set service conntrack-sync failover-mechanism vrrp sync-group vya
tta10
[edit]
vyatta@vyatta# set service conntrack-sync interface eth1
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# save
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
Done
[edit]
vyatta@vyatta# _
```

Figura. 3.24. Configuración del servicio stateful failover

Los mismos pasos de la figura 3.24 se deberán seguir para configurar el modo stateful de las otras interfaces.

Para lograr que el sistema sea de alta disponibilidad al cien por ciento, entonces también se debe configurar un método por el cuál el router secundario se mantenga actualizado en caso de realizar cualquier cambio en el router principal. Para este funcionamiento Vyatta nos ofrece un sistema muy estable

pero que desgraciadamente no se podrá implementar en esta configuración ya que este sólo está disponible para las versiones de subscripción.

3.1.3 Configuración del servicio DHCP

Al momento de definir los distintos pools que se configurarán para entregar el servicio de DHCP a los distintos host, es necesario tomar en cuenta que habrán distintos clientes que deberán tener direcciones lógicas IP fijas en la red por lo que el pool de direcciones sólo abarcará una cantidad mediana de direcciones entregables, por ejemplo para el grupo de usuarios de poder el pool de direcciones lógicas IP será más pequeño que el del grupo de usuarios de no poder. También se debe tomar en cuenta que el área de DMZ siempre tendrá direcciones lógicas IP estáticas por lo que el servicio de DHCP no se levantará en la respectiva interfaz Ethernet. Una vez definidos estos parámetros, la configuración de los distintos pool de direcciones para la topología proyecto queda definida en la Tabla 3.2.

		Eth1	Eth2	Eth3
		Usuarios de No Poder	Usuarios de Poder	DMZ
Direcciones de uso Estático	**Desde**	192.168.1.3	192.168.2.3	192.168.3.3
	Hasta	192.168.1.30	192.168.2.18	192.168.3.29
Pool de Direcciones DHCP	**Desde**	192.168.1.31	192.168.2.19	
	Hasta	192.168.1.125	192.168.2.29	

Tabla. 3.2. Pool de direcciones lógicas IP para servicio DHCP

En este punto de la configuración de Vyatta es importante tomar en cuenta que las puertas de enlace predeterminadas para cualquier host, siempre deberán ser la dirección lógica IP configurada para VRRP respectivamente para cada interfaz ethernet, esto es necesario ya que así el sistema podrá funcionar con tolerancia a fallos, de otra manera, en caso de que uno de los sistemas vyatta deje de funcionar el host que no tenga configurado su puerta de enlace predeterminada con la dirección VRRP de su interfaz, perderá todos los servicios y la conectividad a la red.

El procedimiento que se sigue para configurar el servicio DHCP en Vyatta se muestra en la Figura 3.25. Este proceso deberá ser configurado en la interfaz Eth1 y Eth2 para la topología proyecto.

```
vyatta@vyatta# set service dhcp-server shared-network-name nopoder subnet 192.16
8.1.0/25
[edit]
vyatta@vyatta# set service dhcp-server shared-network-name nopoder subnet 192.16
8.1.0/25 default-router 192.168.1.126
[edit]
vyatta@vyatta# set service dhcp-server shared-network-name nopoder subnet 192.16
8.1.0/25 dns-server 192.168.1.126
[edit]
vyatta@vyatta# set service dhcp-server shared-network-name nopoder subnet 192.16
8.1.0/25 start 192.168.1.31 stop 192.168.1.125
[edit]
vyatta@vyatta# set service dhcp-server shared-network-name nopoder authoritative
 enable
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.25. Configuración servicio DHCP

El comando "*authoritative*" que se usó dentro de la configuración del servicio DHCP permite que los paquetes de DHCP que viajan en la red tengan la mayor prioridad ante otros sistemas DHCP que posiblemente estén ofreciendo este servicio.

Una vez configurado el servicio DHCP en Eth1 como en Eth2 mediante el comando "*show service dhcp-server*" comprobamos que el servicio haya sido levantado. La información que aparecerá después de ejecutar el comando debería ser igual al de la Figura 3.26.

```
Done
[edit]
vyatta@vyatta# show service dhcp-server
 shared-network-name nopoder {
     authoritative enable
     subnet 192.168.1.0/25 {
         default-router 192.168.1.126
         dns-server 192.168.1.126
         start 192.168.1.31 {
             stop 192.168.1.125
         }
     }
 }
 shared-network-name poder {
     authoritative enable
     subnet 192.168.2.0/25 {
         default-router 192.168.2.30
         dns-server 192.168.2.30
         start 192.168.2.19 {
             stop 192.168.2.29
         }
     }
 }
[edit]
vyatta@vyatta# _
```

Figura. 3.26. Detalle de la configuración en el sistema Vyatta del servicio DHCP

Con esto se concluye la configuración del servicio de DHCP.

3.1.4 Configuración del servicio DNS

En el inciso anterior se configuró el sistema Vyatta como servidor DHCP y dentro de esta configuración se ha agregado un servidor DNS por defecto que es la IP del sistema Vyatta que gestiona la red respectivamente para cada interfaz. Para que esto funcione correctamente se debe configurar los sistemas Vyatta de la topología proyecto para que acepten consultas de resolución de nombres de dominio DNS y las resuelvan. Esto se consigue configurando el servicio DNS-forwarding de Vyatta.

El servicio DNS-forwarding permite asignar a este módulo un tamaño de cache, lo que significa que almacenará las consultas externas que tenga que hacer a DNS públicos en ese cache, hasta el límite de entradas dado, para que cuando algún cliente DNS haga una petición de una dirección que ya se haya consultado anteriormente , la resolución la haga el propio módulos DNS de Vyatta sin tener que consultarlo a DNS externos, lo que permite, para numerosos clientes y altas tasas de tráfico a Internet, ahorrar ancho de banda de conexión pública y la respuesta será más rápida que una consulta a DNS público. También hay que tener en cuenta que un tamaño muy grande puede resultar más lento que una consulta a un DNS público, por lo que no es conveniente usar tamaños demasiado grandes de cache.

Otro punto que hay que configurar para el servicio DNS-forwarding de Vyatta es la interfaz o interfaces en las que estará en escucha y en las que responderá las solicitudes DNS.

Por último se debe configurar los DNS públicos a los que el sistema Vyatta hará las consultas en caso de ser necesario.

La forma de configuración de DNS-forwarding se detalla a continuación en la Figura 3.27.

```
vyatta@vyatta# set service dns forwarding dhcp eth0
[edit]
vyatta@vyatta# set service dns forwarding listen-on eth1
[edit]
vyatta@vyatta# set service dns forwarding listen-on eth2
[edit]
vyatta@vyatta# set service dns forwarding listen-on eth3
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.27. Configuración del servicio DNS

Para constatar que el servicio DNS se levantó correctamente entonces ingresamos el comando "*show service dns*", el sistema Vyatta desplegará la información detallada en la Figura 3.28.

```
vyatta@vyatta# show service dns
 forwarding {
     dhcp eth0
     listen-on eth1
     listen-on eth2
     listen-on eth3
 }
[edit]
vyatta@vyatta# _
```

Figura. 3.28. Detalle de la configuración en el sistema Vyatta del servicio DNS

3.1.5 Configuración de QoS

La calidad de servicio es una característica que permite a los administradores de red identificar diferentes flujos de tráfico para poder tratarlos de acuerdo a su individual requerimiento en vez de usar simplemente el mecanismo por defecto.

En Vyatta el mecanismo de QoS por defecto se basa en priorización de colas, a parte de este mecanismo por defecto Vyatta ofrece también una variedad de mecanismos QoS para identificar y tratar los múltiples flujos de tráfico que atraviesan una interfaz. En general se pueden categorizar en mecanismos aplicables a tráfico saliente como entrante.

Para la topología proyecto la implementación de calidad de servicio que se planea dar trata acerca de la priorización del uso del ancho de banda de salida hacia el ISP, la división se dará dependiendo de la interface por la que el tráfico entra, en otras palabras dependiendo del grupo al que pertenece el host que desea navegar en internet se le asignará una cantidad del ancho de banda total, la división del ancho de banda se plantea en la Figura 3.29.

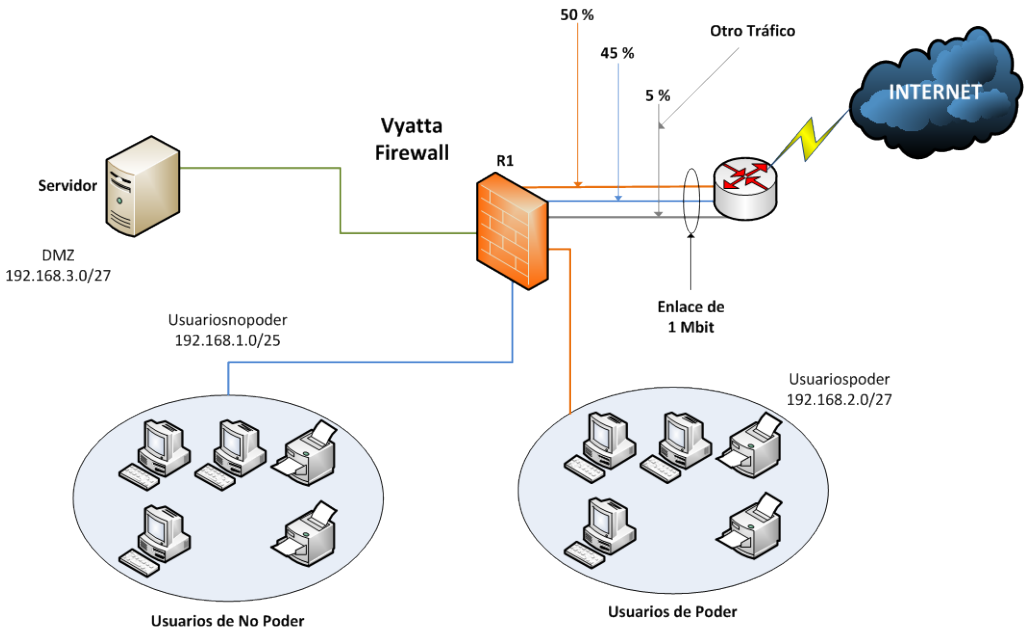


Figura. 3.29. Administración del ancho de banda para QoS

Para poder implementar la configuración descrita de QoS de la topología proyecto entonces tendremos que seguir la configuración descrita en la Figura 3.30.

```
vyatta@vyatta# set traffic-policy shaper LAN description "QoS ancho de banda WAN
"
[edit]
vyatta@vyatta# set traffic-policy shaper LAN bandwidth 1000kbit
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 20 description "poder"
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 20 bandwidth 45%
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 20 ceiling 100%
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 20 match TRAFICO-P interface
eth2
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 30 description "DMZ"
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 30 bandwidth 50%
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 30 ceiling 100%
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 30 match TRAFICO-DMZ interfac
e eth3
[edit]
vyatta@vyatta# set traffic-policy shaper LAN default  bandwidth 5%
[edit]
vyatta@vyatta# set traffic-policy shaper LAN default  ceiling 100%
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.30. Configuración de QoS en el sistema Vyatta para la topología proyecto

Para verificar que el sistema se ha levantado correctamente entonces corremos el comando "*show traffic-policy*", Vyatta nos mostrará una pantalla como la de la Figura 3.31.

```
 shaper LAN {
     bandwidth 1000kbit
     class 10 {
         bandwidth 25%
         ceiling 100%
         description nopoder
         match TRAFICO-NP {
             interface eth1
         }
     }
     class 20 {
         bandwidth 35%
         ceiling 100%
         description poder
         match TRAFICO-P {
             interface eth2
         }
     }
     class 30 {
         bandwidth 40%
         ceiling 100%
         description DMZ
         match TRAFICO-DMZ {
             interface eth3
         }
     }
     default {
         bandwidth 5%
         ceiling 100%
     }
     description "QoS ancho de banda WAN"
 }
[edit]
vyatta@vyatta# _
```

Figura. 3.31. Detalle de la configuración de QoS en el sistema Vyatta

3.1.6 Configuración del módulo firewall

Vyatta está dotado de framework Netfilter, que entre otras herramientas o módulos cuenta con iptables, un potente firewall open source o de código libre, que con la exportabilidad que Vyatta brinda podemos usarlo para proteger y gestionar la seguridad tanto en entornos físicos como en entornos virtualizados actuando como firewall físico o firewall virtual.

Normalmente las reglas de firewall son aplicadas como una pre-interfaz para realizar el filtrado de paquetes. En un sistema firewall basado en zonas, las interfaces son agrupadas en “zonas” de seguridad, donde cada interfaz en la zona tiene el mismo nivel de seguridad.

Las políticas para el filtrado de paquetes son aplicadas al tráfico que fluye entre zonas. El tráfico entre interfaces de la misma zona no es filtrado y fluye libremente.

Para la topología proyecto se crearán 4 zonas de tránsito, la zona de no poder, zona de poder, zona DMZ y zona pública. La interface eth0 será la de la zona pública, eth1 zona de no poder, eth2 zona de poder y eth3 zona de DMZ. Las flechas de la Figura 3.32 representan el tráfico que será permitido entre las distintas zonas, habrá que definir las políticas adecuadas en el sistema Vyatta para que esta configuración sea posible.

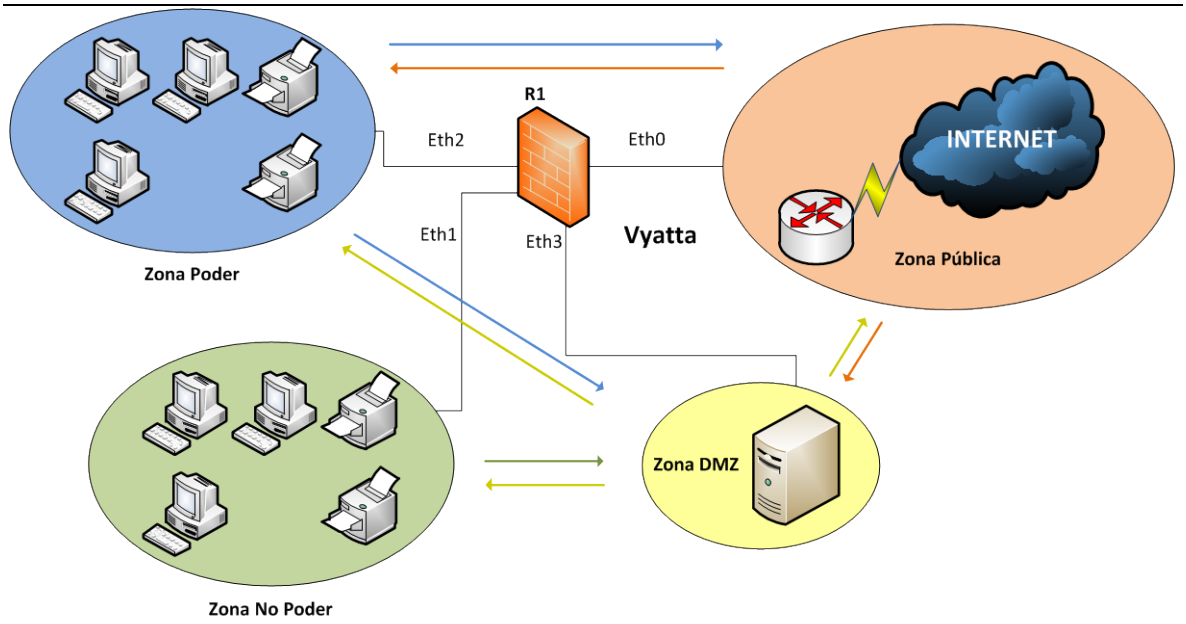


Figura. 3.32. Configuración de las distintas zonas para el módulo de firewall

También es necesario definir una nueva zona llamada “zona local”. Esta zona local es el sistema en sí Por defecto, todo el tráfico de entrada al sistema y originado por el sistema es permitido.

```
vyatta@vyatta# set zone-policy zone dmz description "Zona DMZ"
[edit]
vyatta@vyatta# set zone-policy zone dmz interface eth3
[edit]
vyatta@vyatta# set zone-policy zone poder description "Zona Poder"
[edit]
vyatta@vyatta# set zone-policy zone poder interface eth2
[edit]
vyatta@vyatta# set zone-policy zone nopoder description "Zona no Poder"
[edit]
vyatta@vyatta# set zone-policy zone nopoder interface eth1
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# set zone-policy zone publica description "Zona Publica"
[edit]
vyatta@vyatta# set zone-policy zone publica interface eth0
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.33. Levantamiento de zonas de firewall en el sistema Vyatta

Después de haber corrido los comandos de la Figura 3.33 para poder levantar las distintas zonas del firewall, ningún tipo de tráfico podrá fluir entre las distintas zonas. Todo el tráfico que fluya de una zona a otra será eliminado.

El siguiente paso consiste en crear las reglas de firewall para permitir el tráfico entre zonas. Primero se creará las reglas para permitir el tráfico hacia la zona pública. La configuración se detalla en la Figura 3.34.

```
vyatta@vyatta# set firewall name para_publica description "permite paso trafico
hacia zona publica"
[edit]
vyatta@vyatta# set firewall name para_publica rule 1 action accept
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.34. Permitir tráfico hacia zona pública

Ahora se configuraran las reglas para el tráfico de la Zona DMZ tal como en la Figura 3.35.

```
vyatta@vyatta# set firewall name podernopoder_a_dmz description "filtra el trafi
co desde la zona de poder o no poder hacia DMZ"
[edit]
vyatta@vyatta# set firewall name podernopoder_a_dmz rule 1 action accept
[edit]
vyatta@vyatta# set firewall name podernopoder_a_dmz rule 1 destination port http
,https,ftp
[edit]
vyatta@vyatta# set firewall name podernopoder_a_dmz rule 1 protocol tcp
[edit]
vyatta@vyatta# set firewall name podernopoder_a_dmz rule 2 action accept
[edit]
vyatta@vyatta# set firewall name podernopoder_a_dmz rule 2 icmp ty
type       type-name
[edit]
vyatta@vyatta# set firewall name podernopoder_a_dmz rule 2 icmp type-name any
[edit]
vyatta@vyatta# set firewall name podernopoder_a_dmz rule 2 protocol icmp
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# set firewall name publica_a_dmz description "permite el trafico d
esde la zona publica hacia dmz"
[edit]
vyatta@vyatta# set firewall name publica_a_dmz rule 1 action accept
[edit]
vyatta@vyatta# set firewall name publica_a_dmz rule 1 destination port http,http
s
[edit]
vyatta@vyatta# set firewall name publica_a_dmz rule 1 protocol tcp
[edit]
vyatta@vyatta# set firewall name publica_a_dmz rule 2 action accept
[edit]
vyatta@vyatta# set firewall name publica_a_dmz rule 2 icmp type-name any
[edit]
vyatta@vyatta# set firewall name publica_a_dmz rule 2 protocol icmp
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.35. Reglas de firewall para el tráfico de DMZ

Ahora se seguira con la configuración de la zona de poder y no poder. Las configuraciones se detallan en la Figura 3.36.

```
vyatta@vyatta# set firewall name para_podernopoder rule 1 description "filtra el
 trafico hacia la zona de poder y no poder"
[edit]
vyatta@vyatta# set firewall name para_podernopoder rule 1 action accept
[edit]
vyatta@vyatta# set firewall name para_podernopoder rule 1 state established enab
le
[edit]
vyatta@vyatta# set firewall name para_podernopoder  rule 1 state related enable
[edit]
vyatta@vyatta# set firewall name para_podernopoder rule 1 protocol all
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.36. Reglas de firewall para zona de poder y no poder

Ahora se aplicará las reglas de firewall creadas a las distintas zonas.

Primero se activarán las reglas en la zona DMZ, el procedimiento para esto se lleva a cabo en la Figura 3.37.

```
vyatta@vyatta# set zone-policy zone dmz from poder firewall name podernopoder_a_
dmz
[edit]
vyatta@vyatta# set zone-policy zone dmz from nopoder firewall name podernopoder_
a_dmz
[edit]
vyatta@vyatta# set zone-policy zone dmz from  publica firewall name publica_a_dm
z
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.37. Aplicación de las reglas de firewall a la zona DMZ

Ahora se aplicaran las reglas de firewall para las zonas de poder y de no poder. Esta configuración se lleva a cabo en la Figura 3.38.

```
vyatta@vyatta# set zone-policy zone poder from dmz firewall name para_podernopod
er
[edit]
vyatta@vyatta# set zone-policy zone poder from publica firewall name para_podern
opoder
[edit]
vyatta@vyatta# set zone-policy zone nopoder from dmz firewall name para_podernop
oder
[edit]
vyatta@vyatta# set zone-policy zone nopoder from publica firewall name para_pode
rnopoder
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.38. Levantamiento de reglas de firewall para zona de poder y no poder

Por último hay que configurar las reglas de firewall de la zona pública. Los comandos a seguir se detallan en la Figura 3.39.

```
vyatta@vyatta# set zone-policy zone publica from dmz firewall name para_publica
[edit]
vyatta@vyatta# set zone-policy zone publica from poder firewall name para_public
a
[edit]
vyatta@vyatta# commit
[edit]
```

Figura. 3.39. Levantamiento de reglas de firewall en la zona pública

Como se había comentado anteriormente, también se debe especificar reglas para la zona local, que en este caso viene a ser el sistema Vyatta. Por defecto, todo el tráfico destinado por el sistema y originado desde el sistema está aceptado. Por tanto se debe crear reglas de firewall que permitan sólo el tráfico de una zona específica hacia la zona local, en este caso se permitirá el tráfico de la zona DMZ hacia la zona local. Para efectuar esta configuración se deben seguir la configuración mostrada en la Figura 3.40.

```
vyatta@vyatta# set firewall name poder_a_vyatta description "filtra el trafico d
esde la zona de poder hacia la zona local"
[edit]
vyatta@vyatta# set firewall name poder_a_vyatta rule 1 action accept
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# set zone-policy zone vyatta from poder firewall name poder_a_vyat
ta
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# set firewall name desde_vyatta description "permite todo el trafi
co desde la zona local"
[edit]
vyatta@vyatta# set firewall name desde_vyatta rule 1 action accept
[edit]
vyatta@vyatta# set firewall name desde_vyatta rule 1 protocol all
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# set zone-policy zone poder from vyatta firewall name desde_vyatta

[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# set zone-policy zone publica from vyatta firewall name desde_vyatta
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 3.40. Configuración de la zona local

Con esto concluye la configuración del módulo de firewall de Vyatta. Con el comando "*show firewall*" el sistema Vyatta desplegará la configuración de las distintas reglas para el firewall. La pantalla debería mistrarse tal como en la Figura 3.41.

```
 name desde_vyatta {
     description "permite todo el trafico desde la zona local"
     rule 1 {
         action accept
         protocol all
     }
 }
 name para_podernopoder {
     rule 1 {
         action accept
         description "filtra el trafico hacia la zona de poder y no poder"
         protocol all
         state {
             established enable
             related enable
         }
     }
 }
 name para_publica {
     description "permite paso trafico hacia zona publica"
     rule 1 {
         action accept
     }
 }
 name podernopoder_a_dmz {
     description "filtra el trafico desde la zona de poder o no poder hacia DMZ"
     rule 1 {
         action accept
         destination {
             port http,https,ftp
         }
         protocol tcp
     }
     rule 2 {
         action accept
         icmp {
             type-name any
         }
         protocol icmp
     }
 }
 name poder_a_vyatta {
     description "filtra el trafico desde la zona de poder hacia la zona local"
     rule 1 {
         action accept
     }
 }
 name publica_a_dmz {
     description "permite el trafico desde la zona publica hacia dmz"
     rule 1 {
         action accept
         destination {
             port http,https
         }
         protocol tcp
     }
     rule 2 {
         action accept
         icmp {
             type-name any
         }
         protocol icmp
     }
 }
[edit]
vyatta@vyatta#
```

Figura. 3.41. Configuración de las reglas del módulo de firewall

Para observar como las distintas reglas de firewall están aplicadas a las zonas usamos el comando "*show zone-policy*", el sistema desplegará información idéntica a la de la Figura 3.42.

```
 zone dmz {
     description "Zona DMZ"
     from nopoder {
         firewall {
             name podernopoder_a_dmz
         }
     }
     from poder {
         firewall {
             name podernopoder_a_dmz
         }
     }
     from publica {
         firewall {
             name publica_a_dmz
         }
     }
     interface eth3
 }
 zone nopoder {
     description "Zona no Poder"
     from dmz {
         firewall {
             name para_podernopoder
         }
     }
     from publica {
         firewall {
             name para_podernopoder
         }
     }
     interface eth1
 }
 zone poder {
     description "Zona Poder"
     from dmz {
         firewall {
             name para_podernopoder
         }
     }
     from publica {
         firewall {
             name para_podernopoder
         }
     }
     from vyatta {
         firewall {
             name desde_vyatta
         }
     }
     interface eth2
 }
 zone publica {
     description "Zona Publica"
     from dmz {
         firewall {
             name para_publica
         }
     }
     from poder {
         firewall {
             name para_publica
         }
     }
     interface eth0
 }
 zone vyatta {
     description local-zone
     from poder {
         firewall {
             name poder_a_vyatta
         }
     }
     local-zone
 }
[edit]
vyatta@vyatta#
```

Figura. 3.42. Configuración de zonas con reglas firewall

CAPÍTULO IV

PRUEBAS Y EVALUACIÓN DE VYATTA

4.1 PRUEBAS DE FUNCIONAMIENTO Y EVALUACIÓN DEL DESEMPEÑO DE VYATTA

Para las distintas pruebas de este capítulo se usará distintas herramientas, todas de software libre como Throughput Test, IPNetMonitorX.

4.1.1 Pruebas de funcionamiento y desempeño de DHCP

Las pruebas correspondientes al funcionamiento de este servicio están basadas en el tiempo en el que el servidor es capaz de responder a una petición de dirección IP. Para probar este sistema se usó un programa de uso libre llamado IPNetMonitorX, los resultados que se obtuvieron fueron muy exitosos ya que el servidor respondió a las peticiones de manera acelerada, la prueba mas exhaustiva se realizó al hacer una petición de 100 direcciones IP desde la zona de no poder, con retraso entre cada petición de 0 segundos. Estos resultados se pueden observar en la Figura 4.1.

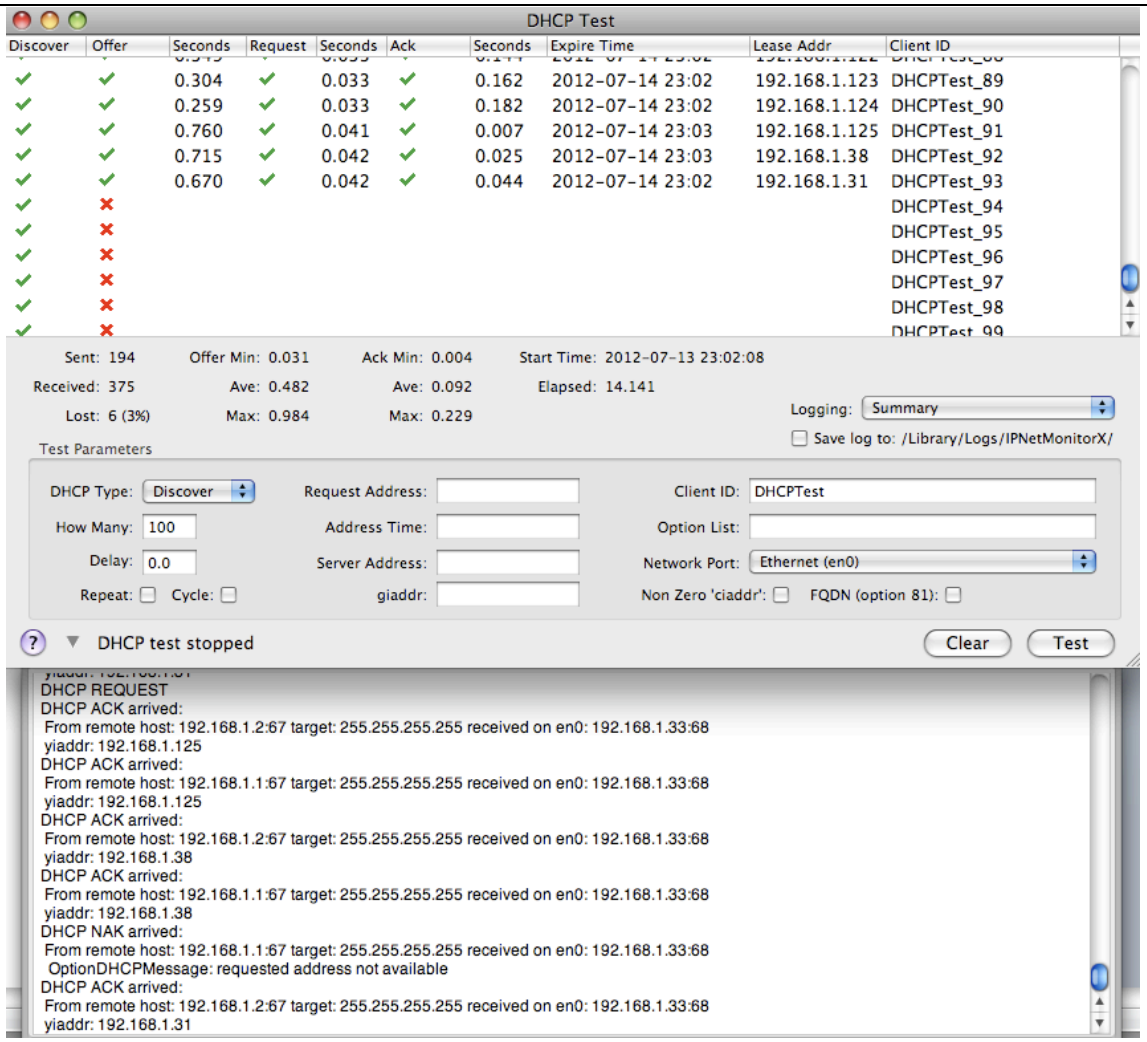


Figura. 4.1. Petición de direcciones al servidor DHCP

4.1.2 Pruebas de funcionamiento y desempeño de DNS

Para las pruebas de DNS lo que se hizo es comprobar que después de haber hecho una consulta, Vyatta haya guardado en su memoria caché los datos de esa consulta, esta característica es muy usual, dado que así las consultas de dominio pueden responderse de una manera más rápida. Mediante el programa IPNetMonitorX se puede ver la información de la petición DNS de una forma más detallada, la interfaz dentro de IPNetMonitorX que se usó se llama Name Server Query.

Name Server Query permite ver información adicional del Sistema de Nombres de Dominio de Internet enviando solicitudes al servidor de nombres por defecto.

Los resultados que se obtuvieron fueron favorables ya que en la segunda petición al mismo nombre de dominio la respuesta fue dada tan sólo por Vyatta y en un tiempo mucho mas corto. Estos resultados son visibles en las Figuras 4.2 y 4.3.

También se puede verificar el servidor desde el que la petición fue respondida, así se comprueba que los nombres de dominio han sido almacenados en memoria caché de Vyatta.

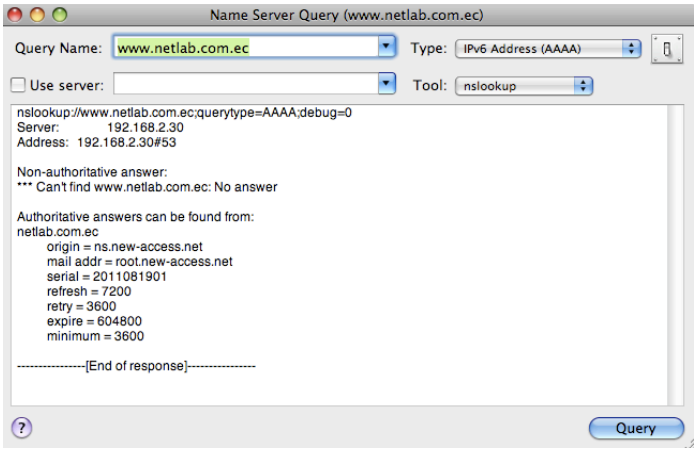


Figura. 4.2. Respuesta de la primera petición DNS a www.netlab.com.ec

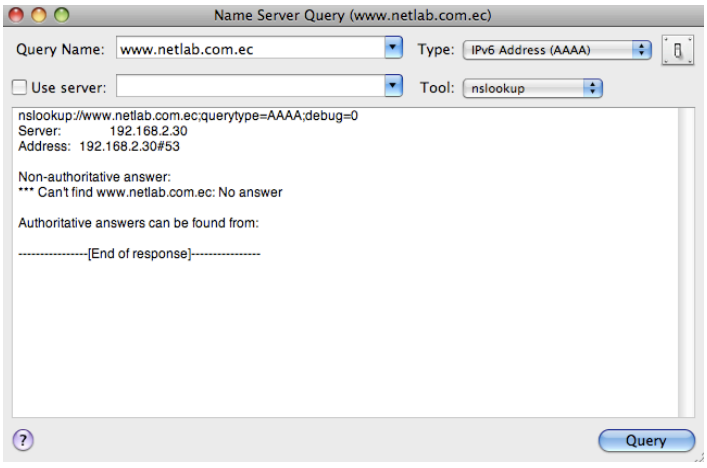


Figura. 4.3. Respuesta de la segunda petición DNS a www.netlab.com.ec

En la Figura 4.4 se puede apreciar las estadísticas servidor DNS dentro de Vyatta, el número de respuestas DNS locales y las peticiones realizadas a servidores externos, mismos que fueron configurados mediante DHCP en la interfaz que se conecta con Internet, estos servidores DNS externos se ven de forma explícita en la Figura 4.5.

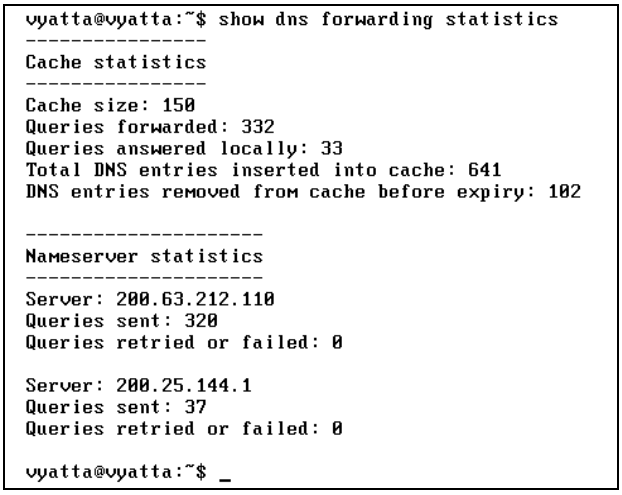


Figura. 4.4. Estadísticas del servidor DNS dentro de Vyatta

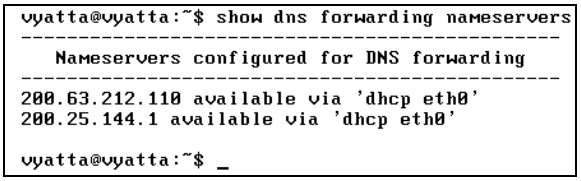


Figura. 4.5. Servidores para consulta externa DNS

4.1.3 Pruebas de funcionamiento y desempeño de QoS

Para las pruebas de QoS se optó por una configuración adecuada para comprobar que en realidad se está dividiendo el ancho de banda para las distintas zonas.

La configuración que se usó se puede notar en la Figura 4.6, un cliente de la zona de poder y otro de la zona de no poder se conectaron a dos servidores en el internet y se midió desde los clientes el throughput de la conexión.

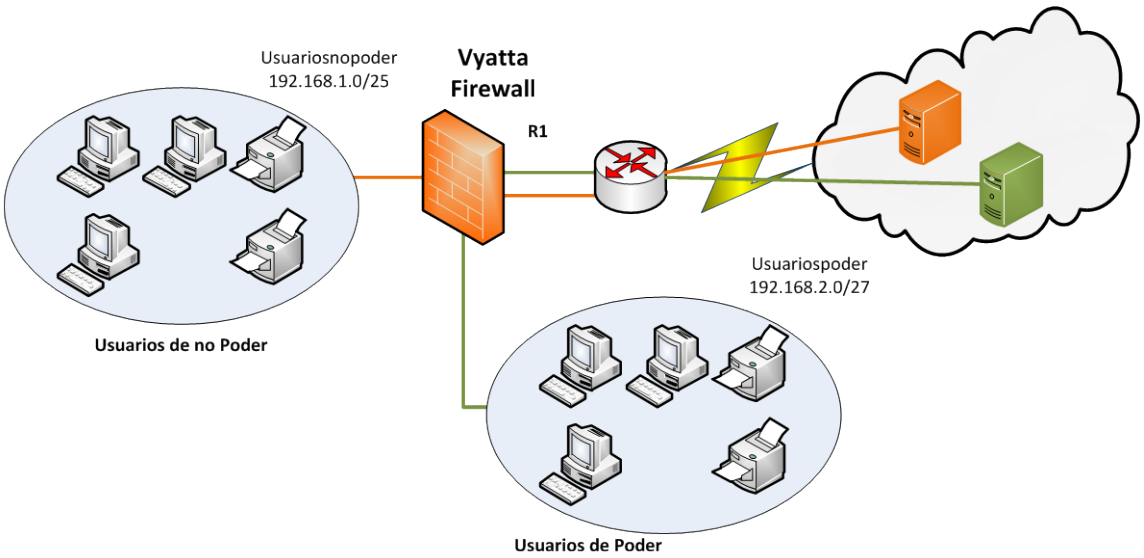


Figura. 4.6. Topología para pruebas de QoS

Con el objetivo de que se pueda apreciar de mejor forma el funcionamiento de la calidad de servicio, se realizaron modificaciones dentro del sistema Vyatta, estas estan detalladas en la Figura 4.7.

```
vyatta@vyatta# delete traffic-policy shaper LAN class 10 bandwidth 45%
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# delete traffic-policy shaper LAN class 20 bandwidth 50%
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 10 bandwidth 15%
[edit]
vyatta@vyatta# set traffic-policy shaper LAN class 20 bandwidth 80%
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

Figura. 4.7. Cambios de la configuración de QoS en el sistema Vyatta

Las Figuras 4.8 y 4.9 muestran los resultados obtenidos al medir el rendimiento de la conexión hacia el internet desde la zona de poder y la zona de no poder.

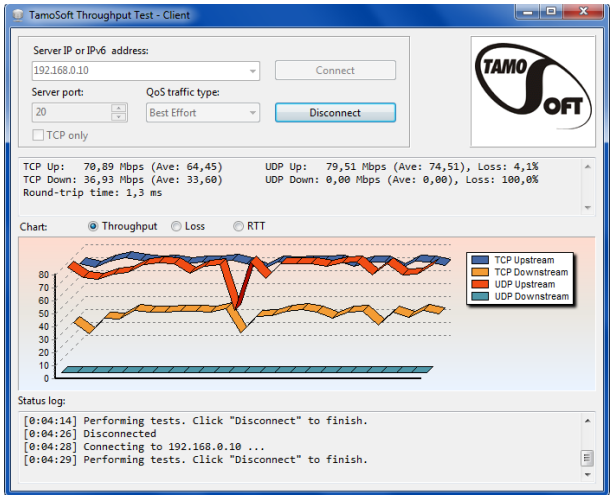


Figura. 4.8. Rendimiento de la conexión a internet desde host en la zona de poder

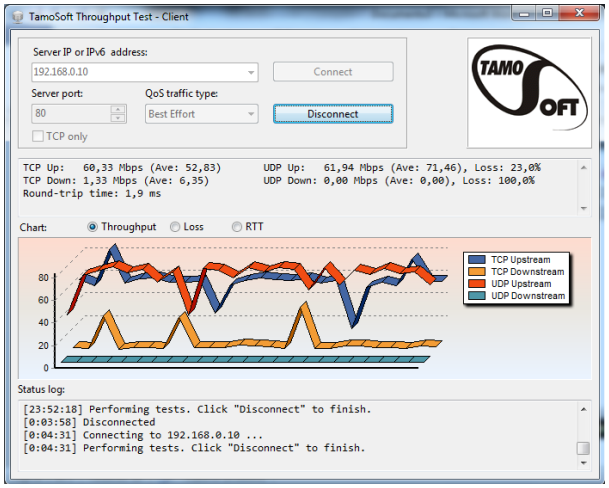


Figura. 4.9. Rendimiento de la conexión a internet desde host en la zona de no poder

El ancho de banda total que se tomó en consideración para salida al internet es de 100Mbps, con esto podemos calcular los valores medios de ancho de banda para cada zona, en consecuencia, la zona de usuarios de poder tendrá un ancho de banda aproximadamente de 80Mbps y la zona de no poder un ancho de banda de 15Mbps, también se debe tomar en consideración que idealmente el

ancho de banda total será de 100Mbps pero existen pérdidas debido a equipos intermedios, cables de transmisión, conectores, etc.

Resumiendo los resultados obtenidos en las pruebas anteriores se obtuvo la Tabla 5.1.

	Zona de Poder			Zona de no Poder		
	Teórico	Experimental	Error Porcentual	Teórico	Experimental	Error Porcentual
TCP Descarga de Datos Media	80	33,6	58	15	6,35	57,67

Tabla. 4.1. Resumen de pruebas de calidad de servicio en una red con ancho de banda de 100Mbps

Teniendo en cuenta que el ancho de banda medio de la red es de 60Mbps y por tanto el ancho de banda para la zona de usuarios de poder sería de 48Mbps y de 9Mbps para la zona de no poder, entonces se recalculan estos errores y se obtiene la Tabla 5.2.

	Zona de Poder			Zona de no Poder		
	Teórico	Experimental	Error Porcentual	Teórico	Experimental	Error Porcentual
TCP Descarga de Datos Media	48	33,6	30	9	6,35	29,44

Tabla. 4.2. Resumen de pruebas de calidad de servicio en una red con ancho de banda de 60Mbps

4.1.4 Medidas de tráfico local y tráfico hacia internet

Esta sección analiza la cantidad de tráfico que es capaz de circular desde la red local hacia el internet mediante Vyatta, y de la misma manera también se analizará la capacidad que tiene Vyatta de manejar tráfico dentro de la red local.

Link Rate es una herramienta que proporciona IPNetMonitorX, esta da una estimación del ancho de banda o una taza de transferencia de una conexión de datos, enviando una serie de peticiones ICMP echo request (pings) y comparando

el tiempo de cada respuesta. La herramienta Link Rate calcula el ancho de banda disponible en función del tiempo medido para transferir estos bytes.

La primera prueba que se realizó, fue levantando una conexión hacia la puerta de enlace predeterminada en la zona de poder, la esquematización de esta prueba se aprecia en la Figura 4.10 y los resultados obtenidos se muestran en la Figura 4.11.

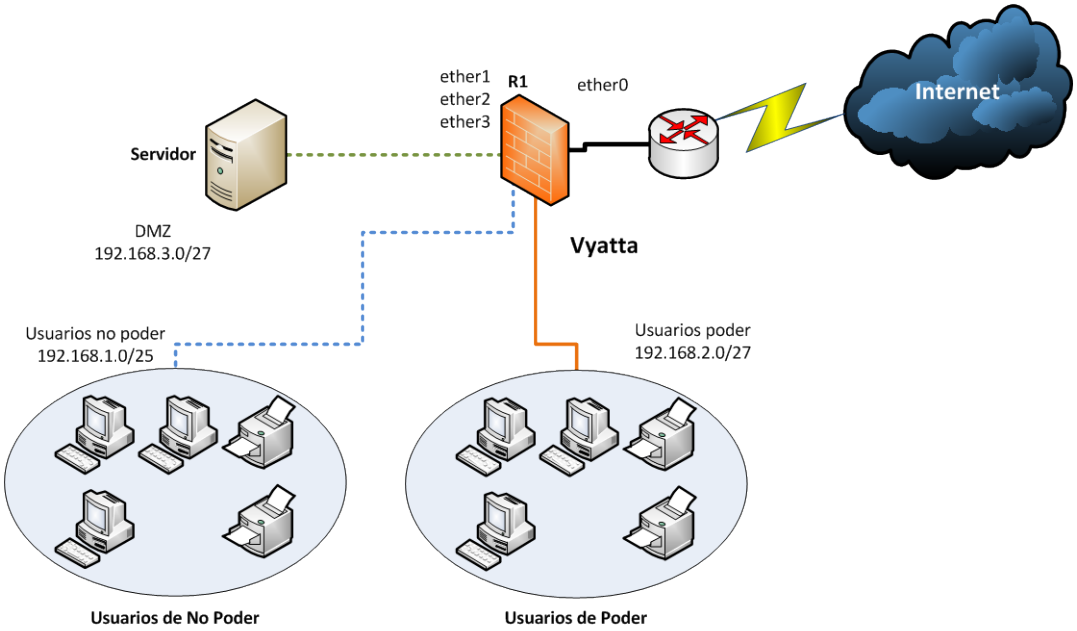


Figura. 4.10. Esquematización conexión desde host de la zona de poder hacia su puerta de enlace predeterminada

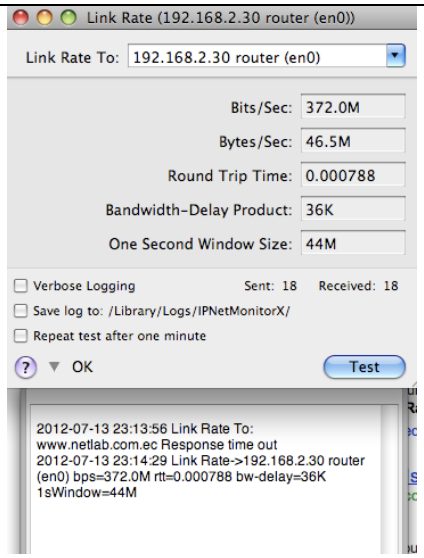


Figura. 4.11. Medida del ancho de banda entre un host de la zona de poder hacia su puerta de enlaze predeterminada

Para la siguiente prueba que se tomó en consideración, de la cual sus resultados se ven reflejados en la Figura 4.13, se realizó una medida del ancho de banda que se puede alcanzar hacia un servidor en internet, en este caso www.google.com, la esquematización de este ejemplo se puede ver en la Figura 4.12.

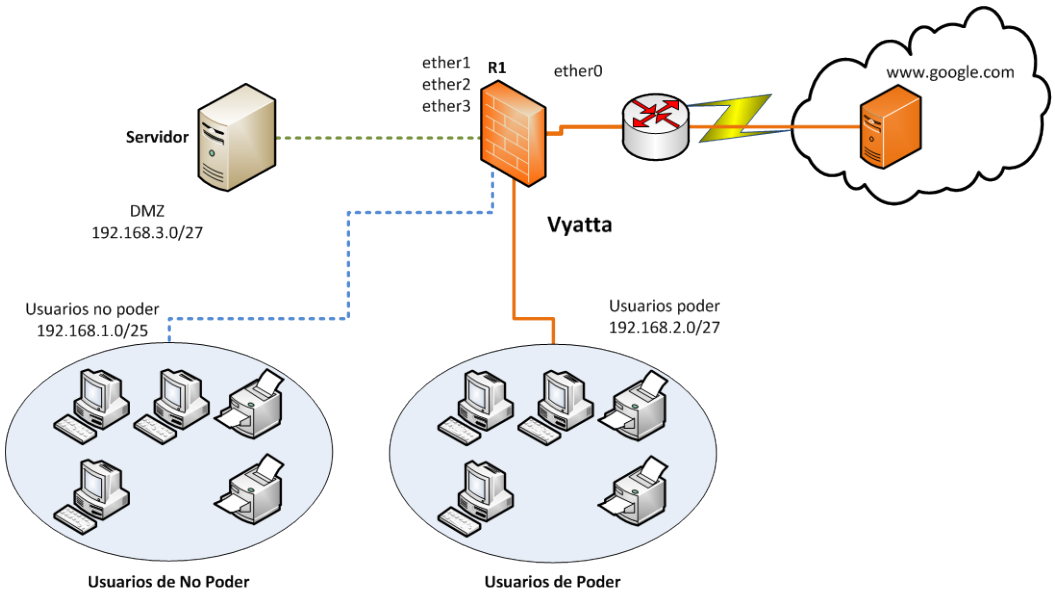


Figura. 4.12. Esquematización conexión desde host de la zona de poder hacia servidor en internet

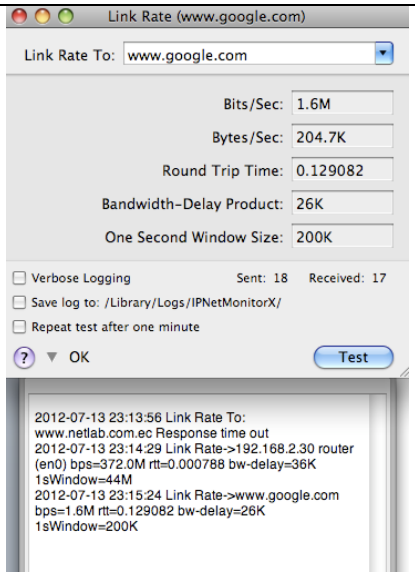


Figura. 4.13. Medida del ancho de banda entre un host de la zona de poder hacia un servidor de internet www.google.com

Para las próximas pruebas la herramienta que se usó es TCP Monitor que al igual que Link Rate es parte de IPNetMonitorX, esta herramienta permite examinar el comportamiento del tráfico TCP/IP de una forma más cercana.

Para esta prueba se procedió a probar las conexiones a internet mientras existe tráfico web así como descargas a servidores ftp, los resultados obtenidos en el momento más álgido del uso del internet desde la zona de poder se pueden apreciar en la Figura 4.14.

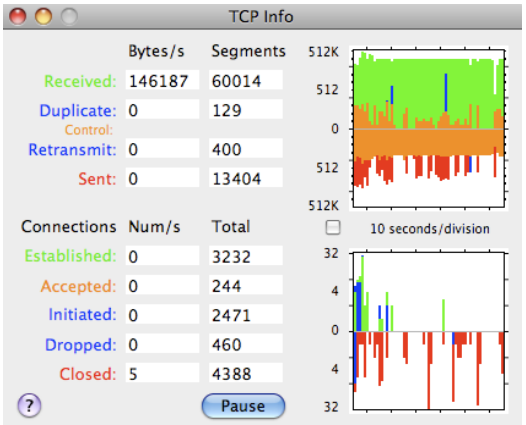


Figura. 4.14. Medida del tráfico TCP/IP desde la zona de poder hacia el internet

Las primeras pruebas que se ejecutaron para probar el desempeño de la red están basadas en una comparación entre una conexión intranet y una conexión internet, El resumen de los datos obtenidos en estas pruebas se presentan en la Tabla 5.3.

Conexiones Desde Zona de Poder			
Hacia el Sistema Vyatta		Hacia www.google.com	
Ancho de Banda (Mbps)	RTT (mseg)	Ancho de Banda (Mbps)	RTT (mseg)
46,5	0,78	0,2047	129

Tabla. 4.3. Tabulación de datos de las pruebas realizadas con conexiones hacia intranet e internet

Lógicamente la velocidad de conectividad o el ancho de banda interno es mucho más rápido que una conexión hacia un servidor en el internet, esta prueba tan sólo nos da una idea del verdadero ancho de banda que se está manejando dentro y fuera de la red.

Las siguientes pruebas se realizaron sobre la red local, tanto desde la zona de poder como desde la zona de no poder hacia la zona DMZ. El tráfico permitido entre estas zonas es web y ftp, por lo que las pruebas se correrán en base a estos servicios, para tratar de ver el máximo alcance del rendimiento de Vyatta también se agregaron servicios de audio y video.

Las pruebas iniciales serán entre la zona de no poder hacia la zona DMZ y se probará el rendimiento entre estas dos zonas usando el programa Throughput Test, este nos provee de un cliente y un servidor, el cliente se correrá desde el host en la zona de no poder y el servidor en la zona DMZ, esta configuración se puede apreciar en la Figura 4.15.

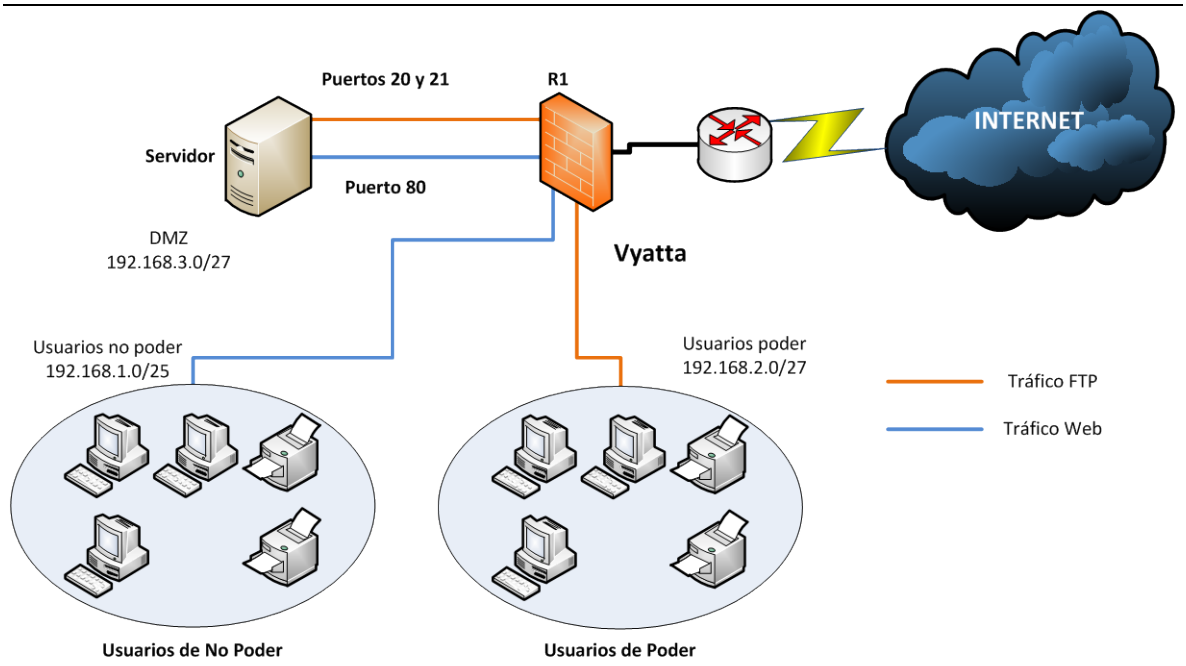


Figura. 4.15. Esquematización de la prueba entre la zona de poder y zona DMZ

En las Figuras 4.16, 4.17 y 4.18 se pueden apreciar los resultados obtenidos durante las pruebas. Cabe recalcar que los picos que son notorios en las gráficas, se deben a que exactamente en ese momento se descargó desde un host en la zona de poder un video de 31M [Bytes] proveniente del mismo servidor usado por el host de la zona de no poder, valga la redundancia dicho servidor se encuentra en la zona DMZ.

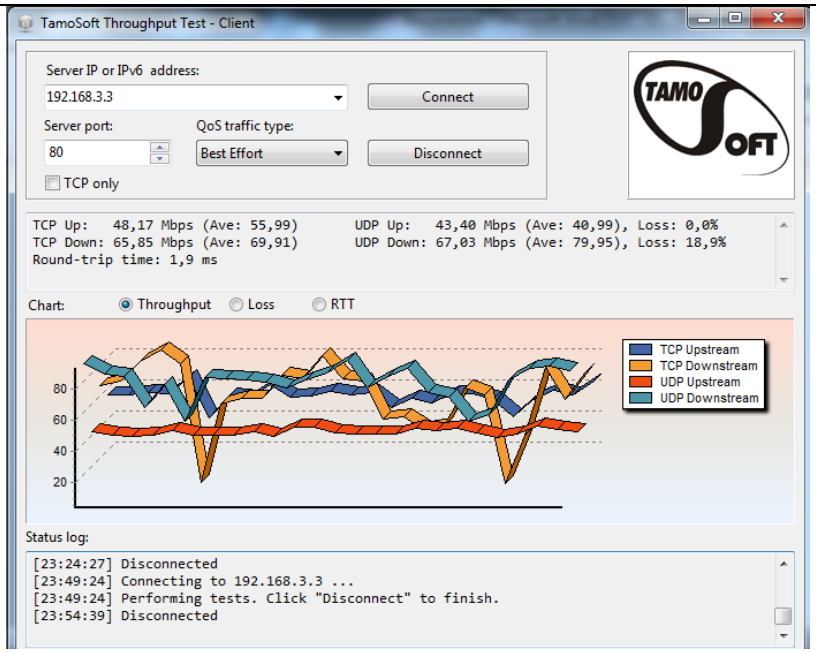


Figura. 4.16. Gráfica de rendimiento del cliente en la zona de no poder

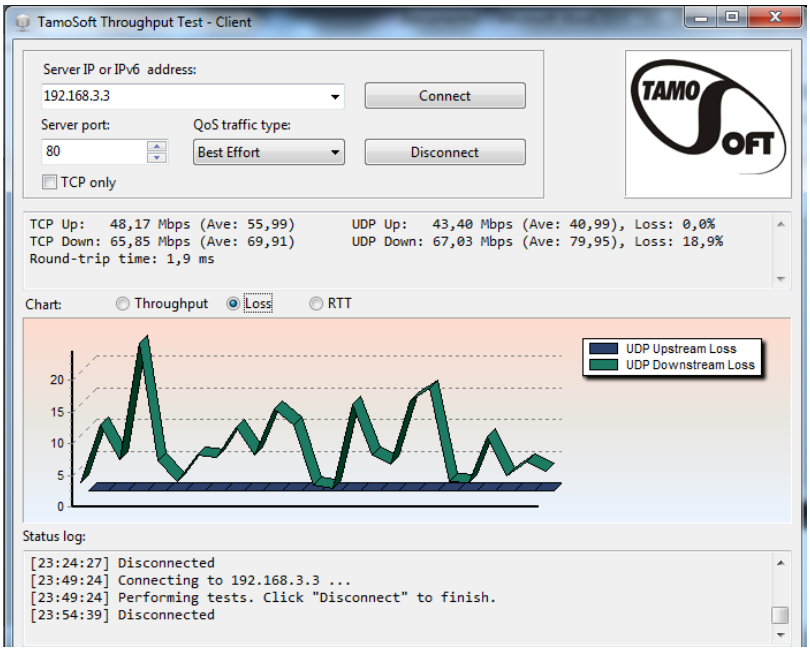


Figura. 4.17. Gráfica de paquetes perdidos del cliente en la zona de no poder

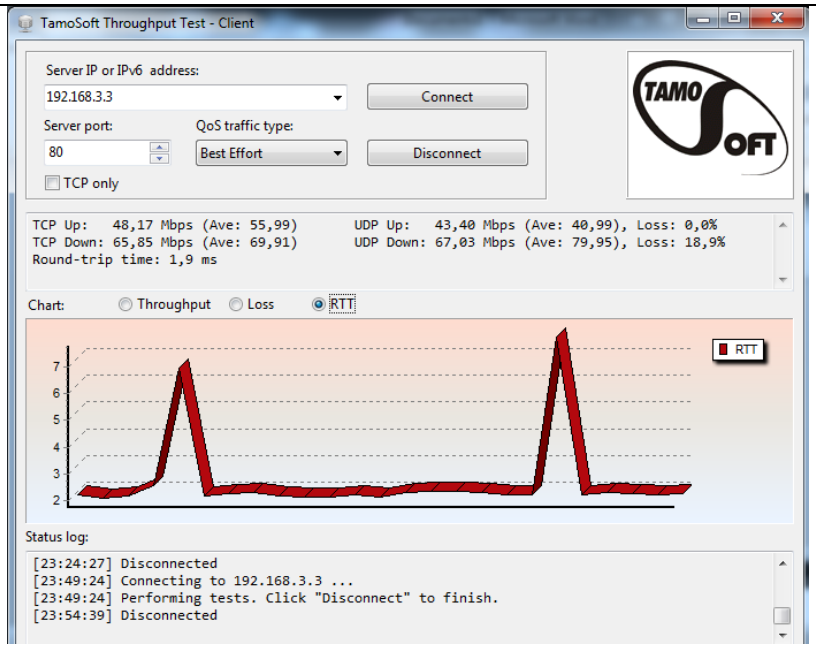


Figura. 4.18. Gráfica de RTT del cliente en la zona de no poder

La Figura 4.19 muestra el flujo de tráfico TCP mientras se efectuaba una descarga desde un host en la zona de poder de un archivo que estaba ubicado en la zona DMZ.

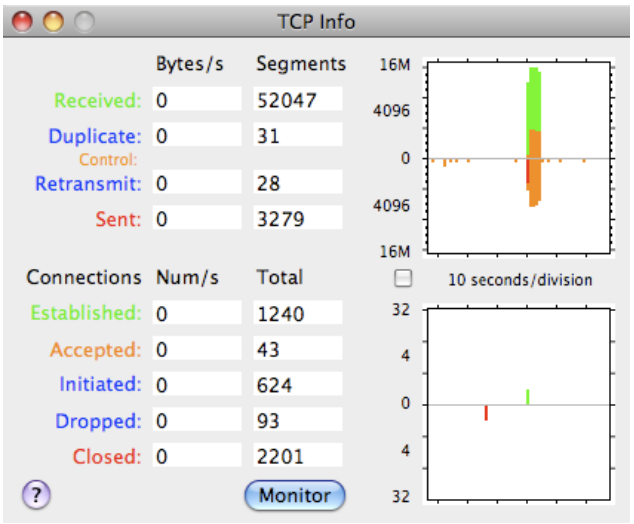


Figura. 4.19. Descarga de archivo en la zona de poder desde la zona DMZ

Ahora para hacer un análisis más exhaustivo del desempeño del flujo de datos tanto en la intranet, se efectuarán una serie de pruebas más rigorosas.

La primera prueba consiste en mantener levantadas 4 conexiones y observar mediante el programa Throughput Test el desempeño de la red. Cuatro servidores fuéron levantados en la zona DMZ, usando los puertos 20, 80, 3650 y 3651, los puertos 3650 y 3651 se los uso para generar tráfico de audio y video. En la Figura 4.20 se puede ver un esquema general de esta configuración.

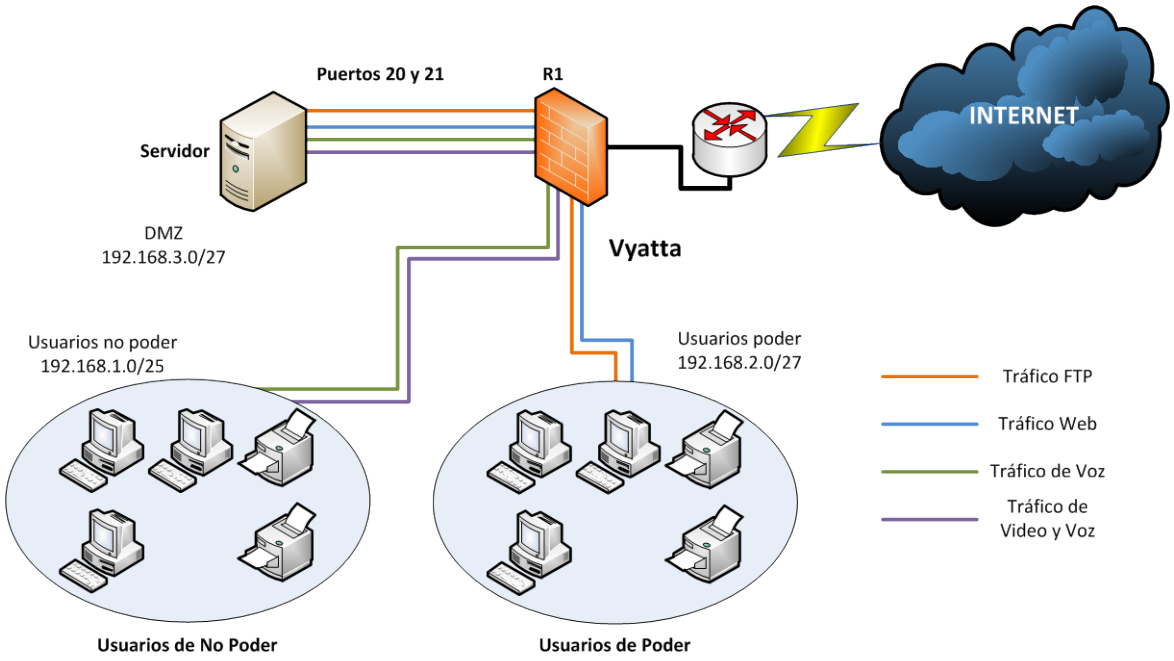


Figura. 4.20. Esquema general para pruebas de rendimiento de la red local

De inicio se levantaron todas las conexiones tal y como se muestra en la Figura 4.20 y los resultados arrojados por el programa Throughput Test para cada uno de los clientes, en los distintos host de cada zona fueron los de las Figura 4.21, 4.22, 4.23 y 4.24, la Figura 4.25 por otro lado muestra las interfaces de Throughput Test como servidor en el servidor de la zona DMZ.

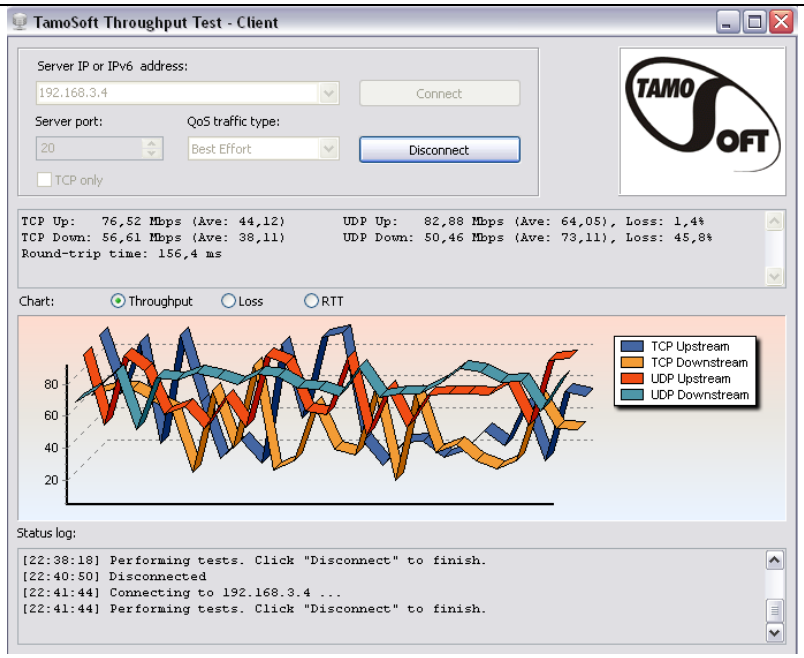


Figura. 4.21. Cliente en la zona de poder con conexión al puerto 20 de la zona DMZ, servicio FTP

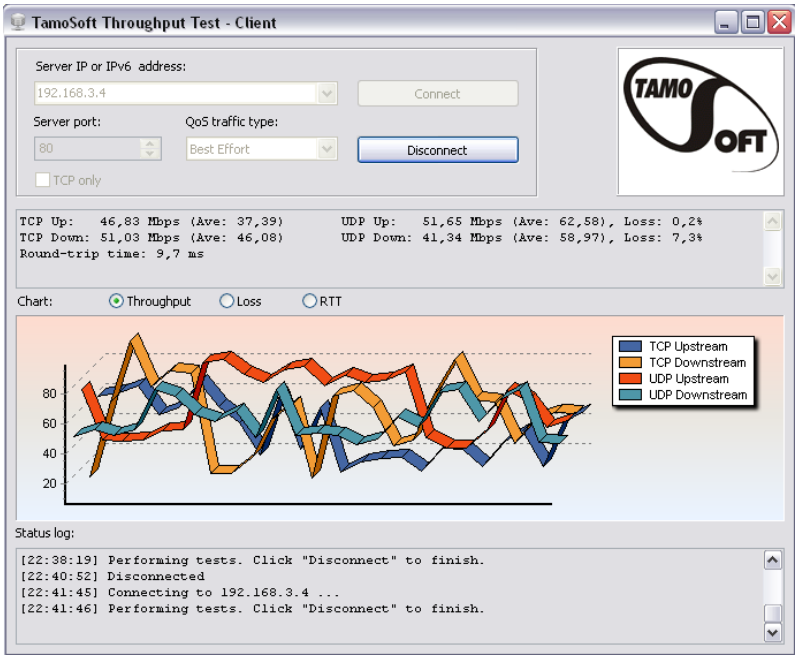


Figura. 4.22. Cliente en la zona de poder con conexión al puerto 80 de la zona DMZ, servicio web

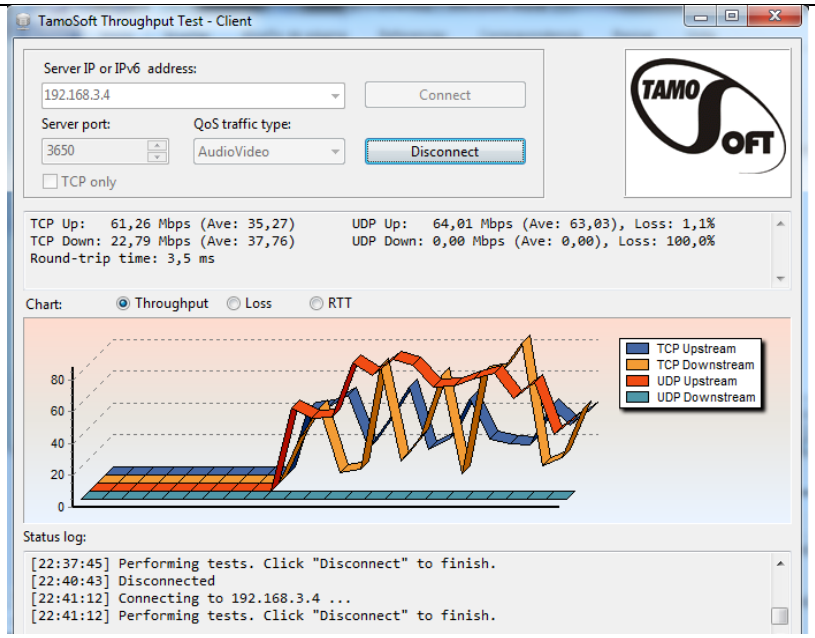


Figura. 4.23. Cliente en la zona de no poder con conexión al puerto 3650 de la zona DMZ, servicio de audio y video

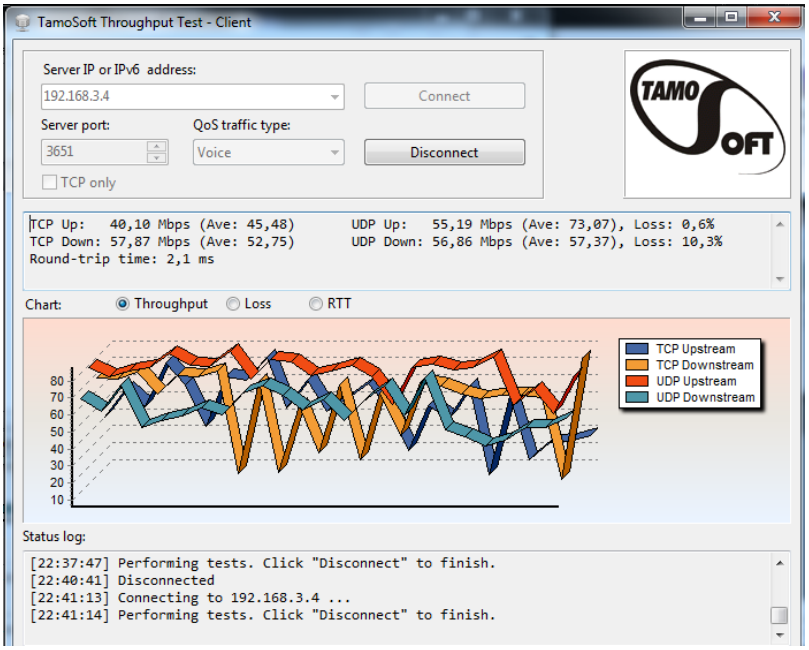


Figura. 4.24. Cliente en la zona de no poder con conexión al puerto 3651 de la zona DMZ, servicio de voz

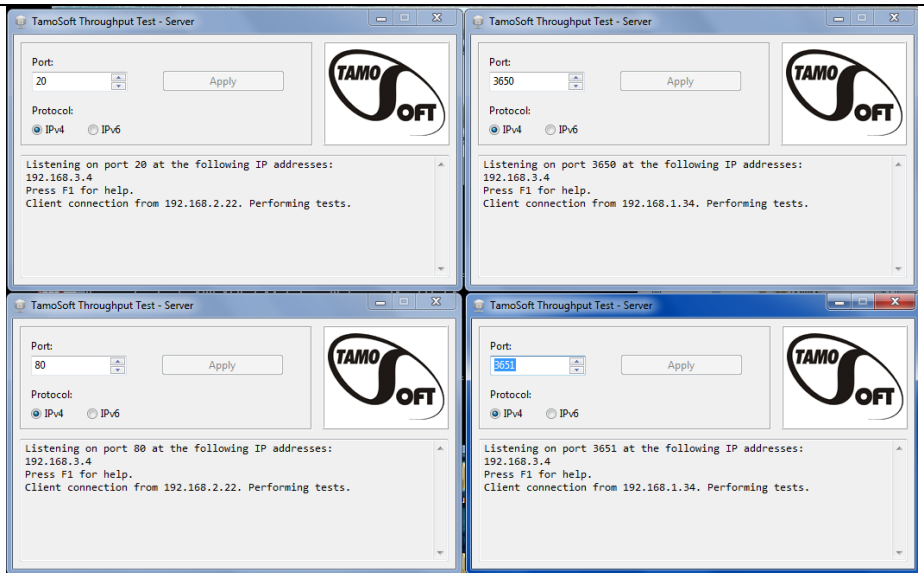


Figura. 4.25. Estado de los servidores levantados através del programa troughput test en el servidor de la zona DMZ

En la Tabla 5.4 se encuentran tabulados los datos obtenidos en las pruebas de desempeño de la red local, en el instante en que los clientes de la zona de poder y de la zona de no poder se conectaron hacia el servidor de la zona DMZ.

	Conexiones Hacia DMZ					
	Zona de Poder			Zona de no Poder		
	TCP	UDP	UDP perdido	TCP	UDP	UDP perdido
	Puerto 20 (Mejor Esfuerzo)			Puerto 3650 (AudioVideo)		
Subida (Mbps)	44,12	64,05	1,40%	35,27	63,03	1,10%
Bajada (Mbps)	38,11	73,11	45,80%	37,76	0	100%
	Puerto 80 (Mejor Esfuerzo)			Puerto 3651 (Voz)		
Subida (Mbps)	37,39	62,58	0,20%	45,48	73,07	0,60%
Bajada (Mbps)	46,08	58,97	7,30%	52,75	57,37	10,30%

Tabla. 4.4. Tabulación de datos de las pruebas realizadas con 4 servicios en la zona DMZ y con conexiones desde la zona de poder y no poder

Es necesario recalcar que en esta prueba las conexiones fueron simultaneas y debido a esto el ancho de banda fue dividido, por tal razón la diferencia del ancho de banda real entre esta prueba al de las siguientes es bastante grande en

el caso del tráfico TCP, ya que éste siendo un protocolo controlado necesita inyectar más paquetes a la red para dicho control.

La Figura 4.26 muestra la configuración que se usó para la siguiente prueba del desempeño de la red local, como se puede apreciar en dicha figura, los servicios de audio y video fueron desconectados para medir el desempeño de la conexión con tan sólo los servicios web y ftp, los resultados que esta configuración produjo fueron los detallados en las Figura 4.27 y 4.28.

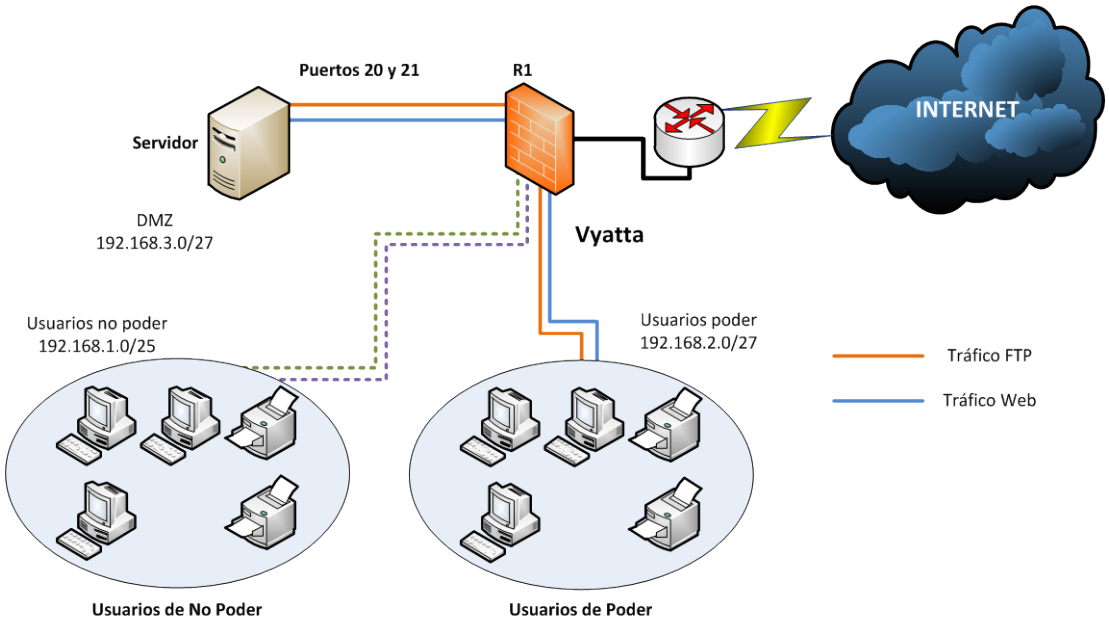


Figura. 4.26. Esquema con sólo dos conexiones a la zona DMZ, tráfico web y FTP

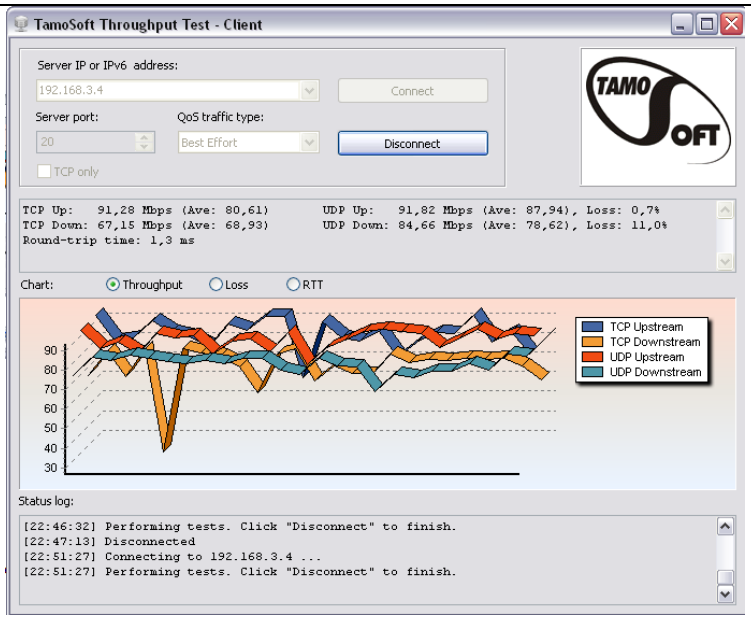


Figura. 4.27. Cliente en la zona de poder con conexión al puerto 20 de la zona DMZ, servicio FTP

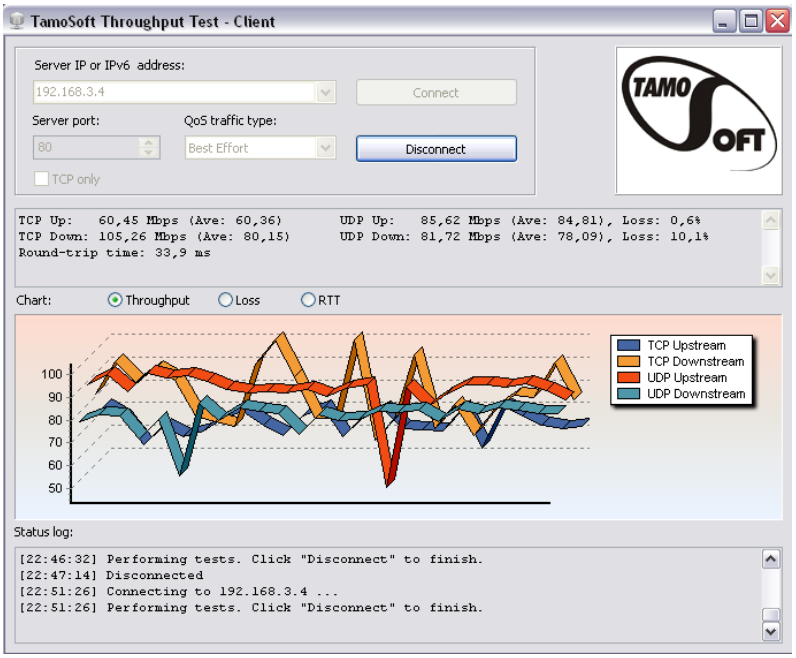


Figura. 4.28. Cliente en la zona de poder con conexión al puerto 80 de la zona DMZ, servicio web

En la Figura 4.29 se puede ver que nuevamente se conectó los servicios de audio y video pero se desconectó los servicios web y ftp, los resultados obtenidos por estas pruebas fueron los de las Figuras 4.30, 4.31.

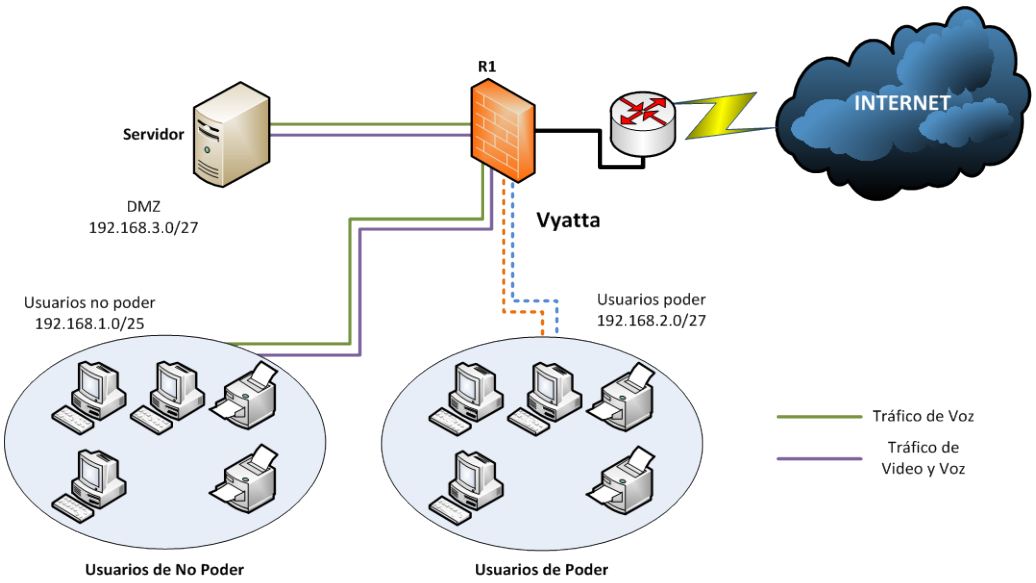


Figura. 4.29. Esquema con sólo dos conexiones a la zona DMZ, audio y video

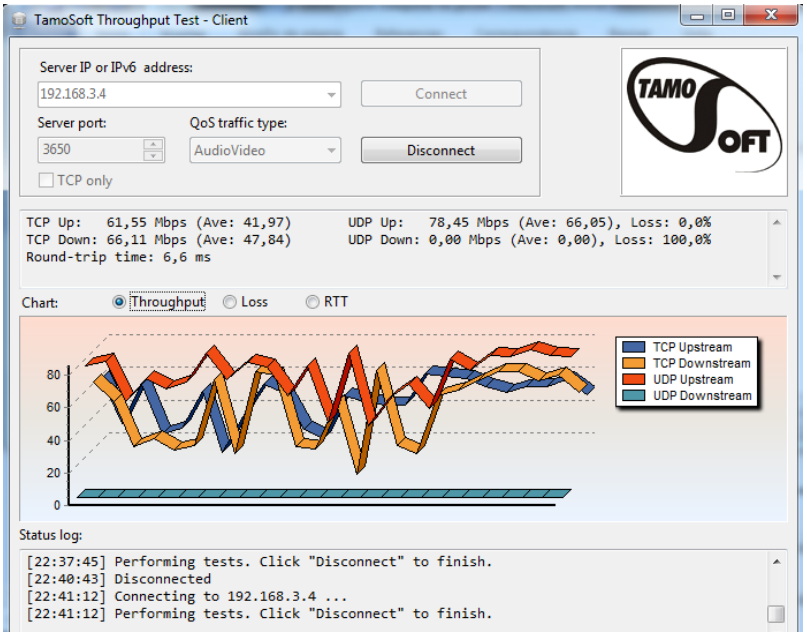


Figura. 4.30. Cliente en la zona de no poder con conexión al puerto 3650 de la zona DMZ con servicios de audio y video

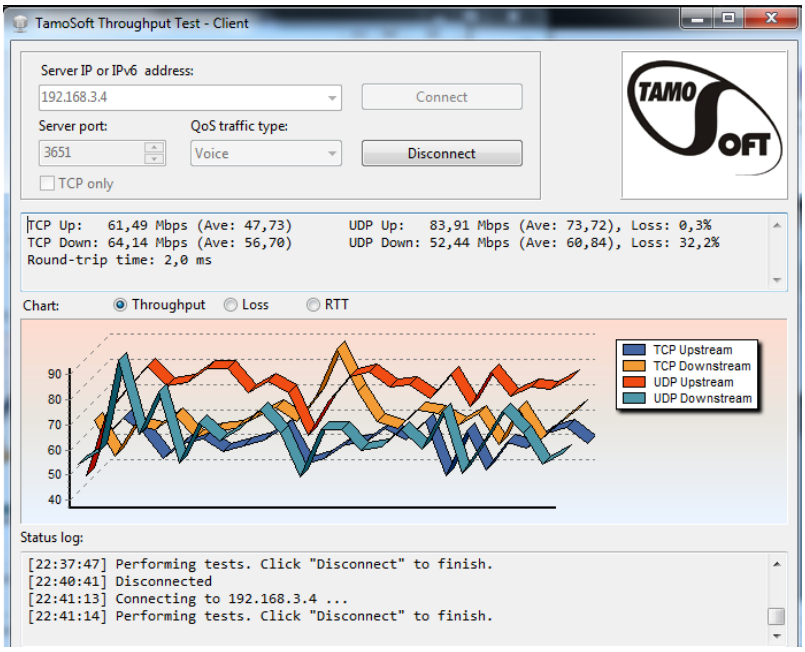


Figura. 4.31. Cliente en la zona de no poder con conexión al puerto 3651 de la zona DMZ con servicio de voz

En la Tabla 5.5 se presenta la tabulación de los datos obtenidos en las pruebas cuando sólo existía conexión desde la zona de poder hacia la zona DMZ, y en la Tabla 5.6 están los datos obtenidos cuando sólo existían conexiones desde la zona de no poder hacia la zona DMZ.

	Zona de Poder		
	TCP	UDP	UDP perdido
	Puerto 20 (Mejor Esfuerzo)		
Subida (Mbps)	80,61	87,94	0,70%
Bajada (Mbps)	68,93	78,62	11,00%
	Puerto 80 (Mejor Esfuerzo)		
Subida (Mbps)	60,36	84,81	0,60%
Bajada (Mbps)	80,15	78,09	10,10%

Tabla. 4.5. Tabulación de datos de las pruebas realizadas con 2 conexiones desde la zona de poder hacia la zona DMZ

	Zona de no Poder		
	TCP	UDP	UDP perdido
	Puerto 3650 (AudioVideo)		
Subida (Mbps)	41,97	66,05	0,00%
Bajada (Mbps)	47,84	0	100%
	Puerto 3651 (Voz)		
Subida (Mbps)	47,73	73,72	0,30%
Bajada (Mbps)	56,7	60,84	32,20%

Tabla. 4.6. Tabulación de datos de las pruebas realizadas con 2 conexiones desde la zona de no poder hacia la zona DMZ

La diferencia que se puede apreciar entre los datos obtenidos en la Tabla 5.4 y la Tabla 5.6 en el caso de TCP son de casi el doble, debido a que el tipo de paquetes TCP que se estaban manejando son BestEffort, esto quiere decir que no se está usando algún tipo de calidad de servicio a nivel MAC. Al momento de enviar paquetes TCP que implican calidad de servicio como en la conexión entre la zona de no poder y la zona DMZ en las que se envían paquetes de audiovideo y de voz, el ancho de banda usado por estos clientes disminuye en relación a los que no usan calidad de servicio, estos datos se pueden apreciar relacionando los resultados tabulados en la Tabla 5.4 y los de la Tabla 5.6.

4.1.5 Pruebas de funcionamiento de redundancia y alta disponibilidad

En este subtema se probará que la alta disponibilidad y por tanto la redundancia del sistema esté funcionando adecuadamente. Las primeras pruebas que se efectuarán serán generando paquetes ICMP echo request (ping) desde un usuario de la zona de poder hacia su puerta de enlace predeterminada, que en este caso sería la dirección virtual VRRP del sistema Vyatta en la interfaz correspondiente a la zona de poder.

La prueba se realizará de la siguiente forma:

Tomando en cuenta que la conectividad de la red está tal y como se muestra en la Figura 4.32, primero se desactivará el sistema Vyatta R1 por tanto se perderá la conectividad con este que es el sistema master en la topología proyecto, como se puede observar en la Figura 4.33, para así notar que el sistema Vyatta R2 remplace al master, luego se activará nuevamente el sistema Vyatta R1 y se verá si el sistema Vyatta R1 toma nuevamente el control, quedando todo el sistema en las condiciones iniciales.

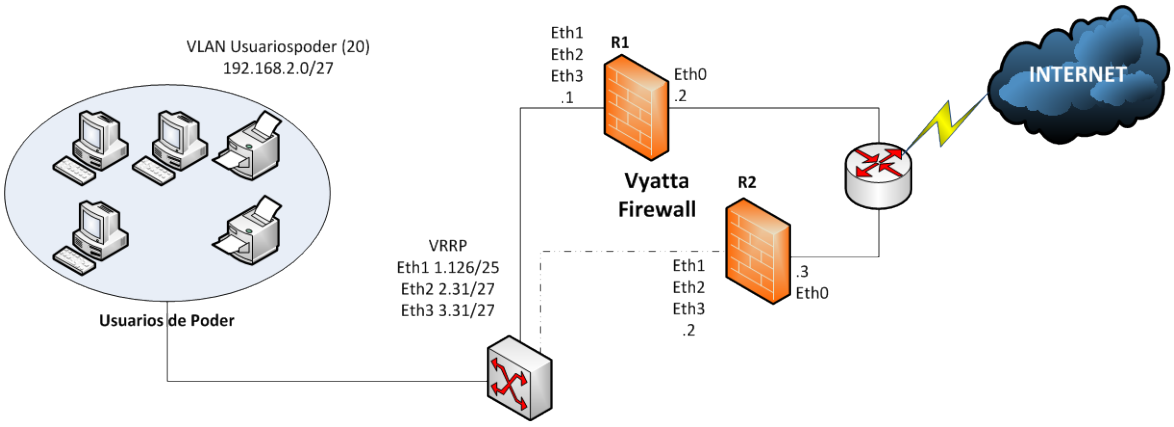


Figura. 4.32. Conectividad de la red para pruebas de redundancia

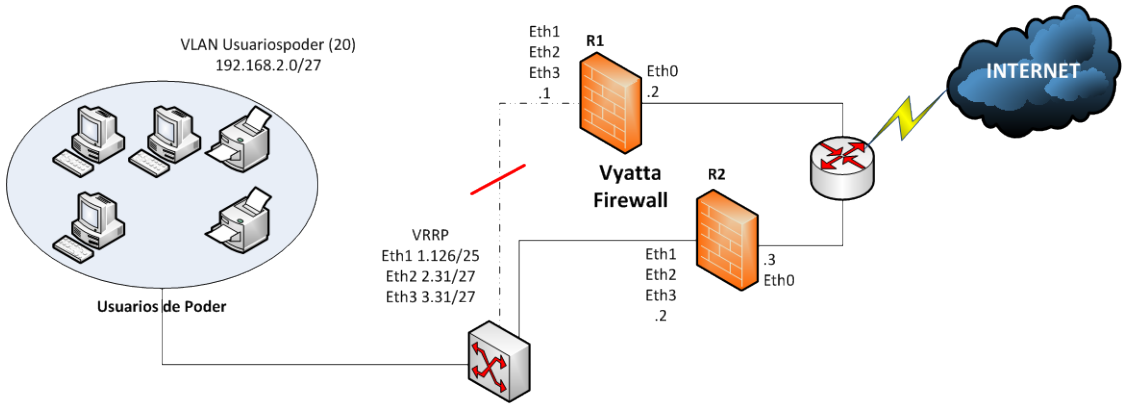


Figura. 4.33. Remplazo de R2 a R1 por redundancia

La Figura 4.34 muestra la desconexión del sistema Vyatta R1 justo cuando se envía el ping 7 y la Figura 4.35 muestra como el sistema R1 toma nuevamente el control después de haber sido remplazado por el sistema Vyatta R2.

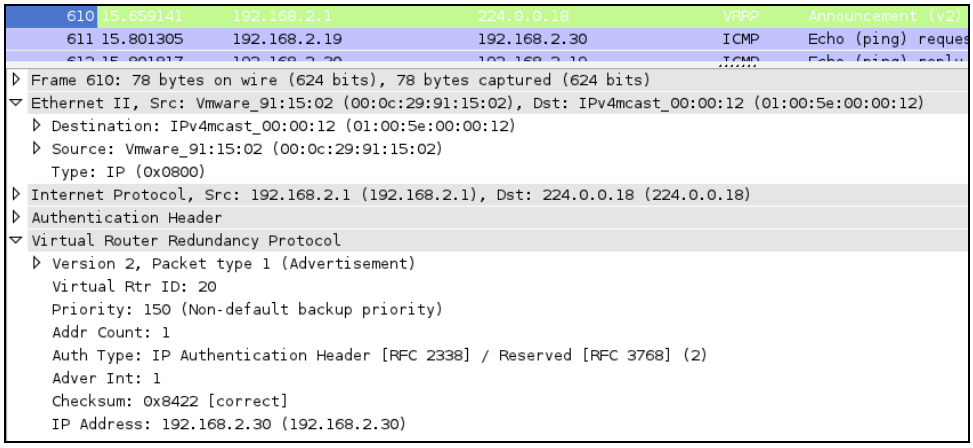
```
Firoos:~ usr$ ping 192.168.2.30
PING 192.168.2.30 (192.168.2.30): 56 data bytes
64 bytes from 192.168.2.30: icmp_seq=0 ttl=64 time=1.616 ms
64 bytes from 192.168.2.30: icmp_seq=1 ttl=64 time=0.577 ms
64 bytes from 192.168.2.30: icmp_seq=2 ttl=64 time=0.601 ms
64 bytes from 192.168.2.30: icmp_seq=3 ttl=64 time=0.579 ms
64 bytes from 192.168.2.30: icmp_seq=4 ttl=64 time=0.598 ms
64 bytes from 192.168.2.30: icmp_seq=5 ttl=64 time=0.664 ms
64 bytes from 192.168.2.30: icmp_seq=6 ttl=64 time=0.648 ms
64 bytes from 192.168.2.30: icmp_seq=7 ttl=64 time=0.645 ms
64 bytes from 192.168.2.30: icmp_seq=12 ttl=64 time=0.652 ms
64 bytes from 192.168.2.30: icmp_seq=13 ttl=64 time=0.589 ms
64 bytes from 192.168.2.30: icmp_seq=14 ttl=64 time=0.546 ms
64 bytes from 192.168.2.30: icmp_seq=15 ttl=64 time=0.556 ms
64 bytes from 192.168.2.30: icmp_seq=16 ttl=64 time=0.564 ms
64 bytes from 192.168.2.30: icmp_seq=17 ttl=64 time=0.626 ms
64 bytes from 192.168.2.30: icmp_seq=18 ttl=64 time=0.665 ms
64 bytes from 192.168.2.30: icmp_seq=19 ttl=64 time=0.682 ms
```

Figura. 4.34. Desactivación del sistema Vyatta R1

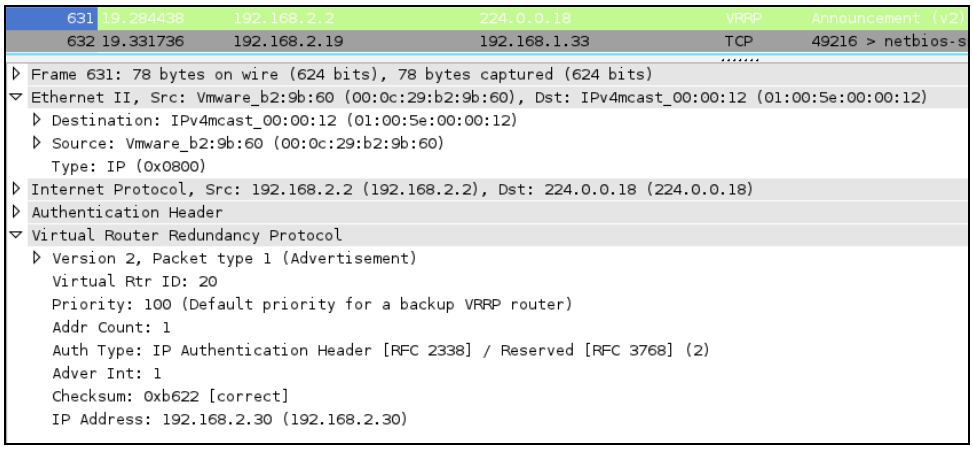
```
64 bytes from 192.168.2.30: icmp_seq=114 ttl=64 time=0.659 ms
64 bytes from 192.168.2.30: icmp_seq=115 ttl=64 time=0.692 ms
64 bytes from 192.168.2.30: icmp_seq=116 ttl=64 time=0.599 ms
92 bytes from 192.168.2.2: Redirect Host(New addr: 192.168.2.30)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 e569   0 0000  3f  01 10be 192.168.2.19  192.168.2.30

92 bytes from 192.168.2.1: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 5400 e569   0 0000  3e  01 11be 192.168.2.19  192.168.2.30

64 bytes from 192.168.2.30: icmp_seq=118 ttl=64 time=1.328 ms
64 bytes from 192.168.2.30: icmp_seq=119 ttl=64 time=0.631 ms
64 bytes from 192.168.2.30: icmp_seq=120 ttl=64 time=0.639 ms
```

Figura. 4.35. Reactivación del sistema Vyatta R1

Mientras se generaban los pings anteriores también se realizaron capturas con wireshark para poder notar cual es el funcionamiento del protocolo VRRP, en la Figura 4.36a sólo se nota como se están moviendo los pings request y replay, en la Figura 4.36b se muestra el desglose del paquete VRRP enviado por el sistema backup, por tanto este fue enviado cuando R1 ya fue desactivado.



a. VRRP enviado por el sistema principal R1



b. Paquete VRRP enviado por el sistema backup R2

Figura. 4.36. Flujo de paquetes VRRP en la red

Es necesario notar como se efectúa el cambio de la dirección MAC en el protocolo VRRP durante la desactivación del sistema Vyatta R1 y de igual forma cuando este recupera el control de la red desactivando al sistema Vyatta R2, para esto VRRP dentro de Vyatta se maneja enviando paquetes ARP gratiutous, estos paquetes sirven para informar a los distintos host que la MAC de una dirección IP a cambiado, el detalle de estos paquetes se pueden notar en la Figura 4.37 cuando se produce el fallo del sistema Vyatta.

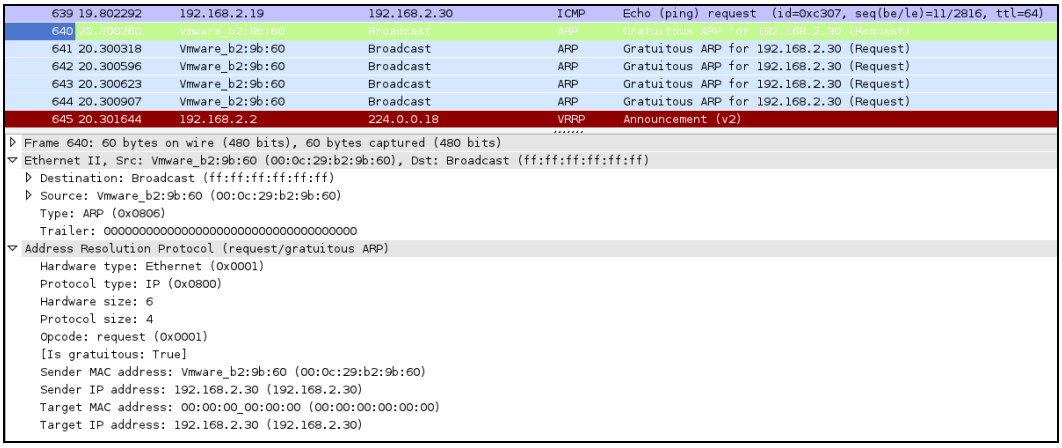


Figura. 4.37. Cambio de MAC para la dirección IP virtual del sistema Vyatta R1

El sistema mediante el uso de VRRP difunde paquetes en la red durante intervalos de tiempo cortos, estos paquetes llevan consigo información de la prioridad del sistema, en este caso el sistema master tiene una prioridad de 150 y el de respaldo una prioridad de 100, los paquetes capturados demuestran que en el momento en que el sistema de respaldo deja de percibir los paquetes VRRP del sistema master, este sistema de respaldo se pone al mando de la red, es posible detectar este funcionamiento viendo que justo en el momento en que el sistema de respaldo se alza como primario aparecen paquetes VRRP difundiéndose por la red, obviamente detallando su prioridad.

La siguiente prueba es similar a la anterior pero mientras se realizan peticiones a una dirección de internet, en este caso el servidor DNS de google. La Figura 4.38 muestra la desactivación del sistema Vyatta R, y la Figura 4.39 muestra su reactivación.

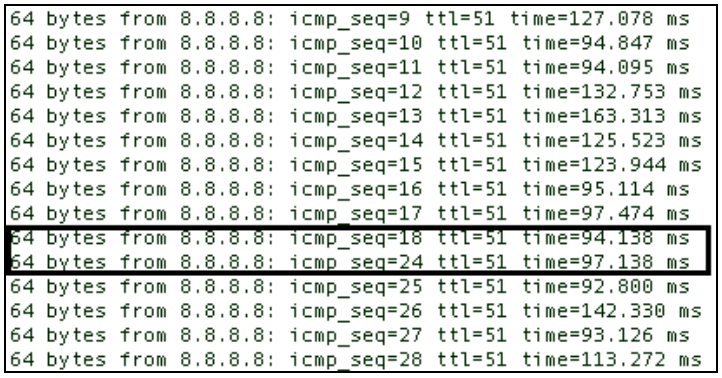


Figura. 4.38. Desactivación del sistema Vyatta R1 mientras se realiza ping a una dirección de internet

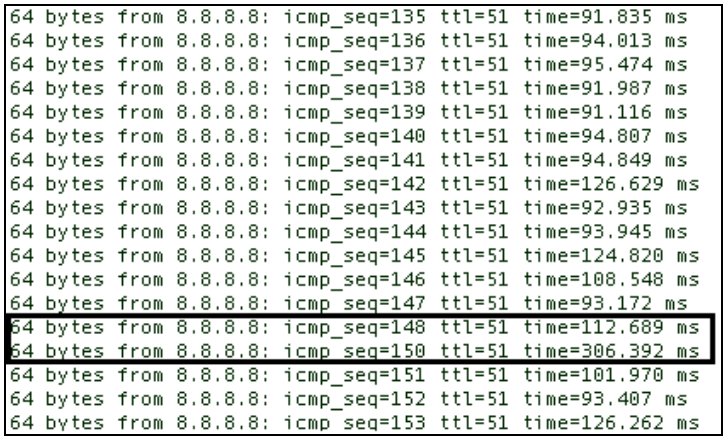


Figura. 4.39. Reactivación del sistema Vyatta R1 mientras se realiza ping a una dirección de internet

Los tiempos que se necesita para levantar al sistema redundante cuando el master deja de funcionar son detallados en la Tabla 5.7, estos valores han sido tabulados de las pruebas de redundancia y alta disponibilidad anteriores.

	Tiempo de Levantamiento del Sistema Prioritario	
	Slave como Primario	Master
Ping al Sistema Vyatta (mseg)	0,652	1,342
Ping a Dirección de Internet 8.8.8.8 (mseg)	97,13	306,392

Tabla. 4.7. Tiempos de levantamiento del sistema de redundancia

Por último se probará el sistema mientras se realiza una descarga desde un host de la zona de poder desde una página web. En la Figura 4.40 se puede notar que la descarga está en progreso y justo en ese momento se desactiva el sistema Vyatta R1, en la Figura 4.41 el sistema Vyatta R2 toma el control y es percibible que se ha descargado un nuevo archivo desde un servidor ftp por lo que se demuestra que R2 está en funcionamiento, ahora se activará el sistema Vyatta R1, en la Figura 4.42 es notable que el primer archivo termina de descargarse.

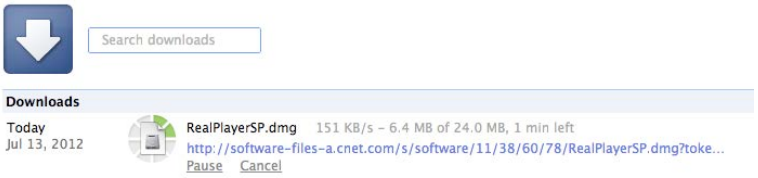


Figura. 4.40. Descarga de archivo desde página web y desconexión del sistema Vyatta R1

Figura. 4.41. Descarga de un nuevo archivo con Vyatta R2 como sistema primario

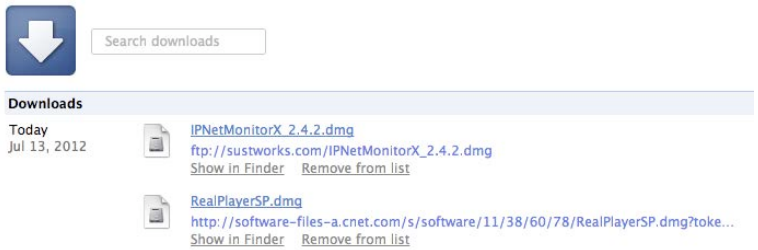
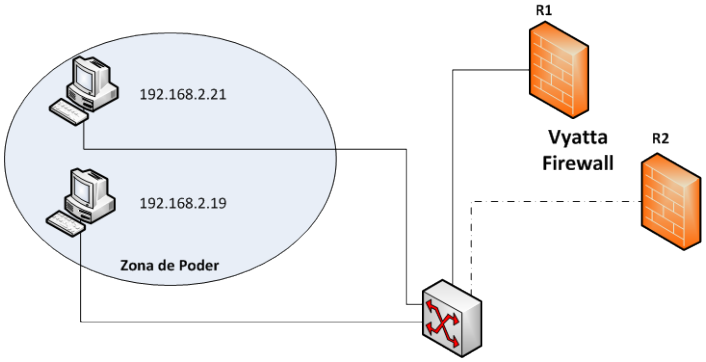
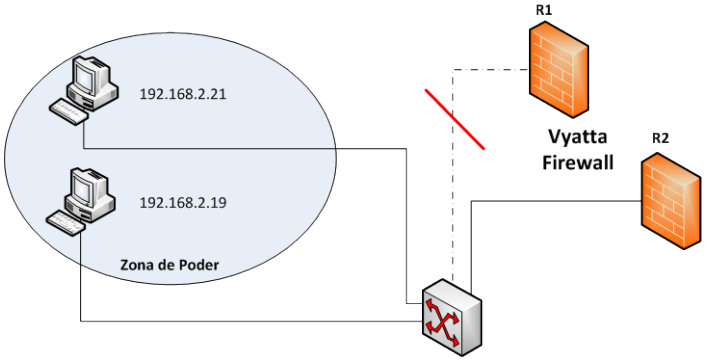


Figura. 4.42. Reactivación del sistema Vyatta R1

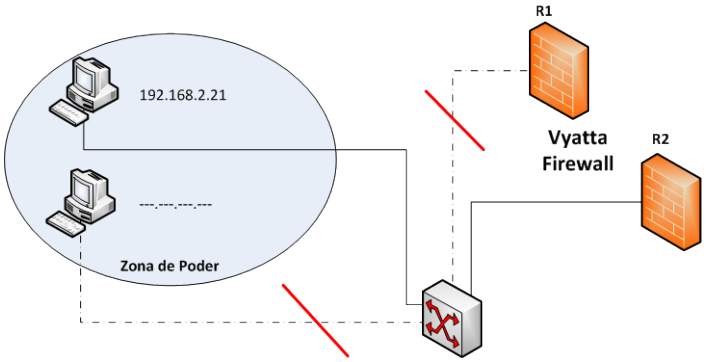
Otra de las configuraciones que se implementó para el sistema de alta disponibilidad es la de stateful failover, esta sirve para que el sistema primario y secundario de Vyatta se mantengan actualizados, por ejemplo en la prestación de dirección IP para el servicio DHCP, para probar que esta configuración está funcionando adecuadamente se realizó una prueba que consta en mantener dos computadores conectados a la zona de poder con direcciones IP rentadas por el servidor DHCP, para luego desconectar el sistema primario R1, desconectar una de las computadoras y conectarlas nuevamente para tratar de renovar la dirección IP antes contratada. Esta prueba se puede notar gráficamente en la Figura 4.43 en sus distintos literales.



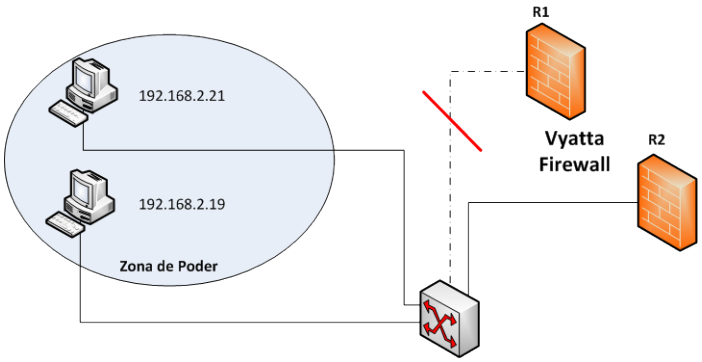
a. Clientes con direcciones IP dadas por el servidor DHCP de R1



b. Desactivación del sistema Vyatta principal R1



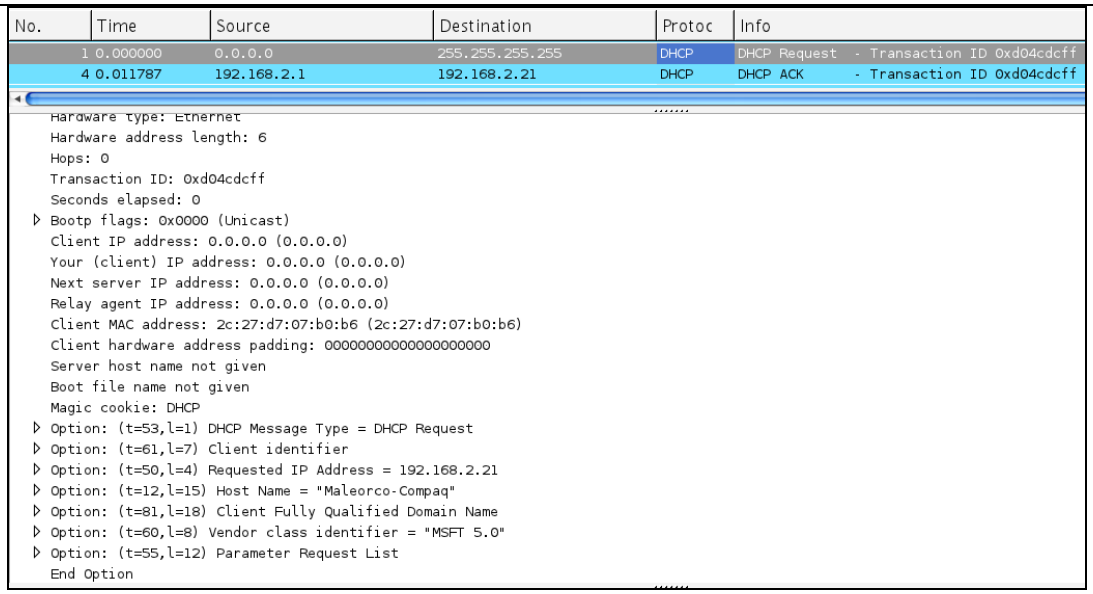
c. Desconexión de un cliente de la red



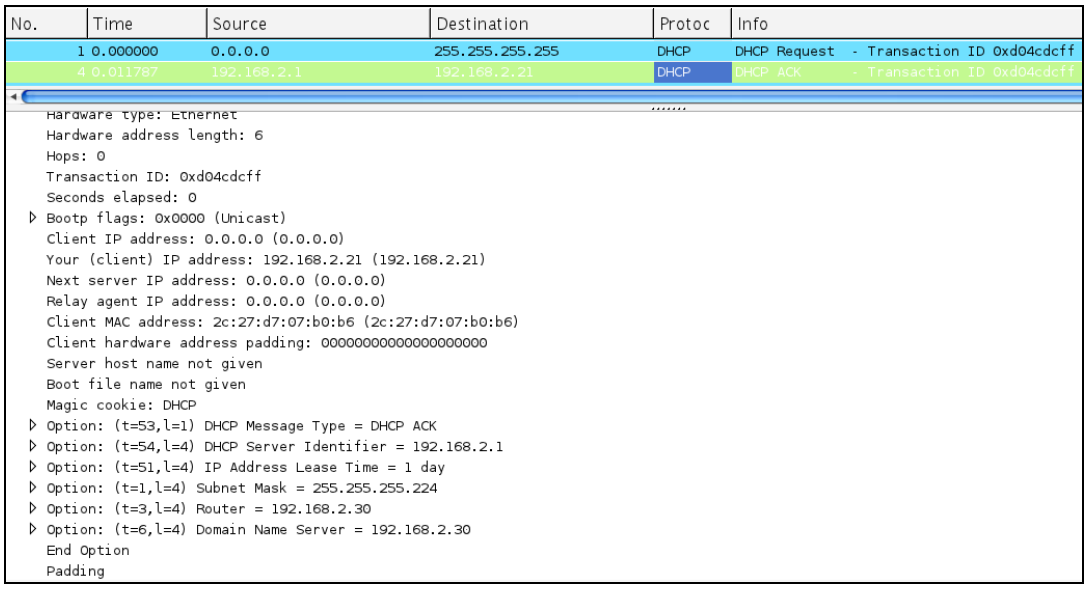
d. Conexión del mismo cliente anterior a la red

Figura. 4.43. Pasos ejecutados para probar la configuración de stateful failover

En primera instancia cuando el usuario recibió una dirección IP se capturaron los paquetes de la Figura 4.44.



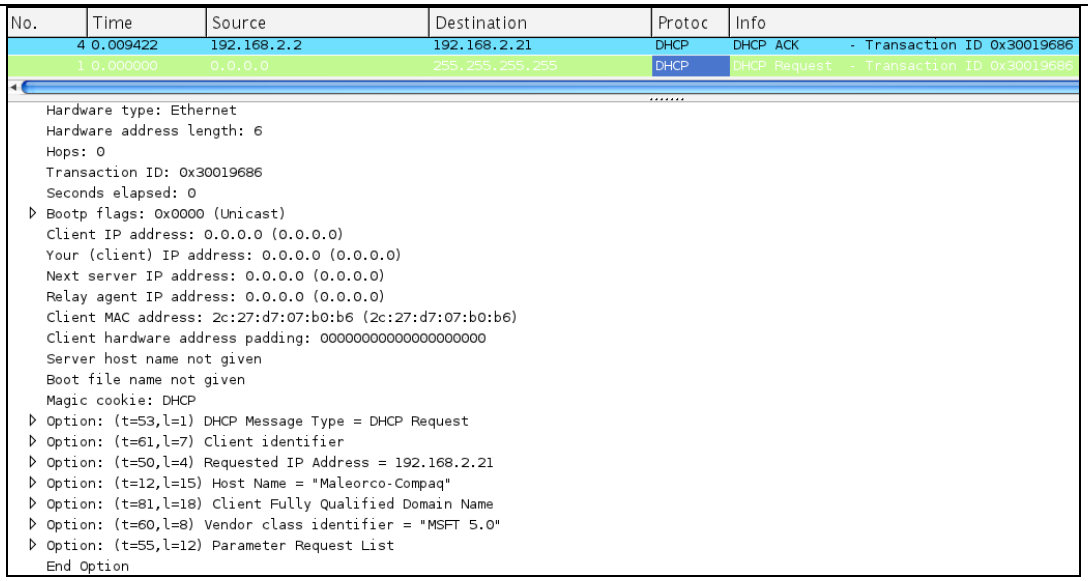
a. Paquete DHCP request enviado por el cliente



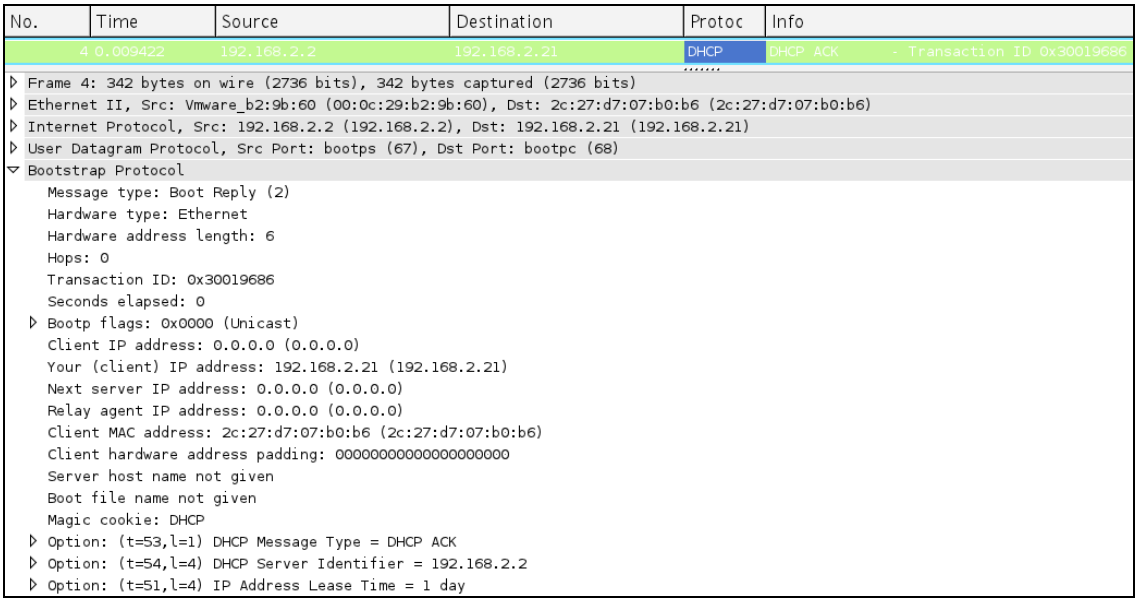
b. Paquete DHCP acknowledge enviado por el servidor primario

Figura. 4.44. Paquetes DHCP al conectar por primera vez al usuario a la zona de poder

Una vez que se desconectó al sistema primario R1 entonces se desconectó al usuario y conectó enseguida con lo que se capturarón los paquetes DHCP de la Figura 4.45.



a. Paquete DHCP request enviado por el cliente



b. Paquete DHCP acknowledge enviado por el servidor secundario

Figura. 4.45. Paquetes dhcp después de haber desconectado y vuelto a conectar al usuario a la zona de poder

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Como principal conclusión se determina que el sistema Vyatta cumple con todos los requerimientos de una red corporativa de pequeña o gran escala, si se desea usar la versión libre se pueden encontrar algunas limitaciones que se analizarán más adelante, pero en definitiva el sistema es completo y uno de los competidores más grandes, incluso para dispositivos físicos como Cisco, la facilidad que este provee para su configuración hace que aparte de dar varias opciones para solucionar problemas, también sean estas muy viables y de configuración rápida.

Las máquinas virtuales de primer nivel son desarrolladas con la intención de que corran bajo máquinas físicas con la capacidad de un servidor, debido a que uno de los objetivos de este proyecto es trabajar con la menor cantidad de recursos físicos necesarios, entonces toda la instalación de Vyatta se la implementó en una arquitectura x86 en un computador común, por tanto este no soporta la instalación de una máquina virtual de primer nivel, en tanto fue necesario instalar Vyatta sobre una máquina virtual que reside dentro de un sistema operativo Windows, la máquina virtual que se usó fue VMware Workstation, las ventajas de esta máquina virtual en relación a VMware ESXi son: la velocidad de procesamiento y la facilidad de configuración, por otro lado como desventaja es muy importante saber que en Workstation no es posible configurar vlans ya que ésta elimina las etiquetas de los paquetes, para solucionar este inconveniente fue necesario crear vlans dentro del sistema operativo host para que exista comunicación con el switch y dentro de VMware workstation las

interfaces aparecen como si fuesen interfaces físicas y de la misma manera dentro de Vyatta.

DHCP y DNS

En el caso de las pruebas que se efectuaron para DHCP y DNS sólo se puede concluir que el servicio está funcionando adecuadamente y que los tiempos de respuesta son rápidos o bien están dentro de un rango aceptable.

En el caso de DHCP, la fijación de los parámetros de priorización del servicio, se puede obtener un desenvolvimiento más estable ya que se optimiza el servicio para que derroque a otros que posiblemente estén funcionando en la red.

Es muy útil que el sistema Vyatta proporcione un servidor DNS debido a que con este se puede mejorar los tiempos de respuesta cuando una dirección es consultada varias veces, además la facultad de poder establecer un tamaño de memoria cache para guardar las correspondencias entre nombres de dominio y direcciones IP hace que el sistema se adapte adecuadamente a disitntos tipos de redes.

Calidad de servicio

Del análisis que ya se había estudiado anteriormente, se puede concluir que la calidad de servicio implementada mediante división del ancho de banda por zonas es adecuada, pero no tan precisa como se esperaba debido a los errores mayores al 10%, se debe recalcar que estos errores tampoco son muy exactos ya que el ancho de banda en la intranet no es fijo, por tanto existirán lapsos de tiempo en los que la división de ancho de banda sea más exacta a los estipulados en la configuración del sistema Vyatta. Lastimosamente no fue posible probar otros tipos de calidad de servicio debido a que se está evaluando la versión libre de Vyatta, pero mediante esta experiencia se deduce que lo más probable es que las otras configuraciones sean igual de buenas.

Desempeño de la red

Es bastante normal que se note una diferencia grande entre el ancho de banda en la intranet y el de internet, de las pruebas realizadas sólo se puede concluir que el ancho de banda real se redujo en prácticamente a dos tercios del total del teórico, lo que demuestra que el sistema que da la conectividad en la red de datos no está reduciendo excesivamente la capacidad de la misma, en el caso de que la red interna sea gigabit la pérdida de ancho de banda será mucho menor en relación al ancho de banda total, pero este no es el caso.

Con la evaluación del resto de pruebas que se hicieron para probar el desempeño de la red, se comprueba lo antes dicho acerca del ancho de banda mínimo, cuando la red está inundada de tráfico el ancho de banda está alrededor de 40Mbps, teniendo la red un ancho de banda de 80Mbps reales, haciendo la relación de estas dos cifras y notando que la red estaba al máximo entonces se determina que el sistema estaba respondiendo adecuadamente para esta red corporativa pequeña.

Redundancia y alta disponibilidad

Lamentablemente no se pudo probar la sincronización del sistema debido a que este proyecto sólo utiliza la versión de distribución libre, la sincronización sólo puede ser implementada comprando alguno de los paquetes que ofrece la compañía Vyatta.

El protocolo VRRP que es el que se implementó para proveer de alta disponibilidad a la red corporativa usa paquetes que se envían después de intervalos de tiempo determinados, en conclusión estos paquetes son bastante pequeños y el tiempo total que toma su análisis es despreciable por lo que el funcionamiento del sistema es bastante aceptable, una de las características que se debe tomar en cuenta es que, en el caso de que exista un fallo del sistema primario el sistema secundario inunda la red con paquetes ARP, informando del

fallo a los distintos usuarios conectados, este intercambio de sistema toma tiempos menores a los 40 mili segundos, por lo que el índice de disponibilidad del sistema sería prácticamente del 100%, aún así no se debe dejar de tomar en cuenta, que la red en estudio es una red corporativa, en caso de redes más grandes este porcentaje aumentará, aún así el sistema es excelente para proveer tolerancia a fallos a las redes de datos.

En relación a la configuración de stateful failover que se levantó en el sistema, se puede concluir mediante las pruebas que se hicieron, que el sistema respondió satisfactoriamente y como se esperaba, entre las pruebas de stateful failover y las de alta disponibilidad se deduce claramente que las sesiones levantadas en el sistema primario son transparentemente levantadas en el sistema backup, por lo que si existiese un fallo en el sistema primario el secundario tomará la administración del sistema rápida y efectivamente.

5.2 RECOMENDACIONES

Es favorable analizar de manera adecuada toda la topología de red física como lógica que se desea implementar antes de empezar con la configuración del sistema Vyatta, así se podrá obtener resultados robustos y velozmente.

Se debe tener muy en cuenta que si se desea implementar Vyatta dentro de una máquina virtual, entonces se debe escoger de manera adecuada el servidor donde esta será instalada, Vyatta presenta distribuciones que son más funcionales con máquinas virtuales de primer nivel como VMware ESXi, XenServer, etc. El problema se presenta cuando estas máquinas virtuales deben ser instaladas en el servidor ya que no todos los procesadores son compatibles con ellas, así como la tarjeta madre del servidor o las tarjetas de red, debido a esto entonces es necesario hacer un estudio antes de instalar la máquina virtual y Vyatta sobre ella.

Dentro de la página de VMware (www.vmware.com) existe una sección donde se detalla los distintos procesadores, tarjetas madre, tarjetas de red, etc. compatibles con VMware ESXi.

Hay que tomar muy en cuenta, que si se desea instalar este sistema dentro de una red corporativa, debe existir una persona que este encargada de su instalación y mantenimiento, en caso de que se desee obviar personal entonces se puede comprar las licencias que son distribuidas por la organización Vyatta, estas incluyen soporte, almacenamiento virtual extendido, clases de entrenamiento en línea, soporte telefónico y acuerdos del nivel de servicio, todas estas características de la licencia varían de acuerdo al tipo de plan contratado.

Existe también la posibilidad, que dentro del entorno corporativo de alta disponibilidad y tolerante a fallos, sean necesarias características en el sistema Vyatta como la sincronización de los distintos sistemas levantados o bien un entorno gráfico para un manejo más amigable y rápido del sistema, en este caso será necesario adquirir una licencia ya que con el programa de uso libre no están incorporadas estas características.

REFERENCIAS BIBLIOGRÁFICAS

Fuentes de Conocimiento: libros, revistas, Internet, catálogos, otros.

- [1] http://www.comnetsa.com/index.php?option=com_content&view=article&id=15&Itemid=9, Mayo 2012
- [2] http://es.kioskea.net/contents/surete-fonctionnement/haute-disponibilite.php3, Mayo 2012
- [3] http://www.txsolutions.com/modules.php?name=News&file=article&sid=2, Mayo 2012
- [4] http://www.sylcom.com/redundancia.htm, Mayo 2012
- [5] http://www.db-system.com/portal/page?_pageid=33,7611&_dad=portal&_schema=PORTAL, Mayo 2012
- [6] www.vyatta.org, Mayo 2012
- [7] http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica) , Mayo 2012
- [8] http://www.vyatta.com/sites/vyatta.com/files/pdfs/Vyatta_Cisco_Replacement_Guide_0.pdf, Mayo 2012
- [9] http://es.wikipedia.org/wiki/Alta_disponibilidad, Mayo 2012

- [10]

  http://es.wikipedia.org/wiki/Virtualizaci%C3%B3n#Tipos_de_virtualizaci.C3.B3n, Junio 2012

- [11]

  Administración de Sistemas Operativos de Red, Autor Miquel Colobran, Capítulo II, Editorial UOC, Junio 2012

- [12]

  http://es.kioskea.net/contents/surete-fonctionnement/haute-disponibilite.php3, Junio 2012

- [13]

  http://www.omicrono.com/2011/11/las-mejores-herramientas-de-virtualizacion-vmware-virtualbox-y-virtualpc/, Junio 2012

- [14]

  Recursos Informáticos Windows Server 2008 – Administración y Explotación, Autor Philippe FREDDI, Editorial ENI, ISSN 1627-8224

- [15]

  http://www.sahw.com/wp/archivos/2006/04/17/comparativa-de-cinco-soluciones-de-virtualizacion/, Junio 2012

- [16]

  http://www.scribd.com/doc/69032555/Virtualizacion, página 9, Junio 2012

- [17]

  http://es.wikipedia.org/wiki/Xen, Junio 2012

- [18]

  http://es.wikipedia.org/wiki/OpenVZ, Junio 2012

- [19]

  http://es.wikipedia.org/wiki/VirtualBox, Junio 2012

- [20]

  http://www.openredes.com/wp-content/uploads/2011/10/Evento-Vyatta.pdf, página 3, Junio 2012

- [21]

  http://www.vyatta.com/files/pdfs/vyatta_solutions_guide.pdf, Junio 2012

- [22]

  http://dspace.epn.edu.ec/bitstream/15000/8668/4/T10140CAP3.pdf, Junio 2012

- [23]

  http://www.ordenadores-y-portatiles.com/tipos-de-ordenador.html, Junio 2012

- [24]

  https://www.google.com.ec/search?sourceid=chrome&ie=UTF-8&q=modem, Junio 2012

- [25]

  http://es.wikipedia.org/wiki/Router, Junio 2012

- [26]

  http://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)#Clasificaci.C3.B3n, Junio 2012

- [27]

  http://sauce.pntic.mec.es/crer0052/dhcp/definici.htm, Junio 2012

- [28]

  Firewall en Alta Disponibilidad, Redklee, Norberto Altalef, Julio 2006

- [29]

  IBM, High Availability Solution for IBM FileNet P8 Systems, ibm.com/redbooks, Agosto 2009, 4 de Mayo de 2012, ISBN 0738433268

- [30]

  IBM, IP Network Design Guide, Martin W. Murhammer, ISBN SG24-2580-01

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

Arquitectura TCP/IP.- Arquitectura de transferencia de paquetes para redes WAN y LAN basado en el modelo OSI, esta arquitectura se basa en tres capas física, red, transporte y aplicación.

OSI.- Open System Interconnection - Sistema de Interconexión Libre.

TCP.- Transfer Control Protocol – Protocolo de Control de Transferencia.

IP.- Internet Protocol – Protocolo de Internet.

Arquitecturas x86.- Arquitectura de computadores basados en procesadores con bus de datos de 32bits.

Clustering. - Sistema desarrollado para el manejo de redes con alta disponibilidad, este permite tener dos dispositivos trabajando conjuntamente uno como primario y otros en calidad de respaldo.

VSE.- Virtual Service Enviroment - Servidor Gráfico.

SLA.- Service Level Agreement - Acuerdo de Nivel de Servicio.

BGP.- Border Gateway Protocol - Protocolo de Puerta de Enlace de Borde.

OSPF.- Open Shortest Path First - Protocolo de Enrutamiento Jerárquico de Pasarela Interior.

RIP.- Routing Information Protocol – Protocolo de Información de Enrutamiento.

SNMP.- Simple Network Management Protocol - Protocolo Simple de Administración de Red.

QoS.- Quality of Service - Calidad de Servicio.

Wireshark.- Programa de uso libre que permite la capturación de paquetes que transitan a través de una tarjeta de red.

Tcpdump.- herramienta que permite el análisis del tráfico que pasa por una red.

DMZ.- Demilitarized Zone - Zona Desmilitarizada.

SSH.- Secure Shell - Intérprete de órdenes seguro.

Telnet.- Protocolo que provee una comunicación interactiva bidireccional mediante texto usando una comunicación virtual.

DHCP.- Dynamic Host Control Protocol - Protocolo de Control de Usuarios Dinámico.

URL.- Uniform Resource Locator - Localizador de Recursos Uniforme, es una secuencia de caracteres que siguen un formato modélico y estándar, que se usa para nombrar recursos en internet para su localización o identificación.

API.- Aplication Programming Interface - Interfaz de Programación de Aplicaciones.

LAN.- Local Area Network - Red de Área Local.

WAN.- Wide Area Network - Red de Área Amplia.

ACL.- Access Control List - Lista de Control de Acceso.

UDP.- User Datagram Protocol - Protocolo de Datagrama de Usuario.

DNS.- Domain Name Service - Servicio de Nombres de Dominio.

HTTP.- Hypertext Transfer Protocol - Protocolo de Transferencia de Hipertexto.

RADIUS.- Remote Authentication Access Control System - Sistema de Control de Acceso de Autenticación Remota.

TACACS.- Terminal Access Controller Access Control System - Sistema de Controlador de Acceso mediante Control del Acceso desde Terminales, protocolo de autenticación remota, propietario de Cisco.

Softphone.- Teléfono virtual.

Callcenter.- Centro de atención de llamadas.

FTP.- File Transfer Protocol - Protocolo de Transferencia de Archivos.

Intranet.- Red interna o red local.

RRHH.- Recursos Humanos.

P2P.- Point To Point - Punto a Punto, conexión punto a punto.

DSL.- Digital Subscriber Line - Línea de Suscripción Digital.

ISP.- Internet Service Provider – Proveedor de Servicio de Internet.

ADSL.- Assymetrical Digital Subscriber Line – Línea de Suscripción Digital Asimétrica.

VPN.- Virtual Private Network - Red Privada Virtual.

MAC.- Media Address Control - Dirección de Control de Media

Broadcast.- Difusión, es una forma de comunicación donde un transmisor envía de forma simultánea paquetes a todos los usuarios dentro de una subred.

Backbone.- Se refiere a las principales conexiones troncales de una red, está compuesta por routers, switchs y medios físicos de comunicación como fibra óptica, etc.

UTP.- Unshielded Twisted Pair - Par Trenzado No Blindado, tipo de cable que se utiliza principalmente para comunicaciones.

RRT.- Round-trip Time - Tiempo de Ida y Vuelta, se define como el tiempo que tarda un paquete enviado desde un emisor en volver a este.

FECHA DE ENTREGA

El día 28 de Septiembre de 2012, en la ciudad de Sangolquí, firman en constancia de la entrega del presente Proyecto de Grado titulado “SOLUCIÓN DE FIREWALL CON ALTA DISPONIBILIDAD PARA REDES CORPORATIVAS UTILIZANDO VYATTA CON VIRTUALIZACIÓN”, en calidad de Autor el Sr. Felipe Andrés Ordóñez Galiano estudiante de la carrera de Ingeniería Electrónica en Redes y Comunicación de Datos, y recibe por parte del Departamento de Eléctrica y Electrónica del Director de Carrera de Redes y Comunicación de Datos, el Señor Ing. Carlos Romero.

_____

Felipe Andrés Ordóñez Galiano

CI: 1721407763

_____

Ing. Carlos Romero

Director de Carrera de Redes y Comunicación de Datos